Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

# BAKALÁRSKA PRÁCA

Petra Fritzová

# Metody komutativní algebry v teorii lineárních kódů

Katedra algebry

Vedúci bakalárskej práce: Mgr. Pavel Příhoda, Ph.D.
Študijný program: Obecná matematika

2010

Na tomto mieste by som chcela poďakovať vedúcemu tejto práce, Mgr. Pavlovi Příhodovi, Ph.D., za ponúknutie zaujímavej témy, konzultácie a pripomienky, ktoré boli veľmi nápomocné, a to po stránke odbornej ako aj motivačnej.

Prehlasujem, že som svoju bakalársku prácu napísala samostatne a výhradne s použitím citovaných prameňov. Súhlasím so zapožičiavaním práce a s jej zverejňovaním.

V Prahe dňa 19. 5. 2010 Petra Fritzová

# Obsah

**1 Úvod** **5**
1.1 Lineárne kódy . . . . . 6
1.2 Ideály a polynómy v komutatívnych okruhoch . . . . . 7

**2 Teória Gröbnerovej báze pre komutatívne okruhy** **11**
2.1 Značenie a základné definície . . . . . 11
2.2 Polynomiálna redukcia . . . . . 15
2.3 Buchbergerov algoritmus . . . . . 17
2.4 Vlastnosti Gröbnerovej báze pri špecializácii . . . . . 18

**3 Odmocninové kódy** **23**
3.1 Počítanie vzdialeností a rozdelenie váh pre odmocninové kódy . . . . . 30
3.2 Polynóm pre detekciu chýb . . . . . 31

Názov práce: Metody komutativní algebry v teorii lineárních kódů
Autor: Petra Fritzová
Katedra: Katedra algebry
Vedúci bakalárskej práce: Mgr. Pavel Příhoda, Ph.D.
e-mail vedúceho: Pavel.Prihoda@mff.cuni.cz

Abstrakt: Trieda lineárnych kódov je obecne veľmi veľká. Avšak nie všetky kódy vlastnia polynóm pre detekciu chýb (napríklad cyklické kódy ho majú). Začneme vstupom do kódovacej teórie, oboznámime sa s teóriou Gröbnerovej báze pre komutatívne okruhy. Ukážeme, že každý binárny kód sa dá napísať ako vlastný odmocninový kód. Nakoniec sa venujeme existencii polynomu pre maximálne vlastné odmocninové kódy.
Kľúčové slová: lineárne kódy, polynóm pre detekciu chýb, Gröbnerova báza

Title: A commutative algebra approach to linear codes
Author: Petra Fritzová
Department: Department of Algebra
Supervisor: Mgr. Pavel Příhoda, Ph.D.
Supervisor's e-mail address: Pavel.Prihoda@mff.cuni.cz

Abstract: The class of linear codes is very wide. However not all of the codes possess general error locator polynomial (f.e. cyclic codes does). We will start with the coding theory and then we will familiarize with the Commutative Gröbner Basis theory. We will find out that every binary code is proper nth-root code. At the end we will take a closer look at polynomial existence for maximal proper nth-root codes.

Keywords: linear codes, general error locator polynomial, Gröbner Basis

# Kapitola 1

# Úvod

Na kód, ako na množinu kódových slov, sa môže postupne vkladať určitá algebraická štruktúra. Tá nám potom umožňuje nie len efektivný popis kódu, ale aj nájdenie dobrých kódov a skúmanie ich vlastností. Kód, ako nijak neštrukturovanú množinu kódových slov, je možné zadať len ich výčtom, čo u veľkého počtu kódových slov môže byť prakticky neuskutočniteľné alebo aspoň velmi neprehľadné. Myšlienka dať kódu štruktúru vektorového priestoru vedie k pojmu lineárneho kódu. Lineárne kódy sa dajú potom popisovať oveľa efektívnejšie ako obyčajné množiny kódových slov, napr. pomocou ich báze.
V prvej kapitole sa budeme venovať lineárnym kódom, ktoré sú v teórii kódovania typom blokového kódu, tj. množiny slov v kódovej abecede majúci pevnú dĺžku, používaným metodami pre detekciu a opravu chýb. Umožňuje realizáciu viac efektivných algoritmov pre kódovanie a dekódovanie než iné kódy. Oboznámime sa s ich základnými definíciami. Uvedieme definíciu polynómu pre detekciu chýb.
Druhá kapitola ma za účel nás oboznámiť s teóriou Gröbnerovej báze pre komutatívne okruhy. Ukážeme si ako sa redukujú polynomy modulo nejakú konečnú množinu polynómov- teda Algoritmus na redukciu. Nasledovať bude Buchbergerov algoritmus, ktorý dokáže rozhodnúť, či je daná množina Gröbnerova báza daného ideálu, a ak nie, tak ju vie nájsť. Uvidíme, ako sa správa Gröbnerova báza pri špecializácii (tzv. dosadzovací homomorfismus).
Tretia kapitola uvedie triedu odmocninových kódov. Bude uvedené napríklad aj ako sa overí, či je daný kód vlastný. Až sa dostaneme k tvrdeniu, že každý binárny kód sa dá napísať ako vlastný odmocninový kód a k tomu ako určiť počet kódových slov danej váhy. Na záver dokážeme vetu, že vlastný odmocninový kód, ktorý neobsahuje nulu vlastní polynóm pre detekciu chýb. Kritérium existencie tohto polynómu nie je pre obecné kódy vôbec známa. V [6] je však dokázaná pre cyklické kódy. Niektoré ich podtriedy ako napríkad Reed-Solomonove a BCH kódy sú veľmi zaujímavé, pretože ich vnútorná štruktúra je dobre známa a majú rýchly dekódovací algoritmus. Takže častokrát sa kódovanie implementuje na základe týchto kódov.

## 1.1 Lineárne kódy

Ukážeme si štruktúru lineárnych kódov ako vektorových priestorov nad nejakým telesom.

- Nech teda máme konečné teleso $F_q$ s $q$ prvkami, kde $q$ je mocnina prvočísla, $n$ je prirodzené číslo, že $NSD(n, q) = 1$ (uvažujme aj naďalej), $1 \leq k \leq N \leq n$, $k$, $n \in \mathbb{N}$
- $(F_q)^N$ je vektorový priestor dimenzie $N$ nad $F_q$

**Definícia 1.1.** *Nech $H$ je $(N-k) \times N$ matica s prvkami z telesa $F_{q^m}$. Množina $C$ všetkých vektorov $c \in (F_q)^N$ takých, že $H \times c^T = 0$ sa nazývá* ***(N,k) lineárny*** *kód nad $F_q$. Prvky $C$ sa nazývajú* ***kódové slová*** *a matica $H$ je* ***paritná matica*** *kódu $C$. Jej stĺpce generujú nad telesom $F_q$ podpriestor dimenzie $N-k$. (V literatúrach sa často používa označenie vektor kódu $C$, namiesto pojmu kódové slovo). Pre $q = 2$, $C$ sa nazýva* ***binárny*** *kód.*

*Matica $G$ $k \times N$, ktorej riadky sú vektory báze kódu $C$, sa nazývá* ***generujúca matica*** *kódu $C$. Ak $C$ je kód s generujúcou maticou $G$, ktorá je v (štadnardnom) tvare $G = (I_k|A)$, kde $I_k$ označuje $k \times k$ jednotkovú maticu, $A$ je nejaká $k \times (N-k)$ matica, tak $H = (-A_t|I_{N-k})$ je paritná matica $C$.*
*Teda:*

- *$N$ je dĺžka kódu $C$ (tzn. dĺžka každého kódového slova v kóde $C$ je $N$)*
- *$k$ je dimenzia kódu $C$, (tzn. generujúca matica má hodnosť $k$; čo je minimálny počet rôznych netriviálnych kódových slov, ktorých je treba na nagenerovanie kódu $C$)*

**Poznámka 1.2.** *Lineárny kód je teda neprázdna množina slov v kódovej abecede, uzavrená na súčet a rozdiel slov a na násobok slova skalárom.*

Pozrieme sa na dalšiu, veľmi dôležitú vlastnosť lineárnych kódov:

**Definícia 1.3.** *Nech x,y sú dva vektory v $(F_q)^N$. Potom:*

1. ***Hammingova vzdialenosť*** *$d(x, y)$ medzi $x$ a $y$ je počet súradníc v ktorých sa $x$ a $y$ odlišujú*
2. ***Hammingova váha*** *$w(x)$ je počet nenulových súradníc vektora $x$*

**Definícia 1.4.** *Nech $C$ je lineárný kód. Číslo*

$$d_C = min_{x,y \in C, x \neq y} d(x, y) = min_{x \in C, x \neq 0} w(c)$$

*sa nazýva (minimálna) vzdialenosť kódu $C$.*

**Poznámka 1.5.** *Keď je jasné, že vravíme o minimálnej vzdialenosti kódu $C$, môže sa užívať namiesto značenia $d_C$ jednoducho $d$. Odteraz bude „kód“ znamenať „lineárny kód“ s $d \geq 2$. Keď má kód $C$ dĺžku $N$, dimenziu $k$ a vzdialenosť $d$, hovoríme, že $C$ je $[N, k, d]$ kód.*

**Definícia 1.6.** *Nech $C$ je $(N, k)$ kód. Označme $A_i = A_i(C)$ počet slov v $C$ váhy $i$. Množina celých čísel $\{A_0, A_1, \ldots, A_N\}$ sa nazýva **rozdelenie váh** pre kód $C$.*

**Definícia 1.7.** *Nech $C \subseteq {F_q}^N$ je $(N, k)$ kód. Pre každé $a \in {F_q}^N$ sa množina*

$$a + C = \{a + x | x \in C\}$$

*volá **rozkladová trieda podľa** $C$.*
*Nech $H$ je paritná matica kódu $C$. Potom vektor $S(y) = Hy^T$ dĺžky $N - k$ sa nazýva **syndróm slova** $y$. Označme $A_i(a + C)$ počet vektorov váhy $i$ v rozkladovej triede $a + C$.*

Pripomeňme si pár informácii, ktoré budú pre nás potrebné:

- $R_n$ budeme uvažovať ako množinu všetkých koreňov polynómu $x^n - 1$, ktoré sa nazývajú n-té odmocniny z jednej a ležia v rozkladovom nadtelese $F_{q^m}$. $R_n$ formuje cyklickú podgrupu $(F_{q^m})^*$
- keď $n = q^m - 1$, korene $x^n - 1$ formujú multiplikatívnu grupu telesa $F_{q^m}$
- $\alpha \in F_{q^m}$ je *primitivná n-tá odmocnina z jednej*, taká že:

$$x^n - 1 = \prod_{i=1}^{n} (x - \alpha^i)$$

## 1.2 Ideály a polynómy v komutatívnych okruhoch

**Definícia 1.8.** *Nech $R$ je komutatívny okruh. Ideál $P$, $P \neq R$ je **prvoideál**, ak pre ľubovoľné dva ideály $I$, $J$ v $R$ platí, že $IJ \subseteq P \Rightarrow I \subseteq P$ alebo $J \subseteq P$.*
*Ideál $I$ okruhu $R$ je **maximálny**, ak pre žiadny ideál $J$ okruhu $R$ neplatí:*
*$I \subsetneq J \subsetneq R$ a $I \neq R$*
*$Spec(R)$ označme množinu všetkých prvoideálov okruhu $R$. $Max(R)$ označme množinu všetkých maximálnych ideálov okruhu $R$.*

Bližie sa tomu venuje [5].

**Tvrdenie 1.9.** *Každý maximálny ideál je prvoideál. Nech $I$ je ideál v $R$. Potom platí:*
*$I$ je prvoideál $\Leftrightarrow$ $R/I$ je obor integrity. $I$ je maximálny $\Leftrightarrow$ $R/I$ je teleso.*

**Definícia 1.10.** *Nech $R \subseteq S$ sú okruhy. Prvok $a \in S$ je* ***celistvý*** *nad $R$, ak je koreňom monického polynómu s koeficientami z $R$. Okruh $S$ je* ***celistvý*** *nad $R$, ak je každý prvok z $S$ celistvý nad $R$.*

**Tvrdenie 1.11.** *Pokud $R \subseteq S$ je celistvé rozšírenie, potom zobrazenie*

$$\varphi : Spec(S) \to Spec(R)$$

*definované vzťahom*

$$\varphi(P) = P \bigcap R$$

*je surjektivné. Naviac $\forall P \in Spec(S)$ je*

$$\varphi(P) \in Max(R) \Leftrightarrow P \in Max(S)$$

**Definícia 1.12.** *$K$ je teleso, $I$ ideál v $K[x_1, \ldots, x_n]$,* ***afinná algebra*** *je okruh tvaru $A = K[x_1, \ldots, x_n]/I$.*

**Definícia 1.13.** *V komutatívnom okruhu $R$, definujeme jeho* ***Krullovu dimenziu****, ako supremum dĺžok ostro rastúcich reťazcov prvoideálov. Krullova dimenzia je stále konečná pre afinnú algebru. (Triviálny okruh uvažujeme za okruh s nulovou Krullovou dimenziou).*

**Poznámka 1.14.** *Teleso $K$ ma Krullovu dimenziu nula, $K[x_1, ..., x_n]$ má Krullovu dimenziu $n$.*

**Definícia 1.15.** *Ideál okruhu $R$, sa nazýva* ***0-dimenzionálny****, ak Krullova dimenzia $R/I$ je nula.*

Dôkaz nasledujúceho tvrdenia sa dá nájsť v [5, Kapitola 2, Corollary 3.8].

**Tvrdenie 1.16.** *Pre afinnú algebru sú nasledujúce podmienky ekvivalentné:*

- *$dim(A) = 0$*
- *$A$ je algebra konečnej dimenzie nad $K$*
- *$Spec(A)$ je konečná*
- *$Max(A)$ je konečná*

**Poznámka 1.17.** *Ak $I$ je 0-dimenzionálny ideál v $K[x_1, \ldots, x_n]$, potom $I \bigcap K[x_2, \ldots, x_n]$ je 0-dimenzionálny ideál v $K[x_2, \ldots, x_n]$. Pretože pre $\bar{I} = I \bigcap K[x_2, \ldots, x_n]$ je $K[x_2, \ldots, x_n]/\bar{I} \hookrightarrow K[x_1, \ldots, x_n]/I$.*

Nech $K$ je teleso a $\bar{K}$ je jeho algebraické rozšírenie, $J$ je ideál v okruhu polynómov $K[Y] = K[y_1, \ldots, y_s], 1 \leq s$.

**Definícia 1.18.** *Buď $f \in K[Y]$, označme $\nu(f)$* ***množinu všetkých koreňov*** *$f$ v $\bar{K}^s$ :*

$$\nu(f) = \{(a_1, \ldots, a_s) \in \bar{K}^s | f(a_1, \ldots, a_s) = 0\}.$$

*Buď $J \subseteq K[Y]$ ideál, označme* ***množinu všetkých koreňov*** *$J$ v $\bar{K}^s$ :*

$$\nu(J) = \{(a_1, \ldots, a_s) \in \bar{K}^s | f(a_1, \ldots, a_s) = 0, \forall f \in J\}.$$

**Definícia 1.19.** *Nech $S \subseteq \bar{K}^s$. Potom množina všetkých polynómov $f \in K[Y]$ takých, že $f(a_1, \ldots, a_s) = 0$ pre všetky body $(a_1, \ldots, a_s) \in S$ formuje ideál v $K[Y]$. Tento ideál nazývame* ***vanishing ideál*** *v $S$ a značíme ho $\Im(S)$.*

Nech $L \subseteq K[Y]$, značíme $(L)$ ideál v $K[Y]$ generovaný $L$.

Pri prenose kódového slova môžu nastať chyby alebo straty. Chyba sa vyskytne keď sa nejaká súradnica slova zmení na iný prvok z daného tělesa a strata nastane keď prijatá súradnica má neznámu hodnotu. Vieme, kde sa vyskytnú straty (pozície strát), ale nevieme, kde nastávajú chyby (pozície chýb). Preto je výhodné zaznamenávať si chyby do vektora (chybový vektor), ktorý dostaneme, keď od prijatého slova odčítame (po zložkách) odoslané slovo.

**Poznámka 1.20.** *Keď pri dekódovacej procedúre pre kód $C$ dokážeme vždy opraviť $\tau$ chýb alebo menej, potom hovoríme, že schopnosť opravy chýb v kóde $C$ je minimálne $\tau$. Písmenom $t$ označujeme maximálnu hodnotu pre $\tau$. Je známe, že $t = \lfloor \frac{d-1}{2} \rfloor$ ($d$ je minimálna vzdialenosť kódu $C$). Navyše, pre každé $\nu$ a $\tau$ prirodzené čísla také, že $2\tau + \nu < d$ vieme, že sme v kóde $C$ schopní opraviť zároveň $\nu$ strát a $\tau$ chýb.*

Uvažujme nasledujúce predpoklady:

Nech $C$ je $[N, k, d]$ kód nad $F_q$, $t$ je schopnosť opravy chýb a $H$ je paritná matica. Nech $d \geq 3$. Syndrómy ležia v $(F_{q^m})^{N-k}$ a formujú vektorový priestor dimenzie $(N - k)$ nad $F_q$. Nech $\alpha$ je primitivná $N$-tá odmocnina z jednej v ${F_q}^m$ taká, že $n = N$. Nech $r = N - k$.

**Definícia 1.21.** *Nech $L_C$ je polynóm v $F_q[X, z]$, kde $X = (x_1, \ldots, x_r)$. Potom $L_C$ je* ***polynóm pre detekciu chýb*** *v $C$ keď*

1. *$L_C(X, z) = z^t + a_{t-1}z^{t-1} + \ldots + a_0$ , $a_j \in F_q[X]$, $0 \leq j \leq t - 1$ také, že $L_C$ je monický polynóm stupňa $t$ s ohľadom na premennú $z$ a koeficienty v $F_q[X]$;*

2. *nech máme syndróm $\boldsymbol{s} = (\bar{s_1}, \ldots, \bar{s_r}) \in (F_{q^m})^{N-k}$, korešpondujúci chybovému vektoru váhy $\mu \leq t$ a pozíciam chýb $\{k_1, \ldots, k_\mu\}$, ak vyhodnotíme premenné $X$ v $\boldsymbol{s}$, potom korene $L_C(\boldsymbol{s}, z)$ sú presne $\{\alpha^{k_1}, \ldots, \alpha^{k_\mu}, \underbrace{0, \ldots, 0}_{t-\mu}\}$.*

**Poznámka 1.22.** *Všimnime si súvislosti z definície:*

- *$L_C$ je monický polynóm stupňa $t$*
- *$t$ je schopnosť opravy chýb*
- *máme $t$ koreňov*
- *chybový vektor má váhu $\mu \leq t$*
- *pozície chýb: $\{k_1, \ldots, k_\mu\}$*

Pre (lineárne) kódy $C$ existencia polynóm pre detekciu chýb nie je známa. Je však dokázaná pre cyklické kódy v [6]. Neskôr sa budeme zaoberať aké to je pre maximálne odmocninové kódy neobsahujúce nulu.

Môžeme rozšíriť Definíciu 9 na prípad s výskytom strát. Nech $2\tau + \nu < d$.

**Definícia 1.23.** *Nech $L$ je polynóm v $F_q[X, W, z]$, kde $X = (x_1, \ldots, x_r)$ a $W = (w_\nu, \ldots, w_1)$, kde $\nu$ je počet strát, ktoré sa vyskytli. Potom $L$ je* ***polynóm pre detekciu chýb typu*** *$\nu$ v $C$ keď:*

1. *$L(X, W, z) = z^\tau + a_{\tau-1}z^{\tau-1} + \ldots + a_0$ , $a_i \in F_q[X, W]$, pre každé $0 \leq j \leq \tau - 1$ také, že $L$ je monický polynóm stupňa $\tau$ s ohľadom na premennú $z$ a koeficienty v $F_q[X, W]$;*
2. *pre každý syndróm $\boldsymbol{s} = (\bar{s}_1, \ldots, \bar{s}_r)$, každý vektor pozícií strát $\boldsymbol{w} = (\bar{w}_1, \ldots, \bar{w}_\nu)$, korešpondujúci chybovému vektoru váhy $\mu \leq \tau$ a pozíciam chýb $\{k_1, \ldots, k_\mu\}$, ak vyhodnotíme premenné $X$ v $\boldsymbol{s}$ a $W$ v $\boldsymbol{w}$, potom korene $L(\boldsymbol{s}, \boldsymbol{w}, z)$ sú $\{\alpha^{k_1}, \ldots, \alpha^{k_\mu}, \underbrace{0, \ldots, 0}_{t-\mu}\}$.*

Keď taký $L$ existuje pre daný kód $C$, budeme ho volať polynóm ${L_C}^\nu$.

Aby sme boli konzistentní s naším značením, $L_C$ je polynóm pre detekciu chýb typu 0, kde zrejme $L_C = {L_C}^0$.
Pre kód $C$ je vlastnenie polynómu pre detekciu chýb ${L_C}^\nu$ typu $\nu$ pre každé $0 \leq \nu \leq d$ môže byť silnejšia podmienka než vlastnenie polynómu pre detekciu chýb $L_C$. Je dokázané v [6], že existuje polynóm pre detekciu chýb typu $\nu$ pre každý cyklický kód, $0 \leq \nu \leq d$.

# Kapitola 2

# Teória Gröbnerovej báze pre komutatívne okruhy

Teória Gröbnerovej báze pre okruhy polynómov bola predstavená Brunom Buchbergerom v roku 1965, ktorý ju pomenoval po jeho poradcovi Wolfgangovi Gröbnerovi. Dnes sú aj s Buchbergerovým algoritmom na hľadanie Gröbnerovej báze dobre známe a široko používané.
Gröbnerove báze sa aplikujú nielen vo výpočtovej algebre, ale tiež vo výpočtovej geometrii (algebraické variety), v kryptografii (napr. pri kryptoanalýze blokových šifier). Keď má systém konečný počet riešení, (v algebraickom uzávere telesa $K$), problém sa dá úplne redukovať na jednoduché výpočty Gröbnerovej báze (s ohľadom na čisto lexikografické usporiadanie), nasledované hľadaním koreňov polynómov s jednou premennou a niekoľkými vyhodnoteniami vo vhodnom algebraickom rozšírení telesa $K$. Prezentácia tohto tématu je prevzaná z [1].

## 2.1 Značenie a základné definície

Nech $\mathbb{N}_0$ značí množinu prirodzených čísel vrátane nuly. $K[x_1, \ldots, x_n]$ značíme komutatívny okruh polynómov v $n$ premenných nad telesom $K$, $n \in \mathbb{N}$. Pre $K[x_1, \ldots, x_n]$, platia nasledujúce fakty:

1. $\forall f \in K[x_1, \ldots, x_n] \setminus \{0\}$, $f = \sum_{i=1}^{t} c_i x_1^{\beta_{i_1}} x_2^{\beta_{i_2}} \cdots x_j^{\beta_{i_j}} \cdots x_n^{\beta_{i_n}}$, kde $t$, $\beta_{i_j} \in \mathbb{N}$, $c_i \in K \setminus \{0\}$, $1 \leq j \leq n$, $1 \leq i \leq t$.

   - $c_i x_1^{\beta_{i_1}} x_2^{\beta_{i_2}} \cdots x_j^{\beta_{i_j}} \cdots x_n^{\beta_{i_n}}$ sa nazýva **term**,
   - $c_i$ je **koeficient termu**,
   - $x_1^{\beta_{i_1}} x_2^{\beta_{i_2}} \cdots x_j^{\beta_{i_j}} \cdots x_n^{\beta_{i_n}}$ je **monóm**,
   - $deg(m) = \sum_{j=1}^{n} \beta_{i_j}$ je **stupeň monómu** $m$.

Množinu všetkých monómov v $n$ premenných značíme $M_n$ alebo jednoducho $M$, keď nie je dôležité zdôrazniť $n$. Pre $\forall j, 1 \leq j \leq n$ je $x_j^0 = 1 \in M$.
Máme $m_1, m_2 \in M$, keď $\exists m_3$ také, že $m_2 = m_3 m_1$, hovoríme $m_2$ je **násobok** $m_1$, alebo $m_1$ **delí** $m_2$, čo značíme $m_1 | m_2$.

2. $\forall f \in K[x_1, \ldots, x_n] \backslash \{0\}$, po rôznych úpravách sa dá dosiahnuť, aby sme napísali $f$ v tomto tvare

$$f = \sum_{i=1}^{t} c_i m_i, \tag{2.1}$$

ktorý budeme nazývať **jednoznačná forma**, kde $t \in \mathbb{N}$, $c_i \in K \setminus \{0\}$, $m_i \in M$, $m_i \neq m_j$, $\forall 1 \leq i \neq j \leq t$.

**Definícia 2.1.** *$\leq$ je **monické usporiadanie** na množine všetkých monómov $M$, ak vyhovuje nasledujúcim podmienkám:*

- *$M$ je úplne usporiadaná s ohľadom na $\leq$,*
- *$1 \leq m, \forall m \in M$,*
- *$m_1 \leq m_2 \Rightarrow m m_1 \leq m m_2, \forall m, m_1, m_2 \in M$.*

*Nech $\leq$ je monické usporiadanie na $M$, predpokladajme, že $m_1, m_2, m_3 \in M, m_2 = m_3 m_1$, podľa predošlých podmienok je $1 \leq m_3$, $m_1 \leq m_3 m_1 = m_2$. Preto môžeme povedať $m_1 | m_2 \Rightarrow m_1 \leq m_2$. Toto ukazuje, že relácia monického usporiadania je rozšírením relácie delenia.*

**Príklad 2.2.** *Nech $\leq_N$ je prirodzené usporiadanie na $\mathbb{N}_0$. Následujúce tri monické usporiadania sú najčastejšie využívané:*

1. *Lexikografické usporiadanie (skrátene **lex**) na $M$ s $x_1 > x_2 > \cdots > x_n$. Platí: $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} < x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n} \Leftrightarrow \alpha_1 = \beta_1, \alpha_2 = \beta_2, \ldots, \alpha_l = \beta_l, \alpha_{l+1} <_N \beta_{l+1}$, pre nejaké $l$.*

2. *Stupňovo lexikografické usporiadanie (skrátene **deglex**) na $M$ s $x_1 > x_2 > \cdots > x_n$. Platí: $\forall m_1, m_2 \in M, m_1 < m_2 \Leftrightarrow$ buď $deg(m_1) <_N deg(m_2)$ alebo $deg(m_1) = deg(m_2)$ a $m_1 <_{lex} m_2$, kde $<_{lex}$ je lexikografické usporiadanie s $x_1 > x_2 > \cdots > x_n$.*

3. *Stupňovo opačné lexikografické usporiadanie (skrátene **degrevlex**) na $M$ s $x_1 > x_2 > \cdots > x_n$. Nech $m_1 = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}, m_2 = x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$, potom $m_1 < m_2 \Leftrightarrow$ buď $deg(m_1) <_N deg(m_2)$ alebo $deg(m_1) = deg(m_2)$ a $\alpha_n = \beta_n, \alpha_{n-1} = \beta_{n-1}, \ldots, \alpha_l = \beta_l, \alpha_{l-1} >_N \beta_{l-1}$, pre nejaké $l$.*

Každý nenulový polynóm $f$, môžeme napísať v uni forme (2.1). Nech $M$ je totálne usporiadaná nejakým monickým usporiadaním $\leq$, zrejme existuje permutácia na termoch v (2.1) taká, že $f = \sum_{i=1}^{t} c_i m_i$ a $m_1 > m_2 > \cdots > m_t$. V tomto prípade voláme:

- $lt(f) = c_1 m_1$ je vedúci term,
- $lm(f) = m_1$ je vedúci monóm,
- $lc(f) = c_1$ je vedúci koeficient $f$.

**Definícia 2.3.** *Nech $I \subseteq K[x_1, \ldots, x_n]$ je ideál.*
*Definujeme **ideál vedúcich monómov** ideálu $I$ s ohľadom na usporiadanie $\leq$ :*

$$lm(I) := (lm(f)|f \in I) = \{\sum_{i=1}^{t} g_i lm(f_i)|t \in \mathbb{N}, g_i \in K[x_1, \ldots, x_n], f_i \in I\}$$

**Definícia 2.4.** *Nech máme monické usporiadanie na $M$, nech $I \subset K[x_1, \ldots, x_n]$ je ideál. **Gröbnerova báza** ideálu $I$ je množina polynómov*

$$\{f_1, \ldots, f_k\} \subset I$$

*taká, že*

$$lm(I) = (lm(f_1), \ldots, lm(f_k)).$$

**Poznámka 2.5.** *(i) Vidíme, že ak $\{f_1, \ldots, f_k\}$ je Gröbnerova báza ideálu $I$, potom $\{f_1, \ldots, f_k\} \subset I$, no zatiaľ nie je jasné, či sa tieto dva ideály rovnajú, t.j. či Gröbnerova báza naozaj generuje ideál $I$.*

*(ii) Gröbnerova báza má rôzne charakteristiky a každá charakteristika môže byť braná za definíciu.*

*(iii) Nech $I \subset K[x_1, \ldots, x_n]$ je hlavný ideál, teda $I = (f), f \in K[x_1, \ldots, x_n]$. Každý polynóm $g \in I$ je násobkom polynómu $f$, t.j. $g = hf$ pre nejaké $h \in K[x_1, \ldots, x_n]$. Keďže každé usporiadanie monómov je kompatibilné s násobením, platí $lm(g) = lm(h)lm(f)$, a teda $lm(g) \in (lm(f))$. Teda máme, že $lm(I) = (lm(f))$, preto generátor hlavného ideálu je aj jeho Gröbnerovou bázou vzhľadom na ktorékoľvek usporiadanie monómov.*

*(iv) Gröbnerova báza závisí na zvolenom monickom usporiadaní, pri rôznych usporiadaniach môže vyzerať úplne rozdielne pre rovnaký ideál. Najčastejšie sa používajú lex a degrevlex. Pri lexikografickom usporiadaní sa eliminujú premenné, ale výsledná Gröbnerova báza je väčšinou veľmi veľká a tažko sa s ňou počíta. Avšak stupňovo opačné lexikografické usporiadanie nám typicky poskytuje najrýchlejšie výpočty s Gröbnerovou bázou.*

Pozrime sa na nejaké základné výsledky.
Nech $R$ označuje komutatívny okruh.

**Definícia 2.6.** *Povieme, že okruh $R$ je **Noetherovský**, ak spĺňa rastúcu reťazovú podmienku (ACC- ascending chain condition) na ideáloch, t.j. neexistuje nekonečný ostro rastúci reťazec ideálov.*

**Definícia 2.7.** *Ideál $I$ v okruhu $R$ je* ***konečne generovaný****, ak $\exists a_1, a_2, \ldots, a_s \in I$ také, že $I = (a_1, a_2, \ldots, a_s) = \{\sum_{i=1}^{s} r_i a_i | r_i \in R\}$.*

**Lemma 2.8.** *Okruh $R$ je Noetherovský $\Leftrightarrow$ každý ideál v $R$ je konečne generovaný.*

**Veta 2.9.** *(Hilbertova veta o báze) Ak $R$ je Noetherovský $\Rightarrow R[x]$ je Noetherovský.*

Je dobré si povšimnúť, že $K[x_1, \ldots, x_n] = K[x_1, \ldots, x_{n-1}][x_n]$ pre $\forall n \in \mathbb{N}$ a teleso $K$ je triviálne Noetherovské, rekurzívnym aplikovaním Hilbertovej vety o báze vidíme, že okruh polynómov $K[x_1, \ldots, x_n]$ je Noetherovský pre $\forall n \in \mathbb{N}$. Skombinovaním tohoto dôsledku s Lemma 2.8, dostávame nasledujúcu vetu.

**Veta 2.10.** *$\forall n \in \mathbb{N}$ je okruh polynómov $K[x_1, \ldots, x_n]$ Noetherovský a každý ideál v $K[x_1, \ldots, x_n]$ je konečne generovaný.*

**Dôsledok 2.11.** *Nech $I$ je nenulový ideál v $K[x_1, \ldots, x_n]$, predpokladajme, že $I$ je generovaný neprázdnou množinou $S$, potom $\exists$ konečná $S' \subseteq S$ taká, že $I = (S) = (S')$*

**Veta 2.12.** *(Dicksonovo Lemma) Nech $S$ je neprázdna množina monómov v $K[x_1, \ldots, x_n]$, potom $\exists$ konečná $S' \subseteq S$ taká, že $(S) = (S')$ alebo ekvivalentne povedané, $\exists$ konečná $S' \subseteq S, \forall m \in S, \exists m' \in S'$ také, že $m$ je násobok $m'$.*

**Veta 2.13.** *(Existencia Gröbnerovej báze pre ideály) Nech máme nejaké monické usporiadanie $\leq$ na $M$. Pre každý nenulový ideál $I$ v $K[x_1, \ldots, x_n]$, existuje nejaká konečná $G \subset I$ taká, že $lm(G) = lm(I)$.*

*Dôkaz.* Podľa definície $lm(I) = (S)$, kde $S = \{lm(f) | f \in I\}$. Podľa Dicksonovho Lemma $\exists$ konečná $S' = \{lm(f_1), lm(f_2), \ldots, lm(f_l)\} \subset S$, že $(S) = (S')$.
Nech $G = \{f_1, f_2, \ldots, f_l\}$, zrejme $G \subset I$, $lm(G) = lm(I)$. $\square$

**Veta 2.14.** *Každé monické usporiadanie $\leq$ na $M$ je dobré usporiadanie.*

**Veta 2.15.** *Nech $\leq$ je monické usporiadanie na množine všetkých monómov $M$ a nech $I$ je ideál v $K[x_1, \ldots, x_n]$. Ak pre konečnú množinu $G$ platí $G \subset I$, $lm(G) = lm(I)$ (takže $G$ je Gröbnerova báza pre ideál $I$), potom $I = (G)$.*

*Dôkaz.* Nech máme daný $f \in I \setminus \{0\}$. Postupujme následujúco:
Nech $f_1 = f$, $f_1 \in I$, $lm(f_1) \in lm(I) = lm(G) \Rightarrow \exists g_1 \in G \subseteq I$, $q_1 \in M$, $c_1 \in K \setminus \{0\}$ také, že $lt(f_1) = lt(c_1 g_1 q_1)$.
Nech $f_2 = f_1 - c_1 g_1 q_1$, zjavne $f_2 \in I$, keď $f_2 \neq 0$, $lm(f_2) \in lm(I) = lm(G) \Rightarrow \exists g_2 \in G \subseteq I$, $q_2 \in M$, $c_2 \in K \setminus \{0\}$ také, že $lt(f_2) = lt(c_2 g_2 q_2)$.
Nech $f_3 = f_2 - c_2 g_2 q_2$, keď $f_3 \neq 0, \ldots$
Povšimnime si, že $lm(f_1) > lm(f_2) > lm(f_3) > \ldots$. Tento proces musí skončiť, pretože monické usporiadanie $\leq$ je dobré usporiadanie. Navyše, posledné $f_l$ musí

byť nula, inak by sme boli schopný urobiť ďalší krok v našom procese a dostali by sme $f_{l+1}$. Preto máme

$$0 = f_l = f_{l-1} - c_{l-1}g_{l-1}q_{l-1} = f_{l-2} - c_{l-2}g_{l-2}q_{l-2} - c_{l-1}g_{l-1}q_{l-1} = \ldots = f_1 - \sum_{i=1}^{l-1} c_i g_i q_i.$$

Takže $f = f_1 = \sum_{i=1}^{l-1} c_i g_i q_i \in (G)$. To implikuje $I \subset G$. Je zrejmé: $G \subset I$. Tým pádom $I = (G)$. □

## 2.2 Polynomiálna redukcia

Predpokládajme, že monické usporiadanie $\leq$ je definované na $M$.

**Definícia 2.16.** *Pre každé $f, g \in K[x_1, \ldots, x_n]$, ak $lm(g)$ delí nejaký nenulový term $cm$ v $f$, nech $h = f - \frac{cm}{lt(g)}g$, potom je ľahko vidieť, že term $cm$ je v $f$ nahradený lineárnou kombináciou monómov $< m$. Túto manipuláciu nazývame* ***polynomiálna redukcia****, značená $f \xrightarrow{g} h$ a hovoríme, že $f$ sa redukuje na $h$ modulo $g$.*

**Definícia 2.17.** *Ak máme konečnú postupnosť polynomiálnych redukcií $f \xrightarrow{g_1} h_1 \xrightarrow{g_2} h_2 \ldots \xrightarrow{g_t} h_t$, kde $g_i \in$ konečnej množine $G \subseteq K[x_1, \ldots x_n]$ a $g_i$ nie sú nutne po dvoch rôzne pre $1 \leq i \leq t$, hovoríme, že $f$ sa redukuje na $h_t$ modulo $G$, označujeme $f \xrightarrow{G} h_t$.*

**Definícia 2.18.** *Polynóm $r$ sa nazýva* ***redukovaný*** *alebo* ***v redukovanej forme*** *s ohľadom na konečnú množinu $G \subseteq K[x_1, \ldots, x_n]$, ak $r = 0$ alebo žiaden monóm vyskytujúci sa v jednoznačnej forme $r$ nie je deliteľný monómom $lm(g), \forall g \in G$ (tzn. $lm(r) \notin lm(G)$). Vravíme, že $f$ je redukovateľný modulo $G$, ak $f \neq 0$ a $lm(f) \in lm(G)$. Ak $f \xrightarrow{G} r$ a $r$ je redukovaný s ohľadom na $G$, hovoríme, že $r$ je* ***v redukovanej forme*** *$f$ s ohľadom na $G$.*
*Ak redukovaná forma $f$ s ohľadom na $G$ je jednoznačná, označíme ju $R(f, G)$.*
*Vo všeobecnosti, keď $f$ je redukovaný s ohľadom na $G$, $R(f, G) = f$.*

**Poznámka 2.19.** *V našej Definícii polynomiálnej redukcie, predpokladáme, že $g$ je v jednoznačej forme, ale $f$ nie je. Vo všeobecnosti nevyžadujeme, aby polynóm, ktorý má byť redukovaný, mal byť zadaný v jednoznačnej forme. Ale v prípade, že potrebujeme uvažovať vedúci monóm $f$ ako bude v príklade za Algoritmom na redukciu, budeme predpokladať $f$ v jednoznačnej forme.*

**Tvrdenie 2.20.** *Keď $G$ je Gröbnerova báza pre $I \subset R$, potom $f \in I$ práve keď $f$ sa redukuje na nulu modulo $G$.*

**Tvrdenie 2.21.** *Nech máme polynóm $f$ a $r$, ak $r$ je redukovaná forma $f$ s ohľadom na nejakú $G$, potom buď $f = r$ alebo $\exists s \in \mathbb{N}$, $c_u \in K \setminus \{0\}$, $m_u \in M$, $g_u \in G$ a nie nevyhnutne po dvoch rôzne $u$, $1 \leq u \leq s$ také, že*

$$f = \sum_{u=1}^{s} c_u g_u m_u + r. \tag{2.2}$$

**Algoritmus na redukciu** Nech máme nenulový polynóm $f$ a konečnú $G = \{g_1, \ldots, g_j, \ldots, g_l\} \subseteq K[x_1, \ldots, x_n]$, nasledujúci algoritmus nám ukáže jednu cestu, ako môžeme počítať redukovanú formu $f$ s ohľadom na $G$.

$i := 1, r := 0, f_i := f$
(*) while $f_i \neq 0$ do
if $\exists j$, že $lm(g_j)|lm(f_i)$, then vyber najmenšie $j$ také, že
$lm(g_j)|lm(f_i)$ and do
$f_{i+1} := f_i - \frac{lt(f_i)}{lt(g_j)} g_j$
$i := i + 1$ and goto (*)
else $r := r + lt(f_i)$
$f_{i+1} := f_i - lt(f_i)$
$i := i + 1$ and goto (*)

**Poznámka 2.22.** *(i) Všimnime si, že v algoritme platí $lm(f_i) > lm(f_{i+1}) \forall i$, lebo monické usporiadanie $\leq$ je dobré usporiadanie, algoritmus musí skončiť. Navyše, ak skončí na nejakom $i = t$, $f_t$ musí byť nula a žiaden monóm vyskytujúci sa v konečnom $r$ nie je deliteľný žiadnym $lm(g), g \in G$. Teda konečné $r$ je redukovaná forma $f$ s ohľadom na $G$.*

*(ii) Nie je ťažké si všimnúť, že algoritmus vyprodukuje $f$ v následujúcej forme:*

$$f = \sum_{u=1}^{s} c_u g'_u m_u + r, \tag{2.3}$$

*kde $s \in \mathbb{N}$ (keď $s = 0$, $f = r$), $c_u \in K \setminus \{0\}$, $m_u \in M$, $g'_u \in G$ a nie nevyhnutne po dvoch rôzne $u, 1 \leq u \leq s$, $r$ je redukovaná forma $f$ s ohľadom na $G$ a $lm(f) = max\{lm(g'_1)m_1, lm(g'_2)m_2, \ldots, lm(g'_s)m_s, lm(r)\}$. (Porovnaj s (2.2)) Vo všeobecnosti, keď $r = 0$, tak sa predchádzajúcej reprezentácii hovorí, že je* ***štandardná reprezentácia*** *$f$ s ohľadom na $G$.*

*(iii) V algoritme si vždy vyberáme najmenšie $j$ také, že $lm(g_j)|lm(f_i)$. To implikuje, že keď zmeníme indexy poradia prvkov v $G$, konečné vyprodukované $r$ sa môže taktiež zmeniť, pretože redukovaná forma polynómov s ohľadom na $G$ nemusí byť jednoznačná.*

**Príklad 2.23.** *Nech $f = x_1^2 x_2^3$, $G = \{x_1^2, x_1x_2 - x_2^2\}$, $\leq$ je lex s $x_1 > x_2$. Aplikujme Algoritmus na redukciu. Máme*

$$f \xrightarrow{x_1^2} x_1^2 x_2^3 - x_1^2 x_2^3 = 0, \tag{2.4}$$

*keď $G = \{g_1 = x_1^2, g_2 = x_1x_2 - x_2^2\}$; alebo*

$$f \xrightarrow{x_1x_2 - x_2^2} x_1^2 x_2^3 - (x_1x_2 - x_2^2)x_1x_2^2 = x_1x_2^4 \xrightarrow{x_1x_2 - x_2^2} x_1x_2^4 - (x_1x_2 - x_2^2)x_2^3 = x_2^5, \tag{2.5}$$

*keď* $G = \{g_1 = x_1x_2 - x_2^2, g_2 = x_1^2\}$. 0 *a* $x_2^5$ *sú dve odlišné redukované formy* $f$ *s ohľadom na* $G$.
*Navyše, z rovnosti (2.4) vidíme, že* $f \in (G)$ *a z (2.5) vidíme, že* $x_2^5 = f - (x_1x_2 - x_2^2)x_1x_2^2 - (x_1x_2 - x_2^2)x_2^3 \in (G)$, $x_2^5$ *je redukované s ohľadom na* $G$. *Potom je* $x_2^5$ *v* $lm((G))$, *ale nie v* $lm(G)$. *To implikuje, že* $G$ *nie je Gröbnerova báza.*

## 2.3 Buchbergerov algoritmus

Nech $m_1m_2 \in M$, vieme, že existuje najmenší spoločný násobok $m_1$ a $m_2$, označovaný $lcm(m_1, m_2)$, že $m_1|lcm(m_1, m_2)$, $m_2|lcm(m_1, m_2)$, $\forall m \in M$: $m_1|m$, $m_2|m$, $lcm(m_1, m_2)|m$.

**Definícia 2.24.** *Nech* $f, g \in K[x_1, \ldots, x_n] \setminus \{0\}, L = lcm(lm(f), lm(g))$, *potom*

$$S(f, g) = \frac{L}{lt(f)}f - \frac{L}{lt(g)}g$$

*sa nazýva* ***S-polynóm*** $f, g$. *Zjavne* $S(g, f) = -S(f, g)$.

**Veta 2.25.** *(Charakterizácia Gröbnerovej báze.) Nech* $G = \{g_1, \ldots, g_j, \ldots, g_l\} \subseteq K[x_1, \ldots, x_n]$, *je konečná* $g_j \neq 0$ *pre* $\forall j = 1, 2, \ldots, l$, *nech* $I = (G)$, *nech* $\leq$ *je monické usporiadanie na* $M$. *Nasledujúce podmienky sú ekvivaletné:*

**(a)** $lm(G) = lm(I)$;

**(b)** $\forall f \in I \setminus \{0\}, \exists j \in \{1, 2, \ldots, l\}$, *že* $lm(g_j)|lm(f)$;

**(c)** $f \in I \Leftrightarrow R(f, G) = 0$;

**(d)** $f \in I \Leftrightarrow f$ *má štandardnú reprezentáciu s ohľadom na* $G$;

**(e)** $\forall f \in K[x_1, \ldots, x_n]$, *redukovaná forma* $f$ *s ohľadom na* $G$ *je jednoznačná;*

**(g)** $\forall g_1', g_2' \in G, R(S(g_1', g_2'), G) = 0$;

**(h)** $\forall g_1', g_2' \in G, S(g_1', g_2')$ *má štandardnú reprezentáciu s ohľadom na* $G$.

**Poznámka 2.26.** *Môžeme pridať nejaké podmienky pre* $G$ *také, že Gröbnerova báza ideálu* $I$ *je jednoznačná s ohľadom na ideál* $I$ *a monické usporiadanie* $\leq$. *Takáto sa nazýva* ***redukovaná Gröbnerova báza***.

Nech máme danú konečnú množinu $G = \{g_1, \ldots, g_j, \ldots, g_l\} \subseteq K[x_1, \ldots, x_n]$, $g_j \neq 0$, pre $\forall j = 1, 2, \ldots, l$, nech $I = (G)$ je ideál generovaný množinou $G$, nech $\leq$ je monické usporiadanie na $M$. Príklad (2.23) ukazuje, že $G$ nemusí byť nutne Gröbnerova báza ideálu $I$. Avšak Vety (2.13) a (2.15) nám ukazujú, že existuje nejaká konečná $G' \subseteq I$, že $I = (G')$ a $lm(G') = lm(I)$.
V nasledujúcej časti si predstavíme Buchbergerov algoritmus, ktorý dokáže rozhodnúť,

či daná $G(= G_1)$ je Gröbnerova báza ideálu $I$ a ak nie je, tak ju nájde : $G'(= G_i)$.

**Buchbergerov algoritmus**

$i := 1, G_1 := \{g_1, \ldots, g_l\}$,
$H := \{(g_{j_1}, g_{j_2}) | g_{j_1}, g_{j_2} \in G, 1 \leq j_1 < j_2 \leq l\}$
(*) while $H \neq \emptyset$ do
vyber $(g'_{t_1}, g'_{t_2})$, potom $H := H - \{(g'_{t_1}, g'_{t_2})\}$
rob Algoritmus na redukciu, aby si vypočítal redukovanú formu
$S(g'_{t_1}, g'_{t_2})$ s ohľadom na $G_i$
ak $r \neq 0$ potom
$H := H \bigcup \{(g, r) | g \in G_i\}$
$G_{i+1} := G_i \bigcup \{r\}$
$i := i + 1$
goto (*)

**Tvrdenie 2.27.** *Buchbergerov algoritmus skončí pre nejaké $i$, $i \geq 1$ a konečná $G_i$ je Gröbnerova báza ideálu $(G_1)$.*

## 2.4 Vlastnosti Gröbnerovej báze pri špecializácii

Budeme označovať $K$ teleso, nejakej charakteristiky, $\bar{K}$ jeho algebraický uzáver. $R = K[x_1, \ldots, x_n, y_1, \ldots, y_m] = K[\bar{X}, \bar{Y}]$ bude okruh polynómov v $m + n$ premenných s koeficientmi v $K$. Špecializácia budeme volať každý homomorfismus $\varphi : R \longmapsto \bar{K}[\bar{X}]$ taký, že $\varphi(K[\bar{Y}]) \subset \bar{K}$ a $\varphi(x_i) = x_i, \forall x_i$. Uvedené vlastnosti Gröbnerovej báze pri špecializácii dokazáli nezávisle M. Kalkbrener a P. Gianni. Teraz postupujeme podľa [2].

**Príklad 2.28.** *Nech $\alpha = (a_1, \ldots, a_m) \in \bar{K}^m$, dosadzovací homomorfismus $\varphi_\alpha(f(\bar{X}, \bar{Y})) = f(\bar{X}, \alpha)$ je špecializácia.*

**Definícia 2.29.** *Buď $>$ usporiadanie na monómoch v $R$, ak $f \in K[\bar{X}, \bar{Y}], f \neq 0$, môžeme písať $f = c\bar{X}^A\bar{Y}^B + f', A \in {\mathbb{N}_0}^n, B \in {\mathbb{N}_0}^m, c \in K, c \neq 0, \bar{X}^A\bar{Y}^B$ najväčší monóm v $f$. Definujeme:*

$$lt(f) = c\bar{X}^A\bar{Y}^B, \textbf{\textit{vedúci term}}$$

$$deg(f) = (A, B) \in {\mathbb{N}_0}^{n+m}, \textbf{\textit{stupeň}}.$$

*Pre podmnožinu $G \subset R$ definujeme pre $g \in G$:*
*$Lt(G)$ je ideál generovaný $lt(g)$, **ideál vedúcich termov** v $G$.*

**Definícia 2.30.** *Nech $\varphi$ je špecializácia, hovoríme, že usporiadanie $>$ na monómoch v $R$ je **$\varphi$-prípustné**, ak všetky $x_i$ sú väčšie než každé $y_j$. Keď označíme $>_1$ (resp. $>_2$) zúženie na usporiadanie na premenné $\bar{X}$ (resp. na premenné $\bar{Y}$), $>$ je $\varphi$-prípustné,*

*ak vyhovuje nasledujúcej podmienke:*
$\bar{X}^A\bar{Y}^B > \bar{X}^C\bar{Y}^D \Leftrightarrow \bar{X}^A >_1 \bar{X}^C$ *alebo* $\bar{X}^A = \bar{X}^C$ *a* $\bar{Y}^B >_2 \bar{Y}^D$,
$\forall A, C \in {\mathbb{N}_0}^n, B, D \in {\mathbb{N}_0}^m$.

Odteraz budeme uvažovať $\varphi$-prípustné usporiadanie na monómoch v $R$.

**Definícia 2.31.** $\forall f \in R, f \neq 0$, *píšeme* $f = c(\bar{Y})\bar{X}^A + f', c(\bar{Y}) \in K[\bar{Y}], c \neq 0$ *a* $\bar{X}^A$ *najväčší monóm v* $\bar{X}$ *objavujúci sa v* $f$, *definujeme:*

$$lt_\varphi(f) = c\bar{Y}^A, \textbf{\textit{vedúci term}}, \textit{(s ohľadom na } \varphi\textit{)}$$

$$deg_{\bar{X}}(f) = A, \textbf{\textit{stupeň}}\ f, \textit{(s ohľadom na } \varphi\textit{).}$$

*Pre podmnožinu* $G \subset R$ *definujeme:*
$Lt_\varphi(G) = (lt_\varphi(g))$, *pre* $g \in G$, ***ideálu vedúcich termov*** *v* $G$ *(s ohľadom na* $\varphi$*).*

**Príklad 2.32.** *Nech* $f \in K[x, y], (n = 1, m = 1), f(x, y) = x^2y^2 + x^2 + xy + 1$. *Ak uvažujeme lexikografické usporiadanie, máme:*
$lt(f) = x^2y^2$
$lt_\varphi(f) = (y^2 + 1)x^2$

Ak $G$ je Gröbnerova báza s ohľadom na $\varphi$-prípustné usporiadanie , potom $Lt_\varphi(G)$ má nasledujúce vlastnosti.

**Poznámka 2.33.** *Ak* $G$ *je Gröbnerova báza pre ideál* $I \subset R$, *potom:*

$$Lt_\varphi(G) = Lt_\varphi(I).$$

*K dôkazu v [2].*

**Poznámka 2.34.** *Pre každú špecializáciu* $\varphi$ *a každý ideál* $I$ *máme*

$$\varphi(Lt_\varphi(I)) \subseteq Lt(\varphi(I)).$$

**Veta 2.35.** *Nech* $I \subset R$ *je ideál,* $\varphi$ *špecializácia,* $G$ *Gröbnerova báza pre* $I$ *(s ohľadom na* $\varphi$*-prípustné usporiadanie). Za predpokladu:*

$$Lt(\varphi(I)) = \varphi(Lt_\varphi(I))$$

*je* $\varphi(G)$ *Gröbnerova báza pre* $\varphi(I)$.

*Dôkaz.* Z predošlej Poznámky a predpokladu máme:

$$Lt(\varphi(I)) = \varphi(Lt_\varphi(I)) = \varphi(Lt_\varphi(G)) \subseteq Lt(\varphi(G)) \subseteq Lt(\varphi(I)).$$

Takže $Lt(\varphi(G)) = Lt(\varphi(I))$ a $\varphi(G)$ je Gröbnerova báza pre $\varphi(I)$. □

**Poznámka 2.36.** *Podmienka vo Vete 2.35 je len postačujúca. V príklade budeme mať špecializáciu, ktorá neuchováva vedúci term, hoci obraz Gröbnerovej báze ostáva Gröbnerova báza.*

**Príklad 2.37.** *Uvažujme ideál* $I = ({x_1}^2 y + x_1 x_2)$. *Ak ohodnotíme premenné y nulou, dostaneme* $\varphi(I) = (x_1 x_2), Lt(\varphi(I)) = (x_1 x_2)$, *zatiaľ čo* $\varphi(Lt(\varphi(I))) = (0)$.

**Definícia 2.38.** *Nech R je komutatívny okruh,* $I \subseteq R$ *ideál. Hovoríme, že I je* ***primary****, ak* $I \neq R$, $\forall a, b \in R$: $ab \in I$, $a \notin I \Rightarrow \exists n \in \mathbb{N}$,*že* $b^n \in I$.
$\sqrt{I} = rad(I) = \{x \in R | \exists n \in \mathbb{N},\ x^n \in I\}$ *je ideál, ktorý nazývame radikál I.*

Zakladné vlastnosti primary ideálu nájdeme napriklad v [5, Kapitola 5, sekcia 4]. Pre nás bude dôležité následujúce:

**Tvrdenie 2.39.** *(i) I je primary* $\Rightarrow \sqrt{I}$ *je prvoideál.*

*(ii) R je komutatívny okruh* $\Rightarrow \sqrt{I}$ *je prienik všetkých prvoideálov obsahujúcich I.*

*(iii) Nech I je* 0*-dimenzionálny,* $I \neq R$. *Potom I je primary* $\Leftrightarrow$ *I je v práve jednom maximálnom ideále.*

*(iv) I je* 0*-dimenzionálny primary a* $I \subseteq K \neq R \Rightarrow K$ *je v práve jednom maximálnom ideále.*

*(v) Keď R je Noetherovský okruh, potom sa dá každý jeho ideál I napísať* $I = \bigcap_{i=1}^{k} I_i$ *(konečný prienik),* $\forall I_i$ *je primary,* $\sqrt{I_i} \neq \sqrt{I_j}$, $i \neq j$.

**Lemma 2.40.** *Nech* $I_1 \neq I_2$ *sú primary* 0*-dimezionálne ideály také, že* $\sqrt{I_1} \neq \sqrt{I_2}$ $\Rightarrow I_1 + I_2 = R$.

*Dôkaz.* Sporom. Nech $I_1 + I_2 \neq R$, potom existuje maximálny ideál $P$ obsahujúci $I_1 + I_2$. Podľa predošlého tvrdenia (iii),(iv) musí byť $P = \sqrt{I_1} = \sqrt{I_2}$. Spor. □

**Lemma 2.41.** *Nech* $\bar{K}$ *je algebraický uzáver K. Potom* $I \subseteq K[x_1, \ldots, x_n]$ *je* 0*-dimenzionálny* $\Leftrightarrow \nu(I) = \{(r_1, \ldots, r_n) \in \bar{K}^n | \forall f \in I f(r_1, \ldots, r_n) = 0\}$ *je konečná.*

Uvažujme teraz nula-dimenzionálny ideál $I = (f_1, \ldots, f_s)$, (teda ideál taký, že systém určený polynómami $f_i$ má konečný počet riešení) a špecializáciu $\varphi$, ktorá špecializuje všetky premenné okrem jednej takto: $\varphi : K[x, y_1, \ldots, y_m] \longmapsto \bar{K}[x]$. S týmito hypotézami máme:

**Veta 2.42.** *Existuje polynóm* $g \in I$, *že:*
$\varphi(g)$ *generuje* $\varphi(I)$, $deg_x(g) = deg_x(\varphi(g))$.

*Dôkaz.* Najprv sa zameriame na primárne nula-dimenzionálne ideály. $G$ je redukovaná Gröbnerova báza pre $I$ (s ohľadom na lexikografické usporiadanie) (taká existuje [3]), máme:

$$G = (g_{01}, \ldots, g_{0s_0}, g_{11}, \ldots, g_{1s_1}, \ldots, g_{n1}),$$

kde (pre jednoduchosť označenia budeme užívať $y_0$ namiesto $x$):

$$g_{i1} \in G \cap K[y_i, \ldots, y_m]$$

je monický polynóm v $y_i, \forall i$

$$g_{ij} \equiv 0 \pmod{\sqrt{G \cap K[y_{i+1}, \ldots, y_m]}}, \forall i,$$

pre $j > 0$.

Rozlíšime dva prípady:

1. $\exists g_{ij} \in G \cap K[y_i, \ldots, y_m]$ taký, že $\varphi(g_{ij}) \neq 0$
   V tomto prípade $\varphi(I) = (1) = (\varphi(g_{ij}))$ a podmienka pre stupeň je splnená, pretože $deg_x(g_{ij}) = deg_x\varphi(g_{ij}) = 0$.

2. $G \cap K[y_i, \ldots, y_m] \subset Ker\varphi$
   Podľa predchodzej poznámky a našich úvah máme:
   $(\varphi(I)) = (\varphi(G)) = (\varphi(g_{01}), \ldots, \varphi(g_{n1})) = (\varphi(g_{01}))$ kde $g_{01}$ je monický polynóm v $x$, preto obzvlášť $deg_x(g_{01}) = deg_x(\varphi(g_{01}))$.

Vo všeobecnosti uvažujme $I = \bigcap I_i = \prod I_i$ primárny rozklad. Z prvej časti dôkazu vieme, že v každom ideále $I_i$ existuje polynóm $g_i$, že $\varphi(I_i) = (\varphi(g_i))$ a $deg_x(g_i) = deg_x(\varphi(g_i))$. Nech $g = \prod g_i$ a $\gamma = \varphi(g) = \prod \varphi(g_i)$. Teda máme $deg_x(g) = deg_x(\gamma)$, $\varphi(\prod I_i) = \prod(\varphi(I_i))$, dostaneme $\varphi(I) = (\gamma)$. □

**Poznámka 2.43.** *Naznačme prečo $G$ má uvedený tvar. Nech máme ideál $I \subseteq K[z_1, \ldots, z_n] = R$, ktorý je 0-dimenzionálny a primary. $I \bigcap K[z_2, \ldots, z_n] =: \bar{I}$, $\bar{R} := K[z_2, \ldots, z_n]$. Pomôžeme si Tvrdením 1.3. Vieme, že $\bar{I}$ je 0-dimenzionálny ideál $\bar{R}$. Ukážeme, že $\bar{I}$ je tiež primary v $\bar{R}$. Uvažujme rozšírenie $\nu : \bar{R}/\bar{I} \hookrightarrow R/I$. Takže $R/I = \nu(\bar{R}/\bar{I})[z_1 + I]$.*
*Prvok $z_1 + I$ je celistvý nad $\bar{R}/\bar{I}$. (Existuje monický polynom $f \in K[z_1]$, pre ktorý je $f \in I$). Teda $\nu$ je celistvé rozšírenie.*
*Zobrazenie $\varphi$ z Tvrdenia 1.2 implikuje: Množina všetkých prvoideálov v $R$ obsahujúcich $I$ sa zobrazí na množinu všetkých prvoideálov $\bar{R}$ obsahujúcich $\bar{I}$, množina všetkých prvoideálov $R$ obsahujúcich $I$ je jednoprvková, teda množina všetkých prvoideálov $\bar{R}$ obsahujúcich $\bar{I}$ je jednoprvková, teda $\bar{I}$ je primary ideál v $\bar{R}$.*
*Z nula dimenzionality plynie že existuje $g \in I$ taký, že jeho vedúci člen je mocnina $z_1$ a $I = (g, \sqrt{\bar{I}R} \bigcap I)$. A Gröbnerovu bázu $I$ získame tak, že ku Gröbnerovej báze $\sqrt{\bar{I}R} \bigcap I$ pridáme $g$.*

**Príklad 2.44.** *Nech $I = (x_1, x_2), J = (x_3, x_2 + x_4y)$ sú dve ideály a uvažujme ohodnotenie $\varphi$ získané položením $y = 0$. Ak uvažujeme prienik $I \bigcap J = (x_1x_3, x_2x_3, x_1(x_2 + x_4y), x_2(x_2 + x_4y))$ a jeho ohodnotenie: $\varphi(I \bigcap J) = (x_1x_3, x_2x_3, x_1x_2, x_2^2)$, zatiaľčo keď vezmeme $\varphi(I) = (x, y)$, $\varphi(J) = (x_3, x_2)$ dostaneme $\varphi(I) \bigcap \varphi(J) = (x_1x_3, x_2)$.*

**Veta 2.45.** *Buď $I \subset R = K[x, y_1, \ldots, y_m]$ nula-dimenzionálny ideál,*
*$\varphi : R \longmapsto \bar{K}[x]$ buď špecializácia, ktorá špecializuje všetky premenné okrem jednej, potom: $G$ je Gröbnerova báza pre $I \Longrightarrow \varphi(G)$ je Gröbnerova báza pre $\varphi(I)$.*

*Dôkaz.* Vieme z Poznámky 2.34, že pre každé $\varphi$, $\varphi(Lt_\varphi(I)) \subset Lt(\varphi(I))$. Keď chceme aplikovat Vetu 2.35, musíme ukázať opačnú inklúziu.
Pretože $K[x]$ je obor hlavných ideálov, tento fakt plynie z predchodzej vety, ktorá garantuje, existenciu $g \in I$ takého, že $(\varphi(g)) = (\varphi(I)), deg_x(g) = deg_x(\varphi(g))$. Môžeme napísať $g(x, y_1, \ldots, y_m) = c(y_1, \ldots, y_m)x^r + h$, aby $h$ bolo v $x$ nižšieho stupňa ako $n$ a $\varphi(c) \neq 0$. Teraz $Lt(\varphi(I)) = (x^r), c(y_1, \ldots, y_m)x^r \in Lt_\varphi(I) \Longrightarrow x^r \in \varphi(Lt_\varphi(I)) \Longrightarrow Lt(\varphi(I)) \subset \varphi(Lt_\varphi(I))$. □

**Poznámka 2.46.** *Podmienka, že špecializácia špecializuje všetky premenné okrem jednej je podstatná. Nasledujúci príklad ukazuje, že keď nie je splnená, nie je vždy pravda, že špecializácia Gröbnerovej báze je stále Gröbnerova báza (dokonca v nula-dimenzionálnom prípade).*

**Príklad 2.47.** *Uvažujme nasledujúci ideál:*
$I = (x_1^2, x_1x_2, x_1x_3^2, x_1y + x_2, x_2x_3 - x_3^2, x_3^3, x_2y, x_3^2y, y^2)$. *Toto je Gröbnerova báza pre tento ideál, ak špecializujeme pre $y = 0$: $\varphi(I) = (x_1^2, x_1x_2, x_1x_3^2, x_2, x_2x_3 - x_3^2, x_3^3)$, zatiaľčo Gröbnerova báza pre $\varphi(I)$ je $(x_1^2, x_2, x_3^2)$.*

Konečne môžeme formulovať dôsledok pre riešenie sústavy polynomiálnych rovníc. Je známe, že ak má systém konečný počet riešení, redukovaná Gröbnerova báza má v korešpondujúcom ideále trojuholníkovu formu. Takže riešenia môžu byť počítané so spätnou substitúciou a problém je úplne redukovaný na nájdenie koreňov polynómov jednej premennej nad algebraickým rozšírením nasledované buď výpočtom NSD alebo vyhodnotením (v algebraickom rozšírení).
Aplikáciou predošlých výsledkov sa ukazuje, že NSD výpočty nie sú potrebné a vystačíme si s „niekoľkými“ vyhodnoteniami.

**Dôsledok 2.48.** *Buď $I \subset K[x_1, \ldots, x_n]$ nula-dimenzionálny ideál, $G = (g_1, \ldots, g_s)$ je jeho Gröbnerova báza s ohľadom na lexikografické usporiadanie s $x_1 > \cdots > x_n$ a nech $(\alpha_k, \ldots, \alpha_n) \in \bar{K}^{n-k+1}$ sú korene $I \bigcap K[x_k, \ldots, x_n]$. Nech $I_k = (g_{k_1}, \ldots, g_{k_r}) = (G \bigcap K[x_{k-1}, \ldots, x_n]) \setminus K[x_k, \ldots, x_n]$. Nech $g \in I_k$ je polynóm minimálneho stupňa v $x_{k-1}$, ktorého vedúci koeficient $c(x_k, \ldots, x_n)$ (s ohľadom na $x_{k-1}$) nezmizne pri ohodnotení $(\alpha_k, \ldots, \alpha_n)$. Máme*

$$g_\alpha = g(x_{k-1}, \alpha_k, \ldots, \alpha_n) = NSD((g_{k_1}(x_{k-1}, \alpha_k, \ldots, \alpha_n)), \ldots, (g_{k_r}(x_{k-1}, \alpha_k, \ldots, \alpha_n))).$$

*Obzvlášť keď $\alpha_{k-1}$ je koreň $g_\alpha$, potom $(\alpha_{k-1}, \alpha_k, \ldots, \alpha_n)$ je koreň $I \bigcap K[x_{k-1}, \ldots, x_n]$.*

*Dôkaz.* Dôkaz plynie priamo z predchodzej vety s uvážením, že špecializácia
$\varphi : I \bigcap K[x_{k-1}, \ldots, x_n] \longmapsto \bar{K}[x_{k-1}]$, definovaná
$\varphi(f(x_{k-1}, \ldots, x_n)) = f(x_{k-1}, \alpha_k, \ldots, \alpha_n)$. □

# Kapitola 3

# Odmocninové kódy

V tejto časti definujeme triedu odmocninových kódov a popíšeme niektoré ich základné vlastnosti.

**Definícia 3.1.** *Nech* $L \subset R_n \cup \{0\}, L = \{l_1, \ldots, l_N\}$ *a* $\mathcal{P} = \{g_1(x), \ldots, g_r(x)\}$ *v* $F_{q^m}[x]$ *také, že* $\forall i = 1, \ldots, N$ *existuje prinajmenšom jedno* $j = 1, \ldots, r$ *také, že* $g_j(l_i) \neq 0$. *Označíme* $\mathcal{C} = \Omega(q, n, q^m, L, \mathcal{P})$ *kód definovaný nad* $F_q$, *ktorého paritná matica je nasledujúca:*

$$H = \begin{pmatrix} g_1(l_1) & \ldots & g_1(l_N) \\ g_2(l_1) & \ldots & g_2(l_N) \\ \vdots & \ddots & \vdots \\ g_r(l_1) & \ldots & g_r(l_N) \end{pmatrix} = \begin{pmatrix} g_1(L) \\ g_2(L) \\ \vdots \\ g_r(L) \end{pmatrix}$$

*Hovoríme, že* $\mathcal{C}$ *je* ***odmocninový kód****.*

**Poznámka 3.2.** *Kód* $\mathcal{C} = \Omega(q, n, q^m, L, \mathcal{P})$ *je lineárny nad telesom* $F_q$, *jeho dĺžka je* $N = |L|$ *a jeho vzdialenosť* $d \geq 2$, *pretože* $H$ *neobsahuje žiaden stĺpec pozostávajúci len z núl.*
*Ak* $0 \in L$, *predpokladáme* $l_N = 0$ *(hociaké preusporiadanie dáva ekvivalentný kód).*
*Budeme označovať* $\overline{L}$ *množinu* $R_n \setminus L$.

**Definícia 3.3.** *Nech* $\mathcal{C} = \Omega(q, n, q^m, L, \mathcal{P})$ *je odmocninový kód a* $\nu \in (F_q)^N$.

- *Ak* $\overline{L} = \emptyset$, *hovoríme, že* $\mathcal{C}$ *je* ***maximálny****.*
- *Ak* $\mathcal{P} \subset F_q[x]$, *hovoríme, že* $\mathcal{C}$ *je* ***vlastný****.*
- *Ak* $0 \notin L$, *hovoríme, že* $\mathcal{C}$ ***neobsahuje nulu****, inak* $C$ ***obsahuje nulu****, ale* $\nu_N = 0$.

**Poznámka 3.4.** *Pretože každá funkcia z* $F_{q^m}$ *do* $F_{q^m}$ *môže byť vyjadrená ako polynóm, môžeme v množine* $\mathcal{P}$ *akceptovať taktiež racionálne funkcie typu* $f/g, f, g \in F_{q^m}$ *také, že* $g(\overline{x}) \neq 0$ *pre každé* $\overline{x} \in F_{q^m}$. *Odteraz budeme uvažovať aj takéto funkcie.*

**Príklad 3.5.** *Nech* $q = 2$, $n = 7$, $q^m = 8$, $L = F_{2^3} = \langle\beta\rangle \cup \{0\}, \beta^3 = \beta + 1$, $\mathcal{P} = \{g_1(x) = \frac{1}{x^2+x+1}, g_2(x) = \frac{x}{x^2+x+1}\}$. *Sedem siedmych odmocnín z jednej sú prvky* $F_8^*$, $R_7 = F_8^*$. *Odmocninový kód* $\mathcal{C} = \Omega(2, 7, 8, F_8, \{g_1, g_2\})$ *obsahuje nulu* ($0 \in L$), *je maximálny* ($\overline{L} = R_n \setminus L = \emptyset$), *vlastný* ($g_1$, $g_2 \in F_2[x]$) *a jeho paritná matica je nasledujúca:*

$$H = \begin{pmatrix} g_1(1) & g_1(\beta) & g_1(\beta^2) & g_1(\beta^3) & g_1(\beta^4) & g_1(\beta^5) & g_1(\beta^6) & g_1(0) \\ g_2(1) & g_2(\beta) & g_2(\beta^2) & g_2(\beta^3) & g_2(\beta^4) & g_2(\beta^5) & g_2(\beta^6) & g_2(0) \end{pmatrix}$$

*Pre konečné teleso* $L = F_{2^3} = \langle\beta\rangle \cup \{0\}$ *platí, že každý z jeho 7 prvkov okrem nuly sa dá vyjadriť ako mocnina generátora, teda ako mocnina prvku* $\beta$ ($\beta$ *je primitivný prvok telesa* $F_8$ *s minimálnym polynomom* $x^3 + x + 1$, $F_8$ *izomorfné s* $F_2[x]/(x^3 + x + 1)$). *S pomocou podmienky* $\beta^3 = \beta + 1$ *si vyjadríme všetky prvky telesa:*

$$\beta = \beta, \beta^2 = \beta^2, \beta^3 = \beta + 1, \beta^4 = \beta^2 + \beta, \beta^5 = \beta^2 + \beta + 1, \beta^6 = \beta^2 + 1, \beta^7 = 1$$

*Teraz upravíme maticu H:*

$$g_1(1) = 1$$

$$g_1(\beta) = \frac{1}{\beta^2 + \beta + 1} \to g_1(\beta)(\beta^2 + \beta + 1) = 1 \to g_1(\beta)\beta^5 = 1 \overset{\beta^7=1}{\to} g_1(\beta) = \beta^2,$$

*z toho ľahko, len prenásobením prvkom* $\beta$ *dostaneme:*

$$g_2(\beta) = \beta g_1(\beta) = \beta^3 = \beta + 1,$$

*ďalej:*

$$g_1(\beta^2) = \frac{1}{\beta^4 + \beta^2 + 1} \overset{\beta^4=\beta^2+\beta}{\longrightarrow} g_1(\beta^2)(\beta^2 + \beta + \beta^2 + 1) = 1 \overset{\beta^3=\beta+1}{\longrightarrow}$$

$$g_1(\beta^2)\beta^3 = 1 \overset{\beta^7=1}{\to} g_1(\beta^2) = \beta^4 = \beta^2 + \beta,$$

$$g_2(\beta^2) = \beta^2 g_1(\beta^2) = \beta^6 = \beta^2 + 1,$$

*Po vyjadrení všetkých prvkov matice dostaneme:*

$$H = \begin{pmatrix} 1 & \beta^2 & \beta^2 + \beta & \beta^2 & \beta & \beta & \beta^2 + \beta & 1 \\ 1 & \beta + 1 & \beta^2 + 1 & \beta^2 + \beta + 1 & \beta^2 + \beta + 1 & \beta^2 + 1 & \beta + 1 & 0 \end{pmatrix}$$

*Teraz hľadáme riešenie paritnej matice H, môžeme si to reprezentovať v takomto tvare:*

$$H \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_8 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

*Kde* $a_i \in F_2$, $\forall i = 1, \ldots, 8$.
*Po roznásobení dostaneme nasledujúce dve rovnice:*

$$a_1 + a_2\beta^2 + a_3(\beta^2 + \beta) + a_4\beta^2 + a_5\beta + a_6\beta + a_7(\beta^2 + \beta) + a_8 = 0$$

$$a_1+a_2(\beta+1)+a_3(\beta^2+1)+a_4(\beta^2+\beta+1)+a_5(\beta^2+\beta+1)+a_6(\beta^2+1)+a_7(\beta+1)+a_80 = 0$$

*Nasledujúca matica je o velkosti* $6\times 8$ *a dostaneme ju spojením dvoch matíc o veľkosti* $3 \times 8$ *pod seba. Tie dve matice získame z našich dvoch rovníc takto:*
*Matica* $3 \times 8$ *má na mieste* $[i, j]$ *číslo* 1, *práve keď* $\beta^i \neq 0$ *pri koeficiente* $a_j$, *pre* $i = 0, 1, 2$ *(v oboch rovniciach vidíme, že sa nám tam vyskytuje* $\beta$ *len do stupňa* 2*),* $j = 1, \ldots, 8$, *inak tam má nulu. Túto maticu následne upravíme pomocou Gaussovej eliminácie na odstupňovaný tvar a výslednú maticu označíme* $M$*:*

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} = M$$

*Ako vidíme, dimenzia riešenia je dva. To bude aj hodnosť matice riešení* $G$*, v ktorej vektory tvorené zo siedmeho a ôsmeho miesta, zvolíme lineárne nezávislé. Ostatné zložky dopočítame tak, aby platilo (*0 *tu predstavuje nulovú maticu* $6 \times 2$*)* $MG^T = 0$*:*

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & \underline{1} & \underline{1} \\ 0 & 1 & 1 & 1 & 1 & 1 & \underline{1} & \underline{0} \end{pmatrix}$$

$G$ *je generujúca matica kódu* $C$ *(Pre overenie* $HG^T = 0$ *(*0 *je nulová matica* $2 \times 2$*)).*
*Ako hneď vidíme váhové rozdelenie kódových slov je* $\{A_0 = 1, A_1 = A_2 = A_3 = A_4 = 0, A_5 = 2, A_6 = 1\}$.
$A_0 = 1$ *pretože každý lineárny kód obsahuje nulové slovo,*
$A_5 = 2$ *pretože prvý, prvý + druhý riadok majú váhu* 5,
$A_6 = 1$ *pretože druhý riadok má váhu* 6.
*Z váhového rozdelenia nám plynie, že kód má minimálnu vzdialenosť* 5.
*Celkom: kód* $C$ *je* $[8, 2, 5]$*-kód.*

**Definícia 3.6.** *Ľubovoľný generátor multiplikativnej grupy telesa* $F_q$*, teda generátor grupy* $F_q^*$ *sa nazýva* ***primitivný prvok****.*
*Prvok* $a$ *je generátorom grupy* $(Z_n, + \pmod n)$ *práve vtedy, keď čísla* $a$ *a* $n$ *sú nesúdelné. Teda počet primitivných prvkov telesa* $F_q$ *je rovný počtu čísel menších než* $q - 1$ *nesoudělných s* $q - 1$.

**Príklad 3.7.** *Nech* $q = 2$, $n = 5$, $q^m = 2^4$, $L = R_5$, $\mathcal{P} = \{g = \gamma^{12}x^4 + \gamma^{11}x^3 + x^2 + \gamma^{14}x + \gamma^3\}$, $\gamma$ *je primitivný prvok telesa* $F_{16}$, $\gamma^4 = \gamma + 1$. *Nech* $\mathcal{C} = \Omega(2, 5, 2^4, R_5, \mathcal{P})$

*neobsahuje nulu ($0 \notin L$), je maximálny ($\overline{L} = R_n \setminus L = \emptyset$) a jeho paritná matica je nasledujúca:*

$$H = \begin{pmatrix} g(\gamma^3) & g(\gamma^6) & g(\gamma^9) & g(\gamma^{12}) & g(\gamma^{15}) \end{pmatrix} = \begin{pmatrix} \gamma^3+\gamma^2 & \gamma^2 & \gamma^3 & \gamma^3+1 & 1 \end{pmatrix}$$

*Tak, ako v predchádzajúcom príklade vieme získať maticu $M$ a z nej generujúcu maticu kódu $C$, maticu $G$.*

$$G = \begin{pmatrix} 1 & 1 & \underline{1} & 0 & \underline{0} \\ 0 & 0 & \underline{1} & 1 & \underline{1} \end{pmatrix}$$

*Platí:* $HG^T = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$.
*Kód $C$ je teda $[5,2,3]$-kód.*

*Je kód $C$ vlastný?*
*Skúsme to spočítať bez pomocí počítača. Iný dôkaz nájdeme v [4] Pripomeňme si, že kód je vlastný, ak pre polynom $f$, ktorý nám určuje riadky paritnej matice $H$, je $f \in F_q[x]$. V našom príklade $q = 2$.*
*Zaveďme si označenie $\theta := \gamma^3$, teda $\theta^5 = 1$, $\theta^4 = \theta^3 + \theta^2 + \theta + 1$.*
*Minimálny polynóm prvku $\theta$ nad $F_2$ je $M_\theta(x) = x^4 + x^3 + x^2 + x + 1$ $(= M_{\gamma^3})$.*
*Dá sa napísať:*
$f(x) = \sum_{i=0}^{m} a_i x^i = g(x) = \sum_{j=0}^{4} (\sum_{i \pmod 5 = j} a_i) x^j$, *ak $x$ je mocnina prvku $\theta$.*
$\theta^i = \theta^{i \pmod 5}$, $f(\theta^k) = g(\theta^k)$, *pre* $\forall k \in \mathbb{N}_0$.
*Urobme si prehľadnú tabuľku výrazov $\theta^1$ až $\theta^5$ dosadených do $x^0$ až $x^4$.*

| | $\theta$ | $\theta^2$ | $\theta^3$ | $\theta^4$ | 1 |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 |
| $x$ | $\theta$ | $\theta^2$ | $\theta^3$ | $\theta^3+\theta^2+\theta+1$ | 1 |
| $x^2$ | $\theta^2$ | $\theta^3+\theta^2+\theta+1$ | $\theta$ | $\theta^3$ | 1 |
| $x^3$ | $\theta^3$ | $\theta$ | $\theta^3+\theta^2+\theta+1$ | $\theta^2$ | 1 |
| $x^4$ | $\theta^3+\theta^2+\theta+1$ | $\theta^3$ | $\theta^2$ | $\theta$ | 1 |

*Preveďme si náš tabuľkový zápis do maticovej formy. Teda matica $A$ predstavuje tabuľku, ktorú si rozpíšeme ako súčet štyroch matíc $A_0, A_1, A_2, A_3$, každú v rade prenásobenou tou správnou mocninou prvku $\theta$:*

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} \theta + \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix} \theta^2 +$$

$$+\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}\theta^3$$

*Máme:* $f(x) = a_0+a_1x+a_2x^2+a_3x^3+a_4x^4 \in F_2[x]$. *Označme:* $\overrightarrow{a} = (a_0, a_1, a_2, a_3, a_4)$. *Ako si môžeme všimnúť, rozpisom do matíc sme dosiahli tejto rovnosti:*
$(f(\theta), f(\theta^2), f(\theta^3), f(\theta^4), f(1)) = \overrightarrow{a}A = \overrightarrow{a}A_0 + \overrightarrow{a}A_1\theta + \overrightarrow{a}A_2\theta^2 + \overrightarrow{a}A_3\theta^3$
*Ak $f$ určuje riadky paritnej matice kódu $C$, $G$ je generujúca matica kódu, tak musí platiť:*

$$\overrightarrow{a}A_0G^T = \overrightarrow{a}A_1G^T = \overrightarrow{a}A_2G^T = \overrightarrow{a}A_3G^T = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

*Teda počítajme (maticu $G$ sme už v tomto príklade určili):*

$$A_0G^T = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \\ 1 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$$A_1G^T = \begin{pmatrix} 0 & 0 \\ 1 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$$

*Podobne postupujeme a vypočítame $A_2G^T$, $A_3G^T$. Urobíme maticu $8 \times 5$. Vznikne postupným pripojením matíc $(A_0G^T)^T$, $(A_1G^T)^T$, $(A_2G^T)^T$, $(A_3G^T)^T$ pod seba. Upravíme ju elimináciou na odstupňovaný tvar. Výslednú maticu označíme $B$.*

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

*Ako vidíme, že vyhovujúci je len jeden vektor a to:*
$\overrightarrow{a} = (a_0, a_1, a_2, a_3, a_4) = (0, 0, 0, 0, 0)$ *(koeficienty určujúce polynom $f$).*

*Záver: Ak $f$ určuje riadky paritnej matice $H$ kódu $C$, tak $f$ je nulový polynom, to znamená, že nenulový polynom s koeficientami v $F_2$ neexistuje, čo nám implikuje, že kód $C$ nie je vlastný. Takto môžme postupovať obecne:*
*Pri zisťovaní, či nejaký kód $C$, s množinou $P \subset F_{q^m}$, ktorej nenulové polynomy vytvárajú paritnú maticu $H$ je vlastný, teda či tie polynomy ležia v $F_q$. Zostavíme si tabuľku za pomoci podmienky pre $\theta$ v tomto príklade to bolo $\theta^4 = \theta^3 + \theta^2 + \theta + 1$ (minimálny polynom primitívnej n-tej odmocniny z jednej). Z nej si urobíme maticu $A$, analogicky postupujeme ďalej, až získame maticu $B$. Riešenie matice $B$ nám udáva koeficienty polynomu, ktorý leží v $F_q$ a určuje riadky matice $H$ kódu $C$. V našom prípade nám vyšli všetky koeficienty nulové, takže polynomy ktoré tvoria paritnú maticu ležia v $F_{q^m}$, teda tu sme dokázali, že kód nie je vlastný.*

**Poznámka 3.8.** *Za účelom definovať rovnaký odmocninový kód, je možné použiť rôzne $n$. Napríklad môžeme definovať lineárny kód s dĺžkou $N = 5$, použiť 5 piatych odmocnín z jednej alebo 5 prvkov vyberieme z množiny 7 siedmych odmocnín z jednej. Pozrime sa nasledujúci príklad.*

**Príklad 3.9.** *Nech $C$ je lineárny kód nad $F_2$ s paritnou maticou:*

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

- *Dá sa ukázať, že $C$ je maximálny, neobsahuje nulu a je to odmocninový kód $C = \Omega(2, 5, 2^4, L_1, \mathcal{P}_1)$, kde $L_1 = R_5 = \{\gamma^3, \gamma^6, \gamma^9, \gamma^{12}, \gamma^{15}\} \subset F_{16} = \langle\gamma\rangle \cup \{0\}, \gamma^4 = \gamma + 1, \mathcal{P}_1 \subset F_{16}[x]$ je $\mathcal{P}_1 = \{g_1, g_2\}$ s*

$$g_1 = \gamma^7 x^4 + \gamma^{14} x^3 + \gamma^{11} x^2 + \gamma^{13} x + 1, g_2 = \gamma^2 x^4 + \gamma^4 x^3 + \gamma x^2 + \gamma^8 x + 1.$$

- *Na kód sa môžeme tiež pozerať ako na nemaximálny odmocninový, neobsahujúci nulu s parametrami $C = \Omega(2, 7, 2^3, L_2, \mathcal{P}_2)$, kde $L_2 \subset R_7 = F_8^* = \langle\beta\rangle, \beta^3 = \beta + 1, L_2 = \{\beta, \beta^2, \beta^3, \beta^4, \beta^5\}, \mathcal{P}_2 \subset F_{2^3}[t]$ je $\mathcal{P}_2 = \{p_1, p_2\}$ s*

$$p_1 = t^4 + t^2 + t + 1, p_2 = \beta^4 t^4 + \beta^6 t^3 + t + \beta^2.$$

- *Navyše kód $C$ môžeme brať ako nemaximálny odmocninový, obsahujúci nulu s parametrami $C = \Omega(2, 7, 2^3, L_3, \mathcal{P}_3)$, kde $L_3 \subset F_8, L_3 = \{\beta, \beta^2, \beta^3, \beta^4, 0\}, \mathcal{P}_3 \subset F_8[z]$ je $\mathcal{P}_3 = \{h_1, h_2\}$ s*

$$h_1 = \beta^5 z^4 + z^3 + \beta^5 z^2 + \beta^4 z, h_2 = \beta^6 z^4 + \beta^3 z^2 + \beta^5 z + 1.$$

- *Povšimnime si, že kód $C$ nemôže byť maximálny odmocninový, obsahujúci nulu.*

Nasledujúce tvrdenie nám ukazuje, že obzvlášť každý samoopravný kód môže byť videný ako odmocninový pre vhodné hodnoty $n$.

**Tvrdenie 3.10.** *Nech $C$ je kód nad telesom $F_q$ dĺžky $N$. Potom $C$ je odmocninový pre každé $n \geq N-1$ také, že $(n,q)=1$. Hlavne:*

1. *ak $n = N$, potom $C$ je maximálny, neobsahujúci nulu,*
2. *ak $n = N-1$, potom $C$ je maximálny, obsahujúci nulu.*

*Dôkaz.* Nech $C$ je lineárny kód nad $F_q$ dĺžky $N$, dimenzie $k$ a $d \geq 2$, s paritnou maticou $H = (h_{i,j}) \in (F_q)^{(N-k)\times N}$. Pretože $d \geq 2$, neexistuje žiadne $j = 1, \ldots, N$ také, že $h_{i,j} = 0, \forall i = 1, \ldots, N-k$. Nech $n$ je prirodzené číslo také, že $n \geq N-1, (n,q) = 1$. Nech $R_n = \{\alpha_1, \ldots, \alpha_n\}$ je množina všetkých n-tých odmocnín z jednej nad $F_q$.

Predpokladajme, že $n \geq N$. Nech $L$ je podmnožina $R_n, |L| = N, r = N-k$. Vďaka Lagrangeovej vete o interpolácii môžeme nájsť $r$ polynómov $g_i(x) \in F_{q^m}[x]$ takých, že $g_i(\alpha_j) = h_{i,j}, \forall \alpha_j \in L, i = 1, \ldots r, j = 1, \ldots, N, h_{i,j}$ je prvok $F_{q^m}$. Dáme polynómy $g_i(x)$ do množiny $P = \{g_i\}_{1 \leq i \leq r}$. Polynómy $g_i(x)$ majú takú vlastnosť, že pre každé $i = 1, \ldots, r$ existuje aspoň jedno také $1 \leq j \leq r$, že $g_j(\alpha_i) \neq 0$. Potom je zrejmé, že kód $C$ neobsahuje nulu a je odmocninový $\Omega(q, n, q^m, L, P)$ kód.
Ak volíme $n = N$, tak $C$ je maximálny, pretože $L = R_n$.
Nech $L$ pozostáva z prvku 0 a z $N-1$ prvkov $R_n$. S argumentom vyššie je ľahké dokázať, že $C$ je odmocninový kód obsahujúci nulu.
Ak $n = N-1$, tak kód $C$ je maximálny, obsahujúci nulu, pretože $L = R_n \cup \{0\}$. □

**Dôsledok 3.11.** *$C$ je kód $\Leftrightarrow$ $C$ je odmocninový kód.*

**Tvrdenie 3.12.** *Nech $NSD(n,q) = 1 \Rightarrow$ rozkladové nadteleso polynómu $x^n - 1 \in F_q[x]$ je teleso $F_q^m$, $m \geq 1$, kde $m$ je najmenšie také, že $q^m \equiv 1 \pmod n$*

**Poznámka 3.13.**
- $NSD(n,q) = 1 \Rightarrow q^{\varphi(n)} \equiv 1 \pmod n$
- $NSD(n,q) \neq 1 \Rightarrow q = p^l \Rightarrow n = pn_1 \Rightarrow x^n - 1 = (x^{n_1})^p - 1 = (x^{n_1} - 1)^p$
  *Rozkladové nadteleso polynómu $x^n - 1$ je to isté ako pre polynóm $x^{n_1} - 1$*

**Tvrdenie 3.14.** *Buď $F = F_q^m$ rozkladové nadteleso $x^n - 1$ nad $F_q$, $\alpha$ primitívna odmocnina z jednej, $NSD(n,q) = 1$. Potom $x^n - 1 = (x-1)(x-\alpha)\cdots(x-\alpha^{n-1})$. Nerozložiteľné faktory polynómu $x^n - 1$ sú minimálne polynómy prvkov $1, \alpha, \ldots, \alpha^{n-1}$.*

**Definícia 3.15.** *Nerozložiteľné faktory polynómu $x^n - 1$ sa nazývajú **cyklotomické polynomy** nad telesom $F_q[x]$. $k \in \{0, \ldots, n-1\}$, položme $C_k = \{k, kq, \ldots, kq^{n-1}\}$ násobenie $\pmod n$, sa nazýva **cyklotomická trieda** prvku $k$ modulo $n$.*

**Tvrdenie 3.16.** *$NSD(k,q) = 1 \Rightarrow$ minimálny polynóm prvku $\alpha^k$ nad $F_q$ je: $M_\alpha^k = \prod_{i \in C_k}(x - \alpha^i)$*

**Tvrdenie 3.17.** *Každý binárny kód dĺžky $N$ sa dá napísať ako vlastný odmocninový kód.*

*Dôkaz.* Nech $q = 2$. Nájdeme $n$, $NSD(n, q) = 1$, aby existovalo aspoň $N$ rôznych cyklotomických tried polynomu $x^n - 1 \in F_2[x]$. A označme $k$ počet týchto tried. Vyberme jeden prvok z každej cyklotomickej triedy: $\alpha_1, \ldots, \alpha_k$. Nech toto sú odpovedajúce cyklotomické polynomy: $c_1, \ldots, c_k$, kde $c_i \in F_2[x] \forall i$. Nech $\tilde{c}_i(x) = \frac{x^n-1}{c_i(x)} \in F_2[x]$. Určite $\tilde{c}_i(\alpha_j) = 0 \forall j \neq i$ a $\tilde{c}_i(\alpha_i) \neq 0$. Potrebujeme polynom $\tilde{c}_i(x)$ modifikovať tak, aby $\tilde{c}_i(\alpha_i) = 1$. Nech $\alpha_i, \alpha_i^2, \ldots, \alpha_i^{2^{l_i}}$ sú presne prvky cyklotomickej triedy $\alpha_i$. Potom $(\tilde{c}_i(\alpha_i)\tilde{c}_i({\alpha_i}^2) \cdots \tilde{c}_i({\alpha_i}^{2^{l_i}}))^2 = \tilde{c}_i({\alpha_i}^2)\tilde{c}_i({\alpha_i}^4) \cdots \tilde{c}_i({\alpha_i}^{2^{l_i+1}}) = \tilde{c}_i({\alpha_i}^2)\tilde{c}_i({\alpha_i}^4) \cdots \tilde{c}_i(\alpha_i)$. (Zrejme platí $\forall p \in F_2$: $p(x)^2 = p(x^2)$). Preto voľme $\bar{c}_i := \tilde{c}_i(x)\tilde{c}_i(x^2) \cdots \tilde{c}_i(x^{2^{l_i}}) \in F_2[x]$, potom: $(\bar{c}_i(\alpha_i))^2 = \bar{c}_i(\alpha_i) \neq 0 \Rightarrow \bar{c}_i(\alpha_i) = 1$. Polynómy $\bar{c}_i$ dávajú po dosadení prvkov $\alpha_1, \ldots, \alpha_N$ vektory kanonickej báze. Potrebujeme nájsť polynomy $g_1, \ldots, g_m$, aby sme po dosadení týchto prvkov z $L$ dostali paritnú maticu $H$ kódu $C$. Teda položme $g_j = \sum_{i=1,\text{t.ž.}H[j,i]=1}^{N} c_i \ \forall j = 1, \ldots, m$.
Nech $L = \{\alpha_1, \ldots, \alpha_N\}$, $\mathcal{P} = \{g_1, \ldots, g_N\}$. Vidíme, že kód $C = \Omega(q, n, q^m, L, \mathcal{P})$ je vlastný ($\forall$ polynóm z $\mathcal{P} \in F_2[x]$). □

## 3.1 Počítanie vzdialeností a rozdelenie váh pre odmocninové kódy

V tejto časti ukážeme metódu, ako počítať vzdialenosť a rozdelenie váh kódu $C$, reprezentovaného ako odmocninový kód.
Pre naše účely potrebujeme definovať nasledujúce ideály.

**Definícia 3.18.** *Nech $C = \Omega(q, n, q^m, L, \mathcal{P})$ je odmocninový kód, $w, \hat{w}$ prirodzené čísla také, že $2 \leq w \leq N = |L|, 1 \leq \hat{w} \leq N - 1$. Označme $J_w(C)$ideál:*

$$J_w = J_w(C) = J_w(q, n, q^m, L, \mathcal{P}) \subset F_{q^m}[z_1, \ldots, z_w, y_1, \ldots, y_w],$$

$$J_w = (\{\sum_{h=1}^{w} y_h g_s(z_h)\}_{1 \leq s \leq r}, \{y_j^{q-1} - 1\}_{1 \leq j \leq w}, \{p_{ij}(z_i, z_j)\}_{1 \leq i < j \leq w}, \{\frac{z_j^n - 1}{\prod_{l \in \overline{L}}(z_j - l)}\}_{1 \leq j \leq w}), \tag{3.1}$$

*kde $p_{ij} = \sum_{h=0}^{n-1} z_i^h z_j^{n-1-h} = \frac{z_i^n - z_j^n}{z_i - z_j}$ je v $F_q[z_i, z_j]$.*
*Označme*

$$\eta(J_w) = |\nu(J_w)|$$

*celé číslo.*

**Poznámka 3.19.** *Ak sme len v binárnom prípade ($q = 2$), premenné $y_j, j = 1, \ldots, w$ a $\nu$ sú 1 a tak ich vynechávame a dostávame ideál:*

$$J_w = J_w(C) = J_w(2, n, 2^m, L, P) \subset F_{2^m}[z_1, \ldots, z_w, y_1, \ldots, y_w],$$

$$J_w = (\{\sum_{h=1}^{w} g_s(z_h)\}_{1 \leq s \leq r}, \{p_{ij}(z_i, z_j)\}_{1 \leq i < j \leq w}, \{\frac{z_j^n - 1}{\prod_{l \in \overline{L}}(z_j - l)}\}_{1 \leq j \leq w}).$$

**Tvrdenie 3.20.** *Nech $C = \Omega(q, n, q^m, L, \mathcal{P})$ je odmocninový kód.*
*Keď neobsahuje nulu, tak*
*existuje aspoň jedno kódové slovo váhy $w$ v $C \Leftrightarrow$ existuje aspoň jedno riešenie $J_w(C)$.*
*Navyše, počet kódových slov váhy $w$ je:*

$$A_w = \frac{\eta(J_w)}{w!}.$$

*Dôkaz.* Označme $C_w$ množinu kódových slov váhy $w$, $S_w$ množinu permutácií $w$ prvkovej množiny. Nájdeme bijekciu $\nu(J_w)$ a $C_w \times S_w$, potom $|C_w| = \frac{|\nu(J_w)|}{w!}$.
Rozmyslíme si, ako vyzerajú prvky množiny $\nu(J_w)$: $y_j^{q-1} - 1 = 0 \ \forall a \leq j \leq w \Leftrightarrow 0 \neq u_j \in F_q$; $\frac{z_j^n - 1}{\prod_{l \in \bar{L}}(z_j - l)} = 0 \ \forall a \leq j \leq w \Leftrightarrow z_j \in L$; $p_{ij}(z_i, z_j) = 0 \Leftrightarrow z_i \neq z_j$, $z_i^n = z_j^n = 1$. Ak $(\bar{y}_1, \ldots, \bar{y}_w, \bar{z}_1, \ldots, \bar{z}_w) \in \nu(J_w)$, $\bar{y}_1, \ldots, \bar{y}_w$ sú nenulové prvky $F_q$ a $\bar{z}_1, \ldots, \bar{z}_w$ sú rôzne prvky z $L$. Nech $\bar{z}_1 = l_{j(i)}$, potom rovnica $\sum_i g_s(\bar{z}_i)\bar{y}_i = 0$ je splnená $\Leftrightarrow c = (c_1, \ldots, c_N) \in C$, kde $c_k = 0$, ak $k \notin \{j(1), \ldots, j(w)\}$, $c(k) = j(i)$, ak $k = j(i)$ pre vhodné $i = 1, \ldots, w$. Nech $c \in C_w$, nenulové prvky na pozíciách $i_1, \ldots, i_w$ označme $\bar{y}_1, \ldots, \bar{y_w}$. Dvojici $(c, \pi)$ priradíme riešenie $(c_{i_{\pi(1)}}, \ldots, c_{i_{\pi(w)}}, l_{i_{\pi(1)}}, \ldots, l_{i_{\pi(w)}})$. Kde $l_1, \ldots, l_{|L|}$ sú prvky $L$ očíslované tak, ako vytvárajú stĺpce matice $H$. Keďže predpokládame, že sú po dvoch rôzne, vidíme, že definované zobrazenie $C_w \times S_w$ je prosté. Ľahko nahliadneme, že je tiež na. (Každý prvok $\nu(J_w)$ vzniká na súradniciach $y_1, \ldots, y_w$ permutáciou prvkov $C_w$). □

## 3.2 Polynóm pre detekciu chýb

V Tvrdení (3.17) bola ukázaná existencia polynómu pre detekciu chýb pre vlastné maximálne odmocninové kódy, ktoré neobsahujú nulu. Ukážeme si hlavné myšienky dôkazu.
Nech $K$ je teleso (nie nutne konečné). $G$ je Gröbnerova báza 0-dimenzionálneho vlastného ideálu $J \subset K[\mathcal{S}, \mathcal{A}, \mathcal{T}]$, $\mathcal{S} = (s_1, \ldots, s_H)$, $\mathcal{A} = (a_1, \ldots, a_L)$, $\mathcal{T} = (t_1, \ldots, t_M)$ s ohľadom na lexikografické usporiadanie $\mathcal{S} < \mathcal{A} < \mathcal{T}$ a s premennými v $\mathcal{A}$ usporiadanými $a_1 > \cdots > a_L$. Potom prvky množiny $G \cap (K[\mathcal{S}, \mathcal{A}] \setminus K[\mathcal{S}])$ môžeme zoradiť do blokov $\{G_i\}_{1 \leq i \leq L}$:

$$G_1 = \{g_{1,1}(S, a_L, \ldots, a_2, a_1), \ldots, g_{1,l_1}(S, a_L, \ldots, a_2, a_1)\},$$

$$G_2 = \{g_{2,1}(S, a_L, \ldots, a_2), \ldots, g_{2,l_2}(S, a_L, \ldots, a_2)\},$$

$$\vdots$$

$$G_L = \{g_{L,1}(S, a_L), \ldots, g_{L,l_L}(S, a_L)\},$$

že platí:

- $\forall i$, $G_i \subset K[S, a_L, \ldots, a_{i+1}][a_i] \setminus K[S, a_L, \ldots, a_{i+1}]$,
- ideál generovaný $\sqcup_{j>i} G_j$ je vlastne $i$-tý eliminačný ideál $J_i$, $J_i = J \cap K[S, a_L, \ldots, a_i]$.

Z vlastností Gröbnerovej báze máme, že $G_i \neq \emptyset$ pre ľubovoľné $1 \leq i \leq L$. Každá $G_i$ sa dá rozložiť do blokov polynómov v závislosti od ich stupňa s ohľadom na premenné $a_i$:

$$G_i = \bigcup_{\delta=1}^{\Delta_i} G_{i\delta},$$

ale nejaké $G_{i\delta}$ môžu byť prázdne. Keď $g \in G_{i\delta}$, máme:

- $g \in K[S, a_L, \ldots, a_{i+1}][a_i] \setminus K[S, a_L, \ldots, a_{i+1}]$
- $deg_{a_i}(g) = \delta; g = ba_i^{\delta} + \cdots, b = Lp(g) \in K[S, a_L, \ldots, a_{i+1}]$ (kde $Lp(g)$ označujeme vedúci polynóm $g$ s ohľadom na $a_i$)

Nech $N_{i\delta}$ je počet prvkov $G_{i\delta}$. Pomenujeme prvky množiny $G_{i\delta} = \{g_{i\delta j}, 1 \leq j \leq N_{i\delta}\}$ po ich poradí:

$$h < j \Leftrightarrow lt(g_{i\delta h}) < lt(g_{i\delta j})$$

**Poznámka 3.21.** *Zosumarizujme:*
*Nech máme dva polynómy $g_{lDh} \in G_{lD}$ a $g_{i\delta j} \in G_{i\delta}$, tak:*

$$g_{lDh} < g_{i\delta j} \Leftrightarrow lt(g_{lDh}) < lt(g_{i\delta j}) \Leftrightarrow \tag{3.2}$$

- *$l > i$ alebo*
- *$l = i$, $D < \delta$ alebo*
- *$l = i$, $D = \delta$, $h < j$.*

*Pretože $J$ je 0-dimenzionálny, môžeme zrejme rozložiť varietu eliminačných ideálov takto: Nech $J_{\mathcal{S}} = J \cap K[S]$, $J_{\mathcal{S}\cup\{a_L\}} = J \cap K[S, a_L]$, …, $J_{\mathcal{S}\cup\{a_L,\ldots,a_1\}} = J \cap K[\mathcal{S}, \mathcal{A}]$. Máme:*

1. $\nu(J_{\mathcal{S}}) = \sqcup_{j=1}^{\lambda(L)} \Sigma_j^L$, *s*

$$\Sigma_j^L = \{(\bar{s}_1, \ldots, \bar{s}_N) \in \nu(J_{\mathcal{S}}) | \exists \textit{práve } j \textit{ rôznych hodnôt}$$

$$\{\bar{a}_L^{(1)}, \ldots, \bar{a}_L^{(j)}\}, (\bar{s}_1, \ldots, \bar{s}_N, \bar{a}_L^{(i)}) \in \nu(J_{\mathcal{S}\cup\{a_L\}}), 1 \leq i \leq j\};$$

2. $\nu(J_{\mathcal{S}\cup\{a_L\}}) = \sqcup_{j=1}^{\lambda(L-1)} \Sigma_j^{L-1}$, *s*

$$\Sigma_j^{L-1} = \{(\bar{s}_1, \ldots, \bar{s}_N, \bar{a}_L) \in \nu(J_{\mathcal{S}\cup\{a_L\}}) | \exists \textit{práve } j \textit{ rôznych hodnôt}$$

$$\{\bar{a}_{L-1}^{(1)}, \ldots, \bar{a}_{L-1}^{(j)}\}, (\bar{s}_1, \ldots, \bar{s}_N, \bar{a}_L, \bar{a}_{L-1}^{(i)}) \in \nu(J_{\mathcal{S}\cup\{a_L, a_{L-1}\}}), 1 \leq i \leq j\};$$

3. $\nu(J_{\mathcal{S}\cup\{a_L,\ldots,a_h\}}) = \sqcup_{j=1}^{\lambda(h-1)}\Sigma_j^{h-1}$, $2 \leq h \leq L$ *s*

$$\Sigma_j^{h-1} = \{(\bar{s}_1,\ldots,\bar{s}_N,\bar{a}_L,\ldots,\bar{a}_h) \in \nu(J_{\mathcal{S}\cup\{a_L,\ldots,a_h\}}) | \exists \textit{práve } j \textit{ rôznych hodnôt}$$

$$\{\bar{a}_{h-1}^{(1)},\ldots,\bar{a}_{h-1}^{(j)}\}, (\bar{s}_1,\ldots,\bar{s}_N,\bar{a}_L,\ldots,\bar{a}_h,\bar{a}_{h-1}^{(i)}) \in \nu(J_{\mathcal{S}\cup\{a_L,\ldots,a_{h-1}\}}), 1 \leq i \leq j\};$$

Všimnime si, že pre ľubovoľný 0-dimenzionálny ideál $J$, nemôžeme nič povedať o $\lambda(h)$, iba to, že $\lambda(h) \geq 1$ pre každé $1 \leq h \leq L$. Predstavme si teraz triedu ideálov dôležitých pre náš kontext.

**Definícia 3.22.** *S doterajším značením hovoríme, že ideál $J$ je* ***rozvrstvený****, ak:*

1. $\lambda(h) = h$, *pre* $1 \leq h \leq L$ *a*
2. $\Sigma_j^h \neq \emptyset$, $1 \leq h \leq L$, $1 \leq j \leq h$

**Veta 3.23.** *Nech $J$ je radikálový, rozvrstvený ideál, potom pre $1 \leq i \leq L$,*

$$G_i = \sqcup_{\delta=1}^{i} G_{i\delta},$$

*s $G_{i\delta} \neq \emptyset$, $1 \leq \delta \leq i$ a $1 \leq i \leq L$.*
*Naviac*

- $\forall 1 \leq i \leq L$, $G_{ii} = \{g_{ii1}\}$ *(existuje len jeden polynóm v $G_i$ so stupňom $i$ a ohľadom na $a_i$);*
- $\forall 1 \leq i \leq L$, $Lp(g_{ii1}) = 1$, $lt(g_{ii1}) = a_i^i$.

V ďalšej definícii adaptujeme ideál $J_w$ z definície na opravovanie chýb.

**Definícia 3.24.** *Nech $C = \Omega(q, b, q^m, L, \mathcal{P})$ je neobsahujúci nulu, maximálny odmocninový kód, so schopnosťou opravy $t$ chýb. Označme $J^{C,t}$ ideál:*

$$J^{C,t} \subset F_{q^m}[x_1,\ldots,x_r,z_1,\ldots,z_t,y_1,\ldots,y_t]$$

$$J^{C,t} = (\{\sum_{h=1}^{t} y_h g_s(z_h) - x_s\}_{1\leq s\leq r}, \{y_j^{q-1} - 1\}_{1\leq j\leq t},$$
$$\{z_i z_j p_{ij}(z_i,z_j)\}_{i\neq j, 1\leq i,j\leq t}, \{z_j^{n+1} - z_j\}_{1\leq j\leq t}). \tag{3.3}$$

*$G^{C,t}$ je Gröbnerova báza ideálu $J^{C,t}$ s ohľadom na $>$.*

Všimnime si, že premenné $x_1,\ldots,x_r$ reprezentujú samoopravné syndrómy, $z_1,\ldots,z_t$ pozície chýb a $y_1,\ldots,y_t$ hodnoty chýb.

**Lemma 3.25.** *Ideál $J^{C,t}$ je radikálový a rozvrstvený.*

**Lemma 3.26.** *V Gröbnerovej báze $G^{C,t}$ existuje polynóm typu:*

$$g = z_t^t + a_{t-1}z_t^{t-1} + \cdots + a_0, a_i \in F_{q^m}[X]$$

*(Stačí vziať $i = t$ a $g = g_{tt1}$).*

**Veta 3.27.** *Ak kód $C$ je vlastný maximálny odmocninový neobsahujúci nulu so schopnosťou opravy $t$, potom $C$ vlastní polynóm pre detekciu chýb.*

*Dôkaz.* Z predošlého faktu, polynóm typu $g = z_t^t + a_{t-1}z_t^{t-1} + \cdots + a_0, a_i \in F_{q^m}[X]$ existuje v $J^{C,t}$. Pretože $C$ je vlastný, všetky polynómy ideálu $J^{C,t}$ majú koeficienty v $F_q$ a teda $g$ musí ležať v $F_q[X, z_t]$. Tvrdíme, že Ł $= g(X, z_t) \in F_q[X, z_t]$ je polynóm pre detekciu chýb pre kód $C$. Polynóm $g$ určite vyhovuje podmienke 1 v Definícii polynómu pre detekciu chýb, k podmienke dva je dobré si uvedomiť, že samoopravné syndrómy $\nu(J^{C,t} \cap F_q[X])$ a $g$ sú v $J^{C,t}$, prečo dostaneme správnu násobnosť nuly článok [4] neobsahuje. □

Pretože cyklické kódy sú vlastné maximálne odmocninové neobsahujúce nulu, dostaneme špeciálny prípad tejto vety. A to, že: Cyklické kódy majú polynómy pre detekciu chýb.

# Literatúra


[1] Ge W.: *Gröebner Bases Theory and The Diamond Lemma*, Master Thesis, (2006), http://hdl.handle.net/10012/2951

[2] P. Gianni: *Properties of Gröbner bases under Specializations* in Lecture notes in Computer Science, vol. 378 (1989) 293-297

[3] P.Gianni, B. Trager, G. Zacharias: *Gröbner bases and primary decomposition of polynomial ideals*. In Journal of Symb. Comp.(6) (1988) 149 - 167

[4] M.Giorgetti, M. Sala: *A commutative algebra approach to linear codes*. In: Journal of Algebra (2009) 1-17

[5] E. Kunz: *Introduction to Commutative Algebra and Algebraic Geometry*, Birkauser Boston, (1985)

[6] E. Orsini, M. Sala: *Correcting errors and erasures via syndrome variety*. In Journal of Pure Appllied Algebra 200 (2005) 191-226