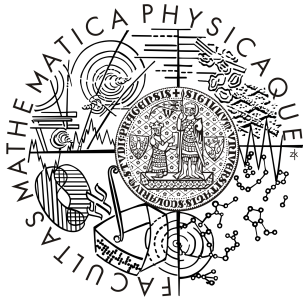
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

DIPLOMOVÁ PRÁCA



Bc. Roman Cinkais

Aplikace samoopravných kódů v steganografii

Katedra algebry
Vedúcí diplomovej práce: prof. RNDr. Aleš Drápal, CSc., DSc.
Študijný program: Matematika
Študijný obor: Matematické metody informační bezpečnosti

Rád by som na tomto mieste poďakoval vedúcemu mojej diplomovej práce, prof. RNDr. Alešovi Drápalovi, CSc., DSc., za cenné pripomienky a podnety k tejto práci, poskytnutie potrebnej literatúry a času stráveného na konzultáciach. Takisto by som rád vyjadril svoje poďakovanie mojim blízkym, ktorí ma počas písania tejto práce a štúdia neustále podporovali. Ďakujem pánu profesorovi Petrovi Lisoňkovi a pani profesorke Jessice Fridrichovej, ktorí mi poskytli podporu pri otázkach a podnetili vo mne nové myšlienky a nápady.

Prehlasujem, že som svoju diplomovú prácu napísal samostatne a výhradne s použitím citovaných prameňov. Súhlasím so zapožičiavaním práce.

V Prahe dňa 15. 7. 2009 Bc. Roman Cinkais

Obsah

Úvod **6**

1 Základné pojmy a definície z teórie kódov **8**
1.1 Niektoré základné príklady kódov 9
1.1.1 Opakovacie kódy 10
1.1.2 Paritný kód 10
1.2 Lineárne kódy 10
1.3 Binárne perfektné kódy 13
1.4 Hammingove kódy 14
1.5 Cyklické kódy 16
1.6 Binárny Golayov kód 21
1.7 Binárne Reed-Mullerove kódy 22
1.8 Nordstrom-Robinsonov kód 24
1.9 Kerdockove kódy 25
1.9.1 Symplektické a kvadratické formy 25
1.9.2 Konštrukcia Kerdockových kódov 31
1.10 $\mathbb{Z}_4$-lineárne kódy 32
1.10.1 Konštrukcia Preparata kódov 33
1.10.2 Kvaterniárne kódy 36
1.10.3 Oktakód 37
1.10.4 Binárne kódy asociované s kvartérniárnymi kódmi 37
1.10.5 Galoisove okruhy 38
1.10.6 Cyklické kódy nad $\mathbb{Z}_4$ 39
1.10.7 Súvislosť s Kerdockovými a Preparata kódmi 40
1.11 Krycie kódy 40

2 Steganografia a teória kódov **42**
2.1 Základy steganografie 42
2.1.1 Základný model digitálnych dat 42
2.1.2 Princíp steganografie na digitálnych nosičoch 44
2.2 Steganoanalýza 46
2.2.1 Analýza histogramu 47
2.2.2 Párová analýza (Raw Quick Pair Analysis) 47
2.2.3 PoVs a Chi-kvadrát útok 48
2.3 Aplikácia teórie kódov 51
2.4 Krycie funkcie 52
2.5 Faktorizácia a direktná suma kódov 54

3 Konštrukcia krycích funkcií **59**
3.1 Krycie funkcie s krycím polomerom 1 59
3.2 Krycie funkcie s krycím polomerom 2 61
3.3 Aplikácie direktnej sumy faktorizácií 62

4 Všeobecný prípad krycích funkcií **65**
4.1 Aplikácie ternárnych kódov v steganografii 68

Záver **74**

Literatúra **75**

Přílohy **78**
Príloha č.1: Porovnanie krycích funkcií 79
Príloha č.2: Tabuľka hodnôt $l(n, \rho)_2$ 83
Príloha č.3: Porovnanie steganografických algoritmov 84
Príloha č.4: Chi-kvadrát test 88
Príloha č.5: Obsah priloženého DVD 90

Názov práce: Aplikace samoopravných kódů v steganografii
Autor: Bc. Roman Cinkais
Katedra: Katedra algebry
Vedúcí diplomovej práce: prof. RNDr. Aleš Drápal, CSc., DSc.
e-mail vedúceho: drapal@karlin.mff.cuni.cz

Abstrakt: Moderná steganografia je pomerne nová disciplína, ktorá si začína vytvárať svoje miesto v informačnej bezpečnosti. Narozdiel od kryptografie, ktorá sa snaží znemožniť tretej strane získať informácie z prebiehajúcej komunikácie prostredníctvom rôzných kryptografických algoritmov, je cieľom steganografie utajiť samotnú komunikáciu medzi stranami. Aplikácie samoopravných kódov a krycích funkcií výrazne zvyšujú schopnosti a bezpečnosť steganografických algoritmov. V tejto práci sa venujeme steganografii založenej na samoopravných kódoch, ktorá v súčasnosti prezentuje najlepšie výsledky, čo sa týka ukrývacej efektivity algoritmov. Nové konštrukcie nám umožňujú pracovať s nelineárnymi kódmi a vytvárať nové steganografické algoritmy. Uvidíme, že takto zkonštruované algoritmy vykazujú zvýšenú schopnosť ukryť komunikáciu, resp. správu do digitálneho nosiča. Ďalším vylepšením takejto steganografie môže byť aplikovanie všeobecných q-árnych kódov. To už so sebou prináša ďalšie otázky, na ktoré je potreba nájsť odpovede. Jednotlivé porovnania a možnosti ukazujú, že táto oblasť je momentálne v plienkách a čaká nás podobný vývoj, aký nastal v kryptografii v posledných dvoch desaťročiach.
Klíčová slova: steganografia, krycie funkcie, samoopravné kódy, ukrývacia efektivita

Title: Applications of error-correcting codes in steganography
Author: Bc. Roman Cinkais
Department: Department of algebra
Supervisor: prof. RNDr. Aleš Drápal, CSc., DSc.
Supervisor's e-mail address: drapal@karlin.mff.cuni.cz

Abstract: Modern steganography is a relatively new discipline with many applications in information security. Contrary to the cryptography which is trying to make a message unreadable to third party using cryptographic algorithms, the aim of steganography is to hide a communication between parties. Applications of error-correcting codes and covering functions markedly increases abilities and security of steganographic algorithms. This thesis is attended to steganography using error-correcting codes which has the best results nowadays regarding embedding efficiency. New constructions will help us to work with non-linear codes and providing new steganographic algorithms. We will see that these algorithms have a better ability to hide communication, resp. a message in a digital medium. Further improvements can be made using applications of general q-ary codes. Many new questions are coming out with that which need to be answered. Several comparisons are showing that the area of steganography is in a beginning and we will be participants of such a progress as cryptography experienced in the last two decades.
Keywords: steganography, covering function, error-correcting codes, embedding efficiency

Úvod

V súčasnosti môžeme zaznamenať obrovský rozmach samotnej kryptológie. Vznikajú nové kryptografické algoritmy, ktoré sú spolu s modernými informačnými nástrojmi stále dokonalejšie a posúvajú hranice informačnej bezpečnosti ďalej. Podnety k rozvoju kryptografie dáva samozrejme aj kryptoanalýza, ktorá tiež smeruje veľkou rýchlosťou vpred. Kryptológia nám dáva možnosti, aby sme mohli komunikovať "bezpečne" v rámci moderného informačného života. Slovo "bezpečne" kryptológia definuje pomocou troch vlastností, ktorými sú dôvernosť, integrita a dostupnosť informácií. Inak povedané komunikujeme takým spôsobom, aby nepozvaná tretia strana nevedela, o čom komunikujeme, teda aby nevedela prečítať pravú podstatu vymieňaných správ.

Niekedy z rôznych dôvodov nechceme ani to, aby tretia strana vôbec vedela o tom, že medzi sebou komunikujeme. V tomto prípade by sme mohli do balíčku vlastností "bezpečne" pridať vlastnosť utajenosť. Veda, ktorá vo svojom balíčku obsahuje utajenosť a prípadne i ďalšie vlastnosti, sa nazýva steganografia. Oproti kryptografii je hlavným cieľom steganografie ukryť výskyt komunikácie medzi dvoma stranami tretej strane. To znamená, že tretia strana netuší, že niekde prebieha komunikácia. Kryptografia v tomto prípade môže hrať akúsi podpornú rolu steganografie a v prípade odhalenia komunikácie poskytovať komunikujúcim stranám ostatné tri vlastnosti bezpečnosti ich informácií. Môžeme si to predstaviť ako škrupinu pozostávajúcu z dvoch vrstiev, ktoré musíme prekonať, aby sme sa dostali k jadru. Prvá z nich je steganografia, a za ňou nasleduje kryptografia.

Termín steganografia sa začal používať na konci 15-teho storočia, no použitie steganografie siaha až do dávnej minulosti. V staroveku boli správy ukrývané na zadnú stranu voskových tabuliek (zaliali sa voskom a nebolo ich vidieť), na králičí žalúdok, alebo boli vytetované na hlavu otroka (a čakalo sa, kým mu dorástli vlasy). Neviditeľný atrament sa používa po stáročia - dnes už skôr pre zábavu. Mikrobody a mikrofilmy, neoddeliteľná súčast vojny a špionážnych filmov, sa začali používať až po vynájdení fotografií. Po príchode takzvanej "digitálnej doby" sa začala rozvýjať steganografia na digitálnych dátach a začali sa rozlišovať dva typy steganografie. Prvá z nich je klasická steganografia, ktorá zahrňuje steganografiu do počiatkov digitálnej doby, a druhá z nich je moderná steganografia, ktorá už používa pre svoje účely digitálne data. Tá moderná využíva hlavne multimediálne dáta pre utajenie komunikácie.

Existuje niekoľko rôznych techník, pomocou ktorých je možné aplikovať steganografiu na digitálne dáta. V tejto práci sa budeme venovať len jednej z nich a tou je steganografia založená na samoopravných kódoch. Samoopravné kódy sú vo svojej podstate algoritmy, ktoré majú vlastnosť, že prakticky dokážu zariadiť integritu dát pri prenose

nejakým kanálom. Štúdium samoopravných kódov a s nimi spojená matematika je súhrne označované ako *teória kódov*. Touto teóriou sa budeme zaoberať v prvej kapitole. Aby sme dokázali efektívne používať steganografiu založenú na samoopravných kódoch, je dôležité, aby sme pochopili, akým spôsobom samoopravné kódy fungujú. V prvej kapitole preto budeme rozoberať kódy od základov až po zložitejšie štruktúry a konštrukcie kódov nad rôznymi telesami a okruhmi. Predstavíme si samoopravné kódy a ich rôzne skupiny. Dôležitými kódmi pre nás budu lineárne kódy nad dvojprvkovým telesom $\mathbb{F}_2$ a varianty kódov nad okruhom $\mathbb{Z}_4$, ktorými reprezentantmi sú hlavne Kerdockove a Preparata kódy.

V druhej kapitole sa začneme venovať modernej steganografii. Zoznámime sa s princípmi steganografie a jej základným modelom, ktorého aplikácie sa dajú veľmi jednoducho preniesť na zložitejšie prípady. Ukážeme si pár analýz, ktoré využíva steganoanalýza ako opačný pól steganografie. Pomocou týchto analýz si neskôr ukážeme rozdiely medzi niektorými steganografiami. Uvedieme súvislosti medzi teóriou kódov a steganografiou. Budeme sa venovať takzvaným krycím funkciám, ktoré tvoria základ stegnografie založenej na samoopravných kódoch. Tieto krycie funkcie všeobecne dosahujú lepšie steganografické vlastnosti ako ostatné typy moderných steganografií. Rôznymi kombináciami a skladaním týchto funkcií môžeme získať ešte lepšie vlastnosti; to uvidíme pri využití direktnej sumy v tejto kapitole.

Tretia kapitola obsahuje praktické ukážky konštrukcie steganografických algoritmov založených na samoopravných kódoch. Všeobecne nie je jednoduché konštruovať zložitejšie krycie funkcie. Uvedené algoritmy využívajú teoretické znalosti uvedené v tejto práci. Nakoniec sa budeme venovať zovšeobecneniu steganografie založenej na samoopravných kódoch, to znamená, že sa pokúsime preniesť aplikácie z dvojprvkového telesa na teleso $\mathbb{F}_q$.

V prílohách je možné nájsť zaujímavé porovnania steganografických algoritmov, o ktorých sa bavíme v tejto práci. Grafická reprezentácia efektívnosti jednotlivých algoritmov poskytuje jednoduchý pohľad na ich porovnanie. Pre úplnosť sú v tabuľkách uvedené niektoré údaje, ktoré súvisia s krycími funkciami. Chi-kvadrát test, ako jeden z techník steganoanalýzy, nám pomôže znázorniť rozdiely medzi steganografiou založenou na samoopravných kódoch a LSB steganografiou a jeho implementácia nám umožňuje jednoducho interpertovať jeho výstup.

Kapitola 1

Základné pojmy a definície z teórie kódov

V tejto časti uvedieme základné informácie o kódoch a ich vlastnostiach. Budeme pri tom predpokladať základnú znalosť lineárnej algebry, ktorú čitateľ môže nájsť napríklad v učebnici od profesora Ladislava Bicana [1].
Nech $\Sigma = \{s_0, \ldots, s_m\}$ je konečná abeceda. Slovo dĺžky l je usporiadaná l-tica symbolov z abecedy Σ. Množinu všetkých slov dĺžky l značíme Σ^l.
Budeme popisovať zariadenie, ktoré sa nazýva *kanál*. Na jednom konci kanálu je odosielateľ správy, na druhom konci je jeho príjemca. Cez tento kanál budeme posielať symboly z konečnej abecedy a budeme predpokladať, že chyba v prenesení niektorého z prvkov abecedy nereflektuje ostatné prenášané prvky. Na tento kanál sa môžeme pozerať ako na prenášanie správy prvok po prvku. Charakteristika kanálu teda závisí na prenášaných prvkoch. Kanál, ktorý má na vstupe a na výstupe abecedu zloženú z m prvkov budeme nazývať *m-árny symetrický kanál*. Povedzme, že tieto prvky sú $x_1, \ldots, x_m$. Kanál je charakterizovaný parametrom p, ktorý značí pravdepodobnosť, že po odoslaní prvky x_j je prijatý prvok $x_i \neq x_j$, to znamená

$$P(x_i|x_j) = p, \text{ pre } i \neq j.$$

S tým je spätá pravdepodobnosť

$$s = (m-1)p,$$

že po odoslaní prvku x_j príjemca nepríjme správny prvok a pravdepodobnosť

$$q = 1 - s = P(x_j|x_j),$$

že po odoslaní prvku x_j príjemca príjme správny prvok. Odosielateľ má teda postupnosť slov $w_1, w_2, \ldots, w_M$ z množiny $W \subset \Sigma^m$, ktorú potrebuje preniesť bez chyby k príjemcovi. Pre zvýšenie kvality komunikácie odosielateľ slová *kóduje*.

Definícia 1.1: *Kód*

> *Kód* nad abecedou Σ je ľubovoľná neprázdna množina $C \subset \Sigma^n$, kde n je ľubovoľné prirodzené číslo a hovoríme o ňom ako o *dĺžke* kódu C. *Veľkosť* kódu C je počet jeho prvkov, to znamená $|C|$. Prvky množiny Σ^n nazývame *slová* a prvky kódu C nazývame *kódové slová*. □

Odosielateľ teda pre účel kódovania používa vhodnú množinu kódových slov $C \subset \Sigma^n$ a bijekciu $\pi : W \to C$. Toto zobrazenie a množinu musí samozrejme poznať aj príjemca. Ak chce odosielateľ poslať slovo w_i, odošle namiesto neho kódove slovo $c = \pi(w_i)$. Príjemca toto kódove slovo zaznamená a jeho úlohou je ho dekódovať. Príjemca sa teda snaží nájsť slovo c, z ktorého potom jednoducho rekonštruuje pôvodné slovo $\pi^{-1}(c)$. Predpokladom je, že odoslané slovo c je prijatému slovu najbližšie v zmysle Hammingovej vzdialenosti definovanej nasledovne.

Definícia 1.2: *Hammingova vzdialenosť*

Nech $x = (x_1, \ldots, x_n)$ a $y = (y_1, \ldots, y_n)$ sú dva prvky množiny Σ^n. Hammingova vzdialenosť $d(x, y)$ prvkov x a y je počet všetkých súradníc, v ktorých sa x a y líšia, teda počet všetkých i, pre ktoré je $x_i \neq y_i$, $i = 1, \ldots, n$. □

Takéto dekódovanie sa nazýva *dekódovanie na najpodobnejšie slovo* (anglicky Maximum Likelihood Decoding). Ekvivalentnou podmienkou v reči pravdepodobnosti je, že ak príjmeme slovo c, musíme ho dekódovať na slovo x, ktoré maximalizuje $P(c|x)$, ak $q > \frac{1}{2}$.

Vráťme sa k definícii kódu. Kódom nad dvojprvkovou abecedou sa hovorí binárne kódy, napríklad kódy nad telesom $\mathbb{F}_2$ sú binárne. Kód nad abecedou o veľkosti q sa nazýva q-árny kód. Na množine Σ^n sa pomocou Hammingovej vzdialenosti definuje pojem minimálnej vzdialenosti kódu.

Definícia 1.3: *Minimálna vzdialenosť*

Minimálna vzdialenosť kódu $C \subset \Sigma^n$ je definovaná vzťahom

$$\triangle(C) = \min_{\substack{x, y \in C \\ x \neq y}} d(x, y)$$

□

Čím väčšia je minimálna vzdialenosť kódu, tým viac chýb môže kód opravovať. Predpokladajme, že $\triangle(C) \geq 2t + 1$, a že pri prenose nejakého slova c nastane najviac t chýb. Prijaté slovo vždy dekódujeme na najpodobnejšie kódové slovo, to znamená na najbližšie slovo kódu C vzhľadom k Hammingovej vzdialenosti. Takéto slovo je za daných predpokladov práve jedno a je to odoslané slovo c, takže dekódovanie prebehne správne. Preto o kóde C s $\triangle(C) \geq 2t + 1$ hovoríme, že má schopnosť opravy t chýb.
Je jednoduché si rozmyslieť, že Hammingova vzdialenosť je metrika. Kód C popisujeme na základe jeho vlastností ako $(n, k, d)_q$-*kód*, kde n označuje dĺžku kódu, k označuje veľkosť kódu, kde uvažujeme jeho logaritmus, teda $k = \log_q |C|$, d je minimálna vzdialenosť kódu a q je veľkosť abecedy Σ. Niekedy, keď je z kontextu zrejmé, o aký parameter q ide, sa toto značenie zjednodušuje na (n, k, d)-kód.

1.1 Niektoré základné príklady kódov

Jedna z najstarších foriem detekčného kódovania je pridanie paritného bitu k prenášanej informácii. Predstavme si, že kanálom posielame reťazec pozostávajúci z 26 bitov. K týmto

bitom pridáme jeden bit, ktorý je určený predchádzajúcimi 26 bitmi. Ak reťazec obsahuje párny počet jedničiek, pridáme na jeho koniec nulu, v opačnom prípade pridáme jedničku. Výsledný reťazec 27 bitov bude vždy obsahovať párny počet jedničiek, to znamená, že má párnu paritu. Pridaním tejto malej redundancie sme nijak nepoškodili originálny reťazec, ale získali sme schopnosť detekovať chybu v prenose informácii. Ak sa počas prenosu objaví chyba, potom príjemca prečíta reťazec, ktorý má nepárnu paritu. Pretože vieme, že posielaný reťazec má párnu paritu, niekde musela nastať chyba, a môžeme požiadať o znovuodoslanie reťazca. Tento princíp neposkytuje ďalšie vlastnosti. Môže nastať viac variant, kedy sa nevyhneme nesprávnemu prijatiu informácii, aj keď prijatý reťazec bude mať stále párnu paritu. Z tejto formy detekčného kódu neskôr vznikli paritné kódy, ktoré budu prezentované ďalej.

1.1.1 Opakovacie kódy

Opakovacie kódy existujú pre každú dĺžku n nad ktoroukoľvek abecedou Σ. Sú tvorené všetkými kódovými slovami tvaru $(xxx\ldots x)$, kde $x \in \Sigma$. Dekódovanie je pritom veľmi jednoduché, zvolíme práve ten znak, ktorý má najväčšiu frekvenciu v prijatom slove. Základným príkladom je binárny opakovací kód, to znamená opakovací kód nad abecedou $\Sigma = \{0, 1\}$.

Príklad 1.4:

Uvažujme binárny opakovací kód dĺžky 5. Slovo 01 sa zakóduje ako

$$0000011111.$$

Dekódovanie takého slova prebieha na základe majoritnej funkcie, to znamená, že z každej pätice vyberieme znak s najväčšou frekvenciou, v tomto prípade len 0 alebo 1. □

1.1.2 Paritný kód

Paritné kódy patria medzi najstaršie rodiny kódov, ktoré sa používajú v praxi. Paritný kód dĺžky n pozostáva zo všetkých binárnych n-tíc, ktoré obsahujú párny počet jedničiek, to znamená, že pre každé kódové slovo $(x_1, \ldots, x_n)$ platí $\sum_{i=1}^{n} x_i = 0$. Takýchto slov je 2^{n-1}. Každá podmnožina $n-1$ súradníc môže byť nosičom informácie, zatiaľ čo zostávajúca súradnica kontroluje paritu informácie. Výskyt jednej chyby pri prenose môže byť zaznamenaný. Pozrime sa, aká je minimálna vzdialenosť týchto kódov. Nech x a y sú dve kódové slová, a nech X resp. Y je množina súradníc i, pre ktoré je x_i resp. y_i rovno 1. Obidve množiny majú párnu mohutnosť. Pretože $|X \oplus Y| = |X| + |Y| - 2|X \cap Y|$ je párne číslo, musí byť veľkosť symetrického rozdielu $X \oplus Y = X \cup Y - X \cap Y$ aspoň 2. Vidíme, že paritný kód dĺžky n je $(n, n-1, 2)_2$ kód.

1.2 Lineárne kódy

Ukazuje sa, že efektívne kódovanie a dekódovanie vyžaduje kódy nad abecedou, ktorá je vybavená vhodnou algebraickou štruktúrou. Takouto štruktúrou je predovšetkým štruktúra konečného telesa. *Lineárny kód* dĺžky n nad telesom $\mathbb{F}_q$ je podpriestor vektorového

priestoru $\mathbb{F}_q^n$. Kódové slová lineárneho kódu teda patria medzi vektory $x \in \mathbb{F}_q^n$. Ak má kód C dimenziu k (ako podpriestor), je $|C| = q^k$. Parametry lineárnych kódov sa uvádzajú v hranatých zátvorkách, teda hovoríme o $[n, k, d]_q$-*kódoch*. Číslo $n - k$ nazývame *redundanciou* kódu C.
Výhodou lineárnych kódov je ich úsporný popis. Stačí namiesto výčtu všetkých q^k prvkov kódu C uviesť k prvkov nejakej jeho báze.

Definícia 1.5: *Generujúca matica*

Generujúca matica kódu C je matica o rozmeroch $k \times n$, ktorej riadky tvoria bázu kódu C. □

Teda generujúca matica kódu C je matica, ktorej riadky sú lineárne nezávislé. Pomocou generujúcich matíc sa dajú jednoducho konštruovať lineárne kódy, ale z tejto matice nie sú zrejmé všetky vlastnosti kódu. Generujúca matica je v *štandardnom tvare*, ak je tvaru

$$(I_{k\times k}|A_{k\times(n-k)}).$$

Definícia 1.6: *Hammingova (minimálna) váha*

Hammingova váha vektoru x je počet nenulových súradníc vektoru x a označujeme ju $w(x)$. Minimálna váha kódu C je definovaná vzťahom

$$w_{min}(C) = w(C) = \min_{0\neq x\in C}(w(x)).$$

□

Platí teda, že $w(x) = d(x, 0)$.

Lemma 1.7:

Hammingova vzdialenosť je v lineárnych kódoch invariantná k posunutiu. □

Dôkaz:

Je zrejmé, že platí $d(x, y) = d(x + z, y + z)$ pre $x, y, z \in C$. Špeciálne platí $d(x, y) = d(x - y, y - y) = d(x - y, 0)$. □

Dôsledok 1.8:

V lineárnych kódoch platí, že minimálna vzdialenosť je rovná minimálnej váhe kódu. □

Z tohoto dôsledku je patrné, že minimálnu vzdialenosť lineárnych kódov je omnoho jednoduchšie počítať. Stačí totiž prejsť všetky kódové slová lineárneho kódu a počítať ich váhu namiesto počítania Hammingových vzdialeností všetkých dvojíc kódových slov kódu.
V priestore $\mathbb{F}_q^n$ je definovaný "skalárny" súčin predpisom

$$\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i,$$

kde $x = (x_1, \ldots, x_n)$ a $y = (y_1, \ldots, y_n)$ sú prvky $\mathbb{F}_q^n$. Skalárny súčin je definovaný v úvodzovkách kvôli jeho formálnej podobnosti so skalárnym súčinom $\langle x, y \rangle$. Štandardná definícia skalárneho súčinu vyžaduje, aby pre $x \neq 0$ bolo $\langle x, x \rangle \neq 0$, zatiaľ čo v našom prípade to tak nemusí byť. Z tejto definície plynie definícia takzvaného duálneho kódu.

Definícia 1.9: *Duálny kód*

Duálny kód k lineárnemu kódu C je jeho ortogonány doplnok, teda podpriestor

$$C^\perp = \{x : \ \langle x, y \rangle = 0 \ \forall y \in C\}.$$

□

Všimnime si, že v tejto definícii duálneho kódu nemusí byť vždy prienik $C \cap C^\perp$ prázdny. Samozrejme platí všeobecne známa vlastnosť ortogonálneho doplnku, a to

$$\dim C^\perp + \dim C = n.$$

Uvedená vlastnosť vyplýva z vety, ktorej dôkaz môžeme nájsť v každej učebnici základov lineárnej algebry. Pripomeňme si pojmy, ktoré sa k nej vzťahujú. Ak A je $m \times n$ matica nad telesom K, potom *riadkový priestor* matice A je podpriestor K^n generovaný riadkami (riadkovými vektormi) matice A. Podobne, *stĺpcový priestor* matice A je podpriestor K^n generovaný stĺpcami (stĺpcovými vektormi) matice A. *Nulový priestor* matice A je priestor takých stĺpcových vektorov $x \in K^n$, že $A \cdot x^\top = 0$. Dimenziu riadkového priestoru matice A nazývame *riadková hodnosť* matice A, a dimenziu stĺpcového priestoru nazývame *stĺpcová hodnosť* matice A. *Nulitou* matice A nazývame dimenziu jej nulového priestoru. Pripomeňme si jednu z viet lineárnej algebry vzťahujúcu sa k tomuto.

Veta 1.10:

Nech A je $m \times n$ matica nad telesom K. Potom:

- Riadková hodnosť matice A je rovná stĺpcovej hodnosti matice A, túto rovnakú dimenziu nazývame *hodnosť* matice A;
- Hodnosť matice A plus nulita matice A je rovno počtu stĺpcov matice A.

□

Duálny kód $C^\perp$ je lineárny aj keď kód C lineárny nie je. To je mimochodom dobrý spôsob dokazovania, že nejaký kód je lineárny. Zároveň môžeme konštruovať duálny kód duálneho kódu a vidíme, že $(C^\perp)^\perp = C^{\perp\perp} \supseteq C$. Ak platí rovnosť $C^\perp = C$ hovoríme, že kód C je *samoduálny*. Ukážeme si, že v lineárnych kódoch táto rovnosť platí. Nech G je generujúca matica lineárneho kódu C. Potom vektor $x \in C^\perp$ práve vtedy ak $G \cdot x^\top = 0$. Pretože platí $\dim C^\perp + \dim C = n$, $C^\perp$ má dimenziu $n - k$ a $C^{\perp\perp}$ má dimenziu k. Tento priestor obsahuje C a zároveň má rovnakú dimenziu ako C, preto musí platiť $C^{\perp\perp} = C$. Môžeme zhrnúť toto pozorovanie do nasledujúceho lemma.

Lemma 1.11:

Ak C je lineárny kód dĺžky n a dimenzie k nad telesom $\mathbb{F}_q$, potom jeho duálny kód $C^\perp$ je lineárny kód dĺžky n a dimenzie $n - k$ nad telesom $\mathbb{F}_q$. □

Definícia 1.12: *Kontrolná matica*

Generujúca matica duálneho kódu $C^{\perp}$ sa nazýva *kontrolná matica* kódu C. □

Riadky kontrolnej matice určujú lineárne rovnice, ktoré musí každé kódové slovo kódu C splňovať a naopak, teda

$$C = \{x : \ M \cdot x^{\top} = 0\}.$$

Niekedy sa kód definuje pomocou jeho kontrolnej matice. Vzhľadom k tomu, že pre generujúcu maticu kódu v štandardnom tvare vieme jednoduchým spôsobom nájsť bázu nulového priestoru, dokážeme to aj pre generujúcu maticu duálneho kódu. Z toho tiež jednoducho plynie, že ak je generujúca matica v štandardnom tvare

$$(I_{k\times k}|A_{k\times(n-k)}),$$

potom kontrolná matica má tvar

$$(-A^{\top}_{(n-k)\times k}|I_{(n-k)\times(n-k)}).$$

Medzi kontrolnou maticou M lineárneho kódu C a jeho minimálnou vzdialenosťou $\triangle(C)$ platí prekvapivý vzťah. Pre nejakú kontrolnú maticu H a riadkový vektor x je súčin $H\cdot x^{\top}$ lineárnou kombináciou stĺpcov matice H s koeficientmi danými vektorom x, teda

$$\sum_i h_i x_i,$$

kde H má i-tý stĺpec h_i a x_i je i-tá súradnica vektoru x. Počet nenulových sčítancov je rovný váhe kódového slova x. Ak je teda každých d stĺpcov matice H lineárne nezávislých, potom kód neobsahuje kódové slová váhy d. Z toho plynie nasledujúce lemma.

Lemma 1.13:

Nech C je lineárny kód s kontrolnou maticou H. Množina w stĺpcov matice H je lineárne závislá práve vtedy, ak existuje nenulové kódové slovo kódu C, ktorého všetky nenulové súradnice sú práve na pozíciach príslušných stĺpcov matice z množiny w. Platí $\triangle(C) = d$ práve vtedy, ak existuje množina d lineárne závislých stĺpcov matice H, a každá množina $d-1$ stĺpcov matice H je lineárne nezávisla. □

1.3 Binárne perfektné kódy

Začneme jednoduchou definíciou.

Definícia 1.14: *Sféra*

Nech $\mathbb{F}_q$ je konečná množina a $x \in \mathbb{F}_q^n$. V $\mathbb{F}_q^n$ definujeme *sféru* s polomerom ρ a stredom v bode x ako

$$S_\rho(x) = \{y \in \mathbb{F}_q^n \mid d(x,y) \leq \rho\}.$$

□

Teda sféra s polomerom ρ okolo prvku x pozostáva zo všetkých prvkov y, ktoré sa od x líšia v najviac ρ súradniciach. Počet prvkov vo vzdialenosti i od stredu x je práve $\binom{n}{i}$, takže

$$|S_\rho(x)| = \sum_{i=0}^{\rho} \binom{n}{i}.$$

Táto hodnota sa nazýva objem sféry $S_\rho(x)$ a značí sa $V_q(n, \rho)$. V binárnom prípade väčšinou vynechávame index a píšeme jednoducho $V(n, \rho)$.

Veta 1.15: *Hammingov odhad*

Pre binárny kód C s minimálnou vzdialenosťou aspoň $2t + 1$ platí

$$|C| \leq \frac{2^n}{V(n,t)}$$

□

Dôkaz:

Pozrime sa na definíciu sféry pre $\rho = t$. Pre každé slovo $x \in \mathbb{F}_2^n$ existuje najviac jedno kódove slovo vo vzdialenosti najviac t od x. To znamená, že sféry $S_t(x)$ sú pre rôzne $x \in C$ disjunktné. V množine $\mathbb{F}_2^n$ je $|C|$ disjunktných sfér a každá z nich má objem $V(n, t)$. Z toho plynie nerovnosť vo vete. □

Definícia 1.16: *Binárny perfektný kód*

Binárny kód sa nazýva *perfektný*, ak pre neho platí rovnosť v Hammingovom odhade. □

Binárne perfektné kódy teda majú práve $\frac{2^n}{V(n,t)}$ prvkov.

1.4 Hammingove kódy

V tomto oddiele zostrojíme nekonečnú triedu lineárnych binárnych kódov s minimálnou vzdialenosťou rovnou 3, ktoré sa označujú ako *Hammingove kódy*. Ak chceme konštruovať čo najväčšie binárne kódy s minimánou vzdialenosťou rovnou 3, tak podľa Lemma 1.13 stačí skonštruovať maticu nad telesom $\mathbb{F}_2$, ktorá neobsahuje žiadne lineárne závislé dvojice stĺpcov, a počet stĺpcov je čo najväčší.
Dva vektory nad telesom $\mathbb{F}_2$ sú lineárne závislé práve vtedy, ak sú zhodné alebo jeden z nich je nulový. Teda pre nejaké r skonštruujeme binárnu $r \times (2^r - 1)$ maticu H. Stĺpce tejto matice sú práve všetky nenulové vektory priestoru $\mathbb{F}_2^r$ a ich počet je $2^r - 1$. Kód s takouto kontrolnou maticou sa nazýva *binárny Hammingov kód* redundancie r a označujeme ho $Ham_r(2)$. Kontrolnú maticu môžeme zostrojiť aj tak, že každý i-ty stĺpec bude reprezentovať binárny tvar čísla i. Takáto kontrolná matica sa označuje ako *lexikografická*. Každý binárny Hammingov kód má minimálnu váhu a vzdialenosť rovnú 3. Tento poznatok plynie z Lemma 1.13. Kód $Ham_r(2)$ s kontrolnou maticou H má dĺžku $2^r - 1$ a podľa ortogonálneho doplnku je jeho dimenzia

$$Ham_r(2) = (2^r - 1) - r = 2^r - r - 1.$$

Veta 1.17:

Pre každé $r \geq 2$ má kód $Ham_r(2)$ parametry $[2^r - 1, 2^r - r - 1, 3]$. □

Hammingove kódy môžeme definovať aj nad konečným telesom $\mathbb{F}_q$. Znova si zvolíme číslo r a skonštruujeme lineárny kód na telesom $\mathbb{F}_q$ redundancie r. Vždy, keď pridávame nový stĺpec do kontrolnej matice, musíme dávať pozor, aby nebol lineárne závislý k predošlým stĺpcom. Vždy sa vyhneme nulovému slovu, takže na začiatku si vyberáme z $q^r - 1$ nenulových r-tíc. Ak pridáme nenulový stĺpec, musíme vymazať z ďalšieho výberu aj jeho $q-1$ násobkov s nenulovými prvkami telesa $\mathbb{F}_q$. Preto je najväčšia možná dĺžka $\frac{q^r-1}{q-1}$. Jeden z najjednoduchších spôsobov, ako skonštruovať takúto maticu, je zvoliť za stĺpce všetky nenulové r-tice, ktorých najvyššia nenulová súradnica je 1. Takýto lineárny kód nad konečným telesom $\mathbb{F}_q$ sa nazýva *Hammingov kód* redundancie r a píšeme $Ham_r(q)$. Všimnime si, že obecná definícia zahrňuje aj binárny prípad Hammingovho kódu.

Veta 1.18:

Pre každé $r \geq 2$ má kód $Ham_r(q)$ parametry $[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3]$. □

Príklad 1.19:

Nasledujúce matice sú kontrolné matice binárneho Hammingovho kódu $Ham_4(2)$:

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

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

Môžeme vidieť, že prvá z nich je v štandardnom tvare, zatiaľ čo druhá je v tvare lexikografickom. □

Ak pridáme paritný bit k binárnemu Hammingovmu kódu $Ham_r(2)$, zvýši sa minimálna vzdialenosť kódu na 4. Tento kód sa nazýva *rozšírený Hammingov kód* a značíme ho $\overline{Ham}_r(2)$. Z predchádzajúceho je jasné, že parametre tohoto kódu sú $[2^r, 2^r - r, 4]$. Ukážme si, ako sa tento kód zostrojuje. Začneme s kontrolnou lexikografickou maticou H kódu $Ham_r(2)$. Kontrolnú maticu EH rozšíreného Hammingovho kódu získame tak, že na začiatok matice H pridáme nulový stĺpec (reprezentovaný nulovým vektorom ako nultý stĺpec) a k výslednej matici pridáme nakoniec riadok, skladajúci sa z jedničiek.

Príklad 1.20:

Modifikujme maticu z príkladu 1.19 tak, aby výsledná matica bola v tvare kontrolnej matice rozšíreného Hammingovho kódu. Výsledná matica bude nasledujúceho tvaru:

$$\left(\begin{array}{c|cccccccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right)$$

□

Všimnime si, že v každej takto zostrojenej kontrolnej matici je $r+1$ riadkov lineárne nezávislých. Ak $c = (c_1, \ldots, c_n)$ je slovo z Hammingovho kódu, potom odpovedajúce rozšírené slovo je $c' = (c_0, c_1, \ldots, c_n)$, kde $c_0 = \sum_{i=1}^{n} c_i$. Každé z takýchto slov má súradnicu c_0 definovanú ako paritný bit. Teda matica EH je v skutočnosti kontrolnou maticou rozšíreného Hammingovho kódu.

1.5 Cyklické kódy

Cyklické kódy patria medzi prvé kódy, ktoré sa prakticky používali. Tieto kódy sú generované cyklickým posunom súradníc a majú bohatú algebraickú štruktúru.

Definícia 1.21: *Cyklický kód*

Lineárny kód C dĺžky n nad telesom $\mathbb{F}_q$ sa nazýva cyklický, ak je invariantný k cyklickému posunu súradníc, to znamená

$$(c_0, c_1, c_2, \ldots, c_{n-2}, c_{n-1}) \in C \Leftrightarrow (c_{n-1}, c_0, c_1, \ldots, c_{n-3}, c_{n-2}) \in C,$$

pre každé slovo $(c_0, c_1, c_2, \ldots, c_{n-2}, c_{n-1}) \in \mathbb{F}_q^n$. □

Pretože cyklický kód je invariantný k takémuto jednému posunutiu súradníc doprava, iteráciou zistíme, že je invariantný pre posunutie súradníc smerom doprava o akýkoľvek počet súradníc. Pretože jedno posunutie súradníc smerom doľava je identické s posunutím súradníc o $n-1$ súradníc smerom doprava, môžeme podobné tvrdenie vysloviť aj pre posúvanie súradníc smerom doľava. Jednoducho hovoríme, že *cyklický kód je invariantný k cyklickému posunu súradníc.*
Je vhodné pomýšľať na cyklické kódy ako na kódy pozostávajúce z polynómov. Pre každé slovo

$$a = (a_0, a_1, a_2, \ldots, a_{n-2}, a_{n-1}) \in \mathbb{F}_q^n$$

asociujeme polynóm

$$a(x) = \sum_{i=0}^{n-1} a_i x_i = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in \mathbb{F}_q^{[}x].$$

Pre kódove slovo $c \in C$ hovoríme o $c(x)$ ako o asociovanom kódovom polynóme. Pretože táto asociácia sa týka iba prvých n mocnín premennej x, môžeme slovo a stotožnit s triedou okruhu

$$R = \mathbb{F}_q[x]/(x^n - 1).$$

Pri tejto konvencii asociuujeme posunuté kódové slovo $\tilde{c}$ s polynómom

$$\tilde{c}(x) = c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1}.$$

Teda cyklický posun súradníc v reči polynómov znamená násobenie polynómom x, pretože

$$x(c_0, c_1, c_2, \ldots, c_{n-2}, c_{n-1}) = c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1},$$

formálnejšie

$$\tilde{c}(x) \equiv xc(x) \pmod{x^n - 1}.$$

Je jasné, že

$$c(x) \in C \pmod{x^n - 1} \Leftrightarrow xc(x) \in C \pmod{x^n - 1}.$$

Pretože cyklický kód je invariantný k cyklickému posunu súradníc, dostávame

$$x^i c(x) \in C \pmod{x^n - 1},$$

pre každé i. Vzhľadom k linearite, pre každé $a_i \in \mathbb{F}_q$ je

$$a_i x^i c(x) \in C \pmod{x^n - 1}$$

a v skutočnosti

$$\sum_{i=0}^{d} a_i x^i c(x) \in C \pmod{x^n - 1},$$

pre každé d. Z toho vyplýva, že polynomiálne reprezentácie cyklických kódov dávajú presne ideály okruhu R.

Veta 1.22:

Nech $C \neq \{0\}$ je cyklický kód dĺžky n nad $\mathbb{F}_q$ a $g(x)$ je monický polynóm minimálneho stupňa, $g(x) \in C$.

1. Potom je $g(x)$ jednoznačne určený v C a

   $$C = \{q(x)g(x) \mid q(x) \in F_q^{n-r}[x]\},$$

   kde $r = \deg(g(x))$. Teda C má dimenziu $n - r$.
2. Polynóm $g(x)$ delí $x^n - 1$ v $\mathbb{F}_q[x]$.

□

Dôkaz:

1. Podľa vety o delení so zvyškom je

$$c(x) = q(x)g(x) + r(x),$$

pre nejaké $q(x), r(x) \in \mathbb{F}_q[x]$ také, že $\deg(r(x)) < r = \deg(g(x))$. Teda

$$r(x) = c(x) - q(x)g(x).$$

Z linearity plynie, že pravá strana rovnice je v C, teda v C musí byť aj $r(x)$. Ak $r(x)$ bolo nenulové, potom má monický skalárny násobok patriaci do C, ktorý je menšieho stupňa. To by znamenalo spor s voľbou polynómu $g(x)$. Musí teda byť $r(x) = 0$ a $c(x) = q(x)g(x)$.
2. Taktiež podľa vety o delení so zvyškom platí

$$x^n - 1 = h(x)g(x) + s(x),$$

pre nejaké $s(x)$ menšieho stupňa ako je stupeň $g(x)$. Platí, že

$$s(x) = (-h(x))g(x)(\text{mod } x^n - 1)$$

patrí do C. Ak $s(x)$ bolo nenulové, tak má monický skalárny násobok patriaci do C, ktorý je menšieho stupňa. Znova to znamená spor s voľbou polynómu $g(x)$, takže $s(x) = 0$ a $g(x)h(x) = x^n - 1$. □

Polynóm $g(x)$ z predchádzajúcej vety sa nazýva *generujúci polynóm* cyklického kódu C a polynóm $h(x)$ sa nazýva *kontrolný polynóm* cyklického kódu C. Dôsledkom vety 1.22 je, že každý cyklický kód obsahuje generujúci polynóm $g(x)$. Nasledujúce tvrdenie vysvetľuje pojem kontrolného polynómu.

Tvrdenie 1.23:

Ak C je cyklický kód dĺžky n s kontrolným polynómom $h(x)$, potom

$$C = \{c(x) \in \mathbb{F}_q^n[x] \mid c(x)h(x) = 0(\text{mod } x^n - 1)\}.$$

□

Dôkaz:

Ak $c(x) \in C$, tak podľa vety 1.22 existuje $q(x) \in \mathbb{F}_q[x]$ tak, že $c(x) = q(x)g(x)$. Potom

$$c(x)h(x) = q(x)g(x)h(x) = q(x)(x^n - 1) = 0(\text{mod } x^n - 1).$$

Uvažujme ľubovoľný polynóm $c(x) \in \mathbb{F}_q^n[x]$ taký, že

$$c(x)h(x) = p(x)(x^n - 1).$$

Potom

$$c(x)h(x) = p(x)g(x)h(x),$$

a teda

$$(c(x) - p(x)g(x))h(x) = 0.$$

Pretože $g(x)h(x) = x^n - 1$, tak $h(x) \neq 0$. Takže

$$c(x) - p(x)g(x) = 0 \text{ a } c(x) = p(x)g(x).$$

□

Z generujúceho polynómu cyklického kódu C môžeme jednoducho skonštruovať jeho generujúcu maticu. Predstavme si maticu

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & \cdots & \cdots & \cdots & g_{r-1} & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & \cdots & \cdots & \cdots & g_{r-1} & g_r & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & \cdots & \cdots & \cdots & g_{r-1} & g_r \end{pmatrix}$$

Táto matica má n stĺpcov a $k = n - r$ riadkov. Každý ďalší riadok je cyklickým posunom predchádzajúceho riadku. Pretože $g(x)h(x) = x^n - 1$, tak je

$$g_0 h_0 = g(0)h(0) = 0^n - 1 \neq 0.$$

Teda $g_0 \neq 0$, $h_0 \neq 0$. V skutočnosti $k = \dim(C)$ riadkov matice G je lineárne nezávislých. Je zrejmé, že riadky matice G patria do C, takže G je generujúca matica cyklického kódu C.

Príklad 1.24:

Ukážeme si, že kód $Ham_3(2)$ je cyklický. Ak kód C je $[7, 4, 3]_2$ binárny cyklický kód s generujúcim polynómom $1 + x + x^3$, tak generujúca matica má tvar

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

□

Reverzný kód $C^{[-1]}$ k cyklickému kódu C získame obratením každého kódového slova C. Je jasné, že reverzný kód je takisto cyklický. Teda pre $(c_0, c_1, \ldots, c_{n-1}) \in C$ máme

$$(c_{n-1}, c_{n-2}, \ldots, c_0) \in C^{[-1]}.$$

V polynomiálnej reprezentácii cyklického kódu máme pre $c(x) \in C$

$$x^{n-1} c(x^{-1}) \in C^{[-1]}.$$

Pre polynóm $p(x)$ stupňa d definujeme *recipročný polynóm* ako

$$p^{[-1]}(x) = \sum_{i=0}^{d} p_{d-i} x^i = x^d p(x^{-1}).$$

Odmocniny recipročného polynómu sú inverzy nenulových odmocnín pôvodného polynómu.

Lemma 1.25:

Ak $g(x)$ generuje cyklický kód C, potom $g_0^{-1}g^{[-1]}(x)$ generuje $C^{[-1]}$. □

Dôkaz:

Nech G je generujúca matica cyklického kódu C. Obrátime jej všetky riadky a napíšeme ich v opačnom poradí. Výsledná matica bude mať tvar

$$\begin{pmatrix} g_r & g_{r-1} & \cdots & \cdots & \cdots & \cdots & g_1 & g_0 & 0 & 0 & \cdots & 0 \\ 0 & g_r & g_{r-1} & \cdots & \cdots & \cdots & \cdots & g_1 & g_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & g_r & g_{r-1} & \cdots & \cdots & \cdots & \cdots & g_1 & g_0 \end{pmatrix}$$

Riadky vyššie uvedenej matice určite patria do $C^{[-1]}$. Takisto ako v generujúcej matici sú tieto riadky lineárne nezávislé, pretože $g_0 \neq 0$. Teda táto matica je generujúca matica kódu $C^{[-1]}$. Prvý riadok matice korešponduje s polynómom nižšieho stupňa ako r, teda $g^{[-1]}(x)$. Podľa vety 1.22 je $g_0^{-1}g^{[-1]}(x)$ generujúci polynóm kódu $C^{[-1]}$. □

Je jednoduché si uvedomiť, že duálny kód k cyklickému kódu C je opäť cyklický. Z vety 1.22 sa zdá, že by jeho generujúci polynóm mohol byť kontrolný polynóm cyklického kódu C. Nech teda C je cyklický kód dĺžky n s generujúcim polynómom $g(x)$ stupňa r a kontrolným polynómom $h(x)$ stupňa $k = n - r = \dim(C)$. Pretože polynóm $h(x)$ delí $x^n - 1$, je $h(x)$ generujúci polynóm cyklického kódu D dĺžky n a dimenzie $n - k = r$. Máme

$$C = \{q(x)g(x) \mid q(x) \in F_q^{n-r}[x]\}$$

a

$$D = \{p(x)h(x) \mid p(x) \in F_q^r[x]\}.$$

Nech $c(x) = q(x)g(x) \in C$ je taký polynóm, že $\deg(q(x)) \leq k - 1$ a $d(x) = p(x)h(x) \in D$ je taký polynóm, že $\deg(p(x)) \leq r - 1$. Potom

$$c(x)d(x) = q(x)g(x)p(x)h(x) = q(x)p(x)(x^n - 1) = s(x)(x^n - 1) = s(x)x^n - s(x),$$

kde $s(x) = q(x)p(x)$ tak, že

$$\deg(s(x)) \leq (k - 1) + (r - 1) = n - 2 < n - 1.$$

Vidíme, že koeficient pri x^{n-1} je rovný 0. Ak $c(x) = \sum_{i=0}^{n-1} c_i x^i$ a $d(x) = \sum_{j=0}^{n-1} d_j x^j$, tak koeficient pri x^m v polynóme $c(x)d(x)$ je rovný $\sum_{i+j=m} c_i d_j$. V skutočnosti teda dostávame

$$\sum_{i+j=n-1} c_i d_j = 0 = \sum_{i=0}^{n-1} c_i d_{n-i} = c \cdot d^*,$$

kde $c = (c_0, c_1, \ldots, c_{n-1})$ a $d^* = (d_{n-1}, d_{n-2}, \ldots, d_0)$. To znamená, že každé kódové slovo kódu C má s každým kódovým slovom kódu $D^{[-1]}$ skalárny súčin rovný 0, takže $D^{[-1]} \subset C^{\perp}$. Predtým než naše poznatky zhrnieme do vety, poznamenajme ešte, že

$$\dim(C^{\perp}) = n - \dim(C) = n - k = r = n - \deg(h^{[-1]}(x)) = \dim(D^{[-1]}).$$

Veta 1.26:

Ak C je cyklický kód dĺžky n s kontrolným polynómom $h(x)$, potom $C^{\perp}$ je cyklický kód s generujúcim polynómom $h_0^{-1}h^{[-1]}(x)$. □

1.6 Binárny Golayov kód

Binárny Golayov kód je jedným z najzaujímavejších lineárnych kódov, pretože je to jediný binárny netriviálny perfektný kód, ktorý má Hammingovu vzdialenosť väčšiu ako 3. V skutočnosti existujú dva Golayove kódy, ktoré dosahujú rovnosti v Hammingovom odhade 1.15. Sú to perfektné kódy binárne kódy $\mathcal{G}_{23}$ $[23, 12, 7]$ a ternárne kódy $\mathcal{G}_{11}$ $[11, 6, 5]$. Existuje mnoho konštrukcií Golayovho kódu, ktoré sú založené kvadratických reziduách, lexikografických úvahách, kombinatorických hrách. My si však ukážeme konštrukciu, ktorá súvisí s cyklickými kódmi.
Golay si povšimol pri hľadaní perfektných kódov, že platí rovnosť

$$\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2^{11} = 2^{23-12},$$

ktorá naznačovala možnú existenciu perfektného binárneho kódu $[23, 12, 7]$. V roku 1949 Golay takýto kód našiel.
Golayov kód môže byť generovaný polynómom

$$g_1(x) = 1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11},$$

alebo polynómom

$$g_2(x) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}.$$

Obidva polynómy sú faktory polynómu $x^{23} - 1$ v telese $\mathbb{Z}_2$, teda

$$x^{23} - 1 = g_1(x)g_2(x)(1 + x).$$

Tento kód môže byť rozšírený pomocou pridania paritného bitu na koniec každého kódového slova, čím vznikne rozšírený Golayov kód $\mathcal{G}_{24}$ $[24, 12, 8]$. Rozšírený Golayov kód môže byť generovaný maticou typu (12×24) tvaru $G = (I, B)$, kde I je jednotková matica (12×12) a B je matica tvaru

$$B = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Matica $G' = (B, I)$ je taktiež generujúcou maticou rozšíreného binárneho Golayovho kódu. Môžeme si všimnúť, že tento kód už nie je perfektný.

1.7 Binárne Reed-Mullerove kódy

Pozrime sa na ďalšiu triedu kódov súhrnne označovanú ako Reed-Mullerove kódy. Tieto kódy sa dajú skonštruovať rôznymi spôsobmi, my si ukážeme ten, ktorý je veľmi úzko spätý s afinnou geometriou nad $\mathbb{Z}_2$.
Nech V je vektorový priestor dimenzie n nad $\mathbb{Z}_2$. Teda $V = \mathbb{Z}_2^n$. Budeme predpokladať, že máme 2^n vektorov priestoru V zoradených v nejakom poradí ako $v_1, \ldots, v_{2^n}$, $v_i \in V$, $i = 1, 2, \ldots, 2^n$. Ďalej budeme uvažovať binárne slovo $(c_1, \ldots, c_N)$ dĺžky $N = 2^n$ ako funkciu

$$f : V \to \mathbb{Z}_2,$$
$$f(v_i) = c_i,$$

pre $i = 1, 2, \ldots, N$.

Lemma 1.27:

Každá funkcia z vektorového priestoru V do $\mathbb{Z}_2$ môže byť reprezentovaná ako polynóm v n premenných $x_1, \ldots, x_n$, v ktorom žiaden člen neobsahuje mocninu x_i vyššiu než prvý člen pre každé $i = 1, 2, \ldots, n$. □

Dôkaz:

Tvrdenie stačí ukázať pre funkciu $\delta_a : V \to \mathbb{Z}_2$ danú ako

$$\delta_a(v) = \begin{cases} 1 & \text{ak } v = a \\ 0 & \text{inak,} \end{cases}$$

pre každé $a \in V$, kde $v \in V$; pretože každá fukcia $f : V \to \mathbb{Z}_2$ je sumou takýchto funkcií, konkrétne

$$f = \sum_{a \in V} f(a)\delta_a.$$

Ak $a = (a_1, \ldots, a_n)$, potom máme

$$\delta_a(v) = \prod_{i=1}^{n} (x_i - a_i - 1),$$

kde $v = (x_1, \ldots, x_n) \in V$. Tým je lemma dokázané. □

Dôsledok 1.28:

Funkcie

$$f_I(v) = \prod_{i \in I} x_i$$

sú na priestore V lineárne nezávislé pre $I \subseteq \{1, 2, \ldots, n\}$, kde $v = (x_1, \ldots, x_n) \in V$. □

Dôkaz:

Týchto 2^n funkcií generuje priestor dimenzie 2^n všetkých funkcií z priestoru V do $\mathbb{Z}_2$. □

Definícia 1.29: *Reed-Mullerov kód*

Pre $0 \leq r \leq n$ definujeme *Reed-Mullerov kód* dĺžky 2^n a rádu r ako kód generovaný množinou polynómov stupňa najviac r na vektorovom priestore V, označujeme ako $\mathcal{R}(n, r)$. □

Veta 1.30:

Reed-Mullerov kód $\mathcal{R}(n, r)$ je

$$\left[N = 2^n, k = \sum_{i=0}^{r} \binom{n}{i}, d = 2^{n-r}\right]_2 - kód,$$

a platí

$$\mathcal{R}(n, r)^{\perp} = \mathcal{R}(n, n - r - 1).$$

□

Dôkaz:

Z definície je zrejmé, že tento kód má dĺžku 2^n. Dimenzia kódu je taktiež zrejmá z definície, keďže počet monómov stupňa najviac r je $\sum_{i=0}^{r} \binom{n}{i}$.

Pretože

$$\dim(\mathcal{R}(n, r)) + \dim(\mathcal{R}(n, n - r - 1)) = 2^n,$$

stačí nám ukázať, že kódy $\mathcal{R}(n, r)$ a $\mathcal{R}(n, n-r-1)$ sú ortogonálne. Nech teda f a f' sú dva monómy stupňa najviac r a $n-r-1$ postupne. Potom existuje nejaká premenná, označme ju ako x_n, ktorá sa nevyskytuje ani v jednom z monómov. To znamená, že f a f' nie sú ovplyvnené zmenou x_n. Z toho vyplýva, že množiny prvkov, na ktorých sú f a f' nenulové, majú párnu kardinalitu a teda $f \cdot f' = 0$, takže tieto dva kódy sú ortogonálne.

To, že kód $\mathcal{R}(n, r)$ má minimálnu vzdialenosť rovnú 2^{n-r} ukážeme indukciou podľa premennej r. Pre $r = 0$ máme kód $\mathcal{R}(n, 0)$, ktorý pozostáva len zo slov $0 = (0, \ldots, 0)$ a $1 = (1, \ldots, 1)$, takže minimálna vzdialenosť je v tomto prípade rovná 2^n. Predpokladajme, že tvrdenie platí pre kód $\mathcal{R}(n, r-1)$. Vezmime si nejaké $f \in \mathcal{R}(n, r)$. Potrebujeme ukázať, že množina prvkov S, na ktorých je f nenulové, má veľkosť aspoň 2^{n-r}. Z indukčného predpokladu môžeme vziať do úvahy podmienku, že f nepatrí do $\mathcal{R}(n, r-1)$. Z duálneho kódu máme, že existuje monóm stupňa $n - r$, ktorý nie je ortogonálny s f, nech je to $x_1 \cdots x_{n-r}$. Označme

$$A = \{(x_1, \ldots, x_n) \in V : x_1 = \cdots = x_{n-r} = 1\}.$$

Je zrejmé, že $|S \cap A|$ je nepárne. A je afinný podpriestor priestoru V dimenzie r. Zjednotenie akýchkoľvek dvoch vzájomne disjunktných translácií množiny A je afinný podpriestor dimenzie $r+1$ a na tejto množine je kódové slovo z kódu $\mathcal{R}(n, n-r-1) = \mathcal{R}(n,r)^{\perp}$ nenulové. Takže $|S \cap (A \cup (A+v))|$ je párne číslo pre všetky vektory $v \notin A$. Z toho plynie, že $|S \cap (A+v)|$ je nepárne pre všetky $v \in V$. V skutočnosti je teda $|S| \geq 2^{n-r}$ a tým je dôkaz dokončený. □

Nasledujúci fakt uvedieme bez dôkazu. Je v ňom zachytená súvislosť Reed-Mullerových kódov s Hammingovými kódmi, s ktorou budeme neskôr pracovať.

Dôsledok 1.31:

Kód $\mathcal{R}(n, n-2)$ je ekvivalentný s rozšíreným kódom $\overline{Ham}_n(2)$. □

V ďalšom sa ukáže, že pre naše účely budú hrať dôležitú rolu Reed-Mullerove kódy druhého rádu.

1.8 Nordstrom-Robinsonov kód

Nordstrom-Robinsonov kód $\mathcal{NR}$ je najmenším prvkom triedy nelineárnych binárnch Kerdockových kódov, ktoré skonštruujeme v nasledujúcej časti. Je to kód s parametrami $(16, 256, 6)$. Je známe, že žiadny iný nelineárny kód s takými parametrami neexistuje, čím je $\mathcal{NR}$ kód unikátny v tomto smere.

Klasická definícia Nordstrom-Robinsonovho kódu vychádza z rozšíreného Golayovho kódu. Nech teda $\mathcal{G}_{24}$ je rozšírený $[24, 12, 8]_2$-kód so súradnicami kódových slov preusporiadaných tak, že $c = (11111111\underbrace{0\ldots0}_{16}) \in \mathcal{G}_{24}$. Nech π je projekcia kódu $\mathcal{G}_{24}$ na prvých osem súradníc a nech $\mathcal{D}$ je jadro projekcie π. Toto jadro má stále minimálnu vzdialenosť aspoň 8. Ďalej využijeme takzvaný *Griesmerov odhad* pre lineárne kódy, ktorý hovorí o tom, že pre $[n, k, d]_2$-kód platí nerovnosť

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil .$$

Vezmime túto nerovnosť ako fakt a dostávame, že dimenzia $\mathcal{D}$ je najviac 5. Projekcia $\pi(\mathcal{G}_{24})$ má teda dimenziu najviac rovnú $12-5=7$. Pretože rozšírený Golayov kód je samoduálny, dostávame v nerovnosti rovnosť. $\pi(\mathcal{G}_{24})$ je potom $[8, 7, 2]_2$-kód a projekcia $\mathcal{D}$ na posledných 16 súradníc je $[16, 5, 8]_2$-kód (kód $\mathcal{R}(4,1)$ podľa predchádzajúcej sekcie).

Z predchádzajúcej úvahy plynie, že binárny Reed-Mullerov kód prvého rádu $\mathcal{R}(4,1)$ pozostáva zo všetkých vektorov $v \in \mathbb{Z}_2^{16}$ takých, že vektory $(00000000v) \in \mathcal{G}_{24}$. Kód $\mathcal{NR}$ obsahuje všetky vektory $v \in \mathbb{Z}_2^{16}$ také, že $(uv) \in \mathcal{G}_{24}$, kde vektor u je jeden z nasledujúcich vektorov

$$(00000000),\ (11000000),\ (10100000),\ (10010000),$$
$$(10001000),\ (10000100),\ (10000010),\ (10000001).$$

$\mathcal{NR}$ kód je teda zjednotením ôsmych posunutých kopií kódu $\mathcal{R}(4,1)$.

Podobne, ak by sme položili $u_0 = (00000000)$ a u_i, pre $i = 1, \ldots, 7$ by boli vektory s dĺžkou 8 a jedničkami na i-tom a poslednom mieste, tak máme

$$\mathcal{NR} = \bigcup_{i=0}^{7} \mathcal{NR}_i,$$

kde

$$\mathcal{NR}_0 = \{v \in \mathbb{Z}_2^{16} : (u_0 b) \in \mathcal{G}_{24}\},$$
$$\mathcal{NR}_i = \{v \in \mathbb{Z}_2^{16} : (u_i b) \in \mathcal{G}_{24}\},\ i = 1, \ldots, 7.$$

Z matice

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

môžeme vidieť, že veľkosť každej z množín $\mathcal{NR}_i$, $i = 1 \ldots, 7$, je 2^5, takže platí $|\mathcal{NR}| = 256$. Minimálna vzdialenosť tohoto kódu je aspoň 6, pretože minimálna vzdialenosť rozšíreného Golayovho kódu je 8 a ľubovoľné dva vektory v_i, v_j, $i, j = 1, \ldots, 7$ majú vzdialenosť najviac 2.

1.9 Kerdockove kódy

1.9.1 Symplektické a kvadratické formy

V tejto časti sa pozrieme na takzvané symplektické a kvadratické formy nad telesom $\mathbb{F}_2$, ktoré budeme neskôr potrebovať pre definovanie Kerdockových kódov. Pre detailnejšie úvahy a hlbšie pochopenie niektorých bližšie nešpecifikovaných pojmov v tejto sekcii môže čitateľ použiť skripta profesora Drápala, Úvod do teorie grúp [15].

Definícia 1.32: *Kvadratická forma*

Nech V je vektorový priestor nad telesom $\mathbb{F}$ a nech f je symetrická bilineárna forma na vektorovom priestore V. *Kvadratickou formou* na V asociovanou s bilineárnou formou f nazveme každé zobrazenie $Q : V \to \mathbb{F}$, ktoré pre nejaké pevné $c \in \mathbb{F}^*$ spĺňuje:

- $Q(u + v) = Q(u) + Q(v) + cf(u, v)$, $\forall u, v \in V$;
- $Q(\lambda u) = \lambda^2 Q(u)$, $\forall u \in V$.

□

Ak je Q kvadratická forma s koeficientom c, tak je pre každé $\rho \in \mathbb{F}^*$ zobrazenie $\rho Q : u \mapsto \rho Q(u)$ kvadratickou formou s koeficientom $c\rho$. Preto sa môžeme obmedziť len na jediné $c \in \mathbb{F}^*$. Pre char $\mathbb{F} \neq 2$ položíme $c = 2$ a v prípade char $\mathbb{F} = 2$ položíme $c = 1$.

Uvažujme ďalej teleso charakteristiky 2. V tomto telese platí $Q(\lambda u) = \lambda Q(u)$, $\forall u \in V$. Poďme sa pozrieť na súvislosť kvadratických foriem s polynómami. Pre tento účel si pripomeňme, čo je to alternujúca a symetrická bilineárna forma f.

Definícia 1.33: *Alternujúca bilineárna forma*

Bilineárna forma f nad V sa nazýva *alternujúca*, ak $f(u, u) = 0$, pre všetky $u \in V$. □

Definícia 1.34: *Symetrická a antisymetrtická bilineárna forma*

Bilineárna forma f nad V sa nazýva *symetrická*, ak $f(u, v) = f(v, u)$, pre všetky $u, v \in V$. Bilineárna forma f nad V sa nazýva *antisymetrická*, ak $f(u, v) = -f(v, u)$, pre všetky $u, v \in V$. □

Ak by sme sa pohybovali nad telesom, ktoré nemá charakteristiku 2, tak by z definície kvadratickej formy 1.32 plynulo $Q(v) = \frac{1}{2} f(v, v)$, pre každé $v \in V$, takže kvadratickú formu Q by sme mohli získať z bilineárnej symetrickej formy f. V telese charakteristiky 2 je každá antisymetrická a alternujúca forma symetrická, a preto týmto spôsobom nemôžeme získať kvadratickú formu Q. V tomto prípade, ak máme dve kvadratické formy Q_1 a Q_2 asociované s formou f, tak $Q = Q_1 - Q_2$ je kvadratická forma asociovaná s nulovou formou f, čo znamená, že

$$Q(v + w) = Q(v) + Q(w).$$

Nakoľko v telese charakteristiky 2 máme $Q(\lambda u) = \lambda Q(u)$, je forma Q lineárna. Naopak, ak sa dve kvadratické formy líšia lineárnou formou, znamená to, že sú asociované s rovnakou bilineárnou formou.

Tvrdenie 1.35:

Nech $f : V \times V \to \mathbb{F}$, char $\mathbb{F} = 2$, je alternujúca bilineárna forma. Nech $e_1, \ldots, e_n$ je báza priestoru V a nech $\eta_1, \ldots, \eta_n$ sú prvky telesa $\mathbb{F}$. Definujeme $Q : V \to \mathbb{F}$ tak, že

$$Q(\sum_{i=1}^{n} \lambda_i e_i) = \sum_{i=1}^{n} \lambda_i^2 \eta_i + \sum_{1 \leq i < j \leq n} \lambda_i \lambda_j f(e_i, e_j).$$

Potom je Q kvadratická forma asociovaná s f. □

Dôkaz:

Je jasné, že $Q(\lambda u) = \lambda Q(u)$, $\forall u \in V$, $\lambda \in \mathbb{F}$. Ďalej

$$Q(\sum_{i=1}^{n} \lambda_i e_i + \sum_{i=1}^{n} \lambda_i' e_i) = \sum_{i=1}^{n} (\lambda_i + \lambda_i')^2 \eta_i + \sum_{1 \leq i < j \leq n} (\lambda_i + \lambda_i')(\lambda_j + \lambda_j') f(e_i, e_j)$$

$$= \sum_{i=1}^{n} \lambda_i^2 \eta_i + \sum_{1 \le i < j \le n} \lambda_i \lambda_j f(e_i, e_j) + \sum_{i=1}^{n} (\lambda_i^{'})^2 \eta_i$$
$$+ \sum_{1 \le i < j \le n} \lambda_i^{'} \lambda_j^{'} f(e_i, e_j) + \sum_{i,j} \lambda_i \lambda_j^{'} f(e_i, e_j)$$
$$= Q(\sum_{i=1}^{n} \lambda_i e_i) + Q(\sum_{i=1}^{n} \lambda_i^{'} e_i) + f(\sum_{i=1}^{n} \lambda_i e_i, \sum_{i=1}^{n} \lambda_j^{'} e_j).$$

Q je teda podľa definície kvadratickej formy kvadratickou formou. □

Ak v tejto forme Q prevedieme substitúciu

$$Q(e_i) = a_i,$$
$$\lambda_i = x_i,$$
$$f(e_i, e_j) = b_{ij},$$

získame kvadratický homogenný polynóm

$$Q(\underbrace{x_1, \ldots, x_n}_{\sum_{i=1}^{n} x_i e_i}) = \sum_{i=1}^{n} x_i^2 a_i + \sum_{1 \le i < j \le n} b_{ij} x_i x_j.$$

Definícia 1.36: *Nedegenerovaná bilineárna forma*

Bilineárna forma f sa nazýva *nedegenerovaná* ak platí:

1. $(f(v, w) = 0, \forall w \in V) \Rightarrow v = 0$;
2. $(f(v, w) = 0, \forall v \in V) \Rightarrow w = 0$.

□

Ak f je symetrická forma, tak každá z týchto podmienok implikuje druhú. Nedegenerovaná alternujúca bilineárna forma na priestore V existuje práve vtedy, ak $\dim V$ je párna.

Definícia 1.37: *Symplektická báza*

Nech f je nedegenrovaná alternujúca bilineárna forma. Báza $\{v_1, \ldots, v_n, w_1, \ldots, w_n\}$ priestoru V taká, že

$$f(v_i, v_j) = 0 = f(w_i, w_j), \ \forall\ i, j,$$
$$f(v_i, w_i) = 1 = -f(w_i, v_i), \ \forall\ i,$$
$$f(v_i, w_j) = 0 = f(w_j, v_i), \ \forall\ i \neq j,$$

sa nazýva *symplektická.* □

Pozrime sa ako vyzerá matica M formy f vzhľadom k symplektickej bázi $\{v_1, \ldots, v_n, w_1, \ldots, w_n\}$. Podmienky z definície nám určujú jej tvar ako

$$M = \left(\begin{array}{ccccc|ccccc} 0 & \cdots & \cdots & \cdots & 0 & 1 & 0 & \cdots & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots & 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & 0 & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & 0 & \cdots & \cdots & 0 & 1 \\ \hline 1 & 0 & \cdots & \cdots & 0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 & 0 & \cdots & \cdots & \cdots & 0 \end{array}\right)$$

Niekedy je výhodnejšie uvedomiť si, ako vyzerá matica M formy f vzhľadom k symplektickej bázi $\{v_1, w_1, v_2, w_2, \ldots, v_n, w_n\}$. V tomto prípade sa výsledná matica bude skladať z diagonály matíc (2×2) typu

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Pre nejaký podpriestor U vektorového priestoru V položíme

$$U^{\perp} = \{x \in V : f(x, u) = 0, \forall u \in U\}.$$

f je nedegenorvaná bilineárna forma a to nám dáva

$$\dim(U) + \dim(U^{\perp}) = \dim(V).$$

Žiaľ, vo všeobecnosti neplatí $V = U \oplus U^{\perp}$, pretože môže nastať $U \cap U^{\perp} \neq \{0\}$. Vektor $v \in V$ budeme nazývať *izotropným*, ak $f(v, v) = 0$. Podpriestor U sa nazýva *úplne izotropný*, ak $f(u, v) = 0$ pre všetky $u, v \in U$, to znamená, práve ak platí $U \subseteq U^{\perp}$.
Vektor $v \in V$ nazveme *singulárnym* vektorom, ak je izotropný a splňuje $Q(v) = 0$. Podpriestor $U \subseteq V$ sa nazýva *úplne singulárny*, ak je každý vektor $u \in U$ singulárny.
Nasledujúce lemma je zrejmé a vychádza z ortogonality vektorov.

Lemma 1.38:

Nech f je bilineárna forma a nech U a W sú podpriestory vektorového priestoru V. Potom

$$U \cap W^{\perp} = 0 \Leftrightarrow \forall u \in U,\ u \neq 0,\ \exists w \in W : f(u, w) \neq 0.$$

□

Dôsledok 1.39:

Nech f je bilineárna forma a nech U je podpriestor vektorového priestoru V. Potom

$$U \cap U^{\perp} = 0 \Leftrightarrow \text{restrikcia } f \text{ na } U \times U \text{ je regulárna.}$$

□

Ak teda platí $U \cap U^{\perp} = \{0\}$, potom je $V = U \oplus U^{\perp}$ a bilineárna forma f je plne určená svojimi restrikciami na $U \times U$ a $U^{\perp} \times U^{\perp}$. Preto za popis formy f považujeme rozklad priestoru $V = U_1 \oplus \cdots \oplus U_n$, kde priestory U_i majú malú dimenziu a $U_j \subseteq U_i^{\perp}$ pre všetky $i \neq j$, $1 \leq i, j \leq n$.
Podpriestor $U \subseteq V$ sa nazýva *anizotropný*, ak pre každý vektor $u \in U$, platí $Q(u) = 0$, práve vtedy, ak $u = 0$.
Hyperbolickou rovinou nazývame podpriestor $U \subseteq V$, $U = \langle e_1, e_1 \rangle$ s $Q(e_1) = Q(e_2) = 0$ a $f(e_1, e_2) = 1$. Takýto podpriestor má dimenziu 2 a obsahuje bázu tvorenú izotropnými vektormi. Platí teda $Q(xe_1 + ye_2) = xy$ pre nejaké x, y.
Nech Q_1 je kvadratická forma na priestore V_1 a Q_2 je kvadratická forma na priestore V_2. Budeme hovoriť, že formy Q_1 a Q_2 sú *ekvivalentné*, ak existuje invertibilné lineárne zobrazenie $T : V_1 \to V_2$ také, že $Q_2(vT) = Q_1(v)$ pre všetky vektory $v \in V_1$.
Nasledujúcu vetu, ktorá nám dáva klasifikáciu všetkých nedegenerovaných kvadratických foriem uvedieme bez dôkazu. Dôkaz môže čitateľ nájsť v každom texte pojednávajúcom o kvadratických formách.

Veta 1.40: *Klasifikácia kvadratických foriem*

1. Anizotropný vektorový priestor má dimenziu najviac 2.
2. Nedegenrované kvadratické formy na vektorovom priestore V existujú.
3. Nech Q je kvadratická forma na vektorovom priestore V. Potom

   $$V = W \oplus U_1 \oplus \cdots \oplus U_r,$$

   kde W je anizotropný podpriestor, $U_1, \ldots, U_r$ sú hyperbolické roviny, a všetky sčítance sú po dvoch ortogonálne.
4. Nech Q_1 je kvadratická forma na priestore V_1 a Q_2 je kvadratická forma na priestore V_2. Nech

   $$V_1 = W_1 \oplus U_{11} \oplus \cdots \oplus U_{1r},$$

   $$V_2 = W_2 \oplus U_{21} \oplus \cdots \oplus U_{2s},$$

   sú rozklady priestorov ako v (2). Potom

   $$Q_1 \text{ a } Q_2 \text{ sú ekvivalentné} \Leftrightarrow r = s \text{ a } \dim(W_2) = \dim(W_2).$$

□

Kvadratické formy nad $\mathbb{Z}_2$ sú teda určené počtom r hyperbolických rovín a dimenziou anizotropného priestoru. Budeme hovoriť, že kvadratická forma má typ $+1$, 0, -1, ak dimenzia anizotropného priestoru je v poradí 0, 1, 2.

Príklad 1.41:

Nech V je vektorový priestor nad $\mathbb{Z}_2$ dimenzie 2 a nech báza priestoru V je $\{x_1, x_2\}$. Potom všetky kvadratické formy na tomto priestore sú

$$0,\ x_1^2,\ x_2^2,\ x_1^2 + x_2^2,\ x_1x_2,\ x_1x_2 + x_1^2,\ x_1x_2 + x_2^2,\ x_1x_2 + x_1^2 + x_2^2.$$

Prvé štyri formy sú lineárne a sú rovné $0,\ x_1,\ x_2,\ x_1+x_2$. Formy $x_1^2,\ x_2^2,\ x_1^2+x_2^2$ majú jednu netriviálnu nulu. Formy $x_1x_2,\ x_1x_2 + x_1^2,\ x_1x_2 + x_2^2$ majú dve netriviálne nuly a odpovedajú hyperbolickej rovine. Pri lineárnej zmene premenných sú všetky ekvivalentné forme x_1x_2. Posledná forma $x_1x_2 + x_1^2 + x_2^2$ nadobúda hodnoty 1 vo všetkých troch nenulových vektoroch priestoru a odpovedá definitnej rovine.

Všeobecne môžeme v priestore $V = \{0, u, v, w\}$ rozlíšiť tri prípady ($Q(0) = 0$):

- Jedna nula, to znamená, že

  $$Q(u) = Q(v) = 1,$$

  $$Q(w) = 0,$$

  tento prípad odpovedá lineárnym formám (typ 0).
- Dve nuly, to znamená, že

  $$Q(u) = Q(v) = 0,$$

  $$Q(w) = 1,$$

  tento prípad odpovedá hyperbolickej rovine. Zvolíme bázu $\{u, v\}$ a $Q(x_1u+x_2v) = x_1x_2$. Typ tejto formy je teda +1.
- Žiadne nuly, to znamená, že

  $$Q(u) = Q(v) = Q(w) = 1,$$

  tento prípad odpovedá definitnej rovine. Zvolíme ľubovoľnú bázu a $Q(x_1u+x_2v) = x_1x_2 + x_1^2 + x_2^2$. Typ tejto formy je -1.

□

V prípade nedegenerovaných foriem na vektorových priestoroch párnej dimenzie nad telesom charakteristiky 2 môžu nastať dva prípady. Buď je kvadratická forma v $2n$ premenných ekvivalentná

$$x_1x_2 + x_3x_4 + \cdots + x_{2n-1}x_{2n} \text{ (hyperbolická rovina, typ +1)},$$

alebo je ekvivalentná

$$x_1x_2 + x_3x_4 + \cdots + x_{2n-1}^2 + x_{2n-1}x_{2n} + x_{2n}^2 \text{ (definitná rovina, typ -1)}.$$

Veta 1.42: *O počte núl*

Nech Q je kvadratická forma typu $\epsilon = \pm 1$ na vektorovom priestore V dimenzie $2n$ nad $\mathbb{Z}_2$. Potom existuje

$$2^{n-1}(2^n + \epsilon)$$

vektorov $v \in V$, že $Q(v) = 0$. □

Dôkaz:

Budeme postupovať indukciou podľa n. Pre prípad vektorového priestoru dimenzie 2 môžeme využiť príklad 1.41. Predpokladajme teda, že veta platí pre $n-1$. $V = U \oplus V'$, kde U je hyperbolická rovina a $\dim(V') = 2(n-1)$, takže Q má na priestore V' $2^{n-2}(2^{n-1} + \epsilon)$ núl. Pretože priestory U a V' sú navzájom ortogonálne, tak $Q(u+v) = Q(u) + Q(v)$, pre $u \in U$, $v \in V'$. Z tohto plynie, že

$$Q(u+v) = 0 \Leftrightarrow (Q(u) = Q(v) = 0 \vee Q(u) = Q(v) = 1).$$

Takže existuje

$$3 \cdot 2^{n-2}(2^{n-1} + \epsilon) + 1 \cdot 2^{n-2}(2^{n-1} + \epsilon) = 2^{n-1}(2^n + \epsilon)$$

núl, čím je dôkaz dokončený. □

1.9.2 Konštrukcia Kerdockových kódov

Stále sa pohybujeme nad telesom $\mathbb{Z}_2$ a vektorovým priestorom V nad ním párnej dimenzie $2n$.
Kerdockov kód $\mathcal{K}(n)$, kde $n \geq 2$, pozostáva z vhodne vybraných posunutých kópií kódu $\mathcal{R}(2n, 1)$. Platí teda, že Kerdockov kód leží medzi Reed-Mullerovým kódom rádu 1 a rádu 2:

$$\mathcal{R}(2n, 1) \subset \mathcal{K}(n) \subset \mathcal{R}(2n, 2).$$

Pretože $x^2 = x$, pre všetky $x \in \mathbb{Z}_2$, je každá lineárna funkcia na priestore V kvadratická, a vo všeobecnosti to znamená, že Reed-Mullerov kód rádu 2 sa skladá zo všetkých kvadratických foriem na priestore V, teda

$$R(n, 2) = \{Q + c : Q \text{ je kvadratická forma na priestore } V,\ c \in \mathbb{Z}_2\}.$$

Dve kvadratické formy, ku ktorým je asociovaná rovnaká bilineárna forma, sa líšia lineárnou formou. To znamená, že posunuté kopie kódu $\mathcal{R}(n, 1)$ v $\mathcal{R}(n, 2)$ korešpondujú s alternujúcimi bilineárnymi formami na priestore V.
Je zrejmé, že Kerdockov kód pozostáva z vybraných kvadratických foriem.
Z predchádzajúcej sekcie vieme, že kvadratické formy Q môžeme zapisovať podľa matice asociovanej bilineárnej formy f. Alternujúca bilineárna forma má maticu tvaru

$$M = \underbrace{\begin{pmatrix} 0 & x_1 & \cdots & x_{2n-1} \\ x_1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & y \\ x_{2n-1} & \cdots & y & 0 \end{pmatrix}}_{2n}.$$

Z toho jednoducho plynie, že alternujúca bilineárna forma f je nedegenerovaná práve vtedy, ak je determinant matice M nenulový. Pretože v matici vzhľadom k takejto forme f je na prvom riadku predpísaná nula, počet všetkých možných prvých riadkov je 2^{2n-1}. Vezmime si množinu všetkých možných takýchto matíc $\{M_1, \ldots, M_{2^{2n-1}}\}$ takú, aby súčet každých dvoch rôznych foriem, ktoré určujú, bol nedegenerovaný, čiže takú, že $\det(M_i + M_j) \neq 0$, $1 \leq i < j \leq 2^{2n-1}$. Táto množina se niekedy nazýva *Kerdockova množina*. Ak f_i je bilineárna alternujúca forma určená maticou M_i, tak máme

$$F_i = \{Q : \mathbb{F}_2^{2n} \to \mathbb{F}_2 |\ Q \text{ je kvadratická forma, } f_i \text{ je asociovaná s } Q\},$$

pre $i = 1, \ldots, 2^{2n-1}$. Označme zjednostenie všetkých týchto množín kvadratických foriem F. Kerdockov kód pozostáva zo všetkých kvadratických foriem a ich doplnkov z množiny F, teda

$$\mathcal{K}(n) = \{Q + c : Q \in F,\ c \in \mathbb{Z}_2\}.$$

Podmienka Kerdockovej množiny, že $\det(M_i + M_j) \neq 0$, je dobrá pre určenie minimálnej vzdialenosti Kerdockového kódu. Pri tom potrebujeme poznať počet núl a počet jedničiek od $Q_i - Q_j$:

- ak $i = j$, tak $Q_i - Q_j \in V^*$ je lineárna forma;
- ak $i \neq j$, tak s formou $Q_i - Q_j$ je asociovaná bilineárna forma, ktorá je určená maticou $M_i + M_j$. Z vety 1.42 o počte núl máme, že počet núl je rovný $2^{2n-1} \pm 2^{n-1}$.

Z vyššie uvedenej konštrukcie Kerdockových kódov vyplýva nasledujúca veta.

Veta 1.43: *Parametre Kerdockového kódu*

Kerdockov kód $\mathcal{K}(n)$ je $(2^{2n}, 2^{4m}, 2^{2n-1} - 2^{n-1})_2$-kód. □

Kerdockove kódy sú nelineárne kódy. V prípade, že $n = 2$, výsledkom Kerdockovej konštrukcie kódu je Nordstrom-Robinsonov kód s parametrami $(16, 256, 6)$.

1.10 $\mathbb{Z}_4$-lineárne kódy

Medzi najlepšie príklady nelineárnych binárnych samoopravných kódov, ktoré sú lepšie ako lineárne kódy, patria *Nordstrom-Robinsonove kódy*, *Preparata kódy* a *Kerdockove kódy* [8] [7] [6]. Existuje niekoľko spojení medzi Kerdockovými a Preparata kódmi a inými matematickými oblasťmi, ako napríklad projektívna geometria a teória grúp. Tým sa v tomto texte ale nebudeme zaoberať. Preparata a Kerdockove kódy sa správajú ako duálny pár binárnych lineárnych kódov. Vysvetlenie tohoto faktu spočíva v tom, že tieto kódy su duálne lineárne kódy nad $\mathbb{Z}_4$. Najmenší člen rodiny Preparata kódov bol skonštruovaný v roku 1967. Jeho rozšírenie je práve významný Nordstrom-Robinsonov kód.
Kerdockove a Preparata kódy existujú pre všetky dĺžky $n = 4^m \geq 16$. Pri dĺžke rovnej číslu 16 tieto kódy splývajú a výsledkom je Nordstrom-Robinsonov kód. Nordstrom-Robinsonov kód nad $\mathbb{Z}_4$ je takzvaný *oktakód*, čo je vlastne samoduálny kód nad $\mathbb{Z}_4$ dĺžky 8 [9].
Všetky tvrdenia, na ktoré sa budeme odkazovať v tejto časti textu, a všetky fakty a dodatky, ktoré nebudeme dokazovať, sa dajú nájsť v knihe o kvaterniárnych kódoch [17].

1.10.1 Konštrukcia Preparata kódov

Nech m je nepárne kladné celé číslo a nech $n = 2^m - 1$. Najprv popíšeme rozšírené Preparata kódy dĺžky $2n + 2 = 2^{m+1}$. Nech zobrazenie

$$x \mapsto x^\sigma$$

je automorfizmus $\mathbb{F}_2^m$, teda σ je mocnina čísla 2. Budeme požadovat (v zmysle predpokladov), aby obidve zobrazenia

$$x \mapsto x^{\sigma+1},$$
$$x \mapsto x^{\sigma-1},$$

boli surjektívne (teda $(\sigma \pm 1, 2^n - 1) = 1$). Pre odpovedajúce hodnoty σ definujeme rozšírené Preparata kódy $\overline{\mathcal{P}}_{m+1}(\sigma)$ a odstránením jednej zo súradníc (prepichnutím) získame Preparata kódy $\mathcal{P}_{m+1}(\sigma)$. Kódové slová rozšíreného Preparata kódu sú dvojice $(X, Y) \in \mathbb{F}_2^{m+1}$, kde $X \subset \mathbb{F}_2^m$, $Y \subset \mathbb{F}_2^m$. Je zrejmé, že pár (X, Y) interpretujeme ako $(0, 1)$-vektor dĺžky 2^{m+1}. Tieto kódové slová splňujú nasledujúce tri podmienky, čím definujú kódy $\overline{\mathcal{P}}_{m+1}(\sigma)$.

Definícia 1.44: *Rozšírené Preparata kódy*

Rozšírené Preparata kódy $\overline{\mathcal{P}}_{m+1}(\sigma)$ dĺžky 2^{m+1} sú zložené zo všetkých kódových slov tvaru $(X, Y) \in \mathbb{F}_2^{m+1}$, $X \subset \mathbb{F}_2^m$, $Y \subset \mathbb{F}_2^m$, splňujúcich:

1. X a Y majú párnu váhu, teda $w(X)$, $w(Y)$ sú párne čísla;
2. $\sum_{x \in X} x = \sum_{y \in Y} y$;
3. $\sum_{x \in X} x^{\sigma+1} + (\sum_{x \in X} x)^{\sigma+1} = \sum_{y \in Y} y^{\sigma+1}$.

□

Preparata kódy $\mathcal{P}_{m+1}(\sigma)$ získame z rozšírených Preparata kódov odstránením súradnice v X, ktorá korešponduje s nulovým prvkom v $\mathbb{F}_2^m$. To znamená, ak by sme predpokladali, že nulový prvok $\mathbb{F}_2^m$ korešponduje so súradnicou na prvej pozícii prvku X, tak by sme Preparata kódy získali prepichnutím rozšíreného Preparata kódu v tejto prvej pozícii.

Pri rozoberaní parametrov rozšírených Preparata kódov budeme vychádzať z nasledujúcich vecí. Označíme symetrický rozdiel dvoch množín X, Y, ako $X \triangle Y$, ktorý korešponduje so sčítaním kódových slov. Množinu $\{x + \alpha : x \in X\}$ budeme klasicky označovať $X + \alpha$. Budeme sa hlavne opierať o rovnosť

$$(a + b)^{\sigma+1} = a^{\sigma+1} + a^\sigma b + ab^\sigma + b^{\sigma+1}$$

a o vlastnosť *invariantnosti vzhľadom k vzdialensti* kódu. Vo všeobecnosti ak veľkosť množiny $\{y \in \mathcal{C} : d(x, y) = i\}$ záleží len na voľbe čísla i a nezáleží na voľbe slova $x \in \mathcal{C}$, tak kód $\mathcal{C}$ nazývame invariantný vzhľadom k vzdialenosti.

Veta 1.45:

Rozšírený Preparata kód $\overline{\mathcal{P}}_{m+1}(2)$ je invariantný vzhľadom k vzdialenosti. □

Dôkaz:

Budeme porovnávať kódové slovo (X_0, Y_0) kódu $\overline{\mathcal{P}}_{m+1}(2)$ so slovom $(0,0) = 0$. Nech $\alpha = \sum_{x \in X_0} x$. Zobrazenie

$$(X, Y) \mapsto (U, V),$$

kde $U = (X \triangle X_0) + \alpha$, $V = Y \triangle Y_0$, je surjektívne. Ukážeme, že platí: ak (X, Y) je kódové slovo, tak ním musí byť i (U, V), a naopak. Pre vlastnosti (1) a (2) z definície kódu 1.44 je to zrejmé. Musíme ešte overiť vlastnosť (3). Máme

$$\sum_{x \in U} x^3 + (\sum_{x \in U} x)^3 = \sum_{x \in X} (x + \alpha)^3 + \sum_{x \in X_0} (x + \alpha)^3 + (\sum_{x \in X} (x + \alpha))^3 =$$

$$= \sum_{x \in X} x^3 + \sum_{x \in X_0} x^3 + (\sum_{x \in X} x)^3 + \alpha^3 =$$

$$= \sum_{y \in Y} y^3 + \sum_{y \in Y_0} y^3 = \sum_{y \in V} y^3.$$

Z definície invariantnosti vzhľadom k vzdialenosti je už tvrdenie tejto vety zrejmé. □

Nasledujúce lemma uvedieme bez dôkazu. Čitateľ si ho môže dokázať sám na základe definície kódov $\overline{\mathcal{P}}_{m+1}(\sigma)$ a rovnosti $(a + b)^{\sigma+1} = a^{\sigma+1} + a^\sigma b + ab^\sigma + b^{\sigma+1}$.

Lemma 1.46: *Automorfizmy $\overline{\mathcal{P}}_{m+1}(\sigma)$*

Grupa automorfizmov $\mathrm{Aut}(\overline{\mathcal{P}}_{m+1}(\sigma))$ obsahuje nasledujúce permutácie:

1. $(X, Y) \mapsto (X + c, Y + c)$, kde $c \in \mathbb{F}_2^m$;
2. $(X, Y) \mapsto (Y, X)$;
3. $(X, Y) \mapsto (\alpha X, \alpha Y)$, kde $\alpha \in (\mathbb{F}_2^m)^*$;
4. $(X, Y) \mapsto (X^\varphi, Y^\varphi)$, kde $\varphi \in \mathrm{Aut}(\mathbb{F}_2^m)$.

□

Veta 1.47: *Minimálna vzdialenosť kódu $\overline{\mathcal{P}}_{m+1}(2)$*

Kód $\overline{\mathcal{P}}_{m+1}(2)$ má minimálnu vzdialenosť $\triangle(\overline{\mathcal{P}}_{m+1}(2)) = 6$. □

Dôkaz:

Podľa vety 1.45 nám stačí ukázať, že minimálna váha tohoto kódu je práve 6. Z definície kódu $\overline{\mathcal{P}}_{m+1}(2)$ je zrejmé, že neobsahuje kódové slová s váhou 2, pretože $w(X)$, $w(Y)$ sú párne čísla, pre nejaké kódové slovo (X, Y). Musíme teda ešte ukázať, že kód neobsahuje kódové slová s váhou 4. Rozlíšime dva prípady:

- Nech $(\{x_1, x_2\}, \{y_1, y_2\})$ je kódové slovo kódu $\overline{\mathcal{P}}_{m+1}(2)$. Podľa lemmy 1.46 môžeme predpokladať, že $x_1 = 0$. Potom z vlastnosti (3) z definície týchto kódov plynie, že
$$y_1^3 + y_2^3 = 0,$$
čo nám dáva spor, pretože $y_1 = y_2$.
- Podľa vety 1.45 a lemmy 1.46 nám ostala overiť možnosť kedy $w(X) = 4$ a $Y = 0$, kde $X = \{0, a, b, c\}$. Z vlastností (2) a (3) definície kódov $\overline{\mathcal{P}}_{m+1}(2)$ plynú rovnosti
$$a + b + c = 0,$$
$$a^3 + b^3 + c^3 = 0.$$
Použijeme rovnosť $(a + b)^{\sigma+1} = a^{\sigma+1} + a^\sigma b + ab^\sigma + b^{\sigma+1}$ a urobíme substitúciu prvej rovnice do druhej, z čoho dostaneme, že
$$ab(a + b) = 0,$$
a teda dostávame znova spor, pretože $a = b$.

Nakoniec ukážme, že v kóde $\overline{\mathcal{P}}_{m+1}(2)$ existujú kódové slová váhy 6. Nech máme navzájom rôzne a, b, c, a definujeme
$$y, y^3 = a^3 + b^3 + c^3,$$
$$x, x = a + b + c + y.$$
Potom $(\{0, x\}, \{a, b, c, y\})$ je kódové slovo s váhou 6, pričom vieme, že $x \neq 0$. □

Veta 1.48:

$|\overline{\mathcal{P}}_{m+1}(\sigma)| = 2^k$, kde $k = 2^{m+1} - 2m - 2$. □

Dôkaz:

Podľa definície 1.44 si môžeme v kódovom slove (X, Y) zvoliť prvok X 2^n rôznymi zpôsobmi. Budeme počítať, koľko existuje takých množín $Y \subset (\mathbb{F}_2^m)^*$, že (X, Y) splňuje podmienky definície kódového slova rozšíreného Preparata kódu. Nech ω je primitívny prvok $\mathbb{F}_2^m$ a nech $m_i(x)$ je minimálnyy polynóm ω^i. Z definície rozšíreného Preparata kódu máme $2m$ lineárnych rovníc nad telesom $\mathbb{F}_2$ (uvedomme si, že sa pohybujeme v m-dimenzionálnom priestore nad telesom $\mathbb{F}_2$) a tieto rovnice sú nezávislé, pretože čísla $(\sigma + 1)$ a n sú nesúdeliteľné a teda $m_{\sigma+1}(x)$ je polynóm stupňa m. Z toho vyplýva, že pre každú voľbu prvku X z dvojice (X, Y) majú rovnice
$$\sum_{x \in X} x = \sum_{y \in Y} y$$
a
$$\sum_{x \in X} x^{\sigma+1} + (\sum_{x \in X} x)^{\sigma+1} = \sum_{y \in Y} y^{\sigma+1}$$
2^{n-2m} riešení $Y \subset (\mathbb{F}_2^m)^*$. Tým sme dokázali tvrdenie vety. □

Rozšírené Preparata kódy $\overline{\mathcal{P}}_{m+1}(\sigma)$ sú teda

$$\left(2^{m+1}, 2^k, 6\right) - \text{kódy},$$

kde $k = 2^{m+1} - 2m - 2$. V prípade $m = 3$ získame práve Nordstrom-Robinsonov kód. Preparata kódy $\mathcal{P}_{m+1}(\sigma)$ sú potom

$$\left(2^{m+1} - 1, 2^k, 5\right) - \text{kódy},$$

kde $k = 2^{m+1} - 2m - 2$.

Preparata kódy sú v skutočnosti obsiahnuté v rozšírených Hammingových kódoch. Položme $C_0 = \overline{\mathcal{P}}_{m+1}(\sigma)$ a nech C_α je kód, ktorý získame pričítaním slova $(\{0, \alpha\}, \{0, \alpha\})$ ku kódovým slovám kódu $\overline{\mathcal{P}}_{m+1}(\sigma)$, $\alpha \in (\mathbb{F}_2^m)^*$. Pomocou rovnakej techniky, ako sme použili pre dokazovanie parametrov rozšíreného Preparata kódu, sa dá ukázať nasledujúce:

- každý kód C_α má minimálnu vzdialenosť rovnú 4;
- kódy C_α sú po dvoch disjunktné;
- kód $\overline{Ham}_{m+1}(2) = \bigcup_{\alpha \in \mathbb{F}_2^m} C_\alpha$ je lineárny;
- $\overline{Ham}_{m+1}(2)$ je rozšírený Hammingov kód redundancie $(m + 1)$.

Na tomto mieste si pripomeňme dôsledok na konci sekcie o Reed-Mullerových kódoch, ktorý dáva do súvislosti kódy $\mathcal{R}(n, n-2)$ s kódmi $\overline{Ham}_n(2)$. Z tohto je zrejmá istá súvislosť medzi Reed-Mullerovými kódmi a Preparata kódmi.

1.10.2 Kvaterniárne kódy

Definícia 1.49: *Kvaterniárny kód*

> Kvaterniárnym kódom $\mathcal{C}$ dĺžky n budeme rozumieť lineárny kód nad $\mathbb{Z}_4$, teda nejakú aditívnu podgrupu $\mathbb{Z}_4^n$. □

Kvaterniárne kódy sa v poslednej doby študovali kvôli súvislosti s binárnymi obrazmi kódov, ktorými sa budeme neskôr v tejto práci zaoberať. Duálny a samoduálny kód sú definováne rovnako ako u lineárnych kódov. V tomto prípade sa definuje *vnútroný súčin* dvoch prvkov $a, b \in \mathbb{Z}_4^n$ ako

$$a \cdot b = a_1 b_1 + \ldots a_n b_n (\text{mod } 4).$$

Ak

$$a \cdot b = 0,$$

tak hovoríme, že x a y sú *ortogonálne*. Kvaterniárne kódy sú v skutočnosti $\mathbb{Z}_4$-moduly. Cyklické kódy nad $\mathbb{Z}_4$ sú definované rovnako ako v prípade kódov nad telesom.

1.10.3 Oktakód

Oktakód $\mathcal{O}_8$ môže byť, rovnako ako väčšina kódov, definovaný viacerými spôsobmi, my si ukážem jeden z nich.

Nech máme cyklický kód nad $\mathbb{Z}_4$ dĺžky 7 s generujúcim polynómom $g(x) = 3+2x+3x^2+x^3$. Pridaním paritného bitu na koniec každého vektoru získame oktakód $\mathcal{O}_8$ ktorý môže byť považovaný za Hammingov kód nad $\mathbb{Z}_4$. Generujúca matica oktakódu má tvar

$$\begin{pmatrix} 3 & 3 & 2 & 3 & 1 & 0 & 0 & 0 \\ 3 & 0 & 3 & 2 & 3 & 1 & 0 & 0 \\ 3 & 0 & 0 & 3 & 2 & 3 & 1 & 0 \\ 3 & 0 & 0 & 0 & 3 & 2 & 3 & 1 \end{pmatrix},$$

alebo ekvivalentne

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 1 & 3 & 1 & 1 \\ 2 & 0 & 1 & 1 & 2 & 2 & 3 & 1 \\ 0 & 1 & 0 & 1 & 2 & 3 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

1.10.4 Binárne kódy asociované s kvartérniárnymi kódmi

V komunikačných systémoch sa veľmi často používá zobrazenie, ktoré dvom informačným bitom priradí dvojicu bitov. Formálne sa definujú tri zobrazenia α, β, γ zo $\mathbb{Z}_4$ do $\mathbb{Z}_2$ nasledujúcim spôsobom:

c	$\alpha(c)$	$\beta(c)$	$\gamma(c)$
0	0	0	0
1	1	0	1
2	0	1	1
3	1	1	0

Zrejmým spôsobom sa tieto zobrazenia dajú rozšíriť na zobrazenia zo $\mathbb{Z}_4^n$ do $\mathbb{Z}_2^n$.
Binárne kódy sa konštruujú z kvartérniárnych kódov pomocou *Grayovej mapy*, čo je zobrazenie $\phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ dané vzťahom

$$\phi(c) = (\beta(c), \gamma(c)),\ c \in \mathbb{Z}_4^n.$$

V jednoduchom prípade zobrazuje Grayova mapa štyri prvky množiny $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ na dvojice bitov takto:

$$0 \to 00,\ 1 \to 01,\ 2 \to 11,\ 3 \to 10.$$

Ako neskôr uvidíme, toto zobrazenie bude jediným nelineárnym krokom pri konštrukcií Preparata a Kerdockových kódov. V prípade Grayovej mapy hovoríme o *binárnom obraze* $\phi(C)$ kódu C.
Budeme hovoriť, že *binárny kód C je $\mathbb{Z}_4$-lineárny*, ak sa súradnice v jeho generujúcej matici dajú preusporiadať tak, že výsledok je obraz Grayovej mapy ϕ kvarterného kódu. Predtým, než si ukážeme zásadnú vlastnosť Grayovej mapy, musíme si vysvetliť a pripomenúť pojmy Leeova vzdialenosť a izometria.

Definícia 1.50: *Leeova vzdialenosť*

Nech $x = (x_1, \ldots, x_n)$ a $y = (y_1, \ldots, y_n)$ sú dva reťazce rovnakej dĺžky n nad q-árnou abecedou, kde $q \geq 2$. *Leeova vzdialenosť* je definovaná ako

$$d_L(x, y) = \sum_{i=1}^{n} \min\{|x_i - y_i|, q - |x_i - y_i|\}.$$

Ak budeme hovoriť o Leeovej váhe nejakého reťazca, budeme tým myslieť $d_L(x, 0)$ a označovať ako $w_L(x)$. □

Z definície Leeovej vzdialenosti je zrejmé, že sa takisto ako u Hammingovej vzdialenosti jedná o metriku. Dokonca v prípade $q = 2$ alebo $q = 3$ je Leeova vzdialenosť totožná s Hammingovou vzdialenosťou. *Izometria* je izomorfizmus medzi dvoma metrickými priestormi, ktorý zachováva vzdialenosti.

Veta 1.51:

Grayova mapa ϕ je zobrazenie zachovávajúce vzdialenosti, teda izometria medzi metrickými priestormi

$$(\mathbb{Z}_4^n, \text{ Leeova vzdialenosť}) \text{ a } (\mathbb{Z}_2^{2n}, \text{ Hammingova vzdialenosť}).$$

□

Dôkaz:

Z definície Grayovej mapy a Leeovej vzdialenosti je jednoduché vidieť, že

$$w(\phi(a)) = w_L(a), \ a \in \mathbb{Z}_4^n,$$

$$d(\phi(a), \phi(b)) = d_L(a, b), \ a, b \in \mathbb{Z}_4^n.$$

□

1.10.5 Galoisove okruhy

Pri štúdiu cyklických kódov dĺžky n nad abecedou dĺžky q sa obvykle pracuje v telese $\mathbb{F}_{q^m}$. Toto teleso je rozšírením stupňa m telesa $\mathbb{F}_q$, ktoré je stotožňované s abecedou. Rozšírenie je volené tak, že obsahuje n-té odmocniny z jednej. Podobný prístup je aplikovateľný na cyklické kódy dĺžky n nad $\mathbb{Z}_4$. V tomto prípade konštruujeme takzvaný *Galoisov okruh* $GR(4^m)$, ktorý je rozšírením $\mathbb{Z}_4$ stupňa m obsahujúci n-té odmocniny z jednej.
Ďalej uvedieme niektoré základné vlastnosti a fakty o Galoisových okruhoch, ktoré budeme neskôr potrebovať. Ak má čitateľ záujem dozvedieť sa viac, môže tak učiniť v [10], [11], [12].

Nech $h_2(x) \in \mathbb{Z}_2[x]$ je primitívny irreducibilný polynóm stupňa m. Potom existuje jednoznačný monický polynóm $h(x) \in \mathbb{Z}_4[x]$ stupňa m taký, že

$$h(x) \equiv h_2(x) (\text{mod } 2)$$

a

$$h(x) \mid x^n - 1 (\text{mod } 4),$$

kde $n = 2^m - 1$ [13]. Polynóm $h(x)$ sa nazýva *základný primitívny ireducibilný polynóm.* Nasledujúca Graeffeova matóda ([14]) je jedna z metód, pomocou ktorej môžeme polynóm $h(x)$ hľadať. Nech $h_2(x) = e(x) - d(x)$, kde $e(x)$ označuje polynóm obsahujúci len párne mocniny s koeficientmi polynómu $h_2(x)$ a $d(x)$ označuje polynóm obsahujúci nepárne mocniny s koeficientmi polynómu $h(x)$. Potom polynóm $h(x)$ je daný pomocou

$$h(x^2) = \pm(e^2(x) - d^2(x)).$$

Nech ξ je taký koreň polynómu $h(x)$, že $\xi^n = 1$. Potom je Galoisov okruh $GR(4^m)$ definovaný ako $R = \mathbb{Z}_4[\xi]$. Existujú v podstate dva spôsoby ako reprezentovať 4^m prvkov R (aditívna a multiplikatívna reprezentácia [17]):

1. Každý prvok $c \in R$ má jednoznačnú 2-adickú reprezentáciu

   $$c = a + 2b,$$

   kde $a, b \in T = \{0, 1, \xi, \xi^2, \ldots, \xi^{n-1}\}$. Zobrazenie $\tau : c \mapsto a$ je dané ako

   $$\tau(c) = c^{2^m},$$

   kde $c \in R$ a zároveň splňuje

   $$\tau(cd) = \tau(c)\tau(d),$$
   $$\tau(c + d) = \tau(c) + \tau(d) + 2(cd)^{2^{m-1}}.$$

   Teda zo znalosti c môžeme určit a a b ([13]).

2. Každý prvok $c \in R$ má jednoznačnú reprezentáciu

   $$c = \sum_{i=0}^{m-1} b_i \xi^i,$$

   kde $b_i \in \mathbb{Z}_4$.

1.10.6 Cyklické kódy nad $\mathbb{Z}_4$

K porozumeniu cyklických kódov nad $\mathbb{Z}_4$ je potrebné poznať štruktúru okruhu $\mathbb{Z}_4[x]/(x^n - 1)$. Ako už vieme, keď pracujeme s cyklickými kódmi dĺžky n, reprezentujeme kódové slová pomocou polynómov modulo $(x^n - 1)$. Kódové slovo $v = (v_0, \ldots, v_{n-1})$ reprezentujeme ako polynóm

$$v(x) = \sum_{i=0}^{n-1} v_i x_i$$

nad okruhom $\mathbb{Z}_4[x]/(x^n - 1)$. S prácou v tomto okruhu musíme byť opatrný, pretože to nie je Gaussov obor, teda rozklady na irreducibilné faktory nie sú jednoznačné.
Taktiež si môžeme všimnúť, že každý prvok tvaru $1 + 2\lambda$, $\lambda \in \mathbb{Z}_4[x]/(x^n - 1)$, je koreň polynómu $x^2 - 1$. Na druhej strane tento okruh je obor integrity hlavných ideálov [16].

1.10.7 Súvislosť s Kerdockovými a Preparata kódmi

Veta 1.52:

Nech

- $h(x)$ je základný primitívny irreducibilný polynóm stupňa m,
- $g(x)$ je recipročný polynóm k polynómu $\frac{x^n-1}{(x-1)h(x)}$, kde $n = 2^m - 1$,
- $\mathcal{K}^-$ je cyklický kód nad $\mathbb{Z}_4$ dĺžky n s generujúcim polynómom $g(x)$,
- $\mathcal{K}$ vznikne z $\mathcal{K}^-$ pripojením paritných bitov na koniec.

Potom pre nepárne $m \geq 3$ je binárny obraz Grayového zobrazenia $K = \phi(\mathcal{K})$ nelineárny

$$(2^{m+1}, 4^{m+1}, 2^m - 2^{\frac{m-1}{2}})_2 - \text{kód},$$

ktorý je ekvivalentný Kerdockovému kódu. Kód K je invariantný vzhľadom k Hammingovej vzdialenosti. □

Veta 1.53:

Nordstrom-Robinsonov kód je binárnym obrazom Grayového zobrazenia oktakódu. □

Veta 1.54:

Nech

- $h(x)$ je základný primitívny irreducibilný polynóm stupňa m,
- $g(x)$ je recipročný polynóm k polynómu $\frac{x^n-1}{(x-1)h(x)}$, kde $n = 2^m - 1$,
- $\mathcal{P}^-$ je cyklický kód nad $\mathbb{Z}_4$ dĺžky n s generujúcim polynómom $h(x)$,
- $\mathcal{P}$ vznikne z $\mathcal{P}^-$ pripojením paritných bitov na koniec, takže $\mathcal{P} = \mathcal{K}^{\perp}$.

Potom pre nepárne $m \geq 3$ je binárny obraz Grayového zobrazenia $P = \phi(\mathcal{P})$ nelineárny

$$(2^{m+1}, 2^{2^{m+1}-2m-2}, 6)_2 - \text{kód}.$$

Kód P je invariantný vzhľadom k Hammingovej vzdialenosti a jeho váhový polynóm je MacWilliamsovej transformácia váhového polynómu Kerdockového kódu rovnakej dĺžky. □

1.11 Krycie kódy

Predstavme si, že by sme chceli mať malú množinu binárnych vektorov dĺžky n s vlastnosťou, že žiadny z týchto vektorov sa nelíši od druhého vo viac než ρ súradniciach. Toto je základný požiadavok takzvaných krycích kódov. Dôležitým pojmom je *krycí polomer*, ktorý je v istom zmysle "duálnym" pojmom k minimálnej vzdialenosti.

Definícia 1.55: *Krycí polomer*

Nech C je kód dĺžky n nad abecedou Σ. Krycí polomer kódu C je najmenšie číslo r také, že sféry o polomere r okolo kódových slov kódu C pokrývajú celý priestor Σ^n. □

Vidíme, že platí $\Sigma^n = \bigcup_{x \in C} S_r(x)$, kde $S_r(x)$ označuje príslušnú sféru kódového slova x. Pre binárny prípad je teda krycí polomer kódu C definovaný ako

$$r = \max\{\min\{|x + c|;\ c \in C\};\ x \in \mathbb{Z}_2^n\}.$$

Definícia 1.56: *Krycí kód*

Kód $C \subset \mathbb{F}_q^n$ sa nazýva q-árny ρ-krycí kód dĺžky n, ak pre každé slovo $y \in \mathbb{F}_q^n$ existuje kódove slovo $x \in C$ také, že pre Hammingovu vzdialenosť platí $d(x, y) \leq \rho$. Ekvivalentne, kód C má krycí polomer najviac ρ. □

Inak povedané, sféry $S_\rho(x)$ okolo kódových slov $x \in C$ pokrývajú celý priestor $\mathbb{F}_q^n$. Z toho tiež vznikol názov pre tieto kódy. Pri samoopravných kódoch nás väčšinou zaujíma hlavne minimálna vzdialenosť kódu, zatiaľ čo pri krycích kódoch je krycí polomer hlavným predmetom záujmu. Minimálna vzdialenosť kódu berie do úvahy len vzdialenosti medzi kódovými slovami. Krycí polomer je na rozdiel od toho definovaný na celom priestore. Všimnime si, že každý perfektný kód je krycí kód minimálnej veľkosti.

Príklad 1.57:

Množina

$$C = \{0134, 0223, 1402, 1431, 1444, 2123, 2234, 3002, 3310, 4010, 4341\}$$

je 5-árny 2-krycí kód dĺžky 4. □

Kapitola 2

Steganografia a teória kódov

2.1 Základy steganografie

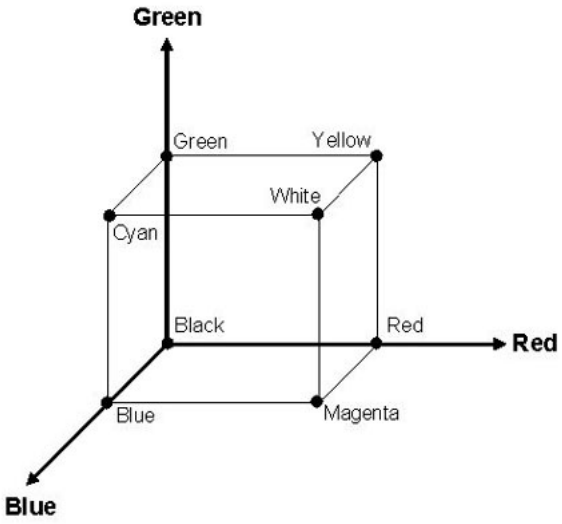
V úvode tejto kapitoly sa oboznámime so základmi modernej steganografie. Viac informácii o steganografii môže čitateľ nájsť v úvode do steganografie a steganoanalýzy [2].
Steganografia je "umenie" ako ukryť alebo zakryť správu. Účel steganografie je kamuflovať (podviesť) komunikáciu - utajiť existenciu správy pre tretiu stranu. Tým sa líši od kryptografie. Niektorí autori však považujú steganografiu ako formu kryptografie odkedy je utajená komunikácia považovaná za tajné informácie [3].
Steganografia ukrýva nejakú správu, ale nie fakt, že medzi oboma partiami prebieha komunikácia. Steganografický proces všeobecne zahŕňa vloženie utajovanej správy na transportné médium nazývané nosič. Tajná správa je vložená (zabudovaná) do nosiča a vytvára takzvané steganografické médium. Steganografický kľúč môže byť použitý pre kódovanie skrývanej správy a/alebo pre vygenerovanie náhodnej steganografickej schémy. V skutočnosti:

steganografické médium = ukrývaná správa + nosič + steganografický kľúč.

Zväčšovaním množstva dát ukladaného na počítač a posielaním jeho obsahu po sieti nie je prekvapujúce, že steganografia vstupuje do digitálneho veku. Steganografia na počítači a na sieti umožnuje ukrývať nejaký typ binárnych súborov do iného binárneho súboru. Obrázok a audio súbor sú dnes najviac používané nosiče.
Vzhľadom k tomu, že používané steganografické metódy na rôznych digitálnych nosičoch pracujú na prakticky rovnakom princípe, obmedzíme sa v tejto práci pre zjednodušenie na základný model digitálneho obrázku.

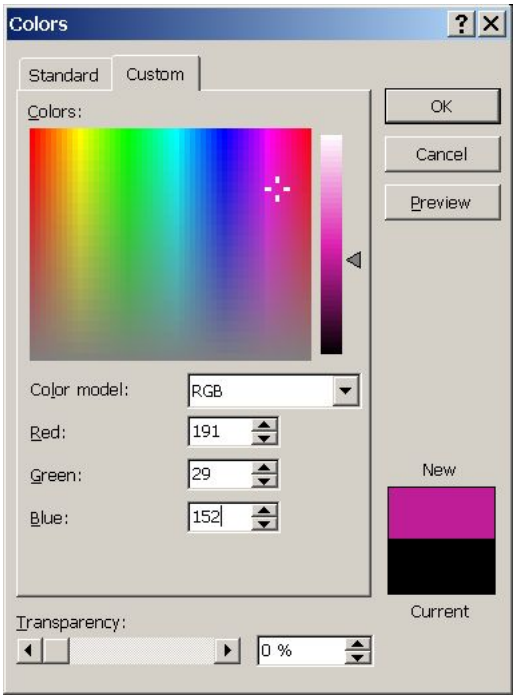
2.1.1 Základný model digitálnych dat

Mnoho súčasných digitálnych steganografických techník využíva grafické obrázky ako nosič média. Je poučné sa pozrieť ako funguje kódovanie obrázkov a audio súborov predtým, než budeme hovoriť o spôsoboch práce steganografie a steganoanalýzy s týmito nosičmi. Obrázok 2.1 znázorňuje rozloženie *RGB* farieb, kde každú farbu reprezentuje nejaká intenzita z každej farebnej komponenty - červená (red), zelená (green), modrá (blue). Absencia všetkých farieb dáva farbu čiernu, znázornen ako prienik všetkých farieb v nule. Mix 100 percent z každej farby dáva farbu bielu. Ostatné farby získame podobne.



Obr. 2.1: Schéma RGB.

Obrázok 2.2 ukazuje intenzitu RGB pri nejakej náhodnej farbe. Každá komponenta je určená jedným bajtom, takže hodnoty pre každú farbu sú v škále od 0 do 255. Na obrázku je konkrétny odtieň (fialová farba) označený takto: červený stupeň 191 (hex BF), zelený stupeň 29 (hex $1D$), modrý stupeň 152 (hex 92). Teda fialová farba by bola kódovaná 24 bitmi ako $0xBF1D98$. Táto 24-bitová kódovacia schéma podporuje $16,777,216$ (2^{24}) unikátnych farieb.
Dnes už väčšina aplikácií, ktoré pracujú s digitálnymi obrázkami podporuje 24-bitové farby (24-bit true color), kde každý element obrázka (pixel) je kódovaný do 24 bitov zahrňujúcich tri RGB bajty, ako sme si ukázali vyššie. Ostatné aplikácie používajú kódovanie farieb do 8 bitov na každý pixel. Tieto schémy takisto používajú 24-bitové farby, ale pri tom využívajú paletu, ktorá označuje aké farby sú používané v obrázku. Každý pixel je kódovaný v 8 bitoch, kde hodnota ukazuje na hodnotu v 24 bitoch na palete. Z tohto dôvodu táto metóda podporuje len 256 (2^8) farieb. Voľba kódovania farieb má prirodzene vplyv na veľkosť obrázka (nie rozmer ale data uložené na disku). 640 x 480 pixelový obrázok, ktorý používa 8-bitové farby môže zaberať približne 307 KB (640 x 480 = $307,200$ bajtov), zatiaľ čo 1400 x 1050 pixelový obrázok používajúci 24-bitové farby potrebuje 4.4 MB (1400 x 1050 x 3 = $4,410,000$ bajtov).
V tomto texte sa obmedzíme na modely s kódovaním farieb do 8 bitoch na každý pixel. Tieto modely sú tiež známe ako *modely so šedou paletou*.
Samozrejme existujú aj ďalšie modely, ktoré sú založené na zložitejších princípoch, ako je napríklad diskrétna kosínová transformácia. Takéto modely už však nereprezentujú autentické digitálne obrázky, zachycujúce presný obraz, ale pomocou transformácií tieto data kompresujú, čím sa "kvalita" obrázku znižuje. Digitálne obrázky založené na prvom modele, a ktorými sa budeme zaoberať, sa obvykle nazývajú *bezstrátové*, obrázky založené na druhom modele sa nazývajú *strátové*.



Obr. 2.2: Ukážka RGB stupňov vo vybranej farbe.

2.1.2 Princíp steganografie na digitálnych nosičoch

Existuje veľa spôsobov, ako môže byť správa v digitálnom médiu utajená. My sa však budeme zaoberať len základným z nich. Najviac používaná steganografická metóda v obrázkových súboroch zahrňuje niektoré typy substitúcie najmenej významných bitov. Termín menej významný bit (least significant bit, LSB) pochádza z číselného významu bitov v bajte. Bit vysokého rádu alebo najviac významný bit je ten jeden s najväčšou aritmetickou hodnotou (napríklad $27 = 128$), zatiaľ čo bit nízkeho rádu alebo najmenej významný bit je ten jeden s najnižšou aritmetickou hodnotou (napríklad $20 = 1$).
Ako jednoduchý príklad substitúcie najmenej významného bitu si predstavte "ukrytie" písmena "G" do nasledujúcich 8 bitov nosiča súboru (najmenej významný bit je zvýraznený):

1001010*1* 0000110*1* 1100100*1* 1001011*0*
0000111*1* 1100101*1* 1001111*1* 0001000*0*

'G' je reprezentované v $ASCII$ (American Standard Code for Information Interchange) kóde ako binárny reťazec 01000111. Týchto 8 bitov môžeme vložiť do najmenej významného bitu z každého z 8 bajtov nosiča nasledovne:

1001010*0* 0000110*1* 1100100*0* 1001011*0*
0000111*0* 1100101*1* 1001111*1* 0001000*1*

Všimnime si, že v tejto ukážke bola v skutočnosti len polovica najmenej významných bitov zmenená.
Táto jednoduchá substitúcia predstavuje bežnú techniku steganografie.

Všeobecný postup si teraz popíšeme detailnejšie. Každý digitálny text pozostáva z postupnosti jednotlivých znakov, ktoré môžeme jednoducho reprezentovať pomocou jedného bajtu ($ASCII$ kód).

Tabuľka 2.1: Príklad bitovej reprezentácie znakov.

časť textu:	H	i		a	l	l
ASCII kód:	72	105	32	97	108	108
binárny kód:	01001000	01101010	00100000	01100001	01101100	01101100

Tabuľka 2.2: Binárny operátor AND.

A	B	$A\ AND\ B$
0	0	0
0	1	0
1	0	0
1	1	1

Máme teda dva bitové toky. Jeden tok reprezentuje dáta v obrázku a druhý reprezentuje našu ukrývanú informáciu. Nemusí to byť len text, môže to byť čokoľvek, čo sa dá reprezentovať binárnym kódom (napríklad iný obraz).
Na vkladanie informácie použijeme metódu LSB. Jedná sa o veľmi jednoduchý algoritmus, ktorý nahradzuje najmenej významné bity v dátovom toku obrazu bitmi utajovanej správy. Vo všeobecnom prípade to nemusí byť len najmenej významný bit, ale môžu to byť napríklad aj posledné dva najmenej významné bity apod.
Na každý bajt z dátovej časti obrazu aplikujeme tzv. **masku** 254 (11111110). Ak máme 'H', teda '01001001' a aplikujeme na to našu masku 11111110, jednoducho "zmažeme" jedničku na konci binárneho kódu písmena 'H'. To znamená, že sa aplikuje bitový operátor AND.
Nasledujúci algoritmus ukazuje, ako prebieha vkladanie informácie do obrazu vo formáte BMP:

1. "Hi" → binárny kód **010**01001 01101001
2. časť dátovej časti BMP súbora

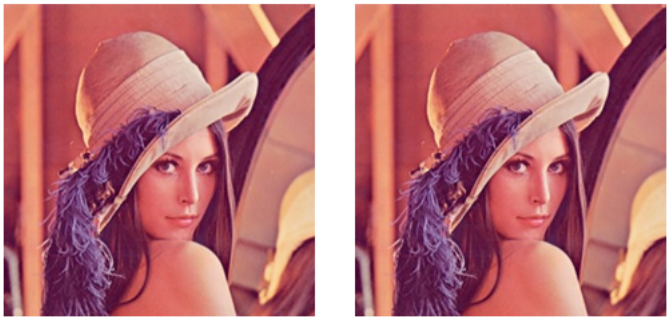
   11000100 10011001 10011100

   aplikujeme masku 254 (1111 1110)

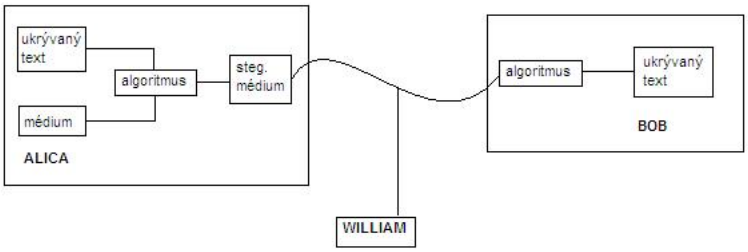
   11000100 10011000 10011100

   substituujeme najmenej významne bity našou správou

   *010*01001 01101001
3. Po aplikovaní substitúcie dostaneme výsledok



Obr. 2.3: Príklad originálneho BMP (naľavo) a steganografického BMP (napravo).



Obr. 2.4: Názorný priebeh komunikácie medzi Alicou a Bobom.

$$1100010\mathit{0}\ 1001100\mathit{1}\ 1001110\mathit{0}.$$

Samozrejme, že do obrazu nemôžeme vkladať nekonečné množstvo bitov. Každý obraz má svoje obmedzenie na dĺžku vkladanej informácie, dané počtom farebných kanálov a hĺbkou farieb.

2.2 Steganoanalýza

V spomínanej bakalárskej práci [2] je vysvetlený model, na ktorom sa zvykne vysvetľovať princíp steganografie a steganoanalýzy, nazývaný *problém väzňa*.
Problém sa týka dvoch väzňov, Alicie a Boba, ktorí sú zatvorení v oddelených celách a chcú sa dohodnúť na nejakom tajnom pláne. Alica a Bob majú povolené vymieňať si správy medzi sebou, ale strážnik William si ich môže všetky prečítať. Alica a Bob vedia, že ak William odhalí ich tajný komunikačný kanál, tak už nebudú môcť spolu komunikovať. William môže zaujať pasívny, alebo aktívny postoj. V pasívnom postoji William preskúma správu a rozhodne sa, či správu posunie ďalej alebo nie. V aktívnom postoji môže William zmeniť správu. Zlomyseľný strážnik by teda mohol meniť každú správu, aby predišiel tajnému kanálu, takže Alica a Bob musia použiť veľmi silnú steganografickú metódu.
To, ako bude strážnik reagovať, závisí od zložitosti steganografického algoritmu a od Williamových vedomostí. Na základe tohoto modelu sa steganoanalýza rozdeľuje podobne ako kryptoanalýza podľa toho, koľko informácií má steganoanalytik k dispozícii. Spomeňme niektoré najviac používané štatistické analýzy obrázkov, ktoré sa používajú v steganoanalýze. Podrobnejšie informácie môžeme nájsť v [2].

2.2.1 Analýza histogramu

Pomocou analýzy histogramov môžeme skúmať rozdiely medzi dvoma digitálnymi nosičmi.

Definícia 2.1: *Histogram*

> Histogram digitálneho obrazu so šedou paletou v rozsahu $[0, L-1]$ je diskrétna funkcia $p(r_k) = \frac{n_k}{n}$, kde r_k je k-ty stupeň šedej farby, n_k je počet pixelov s touto farbou, n je celkový počet pixelov, a $k = 0, 1, 2, \ldots, L-1$. □

Funkcia $p(r_k)$ nám dáva pravdepodobnosť výskytu farby r_k. Graf tejto funkcie pre všetky rôzne k poskytuje globálny popis obrazu. Na základe tohoto popisu môžeme definovať akúsi "stopu", ktorú po sebe zanechá steganografický algoritmus. Táto stopa potom môže byť použitá na detekciu steganografie v digitálnom nosiči.

2.2.2 Párová analýza (Raw Quick Pair Analysis)

Veľký počet steganografických metód pre bezstrátové obrázky používa manipuláciu LSB. Teda najmenej významné bity sú zmenené na dosiahnutie požadovaného výsledku. Táto metóda je populárna, pretože v skutočnosti sa zmení len približne polovica najmenej významných bitov v obrázku. LSB manipulácia tým pádom po sebe nezanechá značné stopy.
Vytvoríme test na detekciu výskytu vloženej správy v digitálnych nosičoch s 24-bitovou kódovaciou schémou RGB. Hodnota každého pixelu je v tejto schéme reprezentovaná hodnotami R, G, B, a každá z týchto hodnôt je reprezentovaná jedným bajtom. Nech počet unikátnych farieb je U. Počtom unikátnych farieb myslíme počet všetkých možných farieb v konkrétnej kódovacej schéme, v tomto prípade v schéme RGB.

Definícia 2.2: *Farebný skoro pár*

> Povieme, že dve farby (R_1, G_1, B_1) a (R_2, G_2, B_2) formujú skoro pár ak $|R_1 - R_2| \leq 1$, $|G_1 - G_2| \leq 1$, $|B_1 - B_2| \leq 1$. Ekvivalentne $(R_1 - R_2)^2 + (G_1 - G_2)^2 + (B_1 - B_2)^2 \leq 3$. □

Počet všetkých farebných párov je:

$$\binom{U}{2} \geq P,$$

kde P je počet skoro párov.
Uvažme pomer R medzi skoro pármi a všetkými pármi:

$$R = \left(\frac{P}{\binom{U}{2}} \right).$$

Pomer R nám dáva relatívny počet skoro párov v digitálnom obrázku.
Popíšeme algoritmus na detekciu steganografie:

- Ako vstup máme nejaký digitálny obrázok.

- Na začiatku potrebujeme vypočítať počet unikátnych farieb a počet skoro párov v nich. Potom vypočítame pomer R.
- Náhodne vyberieme pixely a vykonáme substitúciu LSB našej zvolenej testovacej správy do nosiča.
- Po získaní stego-obrázku vypočítame počet unikátnych farieb a počet skoro párov v ňom. Vypočítame z týchto hodnôt ich pomer. Označme tento počet unikátnych farieb U' a tento pomer R'.

Zaujímavé je pozorovanie správania sa obrázkov vzhľadom k tomuto testu. Ak obraz už v sebe obsahoval nejakú informáciu, tak potom nezistíme markantnú zmenu v porovnaní pomerov, ktoré získame pred a po vložení ďalšej správy. Vidíme, že $R \equiv R'$. Ak obraz neobsahoval informáciu, potom sa budú pomery významne líšiť, teda $R' > R$.
Z pozorovania musíme určiť hranicu Th, pomocou ktorej budeme s určitou pravdepodobnosťou rozlišovať obrazy ako obyčajné alebo ako modifikované steganografickým algoritmom. Potrebujeme minimalizovať dva druhy chýb: že detekujeme správu, kde nemá byť, a naopak. Hranica môže byť vypočítana použitím vzorca:

$$Th = \frac{\mu\sigma(s) + \mu(s)\sigma}{\sigma + \sigma(s)},$$

kde μ, σ sú priemerná a štandardná odchýlka pomeru R'/R pre nejakú databázu obyčajných obrazov. $\mu(s)$, $\sigma(s)$ sú priemerná a štandardná odchýlka pomeru R'/R pre nejakú databázu steganografických obrázkov.
Obrázok, ktorý bude mať pomer pod touto hranicou, tak je s veľkou pravdepodobnosťou steganografický. Ak je pomer nad hranicou, potom to s veľkou pravdepodobnosťou dokazuje, že v sebe nemá žiadnu ukrytú informáciu. Otázkou zostáva, či tento algoritmus spoľahlivo funguje pre rôzne dĺžky správ.

2.2.3 PoVs a Chi-kvadrát útok

Definícia 2.3: *Frekvencia farby*

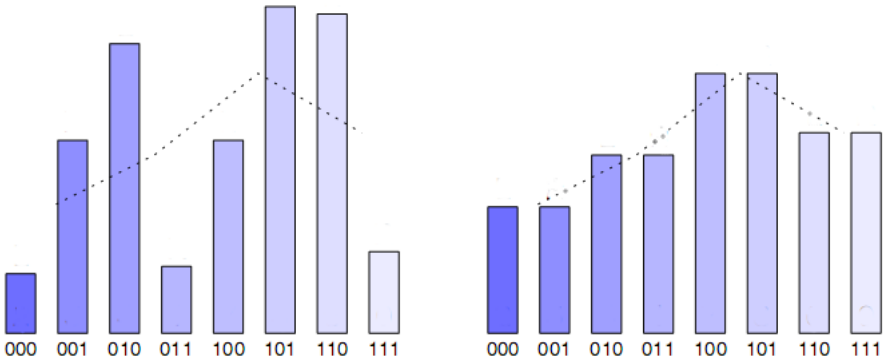
> Frekvenciou farby r_k rozumieme počet všetkých pixelov v obrázku s touto hodnotou. □

Histogram nám teda ukazuje všetky frekvencie farieb vyskytujúcich sa v obrázku.

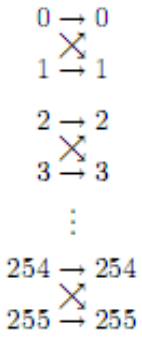
Definícia 2.4: *Distribúcia*

> Distribúciou budeme nazývať rozloženie frekvencií v poradí za sebou pri konkrétnom obrázku. Distribúcia má zjavnú súvisloť s histogramom. □

Prepisovanie LSB transformuje hodnoty na hodnoty, ktoré sa líšia len v LSB. Tieto párové hodnoty sa nazývajú PoV (pairs of values). Ak bity, použité na prepísanie LSB, sú rovnomerne rozložené, frekvencie obidvoch hodnôt každej PoV sú štatisticky rovnaké. Na obrázku 2.5 je znázornený príklad vloženia rovnomerne rozdelenej správy do obrázku, kde je vidieť zmenu histogramu.



Obr. 2.5: Príklad transformácie hodnôt bajtov (PoVs).



Obr. 2.6: Príklad transformácie hodnôt bajtu (možné PoV).

Označme x, y frekvencie PoV v originálnom obrázku. Podobne označme x', y' frekvencie toho istého PoV po prebehnutí steganografického algoritmu. S predpokladom, že bity, použité na prepísanie LSB, sú rovnomerne rozdelené, dostávame

$$x' = \frac{x}{2} + \frac{y}{2},$$
$$y' = \frac{x}{2} + \frac{y}{2},$$

čo súhlasí s obrázkom 2.5.

Príklad 2.5:

Pixel, ktorý má hodnotu 100 v originálnom obrázku, získa buď hodnotu 101, alebo ostane s hodnotou 100 v steganografickom obrázku. Podobne, pixel, ktorý má hodnotu 101 v originálnom obrázku, získa buď hodnotu 100, alebo ostane s hodnotou 101. Teda dvojica $\{100, 101\}$ je PoV. Vo všeobecnom prípade, v 8-bitovej škále, $\{2k, 2k+1 | 0 \leq k \leq 127\}$ formuje PoVs. □

Idea štatistických útokov je porovnať teoreticky očakávané frekvencie distribúcií v steganogramoch s nejakou testovacou distribúciou pri sledovaní na nejakom nosiči. Kritický bod v tomto prípade je, ako získať teoreticky očakávanú frekvenciu distribúcie (napríklad frekvenciu výskytu môžeme sledovať až po aplikovaní steganografických zmien). Táto

frekvencia nesmie byť odvodená z nejakého náhodného príkladu, pretože tento náhodný príklad už môže byť zmenený steganografickými operáciami. Vo väčšine prípadov nemáme k dispozícii originálny obrázok, aby sme ho mohli porovnávať a odvodiť očakávanú frekvenciu. V originále je očakávaná frekvencia aritmetický priemer dvoch frekvencii v PoV. Pretože vkládacia funkcia prepisuje LSB, nemení sa suma týchto frekvencií. Počet nepárnych hodnôt frekvencie je prenesený na korešpondujúce párne hodnoty frekvencie v každých PoV a naopak. Ak suma ostáva konštantná, potom aritmetický priemer je rovnaký pre PoV v obidvoch prípadoch (originálny nosič a každé korešpondujúce steganografické médium). Tento fakt nám pomáha získať teoreticky očakávanú frekvenciu rozloženia z náhodného vzoru. Teda nepotrebujeme originálny nosič pre tento útok.
Stupeň podobnosti získanej distribúcie a teoreticky očakávanej je kritérium pravdepodobnosti, že bola prevedná nejaká steganografická operácia. Stupeň podobnosti je determinovaný použitím Chi-kvadrát testu [4]. Tento test operuje na zmapovaných záznamoch v kategóriách. Uskutočňuje to v nasledujúcich krokoch:

1. Predpokladajme, že máme k kategórií, a že máme nejaký náhodný vzor pozorovania. Každé pozorovanie musí spadať práve do jednej z kategórií. Kategórie sú buď všetky paletové farby, všetky frekvencie farieb, DCT koeficienty atď (záleži od typu obrázka). Bez újmy na obecnosti, sústredime sa na nepárne hodnoty PoV média, na ktoré útočime. Ich minimálna teoreticky očakávaná frekvencia musí byť väčšia ako 4, môžeme unifikovať kategórie kvôli platnosti tejto podmienky.

2. Teoreticky očakávaná frekvencia v kategórii i po vložení rovnomerne rozloženej správy je:
$$n_i^* = \frac{|\{farba|indexfarby \in \{2i, 2i+1\}\}|}{2}.$$

3. Nameraná frekvencia výskytu v našom náhodnom vzore je:
$$n_i = |\{farba|indexfarby = 2i\}|.$$

4. χ^2 hodnota je daná ako:
$$\chi^2_{k-1} = \sum_{i=1}^{k} \frac{(n_i - n_i^*)^2}{n_i^*},$$
s $k-1$ stupňami voľnosti.

5. p je pravdepodobnosť tejto hodnoty pri podmienke, že distribúcie n_i a n_i^* sú rovnaké. Je vypočítaná integráciou hustoty rozloženia:
$$p = 1 - \frac{1}{2^{\frac{k-1}{2}}\Gamma(\frac{k-1}{2})} \int_0^{\chi^2_{k-1}} e^{-\frac{x}{2}} x^{\frac{k-1}{2}-1} dx,$$
kde Γ je Eulerova Gamma funkcia. Teda ak nezamietneme hypotézu H_0, tak sa výsledná pravdepodobnosť bude blížiť k nule (to znamená, že tvrdíme, že teoreticky očakávaná a pozorovaná distribúcia sú skoro rovnaké a pravdepodobnosť ukrytej správy je minimálna).

Príklad 2.6:

Predpokladajme obrázok v šedej škále (tj. 8-bit pp). Nech X, Y sú také vektory, že $x_k = frekvencia(2k)$ a $y_k = frekvencia(2k+1)$, $0 \leq k \leq 127$. Teoreticky očakávaná frekvencia (teda frekvencia, ktorá by mala byť nameraná v obrázku, ktorý skúmame, ak hypotéza platí) je $z_k = \frac{x_k + y_k}{2}$. Predpokladajme, že máme 128 kategórií (pretože $\frac{256 \text{ odtieňov}}{2}$). Bez újmy na všeobecnosti sa môžeme sústrediť na párne hodnoty PoV, takže nameraná frekvencia výskytu v kategórii k je x_k. Kedykoľvek, ak súčet frekvencií $2k$ a $2k+1$ je menší alebo rovný ako 4, počet kategórií je o jednu menší. Vypočítame χ^2 štatistiku s $k-1$ stupňami voľnosti:

$$\chi^2_{k-1} = \sum_{i=0}^{127} \frac{(x_i - z_i)^2}{z_i}, \ kde \ z_i = \frac{x_i + y_i}{2}.$$

Predopkladáme, že pre stego-obrázok bude hodnota χ^2_{k-1} relatívne malá, pretože x_i by mala byť blízko z_i, a pre originál naopak. Vypočítame pravdepodobnosť p, pomocou ktorej si to overíme. □

2.3 Aplikácia teórie kódov

V ďalšom texte budeme predpokladať, že nosičom pre steganografickú komunikáciu je digitálny obrázok, ktorého pixely nadobúdajú celočíselné hodnoty z intervalu 0 až 255 (teda použijeme model obrázku so šedou paletou). Každému pixelu priradíme jednobitovú hodnotu LSB, ktorá reprezentuje posledný bit v binárnom vyjadrení hodnoty pixelu; každému pixelu teda priradíme číslo 0 alebo 1. Označme vektor všetkých LSB digitálneho obrázku ako $X = (x_1, x_2, \ldots, x_k)$, kde $k \in \mathbb{N}$ je počet pixelov v obrázku a $x_i \in \mathbb{F}_2 = \{0, 1\}$ pre $i = 1, 2, \ldots, k$. Teda X je prvok vektorového priestoru $\mathbb{F}_2^k$. Budeme predpokladať, že steganografický algoritmus modifikuje množinu X v smere, aby z nej v druhej fázi bolo možné určiť pôvodnú správu. Ďalej predpokladajme, že ukrývaná správa je binárne kódovaná a teda je tvaru $Y = (y_1, y_2, \ldots, y_l)$, kde $l \in \mathbb{N}$.
Celý proces bude prebiehať po blokoch určitej veľkosti. Z toho dôvodu je nosič rozdelený na bloky o veľkosti N pixelov, ktoré sú reprezentované vektorom $x = (x_1, x_2, \ldots, x_N)$, $N < k$. Podobne, správa je rozdelená na bloky o veľkosti n binárnych znakov, teda $y = (y_1, y_2, \ldots, y_n)$, $n < l$. Zároveň nech platí, že $n < N$. Všetky vstupy x_i, $i = 1, 2, \ldots, N$, y_j, $j = 1, 2, \ldots, n$ sú prvkami telesa $\mathbb{F}_2 = \{0, 1\}$, teda $x \in \mathbb{F}_2^N$ a $y \in \mathbb{F}_2^n$.
Budeme hľadať zobrazenie f, ktoré zobrazí N bitov na n bitov, a pomocou neho dokážeme určiť n bitov ukrytej správy. Hľadáme teda

$$f : \mathbb{F}_2^N \to \mathbb{F}_2^n.$$

To znamená, že pre dané $x \in \mathbb{F}_2^N$ a $y \in \mathbb{F}_2^n$ chceme nahradiť pôvodné x inou N-ticou $x' \in \mathbb{F}_2^N$ tak, že $f(x') = y$. V tom prípade sa nám podarilo ukryť do N pixelov práve n bitov ukrývanej správy (uvedomme si, že sme modifikovali len LSB). Dôležitým aspektom je relácia medzi dvoma vektormi x a x'. Tieto vektory sa medzi sebou líšia v niektorých súradniciach x_i, $i = 1, 2, \ldots, N$. Povedzme, že týchto zmien je práve d. Tým pádom musíme zmeniť v nosiči práve d LSB pixelov, aby sme dosiahli požadovaný výsledok.

Počet súradníc, v ktorých sa líšia vektory x a x' je práve ich Hammingova vzdialenosť. Ak by sme chceli kontrolovať najhorší prípad, to znamená veľkosť $d(x, x')$, zafixujeme hornú hranicu týchto zmien ρ, teda $d(x, x') \leq \rho$.

2.4 Krycie funkcie

V úvode tejto kapitoli sme ukázali princíp takzvanej krycej funkcie, ktorú si teraz definujeme formálne.

Definícia 2.7: *Krycia funkcia*

Krycia funkcia $COV(\rho, N, n)$ je zobrazenie

$$f : \mathbb{F}_2^N \to \mathbb{F}_2^n,$$

ktoré splňuje nasledujúcu podmienku: pre každé $x \in \mathbb{F}_2^N$, $y \in \mathbb{F}_2^n$ existuje nejaké $x' \in \mathbb{F}_2^N$, že $d(x, x') \leq \rho$ a $f(x') = y$. □

Krycie funkcie $COV(\rho, N, n)$ nám umožňujú konštruovať steganografické algoritmy, ktoré sú schopné ukryť n bitov správy do N pixelov (LSB) pomocou najviac ρ zmien v nosiči.

Definícia 2.8: *Parametry steganografického algoritmu*

Nech $COV(\rho, N, n)$ je krycia funkcia a S je steganografický algoritmus z nej skonštruovaný. Potom definujeme:

- relatívnu kapacitu S ako
$$\alpha = \frac{n}{N};$$
- mieru zmeny S ako
$$\beta = \frac{\rho}{N};$$
- ukrývaciu efektivitu S ako
$$e = \frac{\alpha}{\beta} = \frac{n}{\rho}.$$

□

Definícia týchto parametrov je zrejmá. Aby steganografický algoritmus minimalizoval štatistické dopady steganoanalýzy, chceme, aby jeho ukrývacia efektivita bola čo najväčšia. Poďme si ukázať aká je súvislosť parametrov steganografického algoritmu s teóriou kódov. V teórii kódov sa ekvivalentne nazýva N dĺžka, n redundancia, a ρ krycí polomer nejakého kódu C. Chceli by sme dosiahnuť nasledujúce vlastnosti:

- chceme, aby relatívna redundancia $\frac{n}{N}$ bola čo najväčšia;
- chceme, aby relatívny krycí polomer $\frac{\rho}{N}$ bol čo najmenší, aby sme dosiahli vysokú ukrývaciu efektivitu;

- chceme, aby existoval efektívny algoritmus na počítanie x'.

Na tomto mieste je nutné upozorniť, že tieto parametre sú všeobecne definované pre lineárne kódy. V nasledujúcich častiach prenesieme tieto myšlienky aj na nelineárne kódy pomocou faktorizácie, kde definujeme, ako vyzerajú jednotlivé jej parametre.
Definícia 2.7 vyžaduje, aby inverzný obraz $f^{-1}(y)$ bol krycí kód s polomerom ρ pre každú voľbu $y \in \mathbb{F}_2^n$. Z toho vyplýva, že $\mathbb{F}_q^N$ je disjunktné zjednotenie 2^n takýchto kódov. Toto je ekvivalentný popis krycích funkcií.

Teda krycie funkcie $COV(\rho, N, n)$ sa dajú ekvivalentne popísať ako rozklad priestoru $\mathbb{F}_q^N$ na 2^n krycích kódov s krycím polomerom ρ.

Na tomto mieste nás môžu napadnúť rôzne otázky typu, pre aké hodnoty parametrov krycej funkcie takéto funkcie existujú, alebo pre aké parametry majú tieto funkcie vysokú ukrývaciu efektivitu. Z definície krycej funkcie plynú jednoduché vlastnosti týchto funkcií, ktoré zhrnieme do nasledujúceho pozorovania.

Pozorovanie 2.9:

Nech existujú $COV(\rho_i, N_i, n_i)$ pre $i = 1, 2, \ldots$. Potom existuje

$$COV(\sum_i \rho_i, \sum_i N_i, \sum_i n_i).$$

Existencia krycej funkcie $COV(\rho, N, n)$ implikuje existenciu krycích funkcií

$$COV(\rho{+}1, N, n),\ COV(\rho, N{+}1, n),\ COV(\rho, N, n{-}1),\ COV(c{\cdot}\rho, c{\cdot}N, c{\cdot}n),$$

pre každé $c \in \mathbb{N}$. □

Dôkaz:

Reťazec dĺžky $\sum_i N_i$ môžeme napísať ako zloženie za sebou idúcich reťazcov dĺžky N_i. Na každý dielčí reťazec môžeme použiť korešpondujúcu kryciu funkciu $COV(\rho_i, N_i, n_i)$ pre nejaké i. Z toho plynie prvá vlastnosť. Ostatné vlastnosti plynú priamo z definície funkcie COV. □

Veta 2.10: *Sphere-Covering Bound*

Ak existuje $COV(\rho, N, n)$, potom

$$\sum_{i=0}^{\rho} \binom{N}{i} \geq 2^n.$$

□

Dôkaz:

Existencia funkcie $COV(\rho, N, n)$ implikuje existenciu krycieho kódu s najviac 2^{N-n} kódových slov, pretože množiny $f^{-1}(y)$, kde $y \in \mathbb{F}_2^n$, rozkladajú priestor $\mathbb{F}_2^N$. Teda každé kódové slovo určuje $\sum_{i=0}^{\rho} \binom{N}{i}$ vektorov v Hammingovej vzdialenosti najviac ρ. Súčet všetkých týchto čísel musí byť aspoň 2^N, čo je počet všetkých vektorov v pristore $\mathbb{F}_2^N$. □

Napríklad, krycia funkcia $COV(1, N, n)$ môže existovať podľa predchadzajúcej vety len vtedy, ak $N \geq 2^n - 1$. V nasledujúcej kapitole uvidíme, že krycie funkcie zostrojené z Hammingových kódov, ktoré majú krycí polomer rovný 1, dosahujú tejto hranice, v tomto prípade $N = 2^n - 1$.
Prípad, v ktorom je veta 2.10 splnená s rovnosťou, odpovedá priamo perfektným kódom.

2.5 Faktorizácia a direktná suma kódov

V tejto časti si predstavíme takzvanú faktorizáciu kódov a využijeme ju pre konštrukciu krycích funkcií, pomocou ktorých sa dajú zostrojiť steganografické algoritmy s vyššou ukrývacou efektivitou ako majú lineárne krycie funkcie. Túto konštrukciu budeme realizovať pomocou direktnej sumy faktorizácií.

Definícia 2.11: *Faktorizácia kódu*

Nech D a C sú dva kódy také (nie nutne lineárne), že $D \subset C \subset \mathbb{F}_2^N$. C/D nazveme *faktorizáciou kódu C podľa kódu D*, ak C sa dá vyjadriť ako disjunktné zjednotenie posunutí D, a $\mathbb{F}_2^N$ sa dá vyjadriť ako disjunktné zjednotenie posunutí C. Teda existuje $T \in \mathbb{F}_2^N$ a $U \in C$, že

$$\mathbb{F}_2^N = \bigcup_{x \in T} (C + x),\ (C + x) \cap (C + y) = \emptyset\ \forall x \neq y \in T,\ \bigcap_{x \in T} (C + x) = \emptyset,$$

$$C = \bigcup_{x \in U} (D + x),\ (D + x) \cap (D + y) = \emptyset\ \forall x \neq y \in U,\ \bigcap_{x \in U} (D + x) = \emptyset.$$

□

Posunutím množiny C (resp. D) rozumieme množinu tvaru $C + x$ (resp. $D + y$), teda rozkladovú triedu priestoru $\mathbb{F}_2^N$ (resp. rozkladovú triedu C). Posunutia C priestoru $\mathbb{F}_2^N$ faktorizujú tento priestor a podobne je faktorizovaný kód C posunutiami D. Je zrejmé, že posunutia D kódu C tiež faktorizujú celý priestor $\mathbb{F}_2^N$. Počet takýchto posunutí tvaru $D+x$ v C je $\frac{|C|}{|D|}$, čo je index D v C, $[C : D]$. Pretože veľkosť takýchto kódov je vždy mocnina čísla 2, výsledný index bude vždy tvaru 2^n pre nejaké prirodzené číslo n. Príslušný priestor, v ktorom sa všetko odohráva, budeme označovať písmenom U. Všimnime si, že vždy, keď dva lineárne kódy sú tvaru $D \subset C$, tak formujú faktorizáciu C/D. Všeobecne však nemusíme pracovať s lineárnymi kódmi.

Definícia 2.12: *Parametre faktorizácie*

Nech D a C sú dva kódy také, že $D \subset C \subset \mathbb{F}_2^N$. Definujeme nasledujúce parametre faktorizácie C/D:

- dimenziu faktorizácie ako index $[C : D]$;
- redundanciu faktorizácie ako redundanciu kódu C v príslušnom priestore;
- dĺžku faktorizácie ako dimenziu príslušného priestoru.

□

Príklad 2.13:

Uvažujme faktorizáciu $U/Ham_r(2)$ a nech priestor U má dimenziu $2^r - 1$. Pretože $\frac{|U|}{|Ham_r(2)|} = \frac{2^{2^r-1}}{2^{2^r-r-1}} = 2^r$, dimenzia tejto faktorizácie je

$$\dim(U/Ham_r(2)) = r,$$

a jej redundancia je 0, pretože rolu kódu C v definícii hraje príslušný priestor U. □

Dôvodom, prečo sa neobmedzujeme len na lineárne kódy, sú Preparata kódy, ktoré majú zaujímavé vlastnosti a vo faktorizácii a direktnej sume faktorizácií dosahujú lepšie výsledky, čo sa týka ukrývacej efektivity steganografického algoritmu. Pripomeňme si, že tieto kódy sú $\mathbb{Z}_4$-lineárne.
Ako už vieme, Preparata kódy majú dĺžku $2^n - 1$ a dimenziu $2n - 2$, pre nejaké párne $n \geq 4$, a ich minimálna vzdialenosť je 5. Takisto vieme, že platí $\mathcal{P}_n(\sigma) \subset Ham_n(2)$. Počet vektorov vo vzdialenosti 1 alebo 2 od Preparata kódu je

$$|\mathcal{P}_n(\sigma)|(2^n - 1 + \binom{2^n - 1}{2}) = |\mathbb{F}_2^{2^n-1}| - |\mathcal{P}_n(\sigma)|.$$

Pretože žiadne kódové slovo Hammingového kódu nemá takúto vlastnosť, v tomto čísle je zahrnutý každý vektor mimo kódu $Ham_n(2)$ presne jedenkrát. Ďalej vieme, že Hammingov kód môže byť vyjadrený ako disjunktné zjednotenie posunutí Preparata kódu. Keďže Preparata kódy majú minimálnu vzdialenosť rovnú číslu 5 a nie sú perfektné, tak musí platiť, že $\rho \geq 3$. Rovnaký postup môžeme použiť pri rozšírených Preparata kódoch. Zhrňme tieto výsledky do vety.

Veta 2.14:

Nech $n \geq 4$. Máme, že $\dim(Ham_n(2)) = 2^n - n - 1$. Preparata kódy $\mathcal{P}_n(\sigma)$ majú kodimenziu $n - 1$ v $Ham_n(2)$ a $Ham_n(2)/\mathcal{P}_n(\sigma)$ je faktorizácia. Každý vektor $x \notin Ham_n(2)$ má vzdialenosť rovnú 1 alebo 2 od práve jedného kódového slova $\mathcal{P}_n(\sigma)$ a $\rho(\mathcal{P}_n(\sigma)) = 3$.

Rozšírený Preparata kód $\overline{\mathcal{P}}_n(\sigma)$ má minimálnu vzdialenosť rovnú 6, rozšírený Hammingov kód $\overline{Ham}_n(2)$ má vzdialenosť 4. Každý vektor $x \notin Ham_n(2)$ párnej váhy je vo vzdialenosti 2 od práve jedného kódového slova $\overline{\mathcal{P}}_n(\sigma)$ a pre každý vektor $x \notin Ham_n(2)$ platí $d(x, \overline{\mathcal{P}}_n(\sigma)) \leq 3$. $\rho(\overline{\mathcal{P}}_n(\sigma)) = 4$. Pritom $\dim(\overline{Ham}_n(2)/\overline{\mathcal{P}}_n(\sigma)) = n - 1$. □

Definícia 2.15: *Norma faktorizácie*

Nech C/D je faktorizácia. Nech pre každé x v príslušnom priestore U je

- $m(x)$ minimálna vzdialenosť x od jedného z posunutí množiny D faktorizácie, teda $\min_{y \in C}\{d(x, D + y)\}$;
- $M(x)$ maximálna vzdialenosť x od jedného z posunutí množiny D faktorizácie, teda $\max_{y \in C}\{d(x, D + y)\}$.

Normu faktorizácie definujeme ako

$$\nu = \nu(C/D) = \max_{x \in U}\{m(x) + M(x)\}.$$

□

Uvažme prípad, keď $C = U$ dimenzie N. Potom je každé x z príslušného priestoru U obsiahnuté v jednom posunutí definovaným faktorizáciou U/D. To znamená, že hodnota $m(x)$ je rovná nule. V tom prípade je norma faktorizácie $\nu = \max_{x \in U}\{M(x)\}$. Pretože všetky posunutia $D+x$ majú rovnakú štruktúru, je zrejmé, že norma ν je rovná kryciemu polomeru ktorejkoľvek z nich. Označme tento krycí polomer ako ρ. Parametre faktorizácie U/D sú teda:

- dimenzia $\dim(U/D) = n$ pre nejaké prirodzené n;
- redundancia 0;
- dĺžka N.

Je už jednoduché si uvedomiť, že takáto faktorizácia odpovedá krycej funkcii $COV(\rho, N, n)$, kde $\rho = \nu(U/D)$. Faktorizácie redundancie 0 teda odpovedajú krycím funkciám.

Ďalej si definujeme direktnú sumu faktorizácií. Pomocou tejto konštrukcie môžeme zostrojiť faktorizáciu, ktorá má väčšiu dĺžku. V našom prípade to hraje významnú rolu, pretože sme schopní kontrolovať krycí polomer výslednej faktorizácie (uvažovanej ako norma faktorizácie). To nám poskytne silnejší aparát pri konštrukcii krycích funkcií s požadovanými parametrami, a tým pádom aj požadovaných parametrov steganografického algoritmu.

Definícia 2.16: *Direktná suma faktorizácií*

Nech C_1/D_1 a C_2/D_2 sú faktorizácie dĺžky N_1, N_2 postupne a s rovnakou dimenziou n. Označme príslušné posunutia faktorizácií ako $D_1(i)$ a $D_2(i)$ pre $i = 1, 2, \ldots, 2^n$. Direktná suma faktorizácií

$$(C_1/D_1) \vee (C_2/D_2)$$

je definovaná pomocou

$$C = \bigcup_{i=1}^{2^n} D_1(i) \times D_2(i).$$

□

Počet kódových slov je

$$|C| = |C_1| \cdot |D_2| = |C_2| \cdot |D_1|.$$

Definícia direktnej sumy faktorizácií závísí na bijekcii medzi posunutiami faktorizácií $D_1(i)$ a $D_2(i)$. Voľba takejto bijekcie určuje usporiadanie posunutí a výslednú direktnú sumu faktorizácií.
Z definície 2.16 je zrejmé, že dĺžka takto zostrojenej direktnej sumy faktorizácií C_1/D_1 a C_2/D_2 je rovná $N_1 + N_2$ (spomeňme si na definíciu faktorizácie a príslušných pojmov) a $(C_1 \times C_2)/C$ je faktorizácia dimenzie n.

Veta 2.17: *Krycí polomer direktnej sumy faktorizácií*

Nech C je direktná suma dvoch faktorizácií C_1/D_1 a C_2/D_2 s identickou dimenziou n. Nech N_i, ν_i, k_i, $i = 1, 2$, označujú pre príslušnú faktorizáciu dĺžku, normu a redundanciu faktorizácie. Potom C má dĺžku $N_1 + N_2$ a redundanciu $k_1 + k_2 + n$. Krycí polomer direktnej sumy C spĺňuje nerovnosť

$$\rho(C) \leq \left\lfloor \frac{(\nu_1 + \nu_2)}{2} \right\rfloor .$$

□

Dôkaz:

Počet prvkov množiny C je zrejmý. Vezmime nejakú dvojicu (x, y) z príslušného priestoru, v ktorom sa pohybujeme. Ďalej zvoľme čísla $j, k \in \mathbb{N}$ tak, že vzdialenosti $d(x, D_1(j)) = m(x)$ a $d(y, D_2(k)) = m(y)$ sú minimálne. Z definície normy máme $\nu_1 = \max_x\{m(x)+M(x)\}$ a $\nu_2 = \max_y\{m(y)+M(y)\}$. Z toho plynie, že suma vzdialeností od (x, y) do $D_1(j) \times D_2(j)$ a do $D_1(k) \times D_2(k)$ je najviac $\nu_1 + \nu_2$. Teda jedna z týchto vzdialeností musí byť najviac $\frac{(\nu_1+\nu_2)}{2}$. Tým sme dokázali tvrdenie vety. □

Uvedená veta hovorí o tom, že pomocou direktnej sumy faktorizácií môžeme istým spôsobom ovládať krycí polomer. To sa javí ako ďalší dôležitý poznatok vo vývoji silnejšieho steganografického algoritmu založeného na krycích funkciách.

Veta 2.18: *Faktorizácia rozšírených kódov*

Nech C/D je faktorizácia binárnych kódov s normou $\nu(C/D) = N$. Potom rozšírené kódy tiež formujú faktorizáciu $\overline{C}/\overline{D}$ a platí, že $\nu(\overline{C}/\overline{D})$ je párne číslo medzi $\{N + 1, N + 2\}$. □

Dôkaz:

To, že $\overline{C}/\overline{D}$ je faktorizácia je zrejmé a v skutočnosti sú dimenzie obidvoch faktorizácií rovnaké. Z definície normy 2.15 plynie, že norma rozšírenej faktorizácie je párne číslo. Norma ν je definovaná ako súčet dvoch čísel. Ak x leží v príslušnom priestore kódu C a v leží v príslušnom priestore rozšíreného kódu $\overline{C}$, tak $d((x, 0), v) + d((x, 1), v) = 2d(x, v) + 1$. Z toho plynie, že buď $d((x, 0), v) = d(x, v) + 1$ alebo $d((x, 1), v) = d(x, v) + 1$. Je jasné, že $N < \nu(\overline{C}/\overline{D}) \leq N + 2$. □

Veta 2.19:

Nech C_1/D_1 a C_2/D_2 sú faktorizácie dĺžky N_1, N_2 s rovnakou dimenziou n a formujú teda direktnú sumu $(C_1/D_1) \vee (C_2/D_2)$. Potom platí:

1. $(C_1 \times C_2)/C$ je faktorizácia dimenzie n a platí
$$\nu((C_1 \times C_2)/C) \leq \rho(C_1) + \rho(C_2) + \rho(C).$$
2. Ak $\mathbb{F}_2^{N_1}/C_1$ a $\mathbb{F}_2^{N_2}/C_2$ sú faktorizácie, tak potom je faktorizáciou i $\mathbb{F}_2^{N_1+N_2}/C$.

□

Dôkaz:

1. Je zrejmé a plynie z definície faktorizácie, direktnej sumy a normy.
2. Takisto zrejmé, čitateľ sa môže pokúsiť dokázať na základe bodu (1).

□

Poďme si ukázať, aká je súvislosť faktorizácií a ich direktných súm s krycími funkciami. Už vieme, že faktorizácie redundancie 0 sú krycie funkcie. Uvažujme faktorizáciu kódu C podľa kódu D, tak ako je definována v definícii 2.11 a označme písmenom n dimenziu tejto faktorizácie a písmenom k jej redundanciu. Potom môžeme ekvivalentne popísať túto faktorizáciu ako zobrazenie

$$f = (f_l, f_r) : \mathbb{F}_2^N \to \mathbb{F}_2^{k+n},$$

kde $f_l(x) \in \mathbb{F}_2^k$, $f_r(x) \in \mathbb{F}_2^n$, $f^{-1}(0,0) = D$ a všetky funkcie $f^{-1}(a,b)$ sú posunutím D a $C = \bigcup_{b \in D} f^{-1}(0,b)$. V podstate $\mathbb{F}_2^{k+n}$ reprezentuje $(k+n)$-ticu bitov, v ktorých k bitov kóduje posuny C a n bitov kóduje posuny D. Takže funkcie

$$f_l : \mathbb{F}_2^N \to \mathbb{F}_2^k,$$

$$f_r : \mathbb{F}_2^N \to \mathbb{F}_2^n,$$

reprezentujú to, v ktorom posunutí C, a v ktorom posunutí D v rámci posunutia C sa nachádzame.

Nech $f_1 = (f_{1,l}, f_{1,r})$ a $f_2 = (f_{2,l}, f_{2,r})$ sú krycie funkcie popísané faktorizáciami C_1/D_1 a C_2/D_2 dĺžky postupne N_1, N_2, redundancie postupne k_1, k_2, s rovnakou dimenziou n. Potom môžeme faktorizáciu $(C_1 \times C_2)/C$ (ako pri direktnej sume, viz definícia 2.16) ekvivalentne popísať ako

$$(f_1 \vee f_2) = (f_{1,l}, f_{2,l}, f_{1,r} + f_{2,r}) : \mathbb{F}_2^N \to \mathbb{F}_2^{k_1+k_2+n},$$

kde $f_{1,l}(x) \in \mathbb{F}_2^{k_1}$, $f_{2,l}(y) \in \mathbb{F}_2^{k_2}$, $(f_{1,r}(x) + f_{2,r}(y)) \in \mathbb{F}_2^n$, $f^{-1}(0,0,0) = C$, a všetky množiny $f^{-1}(a,b,c)$ sú posunutím C a $(C_1 \times C_2) = \bigcup_{b \in D_1, c \in D_2} f^{-1}(0,b,c)$. Kódovanie jednotlivých bitových polí si môžeme predstaviť podobne, ako je to v prípade krycej funkcie faktorizácie.

Kapitola 3

Konštrukcia krycích funkcií

3.1 Krycie funkcie s krycím polomerom 1

Konštrukcia krycích funkcií s krycím polomerom 1 je vskutku jednoduchá a využívá poznatky z konštrukcie binárnych Hammingových kódov. Začneme voľbou n a zostrojíme kontrolnú maticu H, ktorej stĺpce pozostávajú zo všetkých nenulových n-tíc zoradených vzostupne podľa binárneho vyjadrenia čísla. H má teda $N = 2^n - 1$ stĺpcov. Krycia funkcia

$$f : \mathbb{F}_2^N \to \mathbb{F}_2^n$$

je definovaná ako skalárne súčiny riadkov matice H. Na tomto mieste si môžeme povšimnúť súvislosť s pojmom *syndrom* definovaným v teórii kódov. Táto krycia funkcia vo svojej podstate reprezentuje syndrom slova x, teda $f(x) = H \cdot x^\top$. Z konštrukcie plynie nasledujúca veta.

Veta 3.1:

Pre každé n existuje $COV(1, 2^n - 1, n)$. □

Tieto krycie funkcie sú ekvivalentné binárnemu Hammingovmu kódu a sú teda *lineárne* nad telesom $\mathbb{F}_2$. Každá lineárna krycia funkcia môže byť vyjadrená pomocou (n, N)-matice H. Krycí polomer bude menší alebo rovný ρ práve vtedy, ak sa každý vektor z vektorového priestoru $\mathbb{F}_2^n$ dá vyjadriť ako lineárna kombinácia najviac ρ stĺpcov matice H.
Kód $f^{-1}(0)$ je lineárny kód s krycím polomerom ρ. Naopak, existencia takého kódu môže byť použitá na zostrojenie matice H a funkcie f. Z toho vyplývajú dôležité vlastnosti krycích funkcií.

Lineárna krycia funkcia $COV(\rho, N, n)$ odpovedá binárnemu lineárnemu kódu dĺžky N a dimenzie $N - n$ s krycím polomerom ρ. Takýto kód sa dá vyjadriť ako množina M, pozostavajúca z N nenulových vektorov nad telesom $\mathbb{F}_2^n$, s vlastnosťou, že každý prvok telesa $\mathbb{F}_2^n$ sa dá vyjadriť ako suma najviac ρ vektorov z množiny M.

Z konštrukcie krycích funkcií je zrejmé, že ktorákoľvek n-bitová správa môže byť zložená z práve jedného stĺpca jej kontrolnej matice, pretože sa v nej vyskytujú všetky

kombinácie. Preto majú tieto krycie funkcie krycí polomer 1. Pomocou tohto poznatku môžeme jednoducho zostrojovať lineárne krycie funkcie s požadovaným krycím polomerom. Takisto môžeme jednoducho zistiť krycí polomer lineárnych krycích funkcií. Uvedenú konštrukciu si ukážeme na príklade.

Príklad 3.2:

Skonštruujeme kryciu funkciu $COV(1, 7, 3)$, ktorá je ekvivalentná Hammingovmu kódu $Ham_3(2)$. Zostrojíme kontrolnú maticu H, ktorej stĺpce sú vzostupne zoradené ako

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Lineárne zobrazenie $f : \mathbb{F}_2^7 \to \mathbb{F}_2^3$ je definované ako bodový súčin

$$f(x_1, x_2, x_3, x_4, x_5, x_6, x_7) = (y_1, y_2, y_3),$$

kde

$$y_1 = x_1 + x_4 + x_5 + x_7,\ y_2 = x_2 + x_4 + x_6 + x_7,\ y_3 = x_3 + x_5 + x_6 + x_7.$$

Napríklad $f(0011010) = 100$. Predpokladajme, že naša ukrývaná správa má tvar $y = 111$. Tvrdíme, že je možné nahradiť $x = 0011010$ pomocou x' tak, že $f(x') = y$ a zároveň $d(x, x') = 1$. V skutočnosti súradnica, kde musíme x zmeniť je jednoznačne určená a je to práve súradnica číslo 6, takže $x' = 0011000$. Ukrývacie pravidlo je $f(x) + y$. V našom prípade je táto hodnota rovná 011. Nájdeme stĺpec kontrolnej matice H, ktorý je zhodný s $f(x) + y$. Poradie tohto stĺpca určuje číslo súradnice, ktorú potrebujeme zmeniť, aby sme dosiahli požadovaného výsledku, v našom prípade číslo 6. □

Poďme sa pozrieť na vlastnosti steganografického agoritmu založeného na krycích funkciách s krycím polomerom 1, $COV(1, 2^n - 1, n)$. Ako sme spomínali v predchádzajúcej kapitole, tieto krycie fukcie dosahujú rovnosti $N = 2^n - 1$ vo vete 2.10. Krycie funkcie takto realizované dosahujú nasledujúcich parametrov steganografického algoritmu:

- ukrývajú maximálnu možnú relatívnu kapacitu
$$\alpha = \frac{n}{2^n - 1};$$
- miera zmeny je
$$\beta = \frac{1}{2^n - 1};$$
- ukrývacia efektivita je
$$e = n.$$

Viac-menej prvý steganografický algoritmus založený na krycej funkcii zostrojenej z Hammingovho kódu je algoritmus zostrojený Andreasom Westfeldom, pomenovaný $F5$. Westfeld použil takzvané "maticové ukrývanie" a ukázal, že steganografické algoritmy založené na takýchto konštrukciách výrazne vylepšujú ukrývaciu efektivitu a odolnosť voči štatistickej steganoanalýze [5].

3.2 Krycie funkcie s krycím polomerom 2

Na lineárne krycie funkcie sa môžeme pozerať aj z hľadiska projektívnej geometrie. Nech H je binárna matica typu $(n \times N)$ taká, že akékoľvek 3 stĺpce sú lineárne nezávislé. Budeme uvažovať o stĺpcoch matice H ako o bodoch projektívnej geometrie $PG(n-1,2)$ (vo všeobecnom prípade uvažujeme s q-árnou maticou v projektívnej geometrii $PG(n-1,q)$). Body tejto projektívnej geometrie sú 1-dimenzionálne podpriestory vektorového priestoru $\mathbb{F}_2^n$. Inak povedané, na $PG(n-1,2)$ sa môžeme pozerať ako na binárne reťazce dĺžky n. Lineárna nezávislosť stĺpcov znamená, že žiadne tri body projektívnej geometrie neležia na jednej priamke (priamka odpovedá 2-dimenzionálnemu podpriestoru). Množina bodov, kde žiadne tri body neležia na jednej priamke sa nazýva *ovál*. Vidíme, že matica H popisuje ovál, ktorý pozostáva z n prvkov v projektívnej geometrii $PG(n-1,2)$. Takisto môžeme vidieť, že nejaký kód, ktorého kontrolná matica je rovná matici H, môžeme rozšíriť, ak môžeme tento ovál rozšíriť na $n+1$ prvkov. Ovály, ktoré sa už nedajú ďalej rozšíriť, sa nazývajú *kompletné ovály*.
V tejto súvislosti je lineárna krycia funkcia $COV(2,N,n)$ ekvivalentná množine K bodov projektívnej geometrie $PG(n-1,2)$ (zo všetkých bodov N) takých, že každý bod projektívnej geometrie $PG(n-1,2)$ leží na priamke obshujúcej 2 body K.

Príklad 3.3:

Uvažujme nasledujúcu maticu:

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Pretože ktorákoľvek správa z množiny $\mathbb{Z}_2^3$ sa dá získať z matice H sčítaním najviac dvoch stĺpcov, matica H definuje kryciu funkciu $COV(2,4,3)$. Táto krycia funkcia je geometricky reprezentovaná ako projektívna geometria $PG(2,2)$, ktorá je známa ako *Fanova rovina*.

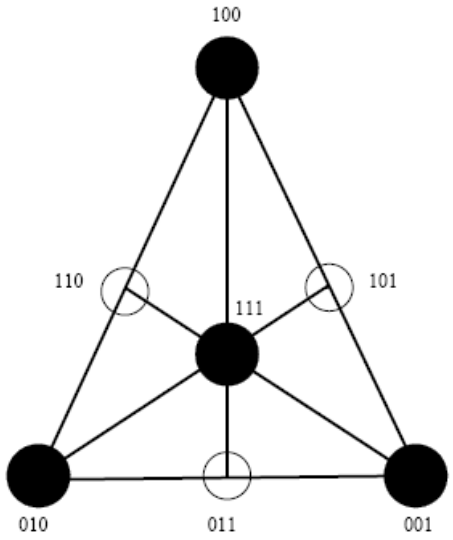
Na obrázku 3.1 je znázornená reprezentácia tejto krycej funkcie pomocou Fanovej roviny. Čierne body odpovedajú stĺpcom matice H. Každá správa môže byť tvorená súčtom najviac dvoch stĺpcov matice H, čomu odpovedajú biele body vo Fanovej rovine. Platí, že každý biely bod leží na nejakej priamke prechádzajúcej dvoma čiernymi bodmi. □

Rodina lineárnych krycích funkcií s krycím polomerom rovným číslu 2, ktoré vykazujú najlepšie výsledky bola zkonštruovaná už v roku 1991 pánmi Gabidulin, Davydov, Tombak [18]. Parametre týchto krycích funkcií sú nasledujúce:

$$COV(2, 5 \cdot 2^{a-1} - 1, 2a+1), \text{ pre } a \geq 1.$$

Pozrime sa, ako v tomto prípade vyzerajú parametre steganografického algoritmu:

- relatívna kapacita
$$\alpha = \frac{2a+1}{5 \cdot 2^{a-1} - 1};$$



Obr. 3.1: Fanova rovina a krycia funkcia $COV(2, 4, 3)$.

- miera zmeny je
$$\beta = \frac{2}{5 \cdot 2^{a-1} - 1};$$
- ukrývacia efektivita je
$$e = \frac{2a + 1}{2}.$$

3.3 Aplikácie direktnej sumy faktorizácií

Zo znalostí, ktoré sme získali, budeme vytvárať rôzne direktné sumy faktorizácií a uvidíme, že ich vlastnosti sú zaujímavé. Na začiatok si ale ukážme pár faktorizácií, aby sme mali lepšiu predstavu, s čím pracujeme. V nasledujúcej tabuľke budeme príslušný priestor faktorizácie označovať písmenom U a jeho dimenzia je jeho dĺžka. Symbolom A_n budeme označovať paritný kód dĺžky n.

Tabuľka 3.1: Niektoré faktorizácie kódov.

Faktorizácia	*Dĺžka*	*Dimenzia*	*Redundancia*	*Norma*
$U/Ham_n(2)$	$2^n - 1$	n	0	1
$U/\overline{Ham}_n(2)$	2^n	$n + 1$	0	2
$Ham_n(2)/\mathcal{P}_n(\sigma)$	$2^n - 1$	$n - 1$	n	3
$\overline{Ham}_n(2)/\overline{\mathcal{P}}_n(\sigma)$	2^n	$n - 1$	$n + 1$	4
$U/\mathcal{P}_n(\sigma)$	$2^n - 1$	$2n - 1$	0	3
$U/\overline{\mathcal{P}}_n(\sigma)$	2^n	$2n$	0	4
$A_n/\overline{Ham}_n(2)$	2^n	n	1	2
$A_n/\overline{\mathcal{P}}_n(\sigma)$	2^n	$2n - 1$	1	4

Príklad 3.4:

Pozrime sa napríklad na faktorizáciu $Ham_n(2)/\mathcal{P}_n(\sigma)$. Poznáme jej dĺžku, dimenziu, a vieme, že $\triangle(Ham_n(2)) = 3$ a $\triangle(\mathcal{P}_n(\sigma)) = 5$. Nech $x \notin Ham_n(2)$. Z vety 2.14 vieme, že platí $d(x, \mathcal{P}_n(\sigma)) \leq 2$. Keďže Hammingove kódy sú perfektné s krycím polomerom 1, tak platí i rovnosť $d(x, Ham_n(2)) = 1$. Nech $x \in Ham_n(2)$. Pripomeňme si, že norma faktorizácie je v podstate súčet dvoch čísel. Prvý sčítanec je v tomto prípade rovný 0 (minimum), a druhý je najviac 3 (maximum). Z toho plynie, že norma tejto faktorizácie je rovná 3, teda

$$\nu(Ham_n(2)/\mathcal{P}_n(\sigma)) = 3.$$

□

Direktná suma pozostáva z dvoch faktorizácií, ktoré majú rovnakú dimenziu. Pri určení parametrov direktnej sumy faktorizácie nám pomôže veta 2.17, pomocou ktorej dokážeme určiť dĺžku, redundanciu a krycí polomer výslednej direktnej sumy.
Z príkladov v tabuľke 3.1 teda môžeme odvodiť nasledujúce krycie funkcie odpovedajúce direktnej sume faktorizácií:

- faktorizácie $Ham_n(2)/\mathcal{P}_n(\sigma)$ a $A_{n-1}/\overline{Ham}_{n-1}(2)$ majú rovnakú dimenziu $n-1$. Parametre direktnej sumy:
  - dĺžka je $2^n - 1 + 2^{n-1} = 2^{n-1} \cdot 3 - 1$;
  - redundancia je $(n-1) + n + 1 = 2n$;
  - krycí polomer je $\lfloor \frac{(3+2)}{2} \rfloor = 2$

  Teda táto direktná suma odpovedá

  $$COV(2, 3 \cdot 2^{n-1} - 1, 2n), \ n \text{ je párne číslo, t.j.}$$

  $$COV(2, 6 \cdot 4^{a-1} - 1, 4a), \ a \geq 1.$$

  Parametre steganografického algoritmu:
  - relatívna kapacita
    $$\alpha = \frac{2n}{3 \cdot 2^{n-1} - 1} = \frac{4a}{6 \cdot 4^{a-1} - 1};$$
  - miera zmeny je
    $$\beta = \frac{2}{3 \cdot 2^{n-1} - 1} = \frac{2}{6 \cdot 4^{a-1} - 1};$$
  - ukrývacia efektivita je
    $$e = \frac{2n}{2} = n = \frac{4a}{2} = 2a.$$
- faktorizácie $Ham_n(2)/\mathcal{P}_n(\sigma)$ a $\overline{Ham}_n(2)/\overline{\mathcal{P}}_n(\sigma)$ majú rovnakú dimenziu $n-1$. Parametre direktnej sumy:
  - dĺžka je $2^n - 1 + 2^n = 2^{n+1} - 1$;
  - redundancia je $(n-1) + n + (n+1) = 3n$;

– krycí polomer je $\lfloor \frac{(3+4)}{2} \rfloor = 3$

Teda táto direktná suma odpovedá

$$COV(3, 2^{n+1} - 1, 3n),\ n \text{ je párne číslo, t.j.}$$

$$COV(3, 2 \cdot 4^a - 1, 6a),\ a \geq 1.$$

Parametre steganografického algoritmu:

– relatívna kapacita

$$\alpha = \frac{3n}{2^{n+1} - 1} = \frac{6a}{2 \cdot 4^a - 1};$$

– miera zmeny je

$$\beta = \frac{3}{2^{n+1} - 1} = \frac{3}{2 \cdot 4^a - 1};$$

– ukrývacia efektivita je

$$e = \frac{3n}{3} = n = \frac{6a}{3} = 2a.$$

- faktorizácie $Ham_n(2)/\mathcal{P}_n(\sigma)$ a $A_{\frac{n}{2}}/\overline{\mathcal{P}}_{\frac{n}{2}}(\sigma)$ majú rovnakú dimenziu $n-1$. Parametre direktnej sumy:

  – dĺžka je $2^n - 1 + 2^{\frac{n}{2}} = 2^{n+1} + 2^{\frac{n}{2}} - 1$;

  – redundancia je $(n-1) + n + 1 = 2n$;

  – krycí polomer je $\lfloor \frac{(3+4)}{2} \rfloor = 3$

  Teda táto direktná suma odpovedá

$$COV(3, 2^{n+1} + 2^{\frac{n}{2}} - 1, 2n),\ n = 4a,$$

$$COV(3, 2^{4a+1} + 2^{2a} - 1, 8a),\ a \geq 1.$$

  Parametre steganografického algoritmu:

  – relatívna kapacita

$$\alpha = \frac{2n}{2^{n+1} + 2^{\frac{n}{2}} - 1} = \frac{8a}{2^{4a+1} + 2^{2a} - 1};$$

  – miera zmeny je

$$\beta = \frac{3}{2^{n+1} + 2^{\frac{n}{2}} - 1} = \frac{3}{2^{4a+1} + 2^{2a} - 1};$$

  – ukrývacia efektivita je

$$e = \frac{2n}{3} = \frac{8a}{3}.$$

Kapitola 4

Všeobecný prípad krycích funkcií

V predchádzajúcich kapitolách sme sa zaoberali aplikáciami binárnych prípadov krycích funkcií na digitálne nosiče. V tejto kapitole sa pozrieme na všeobecné prípady predchádzajúcich aplikácií a pokúsime sa zovšeobecniť steganografické algoritmy. Začnime všeobecnou definíciou krycej funkcie.

Definícia 4.1: *Krycia funkcia nad q-árnym telesom*

Funkcia

$$f : \mathbb{F}_q^N \to \mathbb{F}_q^n$$

sa nazýva *krycia funkcia nad q-árnym telesom*, označujeme $COV(\rho, N, n)_q$, ak pre každý vektor $y \in \mathbb{F}_q^n$ a $x \in \mathbb{F}_q^N$ existuje vektor $x' \in \mathbb{F}_q^N$ taký, že $f(x') = y$ a zároveň $d(x, x') \leq \rho$. □

Videli sme rôzne konštrukcie binárnych krycích funkcií $COV(\rho, N, n)_2$, kde sme sa snažili udržať mieru zmeny $\beta = \frac{\rho}{N}$ čo najmenšiu a naopak relatívnu kapacitu $\alpha = \frac{n}{N}$ čo najväčšiu. Ak zafixujeme vektor $y \in \mathbb{F}_q^n$, tak definícia 4.1 hovorí, že každý vektor $x \in \mathbb{F}_q^N$ je v Hammingovej vzdialenosti najviac ρ od vzoru $f^{-1}(y)$. Inými slovami to znamená, že $f^{-1}(y)$ je krycí kód s krycím polomerom najviac ρ pre každé $y \in \mathbb{F}_q^n$. Ekvivalentne môžeme povedať, že priestor $\mathbb{F}_q^N$ je rozdelený na q^n krycích kódov s krycím polomerov najviac ρ. V niektorých publikáciách a literatúre sa toto rozdelenie nazýva ako *veľké množiny* (large sets) a označuje ako $LCOV[m](N, \rho)_q$, kde m značí počet kódov s krycím polomerom najviac ρ, na ktorý sa priestor $\mathbb{F}_q^N$ rozkladá, v našom prípade q^n.

V prípade lineárnych krycích funkcií bude $f^{-1}(0)$ lineárnym priestorom a teda lineárnym krycím kódom. Podobne, ako sme si ukazovali v binárnom prípade krycích funkcií, pretože pre každé y je $f^{-1}(y)$ posunutím $f^{-1}(0)$ a každé posunutie má rovnaké vlastnosti ako lineárny kód, môžeme vysloviť nasledujúce tvrdenie.

Tvrdenie 4.2: *Súvislosť lineárnej krycej funkcie a lineárneho kódu*

Nasledujúce vety sú ekvivalentné:

- Lineárna krycia funkcia $COV(\rho, N, n)_q$;
- Lineárny kód $[N, N - n]_q$ s krycím polomerom najviac ρ.

□

Z tohoto tvrdenia plynie, že jedna možná všeobecná metóda pre konštrukciu lineárnych krycích funkcií je prostredníctvom kontrolnej matice a syndromu kódového slova, ako sme to rozoberali v kapitole o konštrukciách binárnych krycích funkcií. To znamená, ak H je (n, N) kontrolná matica lineárneho kódu z tvrdenia 4.2, tak korešpondujúcu kryciu fukciu $f = COV(\rho, N, n)$ môžeme popísať ako

$$f(x) = H \cdot x.$$

V tomto prípade píšeme kódové slová ako stĺpcové vektory.

V teórii samoopravných kódov je často zaujímavé zistiť, pre aké najmenšie číslo N existuje lineárny q-árny kód $\mathcal{C}$ dĺžky N, dimenzie $N - n$ a s krycím polomerom najviac ρ. Toto číslo sa označuje ako $l(n, \rho)_q$ a v súvislosti s tvrdením 4.2 je $l(n, \rho)_q$ najmenšie číslo N také, že existuje lineárna krycia funkcia $COV(\rho, N, n)_q$.

Nech $\mathcal{C} \subseteq \mathbb{F}_q^n$ je kód s krycím polomerom ρ. V minulých kapitolách sme rozoberali, že zjednotenie sfér s polomerom ρ okolo kódových slov kódu $\mathcal{C}$ musí byť celý priestor. Nasledujúci dolný odhad počtu kódových slov kódu $\mathcal{C}$ je zovšeobecnením binárneho prípadu.

Veta 4.3:

Nech $\mathcal{C} \subseteq \mathbb{F}_q^n$ je kód s krycím polomerom ρ. Potom

$$|C| \geq \frac{q^n}{V_q(\rho, N)},$$

kde $V_q(\rho, N) = \sum_{i=0}^{\rho} \binom{N}{i}(q-1)^i$ značí počet q-árnych N-tíc váhy najviac ρ.
□

V prípade perfektných kódov vieme, že sféry s polomerom ρ rozkladajú priestor $\mathbb{F}_q^N$. Medzi tieto kódy patria Hammingové kódy, binárny a ternárny Golayov kód. Môžeme vysloviť nasledujúce tvrdenie.

Tvrdenie 4.4:

$$l(k, 1)_q = \frac{q^k - 1}{q - 1},$$
$$l(11, 3)_2 = 23,$$
$$l(5, 2)_3 = 11.$$

□

Lemma 4.5: *Krycí polomer opakovacieho kódu*

Všeobecný opakovací kód $[n, 1, n]_q$ má krycí polomer $n - \left\lceil \frac{n}{q} \right\rceil$. □

Dôkaz:

Nech $x \in \mathbb{F}_q^N$ a λ_i značí počet výskytov prvku $i \in \mathbb{F}_q$ vo vektore x. Určite pre nejaké $i \in \mathbb{F}_q$ platí nerovnosť $\lambda_i \geq \left\lceil \frac{n}{q} \right\rceil$. Z toho plynie, že vzdialenosť x od opakovacieho kódu je najviac $n - \left\lceil \frac{n}{q} \right\rceil$. □

Z prechadzajúceho Lemma plynie nasledujúca veta.

Veta 4.6:

Platí rovnosť

$$l(n, n)_q = n.$$

Ak platí nerovnosť $n + 1 - \left\lceil \frac{n+1}{q} \right\rceil \leq \rho < n$, tak platí

$$l(n, \rho)_q = n + 1.$$

□

Ak máme kód $\mathcal{C}$ s parametrami $[n + 1, k + 1, d]_q$, tak môžeme jednoducho prepichnutím kódu $\mathcal{C}$ zostrojiť kód s parametrami $[n, k, d]_q$. Bohužiaľ, opačný spôsob nie je tak jednoduchý a konštrukcia rozšíreného kódu nemusí byť vždy správnym smerom. Pripomeňme si pojem sily kódu. V súvislosti s lineárnymi kódmi budeme hovoriť, že *kód má silu o veľkosti* s, ak každých s stĺpcov jeho kontrolnej matice je lineárne nezávislých. V súvislosti s rozšírenými kódmi uvedieme nasledujúcu vetu.

Veta 4.7:

Nech $\mathcal{C}$ je $[n, k, d]_q$ kód, ktorý nemôže byť rozšírený na kód $[n + 1, k + 1, d]_q$. Potom existuje lineárna krycia funkcia $COV(d - 2, n, n - k)_q$. Ekvivalentne to znamená, že

$$l(n - k, d - 2)_q \leq n.$$

□

Dôkaz:

Pokiaľ máme q-árnu maticu H typu $(n \times N)$ o sile $s + 1$, tak táto matica je v skutočnosti kontrolnou maticou kódu $\mathcal{C}$ s parametrami $[N, N - n, s + 2]_q$. Predpokladajme, že existuje nejaký vektor $x \in \mathbb{F}_q^n$, ktorý nemôžeme vyjadriť lineárnou kombináciou s stĺpcových vektorov matice H. To je ekvivalentné tvrdeniu, že rozšírená matica H o tento vektor x má silu $s+1$ a je kontrolnou maticou kódu $[N+1, N-n+1, s+2]_q$, čo je vlastne rozšírený kód $\mathcal{C}$. Z tohto plynie tvrdenie vety. □

Jedným z možných spôsobov, ako dokázať, že lineárny kód nemôžeme rozšíriť, je ukázať, že žiadny takýto kód neexistuje. Vezmime si nejaký $[n, k, d]_q$ kód a predpokladajme, že kód $[n+1, k+1, d]_q$ neexistuje. Nech j je minimálne číslo také, že exisuje kód $[n-j, k-j, d]_q$. Takéto číslo určite existuje, pretože v každom prípade môžeme položiť j rovno k. Z toho plynie, že určite existuje aj minimálne číslo j, a takisto $j \geq 0$. Pretože kód $[n-j, k-j, d]_q$ nie je rozšíriteľný, tak podľa vety 4.7 máme

$$l(n - k, d - 2)_q \leq n - j \leq n.$$

Dôsledok 4.8:

Ak neexistuje kód $[n+1, k+1, d]_q$, potom

$$l(n-k, d-2)_q \leq n.$$

□

V kapitole 3, kde sme konštruovali binárne krycie funkcie s krycím polomerom, sme zistili, že sa na nich môžeme pozerať aj z hľadiska projektívnej geometrie. Celý prípad tejto časti môžeme zovšeobecnit na q-árne abecedy. Pripomeňme si, že sme sa zaoberali spojitosťou stĺpcových vektorov matice H o sile 3 s bodmi projektívnej geometrie $PG(n-1, q)$. Množinu bodov, kde žiadne tri body neležia na jednej priamke sme nazvali ovál, a ovály, ktoré sa nedajú rozšíriť sme nazvali kompletné ovály. V tejto súvislosti môžeme prepísať vetu 4.7 v zmysle projektívnej geometrie. Nasledujúce tvrdenie popisuje túto vetu pre $s = 2$.

Tvrdenie 4.9:

Ak v projektívnej geometrii $PG(n-1, q)$ existuje kompletný ovál pozostávajúci z N prvkov, tak

$$l(n, 2)_q \leq N.$$

□

Dolné a horné odhady funkcií $l(n, \rho)_q$ sa v súčasnosti skúmajú a nie sú známe presné výsledky. Pri niektorých parametroch sme schopní odhadnúť presné číslo $l(n, \rho)_q$, pri niektorých len horný alebo dolný odhad. Ukázali sme si niektoré horné odhady. Dolné odhady týchto funkcií, hlavne v binárnom prípade, sú skúmané v publikáciách [20], [21], [22]. Pre binárny prípad platí

$$l(2m-1, 2)_2 \geq 2^m + 1,$$

pre $m \geq 3$.

V prílohe č. 2 je možné nájsť tabuľku známych odhadov funkcií $l(n, \rho)_2$.

4.1 Aplikácie ternárnych kódov v steganografii

Doteraz sme sa zaoberali len aplikáciami binárnych kódov v steganografii. V podstate sme využívali LSB steganografiu. Binárne kódy majú veľkú výhodu v tom, že sa dajú jednoducho aplikovať na steganografiu, keďže každé digitálne steganografické médium je binárne.

V tejto časti sa pozrieme na aplikácie ternárnych kódov na steganografické algoritmy a vysvetlíme si, v čom je ich výhoda, nevýhoda, a nakoniec sa pozrieme na porovnanie s binárnymi kódmi. Aplikáciu budeme vysvetľovať na príklade ternárnych Hammingových kódoch.

Vieme, že ternárny Hammingov kód redundancie r, $Ham_r(3)$, je lineárny kód nad telesom $\mathbb{F}_3$. V kapitole 1 o samoopravných kódoch sme sa zaoberali aj konštrukciou Hammingových kódov. Pripomeňme si, akým spôsobom sa konštruuje kontrolná matica ternárneho Hammingového kódu. Vždy, keď pridávame nový stĺpec do kontrolnej matice, musíme dávať pozor, aby tento stĺpec nebol lineárne závislý k predošlým stĺpcom. Vždy sa vyhneme nulovému slovu, takže na začiatku si vyberáme z $3^r - 1$ nenulových r-tíc. Ak pridáme nenulový stĺpec, musíme vymazať z ďalšieho výberu aj jeho 2 násobky s nenulovými prvkami telesa $\mathbb{F}_3$. Jeden z najjednoduchších spôsobov, ako zkonštruovať takúto maticu, je zvoliť za stĺpce všetky nenulové r-tice, ktorých najvyššia nenulová súradnica je 1. Ukážme si príklady kontrolných matíc dvoch kódov:

- kód $Ham_2(3)$ má kontrolnú maticu

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix},$$

- kód $Ham_3(3)$ má kontrolnú maticu

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}.$$

Pri steganografickej aplikácii bude pre nás znova dôležité dekódovanie pomocou syndrómu slova. Popíšme si, ako toto dekódovanie vyzerá pri ternárnych Hammingových kódoch. Na dekódovanie znova použijeme kontrolnú maticu H kódu $Ham_r(3)$ a vypočítame syndróm prijatého slova x ako

$$s = H \cdot x.$$

Pokiaľ je syndróm slova nulový, nemusíme slovo opravovať, pretože neobsahuje chyby. V opačnom prípade musíme nájsť stĺpcový vektor matice H, ktorému odpovedá nejaký skalárny násobok syndrómu. To znamená, že ak $s = \alpha h_i$, kde h_i je i-ty stĺpec matice H, tak potom chybový vektor e má váhu jedna so skalárom α na i-tej súradnici. Chybový vektor má teda tvar

$$e = (0 \ldots \underbrace{\alpha}_{i} \ldots 0).$$

Potom dekódujeme prijaté slovo ako

$$y = x - e.$$

Poďme sa pozrieť ako dekódovanie pomocou syndrómu slova v prípade ternárnych kódov využijeme v prospech steganografického algoritmu a krycej funkcie. Princíp je v podstate rovnaký pre všetky q-árne kódy, až na niektoré detaily. V tomto prípade je krycia funkcia definovaná ako vo všeobecnom prípade pomocou syndrómu slova a krycie pravidlo je definované výrazom

$$f(x) + y.$$

Musíme ale vedieť, čo presne v každom prípade znamená slovo. V binárnom prípade nemusíme nad ničím premýšľať, pretože digitálne medium a zároveň správa, ktorú chceme ukryť, sa skladajú z binárnych čísel a používame LSB steganografickú metódu. V tomto

prípade je naša abeceda $\Sigma = \{0, 1, 2\}$ a musíme nejakým spôsobom to tejto abecedy transformovať digitálne médium a správu.
Ukrývanú správu nie je problém transformovať do ktorejkoľvek podoby. Podľa toho, akú abecedu používame, upravíme správu do reprezentácie sústavy s konkrétnym základom n, teda pre správu M máme

$$M = a_i n^i + a_{i-1} n^{i-1} + \cdots + a_1 n^1 + a_0 n^0,$$

kde $0 \leq a_i < n$ pre každé i. Reprezentáciu značíme ako

$$M = (a_i a_{i-1} \ldots a_1 a_0)_n.$$

Z kontextu je väčšinou zrejmé, o aký základ n sa jedná, a preto sa táto informácia vynecháva.
Pre digitálne médium je situácia trochu zložitejšia a do úvahy musíme vziať aj podobu digitálneho média (to znamená, či sa jedná o bezstrátový formát alebo strátový apod.). V našom modelovom prípade digitálneho obrázka môžeme použiť metódu, ktorá transformuje každý pixel obrázka na jednu z hodnôt 0,1,2, pomocou operácie modulo. V tomto prípade teda nechápeme vektor kódového slova ako postupnosť posledných bitov každého pixelu, ako to je v binárnom prípade, ale ako postupnosť

$$x = (x_1 \mod 3, x_2 \mod 3, \ldots, x_N \mod 3),$$

kde x_i, pre $i = 1, \ldots, N$, značí hodnotu pixelu v danom bloku.

Predpokladajme, že máme slovo x upravené do ternárnej podoby, ktoré chceme modifikovať na slovo x' tak, že $f(x') = y$, kde y je blok ukrývanej správy upravený do ternárnej podoby. Vychádzame z kontrolnej matice ternárneho kódu H a počítame syndróm slova x,

$$f(x) = H \cdot x^\top.$$

Použijeme krycie pravidlo $f(x) + y$ a tento vektor budeme považovať za pravý syndróm slova x. Dekódujeme slovo x pomocou algoritmu, ktorý sme si popísali vyššie a výsledkom je x' v ternárnej podobe. Vektory $x = (x_1, \ldots, x_N)$ a $x' = (x'_1, \ldots, x'_N)$ sa líšia v súradniciach maximálne o jedničku. Postupne prejdeme všetky súradnice, ktoré reprezentujú jednotlivé pixely, a rozlišujeme tri prípady:

1. $x_i - x'_i = 0$ - nepotrebujeme zmeniť hodnotu pixelu
2. $x_i - x'_i = 1$ - musíme znížiť hodnotu pixelu o 1, aby sme dosiahli správnej hodnoty po operácii modulo
3. $x_i - x'_i = 2$ - musíme zvýšiť hodnotu pixelu o 1, aby sme dosiahli správnej hodnoty po operácii modulo

Počet týchto zmien samozrejme závisí na zvolenej ternárnej krycej funkcii.
Tento steganografický algoritmus sa dá použit aj vo všeobecnom prípade q-árneho kódu s niektorými rozdielmi.

Príklad 4.10:

Skonštruujeme kryciu funkciu $COV(1,4,2)_3$, ktorá je ekvivalentná Hammingovmu kódu $Ham_2(3)$. Zostrojíme kontrolnú maticu H, ktorej stĺpce sú vzostupne zoradené ako

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix}.$$

Lineárne zobrazenie $f : \mathbb{F}_3^4 \to \mathbb{F}_3^2$ je definované ako bodový súčin

$$f(x_1, x_2, x_3, x_4) = (y_1, y_2),$$

kde

$$y_1 = x_2 + x_3 + x_4,\ y_2 = x_1 + x_3 + 2x_4.$$

Napríklad $f(1021) = 02$. Predpokladajme, že naša ukrývaná správa má tvar $y = 21$. Tvrdíme, že je možné nahradiť $x = 1021$ pomocou x' tak, že $f(x') = y$ a zároveň $d(x, x') = 1$. V skutočnosti súradnica, kde musíme x zmeniť je jednoznačne určená a je to práve súradnica číslo 2, ktorú musíme inkrementovať o jedničku, takže $x' = 1121$. Ukrývacie pravidlo je $f(x) + y$. V našom prípade je táto hodnota rovná 20. Nájdeme stĺpec h kontrolnej matice H a jeho skalárny násobok α tak, aby platilo $f(x) + y = \alpha h$. Poradie tohto stĺpca určuje číslo súradnice, ktorú potrebujeme zmeniť, aby sme dosiahli požadovaného výsledku, v našom prípade teda číslo 2. Rozdiel v tejto súradnici medzi vektormi x a x' určuje, akým spôsobom musíme zmeniť hodnotu pixelu. Teda máme $x_2 - x_2' = 1$, to znamená, že hodnotu pixelu, ktorý je reprezentovaný pomocou hodnoty x_2, musíme inkrementovať o jedničku. Nakoniec si overíme, že sme vektor x modifikovali v správnom smere, teda počítame

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix} = 2 \begin{pmatrix} 2 & 1 \end{pmatrix}.$$

Vidíme, že vektor (21) odpovedá ukrývanej správe 21. □

Pomocou parametrov ternárnych krycích funkcií môžeme určiť parametre steganografického algoritmu a výsledky porovnať s funkciami v binárnom prípade. Musíme ale mať na pamäti, že miera zmeny nám v prípade ternárnych krycích funkcií poskytuje iba dolný odhad. Predstavme si pixel s hodnotou 15. Jeho bitová reprezentácia v rámci jedného bajtu má tvar 00001111. Ak budeme potrebovať inkrementovať hodnotu tohoto pixelu, tak sa jeho bitová reprezentácia zmení na 00010000, čo namiesto jednej zmeny znamená zmien 5.
Ďalším, menším problémom môžu byť hraničné hodnoty pixelu, konkrétne hodnoty 0 a 255. V tomto prípade musíme mať ošetrené prechody pod a nad tieto hranice. Ak je hodnota pixelu rovná 0 a potrebujem znížiť jeho hodnotu, musíme to zariadiť zvýšením jeho hodnoty na hodnotu 2, aby sme získali požadovaný výsledok. Podobná situácia je v prípade hodnoty pixelu 255.
Pretože nemôžeme tento algoritmus porovnať v binárnom prípade, musíme nájsť iný spôsob. Jeden, ktorý nás jednoducho napadne, je porovnávať skutočné zmeny v celých

hodnotách jednotlivých bajtov. To znamená, že hodnoty nebudeme vnímať ako osmicu bitov, ale ako celé čísla z intervalu $\langle 0, 255\rangle$. V tomto prípade bude jednu zmenu znamenať zmena hodnoty o jedničku. V skutočnosti aplikácie binárnych kódov tiež menia hodnoty z tohto intervalu o jedničku, a tak tento spôsob porovnávania môžeme uplatniť všeobecne pre binárne a ternárne kódy v steganografii. Pozrime sa na to, ake prípady môžu nastať:

1. Hodnota bajtu sa nemusí zmeniť. Jeho bitová reprezentácia teda zostáva rovnaká a nenastáva žiadna zmena.

2. K hodnote bajtu musíme pripočítať jedničku. V časti o chi-kvadrát teste sme hovorili o párových hodnotách bajtov. Dve hodnoty bajtov tvoria pár hodnôt ak jedna hodnota sa transformuje na druhú pri LSB steganografii. Teda všetky takéto páry sú
$$\{2k, 2k+1|\ 0 \leq k \leq 127\}.$$
Na tomto mieste môžeme rozlíšiť ďalšie dva prípady:

   (a) Ak hodnota bajtu odpovedá jednej z hodnôt $2k$, kde $0 \leq k \leq 127$, tak pripočítaním jedničky nastane rovnaký stav ako v binárnom prípade steganografie. Hodnota najmenej významného bitu sa zmení z nuly na jedničku, a teda nastane jedna zmena, či už pre celú hodnotu bajtu, alebo v jeho bitovej reprezentácii.

   (b) Ak hodnota bajtu odpovedá jednej z hodnôt $2k+1$, kde $0 \leq k \leq 127$, tak pripočítaním jedničky nastanú v bitovej reprezentáciu bajtu prechody medzi jednotlivými mocninami čísla 2. Konkrétnejšie, ak pripočítame jedničku k číslu 1, dostaneme číslo 2, v bitovej reprezentácii nastáva jeden prechod, z 00000001 sa stáva 00000010.

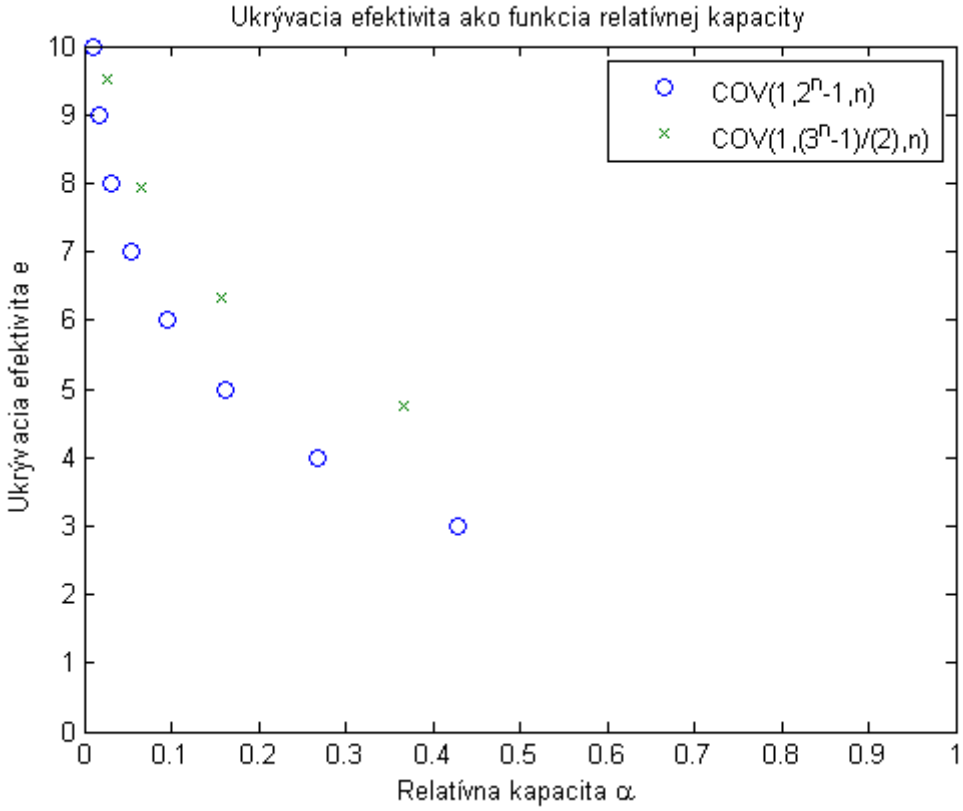
3. Od hodnoty bajtu musíme odčítať jedničku. Nastáva opačná situácia ako v predchádzajúcom prípade.

   (a) Ak hodnota bajtu odpovedá jednej z hodnôt $2k+1$, kde $0 \leq k \leq 127$, tak odčítaním jedničky nastane rovnaký stav ako v binárnom prípade steganografie. Hodnota najmenej významného bitu sa zmení z jedničky na nulu, a teda nastane jedna zmena, či už pre celú hodnotu bajtu, alebo v jeho bitovej reprezentácii.

   (b) Ak hodnota bajtu odpovedá jednej z hodnôt $2k$, kde $0 \leq k \leq 127$, tak odčítaním jedničky nastanú v bitovej reprezentáciu bajtu prechody medzi jednotlivými mocninami čísla 2. Konkrétnejšie, ak odčítame jedničku od číslu 2, dostaneme číslo 1, v bitovej reprezentácii nastáva jeden prechod, z 00000010 sa stáva 00000001.

Ak sa budeme pozerať na jednotlivé pixely ako na celé čísla, tak môžeme aplikovať rovnaké parametre steganografického algortimu v každom prípade. Algoritmus zkonštruovaný z ternárnej krycej funkcie založenej na ternárnom Hammingovom kóde $Ham_r(3)$ má nasledujúce parametre:

- relatívnu kapacitu
$$\alpha = \frac{n}{\frac{3^n-1}{2}} \cdot \log_2 3 = \frac{2n}{3^n-1} \cdot \log_2 3;$$



Obr. 4.1: Porovnanie binárnych a ternárnych krycích funkcií založených na Hammingovom kóde.

- mieru zmeny
$$\beta = \frac{1}{\frac{3^n-1}{2}} = \frac{2}{3^n-1};$$
- ukrývaciu efektivitu
$$e = \frac{\frac{2n}{3^n-1} \cdot \log_2 3}{\frac{2}{3^n-1}} = n \cdot \log_2 3.$$

Na obrázku 4.1 môžeme vidiet grafické znázornenie porovnania ukrývacej efektivity ako funkcie relatívnej kapacity binárnych a ternárnych krycích funkcií $COV(1, 2^n - 1, n)$ a $COV(1, \frac{3^n-1}{2}, n)_3$. Z grafu je patrné, že lepších výsledkov v tomto prípade dosahuje krycia funkcia $COV(1, 4, 2)_3$. Otázkou teda stále ostáva, akým spôsobom môžeme efektívnejšie využiť aplikácie q-árnych kódov a direktnej sumy v steganografii.

Záver

Moderná steganografia je pomerne nová disciplína pre utajovanie informácií. Všeobecne existuje mnoho spôsobov, ako ju aplikovať na digitálne dáta. V práci sme ukázali najjednoduchšiu metódu LSB steganografie, ktorá v prípade digitálnych obrázkov modifikuje najmenej významné bity všetkých pixelov tak, aby sa z nich neskôr dala poskladať ukrytá správa. Táto metóda vykazuje pomerne ľahko odhaliteľné štatistické vlastnosti, ktoré sú jej obrovskou slabinou. Všetky sofistikovanejšie steganoanalytické techniky ju dokážu relatívne spoľahlivo odhaliť.

Práve štatistická steganoanalýza posunula modernú steganongrafiu veľkou rýchlosťou vpred. Cieľom každého steganografického algoritmu je minimalizovať počet zmien v digitálnom nosiči vzniknutých ukrytím správy a maximalizovať množstvo, ktoré je steganografický algoritmus schopný ukryť do digitálneho nosiča. Tieto dva požiadavky sú v istej miere protichodné a je jasné, že nikdy sa nám nepodarí vyhovieť obidvom. Na základe toho vznikla ukrývacia efektivita, ktorá zachycuje tieto parametre steganografického algoritmu v jednej merateľnej premennej. Pre tieto účely môžu výborným spôsobom poslúžiť práve samoopravné kódy.

V prvej časti práce sme sa oboznámili s teóriou kódov a predstavili sme si niekoľko dôležitých konštrukcií samoopravných kódov. Na to sme nadviazali v druhej kapitole a pomocou kódov sme postavili prvé steganografické algoritmy, ktoré majú lepšie vlastnosti ako LSB steganografia a steganografia jej podobná. Lineárne kódy v tejto konštrukcii hrajú veľmi dôležitú rolu. Pomocou syndrómového kódovania nám dávajú všeobecný návod, ako konštruovať lineárne krycie funkcie, ktorých parametre sa významne líšia od moderných metód steganografie, ktoré kódy nevyužívajú.

Direktná suma faktorizácií kódov nám psokytuje návod, ako konštruovať krycie funkcie a steganografické algoritmy na nich založené pomocou nelineárnych kódov. Videli sme, že v tomto prípade vznikajú parametre takto skonštruovanej krycej funkcie zložením parametrov dvoch a viacerých kódov, ktoré vstupujú do direktnej sumy. Tieto algoritmy už je ťažšie zovšeobecniť, pretože už sa nejedná o jednoduché syndrómové kódovanie ako v prípade lineárnych kódov, ale musíme pre každý jednotlivý kód uvažovať konkrétne, špecifické algoritmické schémy. Videli sme teda, že niektoré rodiny nelineárnych kódov môžu dosiahnuť lepšie výsledky pri aplikovaní v steganografii, ako lineárne kódy.

Samozrejme, táto téma nie je uzatvorená, a steganografia založená na krycích funkciách a samoopravných kódoch ešte zďaleka nedosiahla svojich najlepších výsledkov. Doposiaľ sme sa naučili využívať niektoré triedy kódov pre účely steganografie. Jedným z najbliž-

ších cieľou sa stáva využitie $\mathbb{Z}_4$-lineárnych kódov v steganografii. My sme si v tejto súvislosti uviedli využitie Kerdockových a Preparata kódov. Vznikajú otázky, ktoré ďalšie kódy z tejto rodiny kódov dosahujú lepšie výsledky v steganografii. Jedným z nadejných kandidátov sa stávajú Goethalove kódy. V práci sme sa až na poslednú kapitolu obmedzovali na binárny prípad samoopravných kódov, pretože sa jednoducho aplikujú v digitálnom svete, kde v podstate existuje len nula a jednička. V poslednej kapitole sme sa pokúsili preniesť steganografiu na všeobecnejší prípad samoopravných kódov a skonštruovali sme algoritmus, ktorý pomocou ternárnych kódov dokáže využiť steganografiu. Tieto prípady takisto využívajú syndrómové kódovanie. Otázkou je, akým spôsobom všeobecne využívať lineárne i nelineárne kódy. Nakoniec by možno bolo dobré preskúmať aplikácie algebraicko-geometrických kódov a im podobných v súvislosti so steganografiou.

Literatúra

[1] L. Bican, *Lineární algebra a geometrie*, Academia Praha 2000, ISBN 80-200-0843-8

[2] R. Cinkais, *Steganografie a steganoanalýza*, Bakalárska práca MFF UK, 2007

[3] Bauer, F. L. *Decrypted Secrets: Methods and Maxims of Cryptology*, 3rd ed. Springer-Verlag, New York, 2002

[4] Wilfrid J. Dixon, Frank J. Massey: *Introduction to Statistical Analysis.* McGrawhill Book Company, Inc., New York 1957

[5] A. Westfeld: *High Capacity Despite Better Steganalysis (F5 - A Steganographic Algorithm)*, Information hiding, 4th International Workshop, LNCS vol. 2137, Springer-Verlag, Berlin Heidelberg 2001, 289 - 302

[6] A. M. Kerdock, *A class of low-rate nonlinear binary codes*, Inform. Control, 20 (1972), 182-187

[7] F. P. Preparata, *A class of optimum nonlinear double-error correcting codes*, Inform. Control, 13 (1968), 378-400

[8] A. W. Nordstrom and J. P. Robinson, *An optimum nonlinear code*, Inform. Control, 11 (1967), 613-616

[9] G. D. Forney, Jr., N. J. A. Sloane and M. D. Trott, *The Nordstrom-Robinson code is the binary image of the octacode*, Proceedings DIMACS/IEEE Workshop on Coding and Quantization, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Amer. Math. Soc., 1993

[10] R. A. Liebler a R. A. Mena, *Certain distance-regular digraphs and related rings of characteristics 4*, J. Combin. Theory, Series A, 47 (1988), 111-123

[11] B. R. MacDonald, *Finite rings with identity*, Marcel Dekker, NY, 1974

[12] O. Zariski a P. Samuel, *Commutative algebra*, Van Nostrand, Princeton, NJ, 1960

[13] M. Yamada, *Distance-regular digraphs of girth 4 over an extension ring of* $\mathbb{Z}/4\mathbb{Z}$, Graphs and Combinatorics, 6 (1990, 381-394)

[14] J. V. Uspensky, *Theory of equations*, McGraw-Hill, NY, 1948

[15] A. Drápal, *Úvod do teorie grup*, Karolinum Praha 2000, ISBN 80-246-0162-1

[16] A. R. Calderbank , N. J. A. Sloane, Modular and p-adic cyclic codes, *Designs, Codes and Cryptography*, v.6 n.1, p.21-35, July 1995

[17] Wan, Z., *Quaternary codes*, Singapore: World Scientific Pub., ISBN 9810232748, 9789810232740, (1997)

[18] E. M. Gabidulin, A. A. Davydov and I. M. Tombak: *Codes with covering radius 2 and other new covering codes*, IEEE Transactions on Information Theory 37 (1991), 219-224

[19] Galand, F. and Kabatiansky, G.: *Information Hiding by Coverings*, Proc. ITW2003, Paris, France (2003) 151154

[20] A. A. Davydov, A. Labinskaya: *Construction, families and tables of binary linear covering codes*, IEEE Transactions on Information Theory 40 (1994), 1270-1279

[21] R. Struik: *An improvement of the van Wee bound for binary linear covering codes*, IEEE Transactions on Information Theory 40 (1994), 1280-1284

[22] R. Struik: *On the structure of linear codes with covering radius 2 and 3*, IEEE Transactions on Information Theory 40 (1994), 1406-1416

[23] G. Cohen, I. Honkala, S. Litsyn, A. Lobstein: *Covering Codes*, North Holland, Amsterdam 1997, ISBN 0-444-82511-8

[24] A. A. Davydov: *New constructions of covering codes, Designs, Codes and Cryptography*, 22 (2001), 305316

[25] A. A. Davydov, G. Faina, S. Marcugini, F. Pambianco: *Locally optimal (nonshortening) linear covering codes and minimal saturating sets in projective spaces*, IEEE Transactions on Information Theory 51 (2005), 43784387

[26] A. A. Davydov, S. Marcugini, F. Pambianco: *Minimal 1-saturating sets and complete caps in binary projective spaces*, Journal of Combinatorial Theory A 113 (2006), 647663

[27] T. Etzion and B. Mounits: *Quasi-perfect codes with small distance*, IEEE Transactionson Information Theory 51 (2005), 39383946

[28] M. K. Kaikkonen and P. Rosendahl: *New covering codes from an ADS-like construction*, IEEE Transactions on Information Theory 49 (2003), 18091812

Prílohy

Príloha č.1: Porovnanie krycích funkcií

V druhej kapitole zaoberajúcej sa súvislosťou steganografie s teóriou kódov sme sa zoznámili s krycími funkciami, ktoré vo svojej podstate reprezentujú steganografické algoritmy. Tieto algoritmy majú oproti klasickým steganografickým algoritmom založeným na LSB modifikácií výhodu, pretože sa snažia minimalizovať počet zmien v digitálnych nosičoch pri vkladaní správy (správu chápeme ako akékoľvek digitálne dáta).

Vytvorený aparát pre porovnávanie rôznych steganografických algoritmov založených na krycích funkciách $COV(\rho, N, n)$ pozostáva z parametrov steganografického algorimu definových ako:

- relatívna kapacita
$$\alpha = \frac{n}{N};$$
- miera zmeny
$$\beta = \frac{\rho}{N};$$
- ukrývacia efektivita
$$e = \frac{\alpha}{\beta} = \frac{n}{\rho}.$$

Klasickú LSB modifikáciu nemôžeme transforovať do reči krycích funkcií. Tento steganografický algoritmus postupne modifikuje digitálne médium v poslednom bite každého pixelu. S polovičnou pravdepodobnosťou sa modifikovaný bit zmení z aktuálnej hodnoty na opačnú. Parametry N a n krycej funcie by sa v tomto prípade rovnali voľbe veľkosti jednotlivých blokov. V prípade LSB modifikácie platí, že $N = n$. Zo štatistickej teórie vyplýva, že počet zmien v posledných bitoch v digitálnom nosiči vytvorených pomocou tejto metódy je rovný približne polovici vkladaných bitov. Mohli by sme teda aproximovať krycí polomer takejto funkcie polovici vkladaných bitov. Takúto kryciu funkciu môžeme označiť ako $COV(\frac{n}{2}, n, n)$, kde n je zvolená veľkosť blokov. Parametre tejto krycej funkcie sú potom nasledujúce:

- relatívna kapacita
$$\alpha = \frac{n}{n} = 1;$$
- miera zmeny
$$\beta = \frac{\frac{n}{2}}{n} = \frac{1}{2};$$
- ukrývacia efektivita
$$e = \frac{\alpha}{\beta} = \frac{1}{\frac{1}{2}} = 2.$$

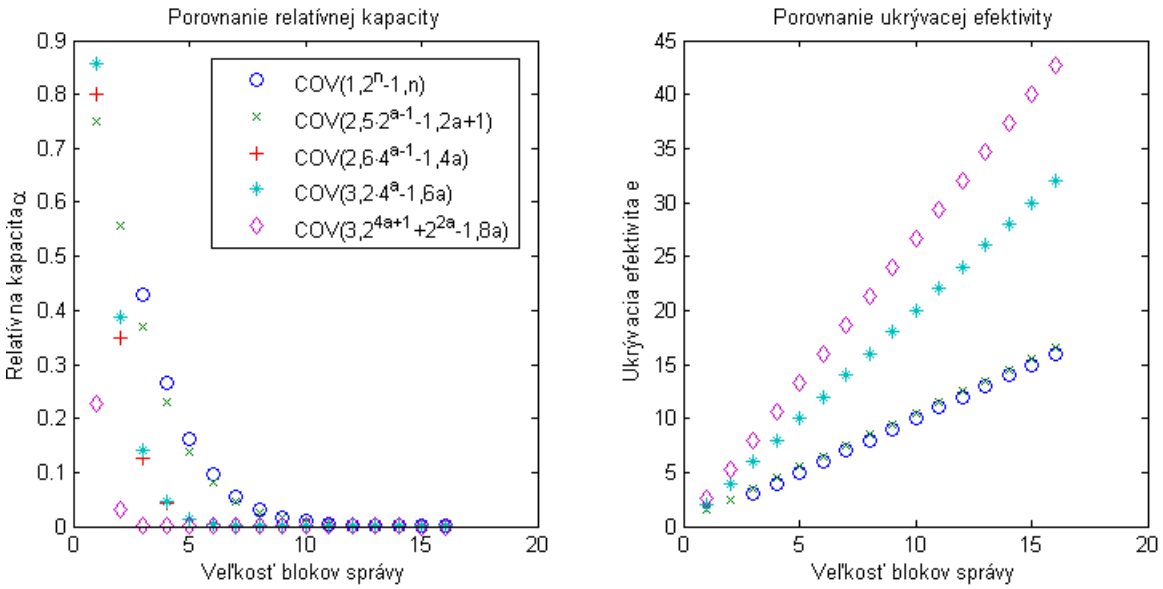
Vidíme, že parametre krycej funkcie založenej na LSB modifikácií vôbec nezávisia na parametroch krycej funkcie a všetky sú konštanty. Krycia funkcia $COV(\frac{n}{2}, n, n)$ preto nemá žiadnu perspektívu a jej ukrývacia efektivita je v porovnaní so steganografickými algoritmami nízka. Pri porovnávaní krycích funkcií sa nebudeme touto krycou funkciou zaoberať.

Pripomeňme si význam parametrov steganografického algoritmu. Najvýznamnejším z nich je ukrývacia efektivita, ktorá nám poskytuje akýsi porovnávací mechanizmus medzi jednotlivými krycími funkciami. Samozrejme to neznamená, že ostatné parametery nás nezaujímajú, koniec koncov, ukrývacia efektivita z nich vychádza. Ideálnym stavom je získať relatívnu kapacitu $\alpha = 1$ a mieru zmeny $\beta = 0$. Tieto parametre sú ale protikladné a prakticky nikdy nie je možné dosiahnuť ideálneho stavu.
Poďme sa pozrieť na porovnanie nasledujúcich krycích funkcií:

- $COV(1, 2^n - 1, n)$, kde $n \geq 3$;
  - $\alpha = \frac{n}{2^n - 1}$;
  - $\beta = \frac{1}{2^n - 1}$;
  - $e = n$;
- $COV(2, 5 \cdot 2^{a-1} - 1, 2a + 1)$, pre $a \geq 1$;
  - $\alpha = \frac{2a+1}{5 \cdot 2^{a-1} - 1}$;
  - $\beta = \frac{2}{5 \cdot 2^{a-1} - 1}$;
  - $e = \frac{2a+1}{2}$;
- $COV(2, 6 \cdot 4^{a-1} - 1, 4a)$, $a \geq 1$;
  - $\alpha = \frac{4a}{6 \cdot 4^{a-1} - 1}$;
  - $\beta = \frac{2}{6 \cdot 4^{a-1} - 1}$;
  - $e = \frac{4a}{2} = 2a$;
- $COV(3, 2 \cdot 4^a - 1, 6a)$, $a \geq 1$;
  - $\alpha = \frac{6a}{2 \cdot 4^a - 1}$;
  - $\beta = \frac{3}{2 \cdot 4^a - 1}$;
  - $e = \frac{6a}{3} = 2a$;
- $COV(3, 2^{4a+1} + 2^{2a} - 1, 8a)$, $a \geq 1$
  - $\alpha = \frac{8a}{2^{4a+1} + 2^{2a} - 1}$;
  - $\beta = \frac{3}{2^{4a+1} + 2^{2a} - 1}$;
  - $e = \frac{8a}{3}$.

Na obrázku 4.2 sa nachádza porovnanie týchto krycích funkcií.
Z obrázku je vidieť niekoľko faktov o krycích funkciách skonštruovaných pomocou direktnej sumy faktorizácií.

- Ukrývacia efektivita krycích funkcií skonštruovaných pomocou direktnej sumy faktorizácií je značne väčší ako ukrývacia efektivita lineárnych krycích funkcií. Preto sú tieto krycie funkcie v zmysle steganografického algoritmu vhodnejšie pre aplikácie.



Obr. 4.2: Porovnanie krycích funkcií.

- Pri voľbe väčších blokov správy, ekvivalentne pri voľbe väčšej ukrývacej efektivity, prudko klesá parametr relatívnej kapacity steganografického algoritmu. Vo všeobecnosti platí, že čím si zvolíme vyššiu ukrývaciu efektivitu (veľkosť blokov), tým sa znižuje schopnosť algoritmu efektívne využívať priestor v digitálnom nosiči.

Môže nás napadnúť otázka, či existuje nejaká hranica alebo obmedzenie pre parameter ukrývacej efektivity. Horný odhad tohto parametru e pre fixovanú hodnotu relatívnej kapacity α môžeme získať z vety 2.10. Páni Galand a Kabatiansky vo svojej práci zistili, že počet rôznych správ, ktoré môžeme vložiť do nosiča vytvorením maximálne ρ zmien v binárnom vektore dĺžky N (parametry sú ekvivalentné tým v krycích funkciách) je zhora ohraničený číslom

$$2^{N \cdot h(\frac{\rho}{N})} = 2^{N \cdot h(\beta)},$$

kde h označuje entropickú funkciu a predpokladáme, že $N \to \infty$, $\frac{n}{N} < \frac{1}{2}$ [19]. Entropická funkcia $h(p) : [0,1] \to \mathbb{R}$ je definovaná predpisom

$$h(p) = \begin{cases} p \cdot \log \frac{1}{p} + (1-p) \log \frac{1}{1-p} & \text{pre } p \in (0,1), \\ 0 & \text{pre } p = 0, 1. \end{cases}$$

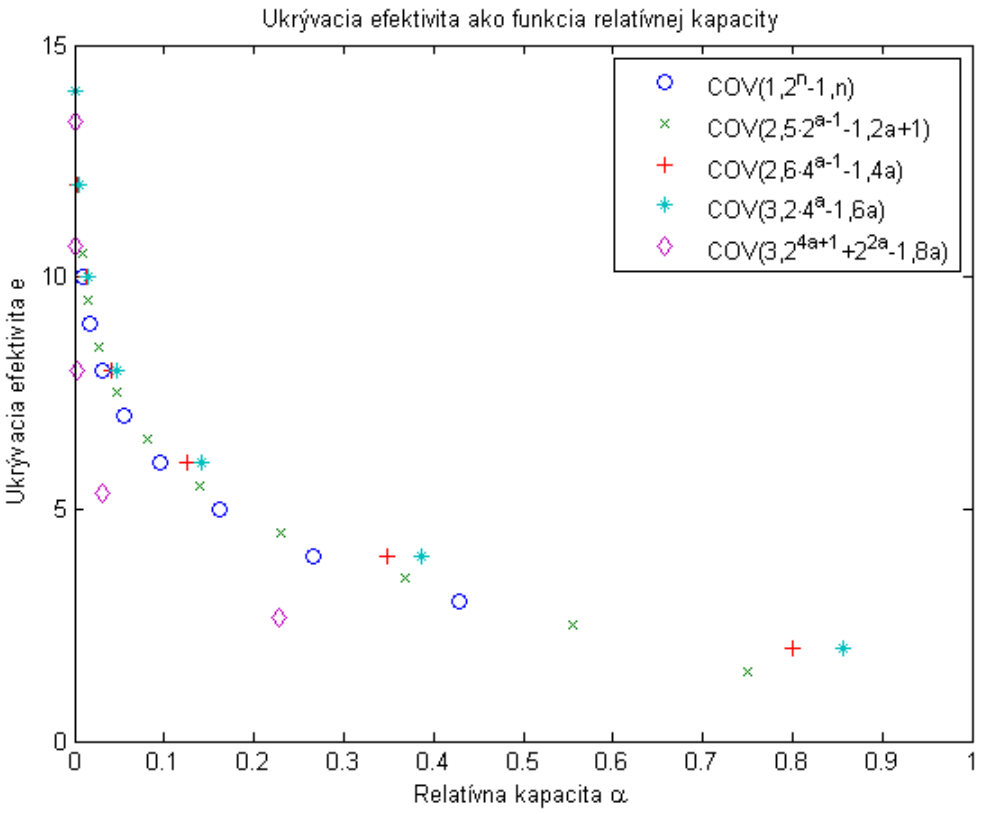
V kapitole o perfektných kódoch sme si definovali pojem objemu sféry $V(n, \rho)$. Entropická funkcia s týmto pojmom súvisí a platí nerovnosť

$$V(n, \rho) < 2^{n \cdot h(\frac{\rho}{n})},$$

pre $0 \leq \rho \leq \frac{n}{2}$. Berme túto nerovnosť ako fakt, jej odvodenie sa dá nájsť v každej literatúre zaoberajúcej sa teóriou kódov.

Nech H je binárna (n, N)-matica definujúca lineárny kód $\mathcal{C}$ a predpokladajme, že vektor $v \in \mathcal{C}$ má Hammingovu váhu najviac ρ (odpovedajúce krycej funkcii $COV(\rho, N, n)$). Potom z vyššie uvedených výsledkov dostávame nerovnosť

$$e \leq \frac{\alpha}{h^{-1}(\alpha)},$$



Obr. 4.3: Ukrývacia efektivita ako funkcia relatívnej kapacity ($e = f(\alpha)$).

kde h^{-1} je inverzia funkcie h na intervale $[0, \frac{1}{2}]$. Pre fixovanú hodnotu α môžeme odhadnúť hornú hranicu ukrývacej efektivity e.
Na obrázku 4.3 je znázornená ukrývacia efektivita e krycích funkcií ako funkcia relatívnej kapacity α. V grafe si môžeme všimúť, akým spôsobom sú tieto paramtre ovplyvňované.

Príloha č.2: Tabuľka hodnôt $l(n,\rho)_2$

V nasledujúcej tabuľke sú znázornené hodnoty $l(n,\rho)_2$ pre niekoľko prvých parametrov. Prvky tabuľky majú tvar $x-y$, kde x značí dolnú hranicu pre N pri konkrétnej voľbe parametrov, a y značí hornú hranicu. V prípade, ak je nietorá z hraníc neznáma, píšeme v tabuľke otáznik. Tieto hodnoty vychádzajú zo súčasných výsledkov a z publikácií [23], [24], [25], [26], [27], [28].

Tabuľka 4.1: Niektoré hodnoty $l(n,\rho)_2$.

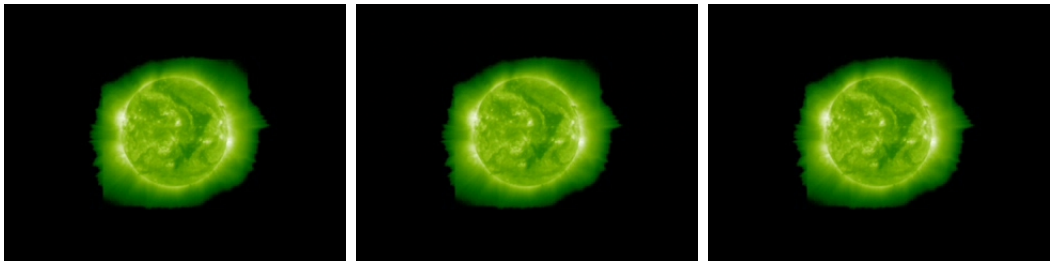
n ρ	1	2	3	4	5
2	3−?	2−?			
3	7−?	4−?	3−?		
4	5−?	5−?	5−?	4−?	
5	31−?	9−?	6−?	6−?	5−?
6	63−?	12 − 13	7−?	7−?	7−?
7	127−?	16 − 19	11−?	8−?	8−?
8	255−?	23−?	13 − 14	9−?	9−?
9	511−?	? − 39	16 − 18	13−?	10−?
10	1023−?	? − 51	20 − 22	14 − 16	11−?
11		? − 72	23−?	17 − 19	15−?
12		? − 95	30 − 31	19 − 23	16 − 18
13		? − 159	? − 47	? − 25	? − 19
14		? − 215	? − 63	? − 29	? − 23
15		? − 274	? − 71	? − 36	? − 27
16		? − 383	? − 94	? − 46	? − 31
17		? − 639	? − 126	? − 62	? − 35
18		? − 863	? − 127	? − 74	? − 41
19		? − 1062	? − 191	? − 82	? − 46
20		? − 1535	? − 254	? − 90	? − 54
21		? − 2559	? − 308	? − 122	? − 63
22		? − 3455	? − 382	? − 144	? − 82
23		? − 4167	? − 510	? − 158	? − 94
24		? − 6143	? − 511	? − 190	? − 104
25		? − 10239	? − 767	? − 238	? − 120

Príloha č.3: Porovnanie steganografických algoritmov

Na tomto mieste si predvedieme jednoduché porovnanie dvoch rozdielných steganografických algoritmov. Na testovanie použijeme chi-kvadrát analýzu a uvidíme, akým spôsobom sa budú chovať jednotlivé algorimty.
Aplikujeme steganografiu na digitálne obrázky vo formáte Joint Photographic Experts Group (JPEG). To, že tento formát nemá štruktúru podobnú modelovému prípadu digitálnych dat, ako sme uvádzali vo všetkých prípadoch tejto práce, nám nevadí. Spätnou transformáciou tejto štruktúry totiž získame práve RGB štruktúru obrázka. Porovnávanie je dobre vidieť na obrázkoch, ktoré majú rozdielne rozloženie farieb. Preto boli vybrané tri typy obrázkov:

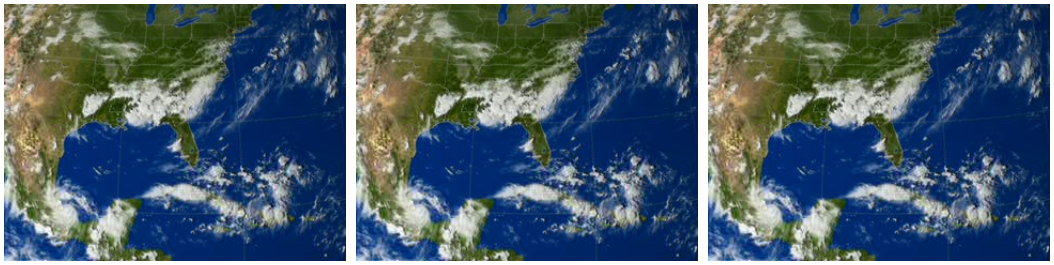
1. S vysokým počtom farieb a malým počtom homogénnych oblastí (obrázok 4.4)
2. Homogénny obrázok (obrázok 4.5)
3. Kompromis predchádzajúcich dvoch (obrázok 4.6)

Obr. 4.4: Médium s vysokým počtom farieb a malým počtom homogénnych oblastí. Postupne zprava je znázornený originálny obrázok, steganografický obrázok vytvorený pomocou LSB steganografie a steganografický obrázok vytvorený pomocu krycej funkcie $COV(1, 7, 3)$.



Obr. 4.5: Homogénne médium. Postupne zprava je znázornený originálny obrázok, steganografický obrázok vytvorený pomocou LSB steganografie a steganografický obrázok vytvorený pomocu krycej funkcie $COV(1, 7, 3)$.

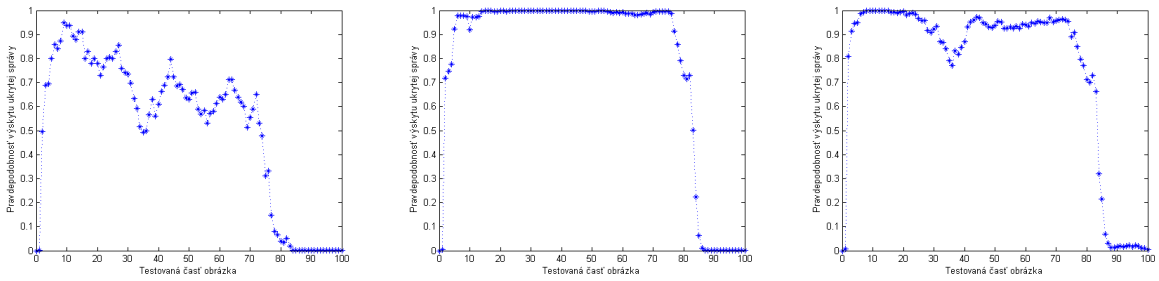
Na obrázky môžeme aplikovať steganografické algoritmy. Použijeme tieto dva steganografické algoritmy, ktoré sme popisovali v druhej kapitole tejto práce:



Obr. 4.6: Médium s priemernými farbami a homogénnosťou. Postupne zprava je znázornený originálny obrázok, steganografický obrázok vytvorený pomocou LSB steganografie a steganografický obrázok vytvorený pomocu krycej funkcie $COV(1,7,3)$.

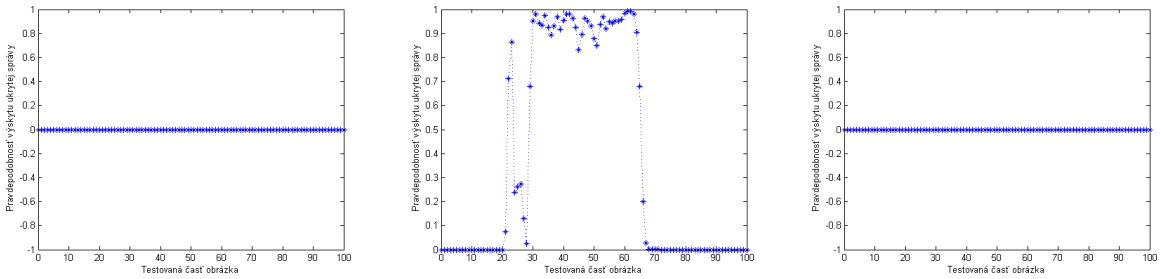
1. LSB steganografia - algoritmus založený na zmene posledného bitu každého pixelu v RGB štruktúre
2. Krycia funkcia $COV(1,7,3)$ - krycia funkcia založená na Hammingových kódoch

Vytvorené steganografické obrázky pomocou týchto dvoch algoritmov sú pre úplnosť znázornené na obrázkoch 4.4, 4.5 a 4.6.
Teraz môžeme použiť chi-kvadrát analýzu na jednotlivé obrázky. Algoritmus chi-kvadrát analýzy bol vytvorený v programe MathWorks Matlab a zdrojový kód je možné nájsť v ďalšej prílohe. Výsledky testov môžeme vidieť na obrázkoch 4.7, 4.8 a 4.9.

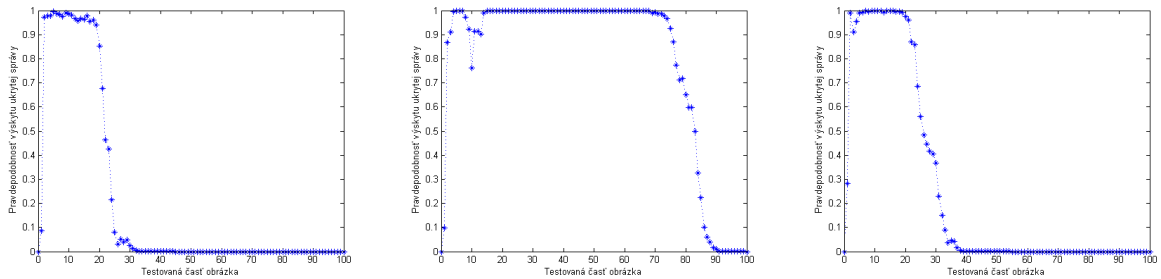


Obr. 4.7: Chi-kvadrát test aplikovaný na médium s vysokým počtom farieb a malým počtom homogénnych oblastí (obrázok 4.4). Postupne zprava je znázornený chi-kvadrát test originálneh obrázka, steganografického obrázka vytvoreného pomocou LSB steganografie a steganografického obrázka vytvoreného pomocu krycej funkcie $COV(1,7,3)$. x-ová os znázorňuje počet pixelov zahrnutých v testovaní (testovaná časť obrázka), a y-ová os ukazuje pravdepodobnosť, že v danej časti obrázka je niečo ukryté (teda pravdepodobnosť výskytu ukrytej správy).

Z chi-kvadrát testu obrázka s vysokým počtom farieb (obrázok 4.4) vidíme, že originálny obrázok nemá predpokladané vlastnosti, ako by sme mali očakávať a teda je možné diskutovať o tom, či tento obrázok nie je steganografický, alebo či je naozaj chi-kvadrát test schopný odhaliť steganografické médium. To ale nie je cieľom tejto prílohy. Z obrázkov je dobre vidieť, že obrázky modifikované pomocou krycej funkcie $COV(1,7,3)$ dosahujú lepších vlastností, čé sa týka chi-kvadrát testu. V podstate sa obidva grafy rezprezentujúce výsledky chi-kvadrát testu u originálneho obrázka a modifikovaného významne



Obr. 4.8: Chi-kvadrát test aplikovaný na homogénne médium. Postupne zprava je znázornený chi-kvadrát test originálneh obrázka, steganografického obrázka vytvoreného pomocou LSB steganografie a steganografického obrázka vytvoreného pomocu krycej funkcie $COV(1, 7, 3)$. x-ová os znázorňuje počet pixelov zahrnutých v testovaní (testovaná časť obrázka), a y-ová os ukazuje pravdepodobnosť, že v danej časti obrázka je niečo ukryté (teda pravdepodobnosť výskytu ukrytej správy).



Obr. 4.9: Chi-kvadrát test aplikovaný na médium s priemernými farbami a homogénnosťou. Postupne zprava je znázornený chi-kvadrát test originálneh obrázka, steganografického obrázka vytvoreného pomocou LSB steganografie a steganografického obrázka vytvoreného pomocu krycej funkcie $COV(1, 7, 3)$. x-ová os znázorňuje počet pixelov zahrnutých v testovaní (testovaná časť obrázka), a y-ová os ukazuje pravdepodobnosť, že v danej časti obrázka je niečo ukryté (teda pravdepodobnosť výskytu ukrytej správy).

nelíšia. Iný prípad nastáva vtedy, keď použijeme klasickú LSB steganografiu. Vtedy, ako už vieme, chi-kvadrát test spoľahlivo odhalí výskyt ukrytej správy na konkrétnom mieste.

Príloha č.4: Chi-kvadrát test

Nasledujúci text reprezentuje zdrojový kód chi-kvadrát testu v programe MathWorks Matlab, ktorý je možné použiť pre analýzu jednotlivých digitálnych obrázkov a hľadanie ukrytej správy.

```
A = double(input_image);
[m,n] = size(A(:,:,2));
percentage = zeros(101,1);
prob = zeros(101,1);
K = zeros(101,1);

%------------------------------------------------------------------------
%------------------------------------------------------------------------

for h=1:100
    k = 128;
    percentage(h) = percentage(h) + h;
    total_pixels = floor((h/100)*m*n);
    whole_rows = floor(total_pixels/n);
    columns_last_row = total_pixels - (whole_rows*n);

    X = zeros(128,1);
    Y = zeros(128,1);
    D = zeros(128,1);

    for q=1:whole_rows
        for r=1:n
            if rem(A(q,r),2) == 0
                X((A(q,r)/2)+1) = X((A(q,r)/2)+1) + 1;
            else
                Y(((A(q,r)-1)/2)+1) = Y(((A(q,r)-1)/2)+1) + 1;
            end
        end
    end

    for q=whole_rows+1
        for r=1:columns_last_row
            if rem(A(q,r),2) == 0
                X((A(q,r)/2)+1) = X((A(q,r)/2)+1) + 1;
            else
                Y(((A(q,r)-1)/2)+1) = Y(((A(q,r)-1)/2)+1) + 1;
            end
        end
    end

    Z = (X + Y);
```

```
    for i=1:128
        if (X(i) + Y(i)) < 5
            X(i) = 0;
            Y(i) = 0;
            k = k - 1;
        end
    end

    Z = Z./2;
    D = (X - Z).^2;

    for i=1:128
        if Z(i) == 0
            D(i) = 0;
        else
            D(i) = D(i)/Z(i);
        end
    end

    format long g;
    C = sum(D);

    Pcheck = 1 - gammainc(C/2, (k-1)/2);
    prob(h) = prob(h) + Pcheck;
    K(h+1) = K(h+1) + k;
end

%-------------------------------------------------------------------------
%-------------------------------------------------------------------------
```

Príloha č.5: Obsah priloženého DVD

Na priloženom DVD na zadnej strane väzby práce môžete nájsť:

- Túto diplomovú prácu v elektronickej podobe vo formáte .PDF.
- Množstvo vedeckých článkov týkajúcích sa steganografie založenej na samoopravných kódoch..
- Zdrojové kódy steganografických algoritmov, ktoré som použil v rámci testovania, a takisto aj vzorové digitálne nosiče.
- Bakalársku prácu "Steganografia a steganoanalýza", na ktorú nadväzuje táto práca.
- Menšiu databázu digitálnych obrázkov, ktoré boli testované pre určenie rôznych vlastností steganografických algoritmov.
- Javovský GUI nástroj "Stegais", pomocou ktorého sa dajú vytvárať steganografické obrázky použitím LSB steganografie a testovať ich pomocou základných steganoanalytických techník.