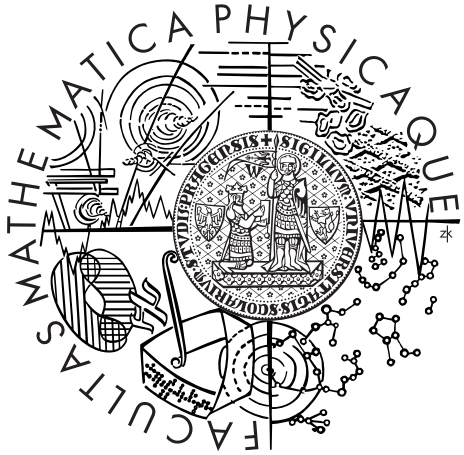
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

DIPLOMOVÁ PRÁCE



Jan Horáček

Kódy, okruhy a moduly

Katedra algebry

Vedoucí diplomové práce:	Mgr. Jan Žemlička, Ph.D.
Studijní program:	Matematika
Studijní obor:	Matematické metody informační bezpečnosti

Praha 2014

Děkuji především svému školiteli Mgr. Janu Žemličkovi, Ph.D. za obětavý přístup, cenné rady a konzultace, které mi vždy ochotně poskytl. Velký dík patří také mým rodičům a mému bratrovi za celkovou podporu.

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Název práce: Kódy, okruhy a moduly

Autor: Jan Horáček

Katedra: Katedra algebry

Vedoucí diplomové práce: Mgr. Jan Žemlička, Ph.D., Katedra algebry

Abstrakt: Tato práce se zabývá lineárními samoopravnými kódy nad řetězcovým okruhem. Lineárním kódem nad řetězcovým okruhem R délky n myslíme nějaký R-podmodul modulu R^n. Představíme základní úvod do teorie konečných komutativních řetězcových okruhů a lineárních kódů nad nimi. Klademe zde důraz především na jejich algebraický popis. Studujeme rozsáhleji minimální homogenní a Hammingovy vzdálenosti těchto kódů. Vysvětlíme, jak lze pomocí zobecněného Grayova zobrazení převádět lineární kódy nad řetězcovým okruhem na obecně nelineární kódy nad tělesem. Zabýváme se konstrukcí lineárních kódů nad řetězcovým okruhem a popíšeme konstrukci generujících matic založenou na náhodném generování. Získané kódy pak srovnáme se známými výsledky.

Klíčová slova: kódy, řetězcové okruhy, zobecněné Grayovo zobrazení

Title: Codes, rings and modules

Author: Jan Horáček

Department: Department of Algebra

Supervisor: Mgr. Jan Žemlička, Ph.D., Department of Algebra

Abstract: This work is focused on linear error-correcting codes over chain rings. By a linear code over a chain ring R of length n, we mean a R-submodule of the module R^n. The basic introduction to the theory of finite commutative chain rings and linear codes over them is given. We especially emphasize here their algebraic description. Minimal homogenous and Hamming distances of these codes are extensively studied. We explain, how the generalized Gray map can transform linear codes over a chain ring into general non-linear codes over a field. We deal with the construction of linear codes over a chain ring and the construction of generator matrices based on random generation is described. Obtained codes are compared with known results.

Keywords: codes, chain rings, generalized Gray map

Obsah

Předmluva **2**
Motivace a historie . . . 2
Použité značení . . . 2
Cíl, struktura a přínos této práce . . . 3

1 Okruhy v teorii kódů **5**
1.1 Řetězcové okruhy . . . 5
1.2 Konečná tělesa . . . 8
1.3 Galoisovy okruhy a okruhy $\mathbb{Z}_{p^e}$ . . . 8
1.4 Další příklady řetězcových okruhů . . . 9
1.5 Algoritmy . . . 11
1.6 Další příklady okruhů . . . 16

2 Kódy nad okruhem **18**
2.1 Definice kódu . . . 18
2.2 Struktura kódů nad řetězcovým okruhem . . . 18
2.3 Duální kódy . . . 24
2.4 Volné kódy . . . 28

3 Váhy a izometrie **30**
3.1 Váhy, homogenní váha . . . 30
3.2 Hammingova váha a projekce . . . 33
3.3 Grayovo zobrazení . . . 38

4 Konstrukce kódů **45**
4.1 Shrnutí předchozí kapitoly . . . 45
4.2 Zvednutí kódu . . . 45
4.3 Minimální homogenní vzdálenost . . . 48
4.4 Testování . . . 51
4.5 Shrnutí testování . . . 55

Závěr **58**

Seznam použité literatury **59**

Seznam tabulek **62**

Příloha **63**

Předmluva

Motivace a historie

Řetězcové okruhy jsou studovány zejména v kontextu algebraické teorie čísel a geometrie. V poslední době se dostaly do ohniska zájmu i ve výzkumu samoopravných kódů. Kódy nad konečnými okruhy však postrádají některé výhody lineárních kódů nad konečnými tělesy. Nemluvě o tom, že už pro některé zajímavé třídy kódů nad tělesem (jako např. BCH kódy, Reed-Mullerovy kódy) byly dobře známy a implementovány dekódující algoritmy. Obecně nebyla tedy potřeba a poptávka pracovat v obecnějším nastavení, a to s okruhy.

Velký průlom nastává, když Calderbank a kol. v článku [4] popíší některé známé nelineární kódy nad tělesem jakožto obrazy tzv. Grayova zobrazení lineárních kódů nad $\mathbb{Z}_4$. Jedná se o Kerdockovy a Preparatovy kódy, které obsahují alespoň dvakrát více kódových slov než lineární kódy při stejné délce a minimální vzdálenosti.

Postupně se začali studovat kódy nad okruhy $\mathbb{Z}_{p^e}$, kde p je prvočíslo a číslo $e \in \mathbb{N}$, posléze kódy nad Galoisovými okruhy až se přirozeně dospělo k obecným řetězcovým okruhům. Strukturou lineárních kódů nad nimi se zabývají Norton a Graham v [24] a společně s Salageanovou shromáždili důležité výsledky ohledně minimální Hammingovy vzdálenosti těchto kódů v [25]. Další variantou, jak lze studovat lineární kódy nad řetězcovým okruhem, je spíše geometrický pohled jako např. v článku [19].

Když byla popsána struktura lineárních kódů nad řetězcovými okruhy, začalo se s pokusy zobecnit koncept Grayova zobrazení na všechny řetězcové okruhy. To se úspěšně podařilo Greferathovi a Schmidtovi v [17], což přineslo úspěchy v lineární konstrukci nelineárních kódů s výbornými parametry např. v [12, 17].

Použité značení

Často opakující značení je připomenuto na začátku každé kapitoly. Shrňme používané značení týkající se okruhů. Okruh R v celé této práci značí konečný komutativní okruh, který je řetězcový. Maximální ideál R je M, M je generován prvkem u a prvek u má stupeň nilpotence m. Zbytkové těleso R/M má q prvků a značíme ho $\mathbb{F}$ či $\mathbb{F}_q$. Pruhem označujeme kanonickou projekci $R \to \mathbb{F}$. Ať $T \subseteq R$ je množina, jejichž prvky modulo M tvoří reprezentanty tříd faktorokruhu R/M. Navíc předpokládáme, že $0 \in T$. Pro okruh S značí S^* množinu všech jeho invertibilních prvků a $S[x_1, \ldots, x_n]$ okruh polynomů nad S v proměnných $x_1, \ldots, x_n$. Generátory ideálů uzavíráme do ostrých závorek $\langle\ \rangle$. Okruhy $\mathbb{Z}_e$, $\mathrm{GF}(p^d)$ a $\mathrm{GR}(p^e, d)$ značí postupně okruhy $\mathbb{Z}/\langle e \rangle$, konečné těleso o mohutnosti p^d a Galoisův okruh

charakteristiky p^e a hodnosti d.

V kapitole o kódech využíváme standardní značení související s maticemi (např. transpozice matice A je A^T). Jednotkovou matici řádu $j \in \mathbb{N}$ značíme I_j. Kód C až na drobné výjimky značí lineární kód délky n nad řetězcovým okruhem R. Generující resp. kontrolní matici ve standardním tvaru označujeme G resp. H.

Cíl, struktura a přínos této práce

Cílem této práce bylo vybrat zajímavou třídu konečných okruhů pro samoopravné kódy a prezentovat základní principy v teorii lineárních kódů nad těmito okruhy. Za tuto třídu jsme vybrali řetězcové okruhy. Téma práce jsme vybírali také s ohledem na zaměření diplomové práce M. Sobotky [27], která je soustředěna na zvedání a ořezávání kódů (s důrazem na samodualitu kódů) a na teorii invariantů pro modulární a p-adické kódy. Proto jsme zdvihání kódů probrali pouze ve zkrácené formě a výsledky ohledně samoduálních kódů, které byly pro konkrétní řetězcový okruh podrobně popsány v [27], jsme vynechali. Zvolili jsme si raději témata nová, jako např. zobecněné Grayovo zobrazení či studium minimální homogenní a Hammingovy váhy lineárního kódu.

V první kapitole studujeme řetězcové okruhy v takové míře, kterou aplikace v kódech v následujících kapitolách vyžaduje. Klademe zde především důraz na algoritmickou práci s řetězcovými okruhy. Dále ve stručnosti zmiňujeme základní příklady řetězcových okruhů a dalších tříd okruhů, které jsou pro samoopravné kódy vhodné. Důkaz Tvrzení 1.2 v této kapitole je vlastní (znění samotného tvrzení je převzato). Argumentace korektnosti invariantů řetězcového okruhu před Větou 1.3 je vlastní. Všechny důkazy, algoritmy a příklady v podkapitole 1.5 jsou také vlastní kromě důkazu jednoznačnosti v Tvrzení 1.7. Znění tvrzení jsou však až na znění Tvrzení 1.5 a 1.8 převzaté a trochu upravené do našeho kontextu.

V druhé kapitole definujeme lineární kód nad řetězcovým okruhem a jeho generující matici ve standardním tvaru. Podáváme zde přehled o struktuře lineárních kódů nad řetězcovým okruhem. Analyzujeme duální a charakterizujeme volné kódy nad řetězcovým okruhem. Sepsání Algoritmu 5 a Algoritmu 6 je vlastní počin, který byl inspirován článkem [24]. Důkaz Tvrzení 2.4 byl proti tvrzení v původnímu článku [24] pozměněn a podrobněji rozebrán. Tvrzení 2.5 je vlastní a Důsledek v [24, Corollary 3.11] jsme zobecnili a sepsali do Důsledku 2.6. Důkaz Tvrzení 2.7 není v [24] uveden. Toto tvrzení jsme rozšířili a podrobně dokázali.

Ve třetí kapitole studujeme lineární kódy nad řetězcovým okruhem vzhledem Hammingově a homogenní váze. Popisujeme důležitou souvislost minimální Hammingovy vzdálenosti lineárního kódu nad řetězcovým okruhem a jeho torzních kódů. Zbytek kapitoly se zabývá zobecněním Grayova zobrazení pro řetězcové okruhy. Pozorování 3.1 a alternativní důkaz třetího bodu Věty 3.3 je vlastní výsledek. Důkaz Lemmatu 3.2 jsme oproti původnímu článku [25] podrobněji rozebrali. V [25, Remarks 4.4] je poznamenáno, že Věta 3.3 se dá zobecnit i pro nelineární kódy uzavřené na násobení prvkem generátoru maximálního ideálu řetězcového okruhu. To však není pravda. Třídu protipříkladů uvádíme ve vlastní Větě 3.4, která zobecňuje Větu 3.3. Pozorování 3.5 je v [17] uvedeno bez důkazu. Důkaz jsme zde proto doplnili. Větu 3.7 jsme oproti původnímu důkazu v [17] podrobněji dokázali.

V poslední kapitole se zabýváme konstrukcí lineárních kódů nad řetězcovým okruhem na bázi Henselova zdvihání a podáváme základní odhady na minimální homogenní váhu těchto kódů. Provádíme zde také testování naší konstrukce kódů založené na náhodném generování. Algoritmus 7 je vlastní. Celá podkapitola 4.4 je vlastní včetně Algoritmu 8, Tvrzení 4.2 a Pozorování 4.3. Během testování se nám podařilo nalézt zajímavé lineární kódy nad řetězcovým okruhem, jejichž Grayovy obrazy mají dobré parametry. Algoritmem 8 jsme obdrželi dva optimální nelineární binární kódy. Optimalita v tomto případě znamená, že neexistuje žádný jiný nelineární binární kód s větší minimální Hammingovou vzdáleností při stejné délce a mohutnosti. Dále jsme zkonstruovali několik lineárních kódů nad $\mathbb{Z}_4$, které měly větší minimální Leeovu vzdálenost než lineární kódy o stejné délce a mohutnosti uvedené v databázi kódů [2]. Následně byly tyto kódy do databáze [2] přidány.

Kapitola 1

Okruhy v teorii kódů

V této kapitole představíme algebraický základ pro teorii okruhů, který později aplikujeme v samoopravných kódech. Nezbytné výsledky pro další kapitoly dokážeme. Důkazy volíme raději elementárního rázu, než abychom se odkazovali na hlubší poznatky. Věříme, že takovýto přístup je přímočařejší a poskytne sám o sobě dostatečné zázemí pro další práci.

Tato kapitola je inspirována článkem Nortona a Sălăgeana [24], kde je na začátku uveden seznam výsledků důležitých pro teorii kódů nad řetězcovými okruhy, které využijeme hned v úvodu kapitoly a v pojednání o algoritmech. Informace o Galoisových okruzích jsme čerpali z [8, Proposition 2.8]. V sekci 1.4 vycházíme ze zdroje [6]. Tam jsou také uvedeny výsledky týkající se určování počtu izomorfních tříd řetězcových okruhů se zadanými invarianty (jedná se o otevřený problém). V poslední sekci, která je přehledová, jsme shromáždili odkazy na zajímavé třídy okruhů jiné než řetězcové, které se využívají v teorii kódů.

1.1 Řetězcové okruhy

Pro potřeby teorie kódů potřebujeme takovou třídu okruhů, aby lineární kódy nad ní měly velmi podobné vlastnosti jako lineární kódy nad konečnými tělesy. V [31] je uvedeno, že identity MacWilliamsové platí právě pro tzv. Frobeniovy okruhy, tudíž je pro naše účely tato třída okruhů vhodná. Frobeniovy okruhy uvedeme v širším kontextu v sekci 1.6. Zároveň v plné obecnosti mají Frobeniovy okruhy velmi složitou strukturu a není lehké s nimi pracovat.

Jako kompromis zvolíme za náš střed zájmu řetězcové okruhy, které jsou podmnožinou Frobeniových okruhů a dají se lépe aplikovat na teorii kódů. Řetězcové okruhy obsahují důležité třídy okruhů jako $\mathbb{Z}_{p^e}$, kde p je prvočíslo a $e \in \mathbb{N}$, nebo Galoisovy okruhy, které byly po konečných tělesech využívány pro účely samoopravných kódů vůbec jako první. O těchto okruzích se zmíníme šířeji v sekci 1.2 a 1.3.

Definice (Řetězcový okruh)**.** *Levý resp. pravý řetězcový konečný okruh R je okruh, jehož svaz levých resp. pravých ideálů tvoří lineární řetězec uspořádaný inkluzí.*

To znamená, že existuje $m \in \mathbb{N}$ takové, že

$$R = I_0 \supseteq I_1 \supseteq \cdots \supseteq I_m = 0$$

jsou všechny jeho levé resp. pravé ideály. Nás budou nadále nejvíce zajímat okruhy konečné a komutativní. V případě komutativity však pojmy levého a pravého řetězcového okruhu splývají triviálně, a proto budeme mluvit pouze o řetězcových okruzích.

Úmluva. *Okruh R v celé této práci značí **konečný komutativní** okruh, který je **řetězcový**. Dále o každém okruhu předpokládáme, že je asociativní a obsahuje jednotku (navíc s vlastností $0 \neq 1$).*

Takovéto okruhy se také nazývají uniseriální. Z řetězcového řazení ideálů vidíme, že řetězcový okruh je lokální, tj. má jeden maximální ideál. Označme ho M. V tomto případě pojmy jako Jacobsonův radikál či maximální ideál splývají. Nadále bude pro nás zásadní, že všechny ideály v R jsou hlavní. Důkaz je převzat z [13, str. 1514].

Pozorování 1.1. *Okruh R je okruhem hlavních ideálů.*

Důkaz. Nepřímo. Mějme ideál I okruhu R, který není hlavní. Jelikož je R konečný, je I konečně generovaný. Ať $I = \langle a_1, \ldots, a_l \rangle$, kde $\{a_1, \ldots, a_l\}$ je nejmenší možná množina generátorů I. Musí platit, že $l \geq 2$, jinak by I byl hlavní. Ideály $\langle a_1 \rangle$ a $\langle a_2 \rangle$ nejsou do sebe vřazeny inkluzí. Pokud by např. $\langle a_1 \rangle \subseteq \langle a_2 \rangle$, tak by to bylo ve sporu s vybráním nejmenší možné množiny generátorů. Okruh tudíž není řetězcový. □

Vidíme tedy, že existuje $u \in R$ tak, že maximální ideál je tvaru $M = \langle u \rangle = uR$. Ukážeme, že u je navíc nilpotentní, tj. existuje $m \in \mathbb{N}$ takové, že $u^m = 0$. Nejmenší možné takové m nazýváme indexem či stupněm nilpotence prvku u.

Tvrzení 1.2 (Nilpotence)**.** *Mějme okruh R s maximálním ideálem $M = uR$.*

1. *Prvek u je nilpotentní. Označme nadále jeho index nilpotence m.*
2. *Všechny ideály R jsou tvaru $u^i R$, kde $i = 0, \ldots, m$. Svaz ideálů R vypadá takto:*
$$R = u^0 R \supsetneq u^1 R \supsetneq \cdots \supsetneq u^m R = 0.$$
3. *Všechny nilpotentní prvky R jsou uR.*
4. *Všechny invertibilní prvky R jsou $R \setminus uR$.*

Důkaz. 1. Sporem předpokládejme, že u není nilpotentní, tj. $u^i \neq 0$ pro všechny $i \in \mathbb{N}$. Definujme pro $i \in \mathbb{N}$ zobrazení $\lambda_i : R \to u^i R$ předpisem $r \mapsto u^i r$. Zobrazení λ_i je surjektivní homomorfismus R-modulů s jádrem $\ker(\lambda_i) \subsetneq R$, protože $\lambda_i(1) = u^i \neq 0$. Dle První věty o izomorfismu pro moduly jest

$$R/\ker(\lambda_i) \simeq u^i R.$$

Tento izomorfismus je indukován λ_i. Maximální ideál v $R/\ker(\lambda_i)$ je $uR/\ker(\lambda_i)$ a zobrazí se izomorfně na maximální ideál $\lambda_i(uR) = u^{i+1}R$ v $u^i R$. Jelikož je $u^{i+1}R$ maximální, tak $u^{i+1}R \subsetneq u^i R$.

Jelikož $u^i R \neq 0$ pro všechna $i \in \mathbb{N}$, tak dostáváme nekonečný řetězec ostře klesajících ideálů:

$$R \supsetneq uR \supsetneq u^2 R \supsetneq u^3 R \supsetneq \ldots.$$

To však v konečném okruhu nastat nemůže. Spor. Musí proto existovat $m \in \mathbb{N}$, že $u^m = 0$. Vezměme nadále takové m nejmenší možné.

2. Z předchozího bodu známe tyto ideály R:

$$u^0R \supsetneq u^1R \supsetneq u^2R \supsetneq \cdots \supsetneq u^mR = 0.$$

Ukážeme, že pro $i = 0, \ldots, m-1$ neexistuje ideál I v R takový, že

$$u^{i+1}R \subsetneq I \subsetneq u^iR.$$

Homomorfismus λ_i upravíme na surjektivní homomorfismus R-modulů $\hat{\lambda}_i : R \to u^iR/u^{i+1}R$ s předpisem $r \mapsto u^ir + u^{i+1}R$. Jistě $uR \subseteq \ker(\hat{\lambda}_i)$, neboť pro $r \in R$ je $\hat{\lambda}_i(ur) = u^{i+1}r + u^{i+1}R = 0 + u^{i+1}R$ v $u^iR/u^{i+1}R$. Zároveň $\ker(\hat{\lambda}_i) \subsetneq R$, protože z předchozího bodu víme, že $u^{i+1}R \subsetneq u^iR$. Dostáváme tak řetězec ideálů

$$uR \subseteq \ker(\hat{\lambda}_i) \subsetneq R.$$

Jelikož uR je maximální v R, tak $\ker(\hat{\lambda}_i) = uR$. Dle První věty o izomorfismu pro moduly jest

$$R/uR \simeq u^iR/u^{i+1}R,$$

kde R/uR je těleso, které má pouze dva nevlastní ideály. Tím jsme dokázali, že $u^iR/u^{i+1}R$ obsahuje pouze dva podmoduly, a tudíž žádný ideál I s vlastností $u^{i+1}R \subsetneq I \subsetneq u^iR$ neexistuje.

3. a 4. Tyto body dokážeme zároveň. Všechny prvky z uR jsou nilpotentní, neboť pro $r \in R$ je $(ur)^m = u^mr^m = 0$. Dokážeme, že další jiné neexistují. Mějme $a \in R \setminus uR$. Platí, že $a + uR \neq 0 + uR$ v tělese R/uR, a proto existuje k prvku $a+uR$ inverz v R/uR. Existuje tedy $b \in R$ takové, že $ab+uR = 1+uR$ v R/uR, neboli $ab = 1 - ur$ pro nějaké $r \in R$. Pak máme

$$(1-ur) \cdot \underbrace{\sum_{i=0}^{m-1} (ur)^i}_{\text{označme jako } c} = 1 - (ur)^m = 1.$$

Inverz k a v R je pak bc, neboť přenásobením rovnosti $ab = 1 - ur$ prvkem c dostáváme $a(bc) = 1$. Proto prvky z $R \setminus uR$ jsou invertibilní v R. Množina všech invertibilních prvků s násobením tvoří grupu, a proto je uzavřená na mocnění. Mocněním invertibilního prvku tedy nulu nedostaneme (jinak by to byl spor s tím, že nula je invertibilní), a tedy prvky $R \setminus uR$ nejsou nilpotentní.

Ukážeme, že žádné jiné invertibilní prvky než z $R \setminus uR$ nejsou. Mějme $0 \neq b \in uR$. Ze začátku důkazu 3. a 4. bodu víme, že b nilpotentní. Ať $i \in \mathbb{N}$ je nejmenší možné takové, že $b^i = 0$. Předpokládejme, že existuje $c \in R$, že $bc = 1$. Přenásobme tuto rovnost b^{i-1} a dostaneme

$$0 = b^ic = b^{i-1},$$

což je spor s minimalitou i. □

Faktorokruh R/M je konečné těleso, neboť $M = uR$ je maximální. Toto těleso nazýváme zbytkové (či reziduální) těleso a budeme ho značit $\mathbb{F}$.

Kanonickou projekci $R \to \mathbb{F}$ budeme značit pruhem. Tj. pro $r \in R$ je $\overline{r} = r + M$. Je snadné nahlédnout, že kanonická projekce je okruhový homomorfismus. Přirozeně rozšíříme kanonickou projekci na více složek, a to na matice a polynomy nad R. Značení pruhem budeme používat i pro tyto varianty. Např. projekce $c = (c_1, \ldots, c_n) \in R^n$ je $\overline{c} = (c_1 + M, \ldots, c_n + M)$ atp. Shrňme značení, které bude platit v celé práci.

Značení. *Maximální ideál R je M, M je generován prvkem u a prvek u má stupeň nilpotence m. Zbytkové těleso R/M má q prvků a značíme ho $\mathbb{F}$ či $\mathbb{F}_q$. Pruhem označujeme kanonickou projekci $R \to \mathbb{F}$. Ať $T \subseteq R$ je množina, jejichž prvky modulo M tvoří reprezentanty tříd faktorokruhu R/M. Navíc předpokládáme, že $0 \in T$.*

Připomeňme ještě, že pro okruh S značí S^* množinu všech jeho invertibilních prvků a $S[x_1, \ldots, x_n]$ okruh polynomů nad S v proměnných $x_1, \ldots, x_n$. Generátory ideálů uzavíráme do ostrých závorek $\langle\ \rangle$. Nyní uvedeme základní příklady tříd řetězcových okruhů.

1.2 Konečná tělesa

Ať p je libovolné prvočíslo a $d \in \mathbb{N}$. Konečné těleso o p^d prvcích se často v literatuře značí $\mathrm{GF}(p^d)$ jako Galoisovo těleso o mohutnosti p^d.

Prvotělesa jsou definována jako $\mathrm{GF}(p) = \mathbb{Z}_p$. Mějme ireducibilní polynom f nad $\mathrm{GF}(p)$ stupně d. Poznamenejme známý fakt, že takovýto polynom f najdeme pro libovolné $d \in \mathbb{N}$. Pak platí

$$\mathrm{GF}(p^d) \simeq \mathrm{GF}(p)[x] / \langle f \rangle .$$

Prvky konečných těles tedy můžeme reprezentovat jako polynomy nad prvotělesem modulo ireducibilní polynom. Těleso $\mathrm{GF}(p^d)$ je příklad poněkud speciálního řetězcového okruhu, neboť má pouze nevlastní ideály $0 \subseteq R$. Jako jeho maximální ideál bereme $M = \langle 0 \rangle$ generovaný 0 mající stupeň nilpotence rovný 1. Ideál $\langle 0^0 \rangle$ považujeme za $\langle 1 \rangle = R$. Zbytkové těleso $\mathrm{GF}(p^d)/\langle 0 \rangle$ je samotné $\mathrm{GF}(p^d)$ či s předchozím značením $\mathbb{F}_q$, kde $q = p^d$.

1.3 Galoisovy okruhy a okruhy $\mathbb{Z}_{p^e}$

Galoisovy okruhy připomínají konstrukci Galoisových těles. Mějme opět libovolné prvočíslo p a $e \in \mathbb{N}$. Ať $f \in \mathbb{Z}_{p^e}[x]$ je monický ireducibilní polynom nad $\mathbb{Z}_{p^e}$ stupně $d \in \mathbb{N}$ takový, že $\overline{f}$ (tzn. redukce jeho koeficientů modulo p) je ireducibilní polynom v $\mathbb{Z}_p[x]$. Takovýto polynom f nazýváme základní ireducibilní polynom nebo Galoisův polynom. Základní ireducibilní polynom f existuje pro libovolné $d \in \mathbb{N}$ (viz [24, Lemma 2.5]). Pak okruh

$$\mathrm{GR}(p^e, d) \simeq \mathbb{Z}_{p^e}[x] / \langle f \rangle$$

nazýváme Galoisovým okruhem. Okruh $\mathrm{GR}(p^e, d)$ je jednoznačně až na izomorfismus určen koeficienty p, e, d (tj. nezáleží na konkrétní volbě f), proto se mu

říká Galoisův okruh charakteristiky p^e a hodnosti (ranku) d. Všimněme si, že $\mathrm{GR}(p^e, 1) \simeq \mathbb{Z}_{p^e}$ a $\mathrm{GR}(p, d) \simeq \mathrm{GF}(p^d)$.

Jeho maximální ideál je generován p, který má stupeň nilpotence e. Reziduální těleso $\mathrm{GR}(p^e, d)/\langle p \rangle$ je $\mathrm{GF}(p^d)$.

1.4 Další příklady řetězcových okruhů

Mějme opět řetězcový okruh R s již zavedeným značením. V [6] jsou následující hodnoty nazývány invarianty okruhu R:

p, e Charakteristika R je p^e, kde p je prvočíslo a $1 \leq e \leq m$.

d Zbytkové těleso R/M má p^d prvků (tj. $q = p^d$).

t Přirozené číslo takové, že $(\underbrace{1 + \cdots + 1}_{p\times})R = pR = u^t R$, kde $1 \leq t \leq m$.

h Přirozené číslo takové, že $m = (e-1)t + h$, kde $1 \leq h \leq t$.

V textu ztotožňujeme přirozené číslo s příslušným součtem 1 v daném okruhu. Nyní zdůvodníme, proč dané hodnoty dávají smysl. Zbytkové těleso R/M je konečné těleso. Je dobře známo, že každé konečné těleso musí mít mohutnost mocniny prvočísla. Toto prvočíslo, které označíme p, je zároveň charakteristikou R/M.

Předpokládejme, že charakteristika R je tvaru $p^e \cdot a$, kde p nedělí $a \in \mathbb{N}$ a $e \geq 0$. Prvek $a + M$ je nenulový v R/M, protože charakteristika p tělesa R/M nedělí a. Proto $a \in R \setminus M$ a z Tvrzení 1.2 je $a \in R^*$. Jelikož $p^e \cdot a = 0$ v R, přenásobením rovnosti a^{-1} obdržíme $p^e = 0$. Z toho, že $p^e \cdot a$ je charakteristika, vyplývá $a = 1$. Charakteristika R je vskutku p^e. Jelikož p je nilpotentní, musí dle Tvrzení 1.2 být tvaru $p = ur$ pro nějaké $r \in R$. Platí $p^m = (ur)^m = 0$. Jelikož index nilpotence p je e, tak $e \leq m$. Pokud by $e = 0$, tak $0 = p^0 = 1$, což je spor s naší úmluvou o okruzích.

Prvek p je nilpotentní a dle Tvrzení 1.2 existuje $r \in R$, že $p = ur$. Tedy určitě $t \geq 1$. Pokud $e = 1$, tak $pR = 0 = u^m R$ a volíme $t = m$. Ze struktury ideálů R popsané v Tvrzení 1.2 nemůže nastat $t > m$.

Rovnost $pR = u^t R$ vlastně znamená, že $p = u^t s$, kde $s \in R^*$. Tímto typem rozkladu se podrobněji zabýváme v Tvrzení 1.7. Dostáváme tak

$$\overbrace{p^{e-1}}^{\neq 0} = u^{(e-1)t} \overbrace{s^{e-1}}^{\neq 0},$$

$$\underbrace{p^e}_{=0} = u^{et} \underbrace{s^e}_{\neq 0}.$$

Z první rovnice plyne, že $u^{(e-1)t} \neq 0$, a proto $(e-1)t < m$. Z druhé rovnice plyne, že $u^{et} = 0$, a proto $m \leq et$. Pišme

$$h = m - (e-1)t = m - et + t.$$

První nerovnost dává $h \geq 1$ a druhá $h \leq t$.

Mezi invarianty není zařazen přímo index nilpotence m ale raději h, což je záležitostí konvence. Proč jsou tato čísla vybrána pro charakterizaci R a proč je nazýváme invarianty bude jasné až z následující věty. Řekneme, že polynom $g \in \mathrm{GR}(p^e, d)[x]$ je Eisensteinův polynom stupně t, pokud je tvaru

$$g = x^t - p(a_{t-1}x^{t-1} + \cdots + a_0),$$

kde $a_1, \ldots, a_{t-1} \in \mathrm{GR}(p^e, d)$ a $a_0 \in \mathrm{GR}(p^e, d)^*$. Důkaz následující věty uvedený v [6] je nad rámec naší práce, jejíž těžiště leží spíše v samoopravných kódech. Tuto větu potřebujeme pouze pro lepší pochopení reprezentace vstupů do algoritmů v následující podkapitole a pro uvedení dalších příkladů řetězcových okruhů.

Věta 1.3 (Charakterizace řetězcových okruhů)**.** *Ať R je s invarianty (p, e, d, t, h) definované výše. Pak existuje $g \in \mathrm{GR}(p^e, d)[x]$ Eisensteinův polynom stupně t takový, že*

$$R \simeq \mathrm{GR}(p^e, d)[x]/\langle g, p^{e-1}x^h\rangle.$$

Na druhou stranu, každý takovýto faktorokruh definovaný hodnotami (p, e, d, t, h) jako výše je řetězcový.

Okruh $\mathrm{GR}(p^e, d)[x]/\langle g, p^{e-1}x^h\rangle$ je tedy řetězcový s maximálním ideálem generovaný x stupně nilpotence $m = (e-1)t + h$. Věta dává mnoho zajímavých příkladů řetězcových okruhů pro teorii kódů. Podívejme se blíže na některé řetězcové okruhy pro konkrétní invarianty. Začněme s případem $e = 1$. Pak $t = h = m$ a $g = x^m$. Dle Věty 1.3

$$R \simeq \mathrm{GR}(p, d)[x]/\langle g, x^m\rangle \simeq \mathrm{GF}(p^d)[x]/\langle x^m\rangle.$$

Žádný jiný zástupce pro $e = 1$ až na izomorfismus neexistuje.

Dále probereme situaci $m = 2$. Jediné přípustné invarianty jsou $(p, 1, d, 2, 2)$ a $(p, 2, d, 1, 1)$. První zmiňovaný je dle předchozího případu tvaru $\mathrm{GF}(p^d)[x]/\langle x^2\rangle$. Druhý je dle Věty 1.3 pro $a \in \mathrm{GR}(p^2, d)^*$ tvaru

$$R \simeq \mathrm{GR}(p^2, d)[x]/\langle x - pa, px\rangle \simeq \mathrm{GR}(p^2, d)[x]/\langle x - pa\rangle \simeq \mathrm{GR}(p^2, d),$$

protože $p(x - pa) = px - p^2a = px$ v $\mathrm{GR}(p^2, d)[x]$. Kromě těchto dvou žádný jiný řetězcový okruh s $m = 2$ až na izomorfismus neexistuje.

Z věty vyplývá, že izomorfní řetězcové okruhy mají stejné invarianty. To je důvod, proč jim říkáme invarianty. Na druhou stranu existují neizomorfní řetězcové okruhy se stejnými invarianty, protože Eisensteinův polynom není určen jednoznačně. Např. okruhy

$$\mathbb{Z}_9[x]/\langle x^2 - 3{,}3x\rangle, \quad \mathbb{Z}_9[x]/\langle x^2 - 6, 3x\rangle$$

jsou řetězcové a mají stejné invarianty, ale nejsou izomorfní. Tento příklad i s důkazem je uveden v [14].

I když se v celé práci zabýváme výhradně komutativními řetězcovými okruhy, tak na tomto místě zdůrazníme, že existují i nekomutativní řetězcové okruhy. Dokonce je lze obdobně charakterizovat jako ve Větě 1.3 (viz [5]). Každý konečný nekomutativní řetězcový okruh S je totiž tvaru

$$S \simeq \mathrm{GR}(p^e, d)[x, \sigma]/\langle g, p^{e-1}x^h\rangle,$$

kde σ je automorfismus $\mathrm{GR}(p^e, d)$ a $\mathrm{GR}(p^e, d)[x, \sigma]$ je polynomiální okruh v nekomutativní proměnné x. Je to tedy polynomiální okruh v proměnné x nad $\mathrm{GR}(p^e, d)$ splňující navíc $xr = \sigma(r)x$ pro každé $r \in \mathrm{GR}(p^e, d)$.

Nejmenší nekomutativní příklad řetězcového okruhu vzhledem k počtu prvků lze popsat jako $\mathbb{F}_4 \times \mathbb{F}_4$ s operacemi definovanými takto

$$(a, b) + (c, d) = (a + c, b + d),$$
$$(a, b) \cdot (c, d) = (ac, ad + bc^2).$$

Nekomutativitu vidíme například z násobení prvků $(0, 1)$ a $(2, 0)$:

$$(0, 1) \cdot (2, 0) = (0, 4) \neq (0, 2) = (2, 0) \cdot (0, 1).$$

Tento příklad řetězcového okruhu uvádí Kleinfeld v [22].

1.5 Algoritmy

Každý algoritmus vyžaduje nějakou datovou realizaci vstupu. Vstupy v našem případě budou prvky řetězcového okruhu R. Detailní časovou analýzou algoritmů se zde zabývat nebudeme. Je totiž úzce spjata s implementací operací v příslušném okruhu. Předpokládejme, že R je reprezentováno jako faktorokruh polynomů nad Galoisovým okruhem ve smyslu Věty 1.3. Toto však není jediná realizace. Mnohdy je výhodnější reprezentace z výstupu Algoritmu 1. Připomeňme, že $T \subseteq R$ je množina, jejichž prvky T modulo M tvoří reprezentanty tříd faktorokruhu R/M. Navíc předpokládáme, že $0 \in T$.

Uvedeme hned dva algoritmy. První bude sloužit k analýze samotné reprezentace (tj. dokázání existence a jednoznačnosti) a druhý bude již více prakticky zaměřen.

Algoritmus 1 Reprezentace $r = \sum_{i=0}^{m-1} u^i r^{(i)}$

Vstup: $r \in R$, $T \subseteq R$ jako výše.
Výstup: $r^{(0)}, \ldots, r^{(m-1)} \in T$ takové, že $r = \sum_{i=0}^{m-1} u^i r^{(i)}$.

1: **for** $0 \leq i \leq m - 1$ **do**
2: Nalezni $t \in T$ takové, že $r + M = t + M$.
3: $r^{(i)} \leftarrow t$
4: Nalezni $s \in R$ takové, že $r - t = us$.
5: $r \leftarrow s$
6: **end for**
7: Vrať $r^{(0)}, \ldots, r^{(m-1)}$ jako výstup.

Tvrzení 1.4 (Algoritmus 1)**.** *Algoritmus 1 je korektní, konečný a na výstupu dá požadovanou reprezentaci. Navíc pro $r \in R$ na vstupu tohoto algoritmu jsou prvky $r^{(0)}, \ldots, r^{(m-1)} \in T$ na výstupu Algoritmu 1 s vlastností $r = \sum_{i=0}^{m-1} u^i r^{(i)}$ určeny jednoznačně.*

Důkaz. Konečnost je zřejmá, protože vnitřek cyklu se provede m-krát. Ve 4. kroku takové s existuje, neboť $r - t \in M = uR$. Pro $i = 0$ platí ve 4. kroku $r = us_0 + r^{(0)}$ a v dalším cyklu rozkládáme dále s_0. Dostaneme tak v i-té iteraci:

$$r = u^{i+1} s_i + \sum_{j=0}^{i} u^j r^{(j)}.$$

V poslední iteraci $i = m - 1$ máme $u^m s_{m-1} = 0$. Proto dostaneme na výstupu požadovaný rozklad.

Dokažme jednoznačnost. Mějme

$$\sum_{i=0}^{m-1} u^i r^{(i)} = \sum_{i=0}^{m-1} u^i s^{(i)},$$

kde $r^{(i)}, s^{(i)} \in T$ pro $i = 0, \ldots, m-1$. Postupujme sporem. Vyberme nejmenší možné $j = 0, \ldots, m-1$, že $r^{(j)} \neq s^{(j)}$. Jelikož to jsou různí reprezentanti, tak $r^{(j)} - s^{(j)} \in R \setminus uR$. Z Tvrzení 1.2 je $r^{(j)} - s^{(j)} \in R^*$. Převedením na jednu stranu (nulové členy vynecháme) dostaneme $\sum_{i=j}^{m-1} u^i (r^{(i)} - s^{(i)}) = 0$. Vynásobme sumu prvkem $(r^{(j)} - s^{(j)})^{-1}$ a obdržíme

$$u^j + \sum_{i=j+1}^{m-1} u^i (r^{(i)} - s^{(i)})(r^{(j)} - s^{(j)})^{-1} = 0.$$

Neboli

$$u^j = -\sum_{i=j+1}^{m-1} u^i (r^{(i)} - s^{(i)})(r^{(j)} - s^{(j)})^{-1} \in u^{j+1} R.$$

Proto $u^j R \subseteq u^{j+1} R$. Jelikož je $j < m$, z Tvrzení 1.2 plyne, že $u^j R \supsetneq u^{j+1} R$, což je spor.

□

Značení v kulatých závorkách v horních indexech $r^{(i)}$ budeme nadále používat výhradně ve smyslu, jaký je uveden ve výstupu Algoritmu 1. Tato reprezentace je výhodná pro násobení mocninou u, což je vlastně realizováno pouze nulováním a posunem složek $r^{(i)}$.

Algoritmus 2 Reprezentace $r = \sum_{i=0}^{m-1} u^i r^{(i)}$ (výpočetní verze)

Vstup: $r \in R$, $T \subseteq R$ jako výše.
Výstup: $r^{(0)}, \ldots, r^{(m-1)} \in T$ takové, že $r = \sum_{i=0}^{m-1} u^i r^{(i)}$.

1: $s \leftarrow r$
2: **for** $0 \leq i \leq m-1$ **do**
3: Nalezni $t \in T$ takové, že $u^{m-i-1} s = u^{m-1} t$.
4: $r^{(i)} \leftarrow t$
5: $s \leftarrow s - u^i r^{(i)}$
6: **end for**
7: Vrať $r^{(0)}, \ldots, r^{(m-1)}$ jako výstup.

Tvrzení 1.5 (Algoritmus 2)**.** *Algoritmus 2 je korektní, konečný a na výstupu dá požadovanou reprezentaci.*

Důkaz. Nejdříve ukážeme rovnost $u^{m-1} T = u^{m-1} R$. Inkluze $u^{m-1} T \subseteq u^{m-1} R$ je zřejmá. Naopak mějme $r \in R$. Vezměme $t \in T$ takové, že $\overline{r} = \overline{t}$. To znamená, že $r - t \in uR$. Existuje tedy $a \in R$, že $r = ua + t$. Tuto rovnost přenásobme u^{m-1} a dostaneme rovnost $u^{m-1} r = u^{m-1} t \in u^{m-1} T$.

Dle Tvrzení 1.4 předpokládejme, že na vstupu je již prvek r jednoznačně reprezentován Algoritmem 1.4 jako $r = \sum_{j=0}^{m-1} u^j \hat{r}^{(j)}$, kde $\hat{r}^{(0)}, \ldots, \hat{r}^{(m-1)} \in T$.

Zřejmě v 0-té iteraci v 5. kroku je $r^{(0)} = \hat{r}^{(0)}$ a $s = r - \hat{r}^{(0)}$, neboť $u^m = 0$. Obecněji dostáváme v i-té iteraci v 5. kroku $s \in u^{i+1}R$, neboť

$$s = r - \sum_{j=0}^{i} u^j \hat{r}^{(j)} = \sum_{j \geq i+1} u^j \hat{r}^{(j)}.$$

Ve 3. kroku $(i+1)$-té iterace je $u^{m-i-2}s \in u^{m-1}R$, a proto existuje $t \in T$, že $u^{m-i-2}s = u^{m-1}t$. Navíc je $t = \hat{r}^{(i+1)}$. Tento prvek je později prohlášen za $r^{(i+1)}$. Výstupy z Algoritmu 1 a 2 pro dané r jsou proto shodné.

□

Jak vypadají prvky ideálu u^iR vzhledem k této reprezentaci? Vyjádřeme prvek $r \in R$ jako $r = \sum_{i=0}^{m-1} u^i r^{(i)}$ pomocí Algoritmu 1 popř. Algoritmu 2. Pak

$$u^i r = u^i r^{(0)} + \cdots + u^i u^{m-i-1} r^{(m-i-1)} + \underbrace{u^i u^{m-i} r^{(m-i)} + \cdots + u^i u^{m-1} r^{(m-1)}}_{=0},$$

protože $u^m = 0$. Pro každý ze zbývajících $m - i$ koeficientů $r^{(0)}, \ldots, r^{(m-i-1)}$ v rozpisu máme $|R/M| = q$ možností, jak ho zvolit. Jako snadný, ale důležitý důsledek tvrzení dostáváme:

Důsledek 1.6 (Mohutnost ideálů)**.** *Pro $i = 0, \ldots, m$ je $|u^iR| = q^{m-i}$.*

Z toho ihned plyne pro $i = 0$, že $|R| = q^m$. Společně s Tvrzením 1.2 dostáváme, že $|R^*| = q^m - q^{m-1}$ a počet nilpotentních prvků R je q^{m-1}.

Díky charakterizaci ideálů ve 4. bodu z Tvrzení 1.2 lze prvky R rozkládat podle mocnin u.

Algoritmus 3 Rozklad $r = u^i s$

Vstup: $0 \neq r \in R$.
Výstup: $i \in \{0, \ldots, m-1\}$ a $s \in R^*$ takové, že $r = u^i s$.
1: $i \leftarrow 0$
2: $s \leftarrow r$
3: **while** s je násobek u **do**
4: Nalezni $t \in R$ tak, aby $s = ut$.
5: $s \leftarrow t$
6: $i \leftarrow i + 1$
7: **end while**
8: Vrať i, s jako výstup.

Nulu můžeme v duchu Algoritmu 3 rozložit třeba na $0 = u^m \cdot 1$. Pro důkaz jednoznačnosti v následujícím tvrzení jsme vycházeli z [23, Proposition 5.2].

Tvrzení 1.7 (Algoritmus 3)**.** *Algoritmus 3 je korektní a konečný. Navíc pro $0 \neq r \in R$ na vstupu je index $i \in \{0, \ldots, m-1\}$ na výstupu s vlastností $r = u^i s$ určen jednoznačně.*

Důkaz. Nejdříve dokážeme korektnost algoritmu. V 8. kroku je již ukončen while cyklus (tj. není splněna podmínka v kroku 3), a tudíž $s \in R \setminus uR$, což dle Tvrzení 1.2 znamená, že $s \in R^*$. Navíc algoritmus dá postupným dělením prvkem u zřejmě požadovaný rozklad.

Vezměme $i \in \{0, \ldots, m-1\}$ největší možné, že $r \in u^i R$. Existuje pak prvek $a \in R$ takový, že $r = u^i a$. Dokážeme sporem, že $a \in R^*$. Pokud $a \notin R^*$, což dle Tvrzení 1.2 znamená $a \in uR$. Pak existuje $b \in R$ takové, že $a = ub$. Dohromady máme

$$r = u^i a = u^i(ub) = u^{i+1}b,$$

což je spor s maximalitou i. Cyklus v algoritmu proběhne nejvýše $m-1$ krát, a proto algoritmus skončí po konečně mnoha krocích.

Dokažme ještě sporem jednoznačnost. Předpokládejme bez újmy na obecnosti, že existují čísla $0 \leq i < j \leq m-1$ a $a, b \in R^*$ takové, že

$$u^j a = r = u^i b.$$

Pak platí, že $u^i a(u^{j-i} - a^{-1}b) = u^j a - u^i b = 0$. Navíc $a^{-1}b \in R^*$, a tedy z Tvrzení 1.2 $a^{-1}b \notin uR$. Dostaneme tak

$$\overline{u^{j-i} - a^{-1}b} = \overline{u^{j-i}} - \overline{a^{-1}b} = -\overline{a^{-1}b} \neq 0.$$

Proto $u^{j-i} - a^{-1}b \notin uR$, což opět z Tvrzení 1.2 znamená, že $u^{j-i} - a^{-1}b$ je invertibilní. To ovšem implikuje, že $u^i = 0$ pro $i < m$, což je spor. □

V Algoritmu 3 se setkáváme s instrukcí typu „pro zadané $s \in uR$ najdi prvek $t \in R$ takový, že $s = ut$“. Jedná se o vytýkání u z prvku s. Tento krok je velmi jednoduchý v reprezentaci z Algoritmu 2, který vydá $s = \sum_{i=0}^{m-1} u^i s^{(i)}$. Jelikož $s \in uR$, tak $s^{(0)} = 0$. Pak můžeme položit $t = \sum_{i=1}^{m-1} u^{i-1} s^{(i)}$. Potom

$$ut = u\left(\sum_{i=1}^{m-1} u^{i-1} s^{(i)}\right) = s.$$

Tvrzení 1.7 má několik důsledků. Často se v našich úvahách budeme setkávat s rovnicemi typu

$$u^i c = 0, \text{ kde } i = 0, \ldots, m-1 \text{ a } c \in R.$$

Ve smyslu předchozího tvrzení rozepíšeme c jako $c = u^j a$, kde $j = 0, \ldots, m-1$ a $a \in R^*$. Aby pravá strana byla nulová, musí být $j \geq m-i$ čili $c \in u^{m-i}R$, neboť násobením invertibilním prvkem a s nenulovým prvkem nulu nedostaneme.

Pomocí předchozího tvrzení lze snadno dokázat, že ideály R jsou tvaru $u^i R$, kde $i = 0, \ldots, m$, což již bylo dokázáno v Tvrzení 1.2. Mějme ideál I v R. Dle Pozorování 1.1 existuje $a \in R$ takové, že $I = aR$. Prvek rozložíme dle Algoritmu 3 na $a = u^i r$, kde $r \in R^*$. Násobení invertibilním prvkem je permutace na R. Proto

$$I = aR = u^i rR = u^i R.$$

Vraťme se zpátky k posledního bodu Tvrzení 1.2. Důkaz pro hledání inverzu byl konstruktivní. Některé kroky ještě optimalizujeme. Myšlenky k počítání inverzu shrneme do Algoritmu 4. Počítání inverzního prvku v R redukujeme Algoritmem 4 na počítání inverzního prvku v $\mathbb{F}$.

Algoritmus 4 Počítání inverzu v R

Vstup: $a \in R$.
Výstup: $d \in R$ takové, že $ad = 1$ nebo „a není invertibilní“.

Spočítej $\overline{a}$.
if $\overline{a} = 0 + M$ **then**
  Vrať na výstupu „a není invertibilní“.
else
  Nalezni $b \in R$ tak, že $b + M$ je inverz k $a + M$ v tělese $\mathbb{F}$.
  $s \leftarrow 1 - ab$
  $c \leftarrow 1$
  while $s \neq 0$ **do**
    $c \leftarrow c + s$
    $s \leftarrow s(1 - ab)$
  end while
  Vrať $d = bc$ jako výstup.
end if

Tvrzení 1.8 (Algoritmus 4)**.** *Algoritmus 4 je korektní, konečný a na výstupu dá požadovaný inverz, pokud byl na vstupu invertibilní prvek z R.*

Důkaz. Vše je již dokázáno v Tvrzení 1.2. Jedinou odlišností je výpočet c. Jistě existuje $r \in R$, že $1 - ab = ur$. Vezměme $j \in 0, \ldots, m-1$ minimální možné, že $u^j(ur) = 0$. Pak $ur \in u^{m-j}R$. Tedy existuje $s \in R$, že $ur = u^{m-j}s$. Platí

$$(1 - ur) \cdot \sum_{i=0}^{m-1} (ur)^i = 1 - (ur)^m = 1.$$

Vezměme horní celou část $k = \left\lceil \frac{m}{m-j} \right\rceil$. Sumu můžeme sčítat pouze do $k-1$, neboť $(ur)^k = (u^{m-j}s)^k = 0$. □

Jednotlivé algoritmy nyní předvedeme na příkladu Galoisova okruhu $\mathrm{GR}(8, 3)$, který reprezentujeme jako $\mathbb{Z}_8[x]/\langle x^3+x+1\rangle$, kde $x^3+x+1 \in \mathbb{Z}_8[x]$ je základní ireducibilní polynom. Využijeme stejné značení proměnných jako v popisu algoritmu (popř. s dolním indexem pro rozlišení různých iterací). V souladu s používaným značením máme $u = 2$, $M = \langle 2\rangle$, $m = 3$, $\mathbb{F} = \mathrm{GF}(8) = \mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$. Položme

$$T = \{0, 1, x, 1 + x, x^2, 1 + x^2, x + x^2, 1 + x + x^2\}.$$

Algoritmus 2

- Vstup: $s_o = 3 + 5x + 2x^2$.
- $4s_0 = 4 + 4x = 4(1 + x)$, $r^{(0)} = 1 + x$.
- $s_1 = 2 + 4x + 2x^2$.
- $2s_1 = 4 + 4x^2 = 4(1 + x^2)$, $r^{(1)} = 1 + x^2$.
- $s_2 = 4x$.
- $s_2 = 4(x)$, $r^{(2)} = x$.

- Výstupní reprezentace: $r = (1 + x) + 2(1 + x^2) + 4(x)$.

Algoritmus 3

- Vstup: $r = 2 + 4x + 2x^2$.
- Nastavme $i = 0$, $s_0 = 2 + 4x + 2x^2$.
- Prvek s_0 je násobkem 2.
- $s_0 = 2(1 + 2x + x^2)$.
- $s_1 = 1 + 2x + x^2$, $i = 1$.
- Prvek s_1 není násobkem 2.
- Výstup: $r = 2(1 + 2x + x^2)$.

Algoritmus 4

- Vstup: $a = 3 + 5x + 2x^2$.
- $\overline{a} = 1 + x \neq 0 + M$.
- $b = x + x^2$, $\overline{a}\overline{b} = 1$ v $\mathbb{F}$.
- $1 - ab = 6x + 2x^2$.
- $s_0 = 6x + 2x^2$, $s_1 = s_0^2 = 4x$, $s_2 = s_0^3 = 0$.
- $c = 1 + s_0 + s_1 = 1 + 2x + 2x^2$.
- Výstup: $d = bc = 4 + 3x + x^2$.

1.6 Další příklady okruhů

Tato sekce je přehledová a mapuje některé další zajímavé třídy okruhů vhodné pro teorii kódů. Budeme se zabývat pouze komutativními a konečnými okruhy. Nebudeme zde zacházet do detailů a uvedeme jen odkazy pro další možné studium.

Ve své bakalářské práci [20] jsem se zabýval kódy nad grupovými okruhy. Ústředním motivem byl izomorfismus grupového okruhu a jistého okruhu matic, jehož tvar závisel na grupě, z které jsme grupový okruh zkonstruovali. Díky tomuto izomorfismu je možné dále určovat generující a kontrolní matici či některé vlastnosti kódu.

Okruhy $\mathbb{Z}_{p^e}$ lze přirozeně dále zobecnit pomocí Čínské věty o zbytcích na okruhy $\mathbb{Z}_m$, kde máme prvočíselný rozklad $m = p_1^{e_1} \dots p_k^{e_k}$. Analogicky můžeme redukovat zkoumání okruhů hlavních ideálů na řetězcové okruhy. Platí totiž, že S je konečný okruh hlavních ideálů právě tehdy, když je S izomorfní (konečnému) součinu řetězcových okruhů (viz [9, Proposition 2.7]). Další informace o okruzích hlavních ideálů lze nalézt v [9].

Zajímavou další možností, jsou různé faktory polynomiálních okruhů více proměnných nad konečnými tělesy, jako např. ve [13]

$$\mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^2, \ldots, x_n^2, x_1x_2 - x_2x_1, \ldots, x_ix_j - x_jx_i, \ldots \rangle, i \neq j,$$

$$\mathbb{F}_q[x, y]/\langle x^i, y^j, xy - yx \rangle, i, j \in \mathbb{N} \setminus \{0\}.$$

Nebo ve tvaru $R[x]/I$, kde R je řetězcový okruh a I je vlastní ideál $R[x]$. Právě v takovém tvaru se často v literatuře objevují příklady tzv. Frobeniových okruhů, jak se lze dočíst v [21]. Konečný komutativní okruh S nazýváme Frobeniovým okruhem právě tehdy, když anihilátor každého maximálního ideálu S je minimální ideál v S (viz [21]).

Frobeniovy okruhy jsou pro studium kódů vhodné. Důvodem je, že na Frobeniových okruzích platí tzv. Věty o rozšíření a dají se na ně zobecnit identity MacWilliamsové, což je studováno v [31]. Uspořádejme tyto třídy okruhů do inkluze a dostaneme:

Frobeniovy okruhy
$\cup^4$
Okruhy hlavních ideálů
$\cup^3$
Řetězcové okruhy
$\cup^2$
Galoisovy okruhy
$\cup^1$
Okruhy $\mathbb{Z}_{p^e}$

Všechny inkluze jsou ostré. Příklady, které to dosvědčují jsou odspoda:

1. $\mathbb{F}_4$.
2. $\mathrm{GR}(9, 2)[x]/\langle x^2 - 3, 3x^2 \rangle$ je řetězcový, ale není to Galoisův okruh. Příklad je převzatý z [10, Example 2.1].
3. $\mathbb{Z}_6$, jehož ideály $\langle 2 \rangle$ a $\langle 3 \rangle$ nejsou porovnatelné inkluzí.
4. $\mathbb{F}_2[x,y]/\langle x^2, y^3 \rangle$ má maximální ideál $\langle x,y \rangle$, který není jednogenerovaný. Příklad je převzatý z [9, Example 2.].

Kapitola 2

Kódy nad okruhem

V této kapitole vycházíme zejména z článku [24]. Budeme zde navazovat na výsledky z předchozí kapitoly, kde jsme se zabývali řetězcovými okruhy. Zavedené značení a předpoklady pro řetězcový okruh R z minulé kapitoly používáme i nadále. Postupně studujeme strukturu lineárních kódů nad R, duálních kódů k lineárním kódům a charakterizujeme kódy volné.

Při práci s maticemi značíme jednotkovou matici řádu $j \in \mathbb{N}$ jako I_j.

2.1 Definice kódu

Kód resp. lineární kód nad konečným tělesem $\mathbb{F}$ se definuje jako podmnožina $\mathbb{F}^n$ resp. jako vektorový podprostor aritmetického vektorového prostoru $\mathbb{F}^n$. Tuto definici lze přímočaře zobecnit na situaci nad konečným komutativním okruhem S.

Definice (Kód nad okruhem)**.** *Za kód nad konečným komutativním okruhem S délky $n \in \mathbb{N}$ považujeme libovolnou podmnožinu S^n. Lineární kód nad konečným komutativním okruhem S délky $n \in \mathbb{N}$ definujeme jako S-podmodul modulu S^n.*

Délka kódu v definici může být lehce zavádějící. Například je známo, že lineární cyklické kódy délky (v klasické terminologii) l nad tělesem $\mathbb{F}$ lze popsat jako ideály v okruhu $S = \mathbb{F}[x]/\langle x^l - 1\rangle$. Podle naší definice jsou však tyto kódy S-modulem (ideálem) modulu S, a tedy délky 1. Délka tedy závisí na zvoleném okruhu, nad kterým kódy uvažujeme.

Na rozdíl od situace nad konečným tělesem, nemusí být lineární kód, jakožto podmodul, nutně volný. Lineární kód, který je jako podmodul volný, nazýváme volným kódem. Přirozené číslo n vyhradíme pro délku kódu.

V celé této kapitole jsou středem zájmu lineárními kódy, které jsou netriviální (tj. různé od 0 nebo S^n). Jelikož se budou v dalších kapitolách vyskytovat i nelineární kódy budeme linearitu přesto zdůrazňovat. Kód C značí lineární kód nad řetězcovým okruhem R.

2.2 Struktura kódů nad řetězcovým okruhem

V této sekci se budeme zabývat strukturou lineárních kódů nad řetězcovým okruhem a odvodíme tvar tzv. generující matice kódu ve standardním tvaru.

Pro další úvahy bude pro nás důležité Tvrzení 1.7, že pro každé $r \in R \setminus \{0\}$ existuje jednoznačně $i \in \{0, \ldots, m-1\}$ takové, že r lze zapsat ve tvaru $r = u^i s$, kde $s \in R^*$.

Mějme nyní netriviální lineární kód C nad R délky $n \in \mathbb{N}$. Jelikož je R-modul R^n konečný je konečný i libovolný jeho R-podmodul. Vezměme tedy libovolnou konečnou množinu generátorů kódů C. Z těchto generátorů pak můžeme vytvořit generující matici Q. Generující matice kódu nad tělesem je volná báze zapsaná v řádcích. Obecně však kód C nemusí být volný a abychom se vyhnuli pojmům jako lineární nezávislost, což může být problematické díky přítomnosti netriviálních dělitelů nuly, vyslovíme raději následující definici (viz [24, Definition 3.1]).

Definice (Generující matice)**.** *Matice Q nad okruhem R je generující matice lineárního kódu C nad R, pokud splňuje tyto dvě podmínky:*

1. *Řádky Q generují C jako R-podmodul modulu R^n.*
2. *Žádný řádek Q nelze vyjádřit jako R-lineární kombinaci ostatních řádků Q.*

Mějme řádky $q_1, \ldots, q_k$ matice Q. Druhý bod znamená, že neexistuje index $j \in \{1, \ldots, k\}$ a $r_i \in R$ pro $i \in \{1, \ldots, k\} \setminus \{j\}$ taková, že

$$q_j = \sum_{i \neq j} r_i q_i.$$

Z nějaké množiny generátorů C obdržíme generující matici postupnou eliminací generátorů, které můžeme vyjádřit pomocí ostatních generátorů. Nyní popíšeme Algoritmus 5, který generující matici převede do tzv. standardního tvaru. Algoritmus 5 postupuje tak, že provádí modifikaci Gaussovy eliminace pro řetězcové okruhy a zároveň permutuje sloupce. Standardní tvar generující matice vypadá následovně:

$$G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & \ldots & A_{0,m-1} & A_{0,m} \\ 0 & uI_{k_1} & uA_{1,2} & \ldots & uA_{1,m-1} & uA_{1,m} \\ 0 & 0 & u^2 I_{k_2} & \ldots & u^2 A_{2,m-1} & u^2 A_{2,m} \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & u^{m-1} I_{k_{m-1}} & u^{m-1} A_{m-1,m} \end{pmatrix}$$

Blokovou matici G pak také nazýváme standardní generující matice lineárního kódu C. Vždy když budeme mluvit o standardních maticích budeme předpokládat, že mají výše uvedený tvar a stejné značení bloků. Navíc písmeno G v tomto kontextu vyhradíme pro samotnou matici. Uveďme ještě, jak označujeme rozměry jednotlivých bloků:

$$\text{rozměry bloku } A_{i,j} \text{ jsou } \begin{cases} k_i \times k_j & 0 \leq i < j < m, \\ k_i \times (n - \sum_{j=0}^{m-1} k_j) & 0 \leq i \leq m-1, j = m. \end{cases}$$

Může nastat, že pro nějaké i je $k_i = 0$, což znamená, že příslušné bloky se vůbec v matici nevyskytují. Např. generující matice $G = (2, 2) = 2(1, 1)$ lineárního kódu nad $\mathbb{Z}_4$ je ve standardním tvaru a $k_0 = 0$.

Předpokládáme, že všechny nenulové prvky generující matice Q jsou zapsány ve tvaru $u^i r$ z Tvrzení 1.7, kde $r \in R^*$ a $i = 0, \ldots, m-1$. Řádky i sloupce číslujeme

Algoritmus 5 Generující matice ve standardním tvaru

Vstup: generující matice Q se složkami $Q_{e,f}$ lineárního kódu $C \neq \{0\}$.
Výstup: generující matice G kódu C ve standardním tvaru.

1: $i \leftarrow 0$
2: $j \leftarrow 0$
3: **for** $0 \leq k \leq m-1$ **do**
4: **while** existuje řádek $e \geq i$, sloupec $f \geq j$ v Q a $r \in R^*$, že $Q_{e,f} = u^k r$ **do**
5: Vynásob všechny složky e-tého řádku prvkem r^{-1}.
6: Prohoď j-tý sloupec s f-tým sloupcem v Q.
7: Prohoď i-tý řádek s e-tým řádkem v Q.
8: // Q se změnilo, od teď uvažujeme nové číslovaní řádků a sloupců!
9: Pomocí $Q_{i,j} = u^k$ eliminuj složky ve sloupci pod a nad touto složkou na 0 do tvaru uvedeného výše.
10: $i \leftarrow i + 1$
11: $j \leftarrow j + 1$
12: **end while**
13: **end for**
14: Vymaž všechny nulové řádky z Q.
15: Vrať $G = Q$ jako výstup.

od nuly. V každém kroku vytvoříme jednotkovou matici $u^i I_{k_i}$ a vynulujeme prvky pod ní.

Upřesněme eliminaci v kroku 9. Předpokládejme, že $Q_{i,j} = u^k$ a chceme vynulovat prvek $u^l s$, kde $s \in R^*$ a $l > k$. Vhodným násobkem dostaneme

$$(u^{l-k}s)u^k - u^l s = 0.$$

Pokud $l \leq k$. Tak vhodným násobkem dostaneme

$$u^k - (u^{k-l}s^{-1})u^l s = 0.$$

Lineární kód generovaný maticí Q je permutačně ekvivalentní kódu generovaného maticí G. Všechny složky matic $u^i A_{i,j}$, kde $0 \leq i \leq m-1$ a $1 \leq j \leq m$ leží v $\langle u^i \rangle$.

Poznamenejme, že stanovení standardního tvaru generující matice nad okruhem, který není řetězcový je složitější. Například pro situaci nad $\mathbb{Z}_m$, kde $m \in \mathbb{N}$ je složené, odkážeme na článek [26], kde se řeší modulární nezávislost (což je obdoba lineární nezávislosti) a standardní generující matice kódu nad okruhem $\mathbb{Z}_{p^e}$. Následně je možné základní koncepty nezávislosti a standardní generující matice přemístit do okruhu $\mathbb{Z}_m$ pomocí Čínské věty o zbytcích. Uveďme jednoduchý příklad z [26, str. 150]. Matice

$$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, (2, 3).$$

generují stejný lineární kód nad $\mathbb{Z}_6$. První matici nelze převést na druhou pomocí elementárních řádkových úprav (nesmíme násobit řádek neinvertibilním prvkem). Kterou matici však označit za standardní generující matici kódu? Odpověď záleží na definici modulární nezávislosti a dle [26] má první matice modulárně závislé řádky.

Nyní budeme zkoumat, jaké parametry standardní generující matice jsou invariantní vzhledem k různé volbě generující matice, která vstupovala do Algoritmu 5. Standardní generující matice totiž není určena jednoznačně. Ukážeme, že pokud vezmeme dvě různé generující matice lineárního kódu C a převedeme je Algoritmem 5 do standardního tvaru budou mít stejné hodnoty $k_0, \ldots, k_{m-1}$, tj. stejné velikosti bloků. K tomu budeme potřebovat následující definice. Mějme lineární kód C nad R. Projekcí kódu C myslíme $\overline{C} = \{\overline{c} \mid c \in C\}$. Kódu C a prvku $r \in R$ můžeme přiřadit kód

$$(C : r) = \{x \in R^n \mid rx \in C\}.$$

Například $(C : 0) = R^n$ nebo $(C : 1) = C$. Dále kódu C přiřadíme řetězec lineárních kódů příslušející C

$$C = (C : u^0) \subseteq \cdots \subseteq (C : u^i) \subseteq \cdots \subseteq (C : u^{m-1})$$

a jejich projekce

$$\overline{C} = \overline{(C : u^0)} \subseteq \cdots \subseteq \overline{(C : u^i)} \subseteq \cdots \subseteq \overline{(C : u^{m-1})}.$$

Lineárním kódům $\overline{(C : u^i)}$ pro $i = 1, \ldots, m-1$ říkáme torzní a $\overline{C}$ někdy označujeme jako reziduální kód kódu C. Standardní generující matici kódu můžeme psát také ve zkráceném tvaru tak, že sloučíme blokové matice v řádku G do jedné blokové matice, tj.

$$G = \begin{pmatrix} A_0 \\ uA_1 \\ u^2A_2 \\ \vdots \\ u^{m-1}A_{m-1} \end{pmatrix}.$$

Umazáním mocnin generátorů maximálního ideálu u složek matice G dostaneme matici A.

$$A = \begin{pmatrix} A_0 \\ A_1 \\ A_2 \\ \vdots \\ A_{m-1} \end{pmatrix}.$$

Předchozí definice využijeme pro ekvivalentní popis velikostí bloků $k_0, \ldots, k_{m-1}$ ve standardní generující matici. Vše zapíšeme do tvrzení převzatého z [24, Lemma 3.4, Theorem 3.5].

Tvrzení 2.1. *Mějme lineární kód C nad R délky n generovaný maticí G v (zkráceném) standardním tvaru. Nechť rozměry bloků matice G jsou popořadě $k_0 \times n, \ldots, k_{m-1} \times n$.*

1. *Kód $\overline{(C : u^i)}$ nad $\mathbb{F}$, kde $0 \leq i \leq m-1$, má generující matici $\overline{A}_{(i)}$, která vznikne vybráním prvních $\sum_{j=0}^{i} k_j$ řádků z A a následného uplatnění kanonické projekce na každý řádek. Tzn.*

$$\overline{A}_{(i)} = \begin{pmatrix} \overline{A_0} \\ \overline{A_1} \\ \vdots \\ \overline{A_i} \end{pmatrix}.$$

2. $\dim_{\mathbb{F}} \overline{(C : u^i)} = \sum_{j=0}^{i} k_j$.

3. $k_0 = \dim_{\mathbb{F}} \overline{C}$ *a* $k_i = \dim_{\mathbb{F}} \overline{(C : u^i)} - \dim_{\mathbb{F}} \overline{(C : u^{i-1})}$ *pro* $1 \leq i \leq m-1$.

4. *Každá jiná generující matice kódu* C *ve (zkráceném) standardním tvaru má stejné velikosti bloků* $k_0, \ldots, k_{m-1}$ *jako* G.

Důkaz. Označme matici, která vznikne vybráním prvních $\sum_{j=0}^{i} k_j$ řádků matice A jako $A_{(i)}$. Ať D je kód nad R generovaný $A_{(i)}$. Pak $\overline{D}$ je kód nad $\mathbb{F}$ generovaný maticí $\overline{A}_{(i)}$. Vezměme libovolný s-tý řádek b z matice $A_{(i)}$. Ten vznikl z s-tého řádku matice G tvaru $u^j b$, kde $0 \leq j \leq i$. Pak jistě $u^i b \in C$, protože G je generující matice kódu C. Ukázali jsme $D \subseteq (C : u^i)$, protože k tomu stačilo ověřit náležení generátorů kódu D v $(C : u^i)$. Z toho plyne inkluze $\overline{D} \subseteq \overline{(C : u^i)}$.

Ukažme druhou inkluzi $\overline{D} \supseteq \overline{(C : u^i)}$. Mějme $b \in \overline{(C : u^i)}$ a k němu prvek $c \in (C : u^i)$, že $\overline{c} = b$. Z definice $u^i c \in C$. Tedy existuje $x = (x_1, \ldots, x_{m-1}) \in R^n$, kde $x_i \in R^{k_i}$ pro $0 \leq i \leq m-1$, že platí

$$u^i c = xG = \Bigg(\underbrace{x_0}_{k_0 \text{ složek}}, \underbrace{x_0 A_{0,1} + u x_1}_{k_1 \text{ složek}}, \ldots, \underbrace{\sum_{i=0}^{m-2} u^i x_i A_{i,m} + u^{m-1} x_{m-1}}_{k_{m-1} \text{ složek}}, \underbrace{\sum_{i=0}^{m-1} u^i x_i A_{i,m}}_{n-k \text{ složek}} \Bigg),$$

kde $k = \sum_{j=0}^{m-1} k_j$. Každá složka xG musí být dělitelná u^i. Existuje $y_0 \in R^{k_0}$, že $x_0 = u^i y_0$. Pro druhý blok je $x_0 A_{0,1} + u x_1 = u^i y_0 A_{0,1} + u x_1$, a tedy existuje $y_1 \in R^{k_1}$, že $x_1 = u^{i-1} y_1$. Postupně dostaneme $x_j = u^{i-j} y_j$, kde $y_j \in R^{k_j}$ pro $0 \leq j \leq i$. Odtud máme

$$u^i c = \sum_{j=0}^{i} x_j u^j A_j + \sum_{j=i+1}^{m-1} x_j u^j A_j = \sum_{j=0}^{i} u^i y_j A_j + \sum_{j=i+1}^{m-1} x_j u^j A_j,$$

$$u^i \Bigg(c - \underbrace{\sum_{j=0}^{i} y_j A_j + \sum_{j=i+1}^{m-1} x_j u^{j-i} A_j}_{\text{označme jako } q} \Bigg) = 0.$$

Z $u^i(c-q) = 0$ vyplývá, že $c - q$ je násobkem u^{m-i}, tj. $c - q = u^{m-i} r$ pro nějaké $r \in R$. Máme tedy:

$$c = \sum_{j=0}^{i} y_j A_j + \sum_{j=i+1}^{m-1} x_j u^{j-i} A_j + u^{m-i} r.$$

Vidíme, že $b = \overline{c} = \sum_{j=0}^{i} \overline{y_j} \overline{A_j}$. Z toho plyne požadovaná inkluze. Ostatní body plynou snadno z prvního a z faktu, že řádky $\overline{A}_{(i)}$ jsou v odstupňovaném tvaru, a proto jsou lineárně nezávislé nad $\mathbb{F}$.

Mějme generující matici W kódů C ve standardním tvaru různou od G. Dvojím použitím 3. bodu na matice W a G dostaneme rovnost rozměrů bloků. Tím je dokázán poslední bod tvrzení. □

Matice $\overline{A}_{(i)}$ jsou v redukovaném odstupňovaném tvaru, tj. $\overline{A}_{(i)} = (I_e \mid W)$, kde $e = \sum_{j=0}^{i} k_j$ a W je matice o rozměrech $e \times (n-e)$. Kódu, který generuje matice v takovémto tvaru, se často říká systematický. Díky poslednímu bodu Tvrzení 2.1 má smysl zavést typ a hodnost lineárního kódu následovně [24, Definition 3.6].

Definice (Typ a hodnost lineárního kódu)**.** *Každému lineárnímu kódu C přiřadíme jeho typ $(k_0, \ldots, k_{m-1})$, kde $k_0 = \dim_{\mathbb{F}} \overline{C}$ a $k_i = \dim_{\mathbb{F}} \overline{(C : u^i)} - \dim_{\mathbb{F}} \overline{(C : u^{i-1})}$ pro $1 \leq i \leq m-1$. Hodností (rankem) lineárního kódů myslíme číslo* $\operatorname{rank}(C) = \sum_{i=0}^{m-1} k_i$.

Hodnost kódu C je minimální počet generátorů C. Jednotlivé projekce $\overline{(C : u^i)}$ jsou kódy nad tělesem $\mathbb{F}$, čili se jedná o vektorové podprostory $\mathbb{F}^n$. Místo hodnosti lineárních kódů nad tělesem, se držíme standardní notace, a raději mluvíme o dimenzi. Vidíme, že k_i je také počet řádků ve standardní generující matici, které jsou dělitelné u^i a zároveň nedělitelné u^{i+1}. V literatuře se také často setkáme s tímto značením typu kódů:

$$1^{k_0}(u)^{k_1}(u^2)^{k_2}\ldots(u^{m-1})^{k_{m-1}}.$$

My však budeme raději upřednostňovat kratší zápis. Pro následující větu uvedenou v [24, Theorem 3.5, Corollary 3.7] budeme potřebovat tento jednoduchý poznatek. Mějme $0 \leq i \leq m-1$. Zobrazení $\zeta : (u^i R)^k \to (R/u^{m-i}R)^k$ zadané předpisem

$$u^i(x_1, \ldots, x_k) \mapsto (x_1 + u^{m-i}R, \ldots, x_k + u^{m-i}R)$$

je izomorfismus R-modulů. To stačí ukázat pro jednu jeho složku. Zobrazení $R \to u^i R$ definované jako $r \mapsto u^i r$ je jistě epimorfismus a jeho jádro je $u^{m-i}R$. Pak stačí použít První větu o izomorfismu pro moduly.

Věta 2.2 (Struktura lineárních kódů nad řetězcovým okruhem)**.** *Ať C je lineární kód nad R délky n typu $(k_0, \ldots, k_{m-1})$ a hodnosti k. Nechť G je jeho generující matice ve standardním tvaru.*

1. *Každé kódové slovo $c \in C$ lze jednoznačně zapsat jako*

$$c = (x_0, \ldots, x_{m-1}) \cdot G,$$

   kde pro $0 \leq i \leq m-1$ je $x_i \in R_{m-i}^{k_i}$, kde $R_{m-i} \subseteq R$ taková množina, že modulo ideál $u^{m-i}R$ tvoří reprezentanty faktorokruhu $R/u^{m-i}R$.

2. *Kód C lze jednoznačně (až na pořadí) rozložit jako $C \simeq \bigoplus_{i=0}^{m-1} u^i R^{k_i}$.*

Důkaz. Uvažme zobrazení $\varphi : R^k \to R^n$ definované předpisem $(x_1, \ldots, x_k) \mapsto (x_1, \ldots, x_k) \cdot G$. Nyní ukážeme, že $\operatorname{Ker}(\varphi) = \prod_{i=0}^{m-1} u^{m-i} R^{k_i}$. Předpokládejme, že $x = (x_0, \ldots, x_{m-1}) \in \operatorname{Ker}(\varphi)$, kde $x_i \in R^{k_i}$ pro $0 \leq i \leq m-1$. Pak platí

$$\varphi(x) = \Bigg(\underbrace{x_0}_{k_0 \text{ složek}}, \underbrace{x_0 A_{0,1} + u x_1}_{k_1 \text{ složek}}, \ldots, \underbrace{\sum_{i=0}^{m-2} u^i x_i A_{i,m} + u^{m-1} x_{m-1}}_{k_{m-1} \text{ složek}}, \underbrace{\sum_{i=0}^{m-1} u^i x_i A_{i,m}}_{n-k \text{ složek}} \Bigg) = 0.$$

Z toho vyplývá, že první blok je nutně $x_0 = 0$. Pro druhý blok po dosazení x_0 je $ux_1 = 0$, a proto $x_1 \in u^{m-1}R^{k_1}$. V třetím bloku s využitím $x_1 \in u^{m-1}R^{k_1}$ máme $u^2 x_2 = 0$, a tedy $x_2 \in u^{m-2}R^{k_2}$ atp. Postupné vyjadřování skončíme předposledním blokem a celkově dostaneme, že $x_i \in u^{m-i}R^{k_i}$ pro $0 \leq i \leq m-1$. Jelikož $\varphi(R^k) = C$, tak z první věty o izomorfismu plyne

$$C \simeq R^k \Big/ \prod_{i=0}^{m-1} u^{m-i} R^{k_i} = \prod_{i=0}^{m-1} R^{k_i} \Big/ \prod_{i=0}^{m-1} u^{m-i} R^{k_i} \simeq \prod_{i=0}^{m-1} R^{k_i}/u^{m-i}R^{k_i}.$$

Nyní po drobné úpravě použijeme izomorfismus ζ definovaný před větou a dostaneme:

$$\prod_{i=0}^{m-1} R^{k_i}/u^{m-i}R^{k_i} \simeq \prod_{i=0}^{m-1} (R/u^{m-i}R)^{k_i} \simeq \prod_{i=0}^{m-1} (u^i R)^{k_i} = \prod_{i=0}^{m-1} u^i R^{k_i} = \bigoplus_{i=0}^{m-1} u^i R^{k_i}.$$

Poslední rovnost platí, protože konečné součiny a direktní sumy splývají. □

Nyní již bude snadné určit počet kódových slov kódů. Mohutnost množiny $u^i R$ totiž již známe z Důsledku 1.6. Následující důsledek je sepsán v [24, Theorem 3.5].

Důsledek 2.3. *Ať C je lineární kód nad R délky n typu $(k_0, \ldots, k_{m-1})$, pak $|C| = q^{\sum_{i=0}^{m-1}(m-i)k_i}$.*

Důkaz. Z Důsledku 1.6 víme, že pro $i = 0, \ldots, m$ je $|u^i R| = q^{m-i}$. Z druhého bodu předchozí věty dostáváme

$$|C| = \bigoplus_{i=0}^{m-1} |u^i R|^{k_i} = \prod_{i=0}^{m-1} q^{(m-i)k_i} = q^{\sum_{i=0}^{m-1}(m-i)k_i}.$$

□

2.3 Duální kódy

Přidejme na R^n bodový součin definovaný jako nedegenerovaná bilineární forma reprezentovaná jednotkovou maticí. Poznamenejme, že řetězcový okruh nemusí být nutně komutativní, a tudíž není bodový součin na obecném řetězcovém okruhu symetrická forma. My však předpokládáme komutativitu R, a tudíž bodový součin bude symetrický.

Pro $x = (x_1, \ldots, x_n) \in R^n$ a $y = (y_1, \ldots, y_n) \in R^n$ máme tedy definovaný jejich bodový součin jako:

$$[x, y] = \sum_{i=1}^{n} x_i y_i.$$

Můžeme pak definovat příslušné duální kódy vzhledem k tomuto bodovému součinu. Je jasné, že může nastat $[x, x] = 0$ pro nenulové $x \in R^n$ (např. pro $R = \mathbb{Z}_2$), a tudíž se nejedná o klasický skalární součin, jaký známe z vektorových prostorů nad $\mathbb{R}$. Duální kód kódu C značíme jako $C^\perp$ a myslíme tím tuto množinu:

$$C^\perp = \{x \in R^n \mid [x, c] = 0 \text{ pro všechna } c \in C\}.$$

Pokud C je lineární, tak $C^\perp$ je také lineární. Řekneme, že kód C je samoortogonální resp. samoduální pokud nastává $C \subseteq C^\perp$ resp. $C = C^\perp$.

Mějme lineární kód C nad R typu $(k_0, \ldots, k_{m-1})$ se standardní generující maticí G. Nyní směřujeme k odvození tvaru generující matice duálního kódu $C^\perp$, která je, jak později ukážeme, také kontrolní maticí C. Tuto matici označme H. Sestrojíme dle Algoritmu 6. Označme $k = \operatorname{rank}(C)$. Matice H na výstupu Algoritmu 6 bude mít tvar:

$$H = \begin{pmatrix} B_{0,m} & B_{0,m-1} & \ldots & B_{0,2} & B_{0,1} & I_{n-k} \\ uB_{1,m} & uB_{1,m-1} & \ldots & uB_{1,2} & uI_{k_{m-1}} & 0 \\ u^2B_{2,m} & u^2B_{2,m-1} & \ldots & u^2I_{k_{m-2}} & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ u^{m-1}B_{m-1,m} & u^{m-1}I_{k_1} & \ldots & 0 & 0 & 0 \end{pmatrix}.$$

Pro zbytek kapitoly má matice H tvar jaký je uveden výše. Upozorněme, že indexování sloupců je zprava doleva. Bloky na vedlejší diagonále, což jsou až na mocniny prvku u jednotkové matice, budeme pro další rozbor značit $B_{i,i}$ pro $i = 0, \ldots, m-1$. Uveďme ještě rozměry jednotlivých bloků:

$$\text{rozměry bloku } B_{i,j} \text{ jsou } \begin{cases} (n - \sum_{j=0}^{m-1} k_j) \times k_{m-j} & i = 0;\ 1 \le j \le m, \\ k_{m-i} \times k_{m-j} & 1 \le i < j \le m. \end{cases}$$

Algoritmus 6 Generující matice $C^\perp$

Vstup: generující matice G ve standardním tvaru lineárního kódu C nad R typu $(k_0, \ldots, k_{m-1})$.
Výstup: generující matice H kódu $C^\perp$.

1: **for** $0 \le i \le m-1$ **do**
2: **if** $i = 0$ **then**
3: $B_{i,i} \leftarrow I_{n-k}$
4: **else**
5: $B_{i,i} \leftarrow I_{k_{m-i}}$
6: **end if**
7: **for** $i < j \le m$ **do**
8: $B_{i,j} \leftarrow -(\sum_{e=i+1}^{j-1} B_{i,e} A_{m-j,m-e}^T) - A_{m-j,m-i}^T$
9: **end for**
10: **end for**
11: Uspořádej bloky $B_{i,j}$ do matice H tvaru popsaného výše.
12: Vrať matici H jako výstup.

Postupně dokážeme, že na výstupu Algoritmu 6 je vskutku generující matice kódu $C^\perp$. Nyní dokážeme, že $HG^T = 0$. Součin i-tého řádku matice H s j-tým sloupcem matice G^T je

$$u^i \begin{pmatrix} B_{i,m} & B_{i,m-1} & B_{i,m-2} & \ldots & B_{i,i+1} & I & 0 \ldots 0 \end{pmatrix} \cdot u^j \begin{pmatrix} 0 \\ \vdots \\ 0 \\ I \\ A_{j,j+1}^T \\ A_{j,j+2}^T \\ \vdots \\ A_{j,m}^T \end{pmatrix}.$$

Upozorněme, že první činitel v součinu má číslování složek netypicky zprava doleva. Tento součin se rovná

$$u^{i+j}\big(B_{i,m-j} + B_{i,m-j-1}A_{j,j+1}^T + \cdots + B_{i,i+1}A_{j,m-i-1}^T + IA_{j,m-i}^T\big)$$

Uvědomme si, že všechny maticové součiny jsou dobře definovány, tj. mají správné rozměry. Pokud položíme

$$B_{i,m-j} = -\sum_{e=i+1}^{m-j-1} B_{i,e}A_{j,m-e}^T - A_{j,m-i}^T,$$

tak zajisté dostaneme nulovou matici. Poznamenejme, že sumu přes e jsme vlastně zapsali zprava doleva z předchozího výrazu. Po provedení substituce $m - j \mapsto j'$ dostaneme tvar, který je napsán v algoritmu, tj.

$$B_{i,j'} = -\sum_{e=i+1}^{j'-1} B_{i,e} A^T_{m-j',m-e} - A^T_{m-j',m-i}.$$

Takovýto předpis bloků v H tedy dává vskutku $HG^T = 0$. Buď nyní D kód generovaný maticí H. Ihned vidíme, že D je typu $(n-k, k_{m-1}, \ldots, k_1)$ a hodnosti $\operatorname{rank}(D) = n - k_0$, neboť přeuspořádáním sloupců obdržíme standardní tvar generující matice. Inkluzi $D \subseteq C^\perp$ již máme z $HG^T = 0$. Pokud dokážeme rovnost typů kódů $C^\perp$ a D, tak z Věty 2.2 plyne existence bijekce $C^\perp \simeq D$, a proto $C^\perp = D$. Následující tvrzení je uvedeno v [24, Theorem 3.10]

Tvrzení 2.4 (Duální kód)**.** *Mějme lineární kód C nad R délky n hodnosti k a typu $(k_0, \ldots, k_{m-1})$. Pro $i \in \{0, \ldots, m-1\}$ platí $\overline{(C^\perp : u^i)} = \overline{(C : u^{m-i-1})}^\perp$. Kód $C^\perp$ je typu $(n-k, k_{m-1}, \ldots, k_1)$ a hodnosti $\operatorname{rank}(C^\perp) = n - k_0$.*

Důkaz. Již máme v diskuzi před tvrzením dokázáno $D \subseteq C^\perp$ a známe typ a hodnost D. Ať $i \in \{0, \ldots, m-1\}$. Dokážeme nejdříve, že $\overline{(C^\perp : u^i)} \subseteq \overline{(C : u^{m-i-1})}^\perp$. Vezměme libovolně $x \in (C^\perp : u^i)$ a $y \in (C : u^{m-i-1})$. Z definice platí, že $u^i x \in C^\perp$ a $u^{m-i-1} y \in C$, a tedy z ortogonality máme $[u^i x, u^{m-i-1} y] = 0$. Rovnost můžeme přepsat na $u^{m-1}[x, y] = 0$. To znamená, že $[x, y] \in uR$, a proto $\overline{[x, y]} = 0$. Označme složky jako $x = (x_1, \ldots, x_n)$ a $y = (y_1, \ldots, y_n)$. Pak

$$[\overline{x}, \overline{y}] = \sum_{i=1}^{n} \overline{x}_i \overline{y}_i = \sum_{i=1}^{n} \overline{x_i y_i} = \overline{\sum_{i=1}^{n} x_i y_i} = \overline{[x, y]} = 0.$$

Tím je inkluze dokázána. Uvažme nyní kód D generovaný maticí H stejně jako v diskuzi před tvrzením. Víme, že $D \subseteq C^\perp$. Celkově dostáváme tento řetězec inkluzí:

$$\overline{(D : u^i)} \subseteq \overline{(C^\perp : u^i)} \subseteq \overline{(C : u^{m-i-1})}^\perp.$$

Z teorie o duálních kódech na tělesem je dobře známo, že

$$\dim_{\mathbb{F}} \overline{(C : u^{m-i-1})}^\perp = n - \dim_{\mathbb{F}} \overline{(C : u^{m-i-1})}.$$

Dimenzi posledního kódu známe z Tvrzení 2.1, tj. $\dim_{\mathbb{F}} \overline{(C : u^{m-i-1})}^\perp = n - \sum_{j=0}^{m-i-1} k_j$. Dimenze torzního kódu $\overline{(D : u^i)}$ je dle stejného Tvrzení 2.1 součet prvních $i+1$ složek typu kódu D, jimiž je $(n-k, k_{m-1}, \ldots, k_1)$. Porovnáním zjistíme, že $\dim_{\mathbb{F}} \overline{(D : u^i)} = \dim_{\mathbb{F}} \overline{(C : u^{m-i-1})}^\perp$. Kódy v řetězci tedy splývají:

$$\overline{(D : u^i)} = \overline{(C^\perp : u^i)} = \overline{(C : u^{m-i-1})}^\perp.$$

□

Jelikož se typy kódů $C^\perp$ a D rovnají, tak H je vskutku generující matice kódu $C^\perp$. Tvrzení má jako důsledek rovnost

$$|C| \cdot |C^\perp| = |R^n|.$$

Předpokládejme značení z předchozího tvrzení. Z Důsledku 1.6 je $|R^n| = q^{mn}$. Dle Důsledku 2.3 stačí ověřit, zda

$$\sum_{i=0}^{m-1}(m-i)k_i + m(n-k) + \sum_{i=1}^{m-1}(m-i)k_{m-i} \stackrel{?}{=} mn.$$

Poslední suma se rovná $\sum_{i=1}^{m-1} ik_i$. Navíc ji můžeme indexovat již od nuly. Celkem se levá strana rovná

$$\sum_{i=0}^{m-1} mk_i - m\left(\sum_{i=0}^{m-1} k_i\right) + mn = mn.$$

Kontrolní matice lineárního kódu C nad řetězcovým okruhem je taková matice P, že

$$c \in C \iff Pc^T = 0.$$

Pro lineární kód K nad tělesem pojmy generující matice $K^\perp$ a kontrolní matice K splývají. Jinak to nebude ani v situaci nad řetězcovým okruhem R. Klíčem k důkazu je ověření rovnosti $(C^\perp)^\perp = C$.

Tvrzení 2.5. *Mějme lineární kód C nad R délky n. Generující matice $C^\perp$ je kontrolní maticí C.*

Důkaz. Nechť G je generující matice C ve standardním tvaru a Y je generující matice lineárního kódu $C^\perp$. Dokážeme, že Y je kontrolní matice kódu C přímo z definice.
($\Rightarrow$) Každé $c \in C$ zapíšeme jako $c = xG$, kde $x \in R^{\mathrm{rank}(C)}$. Jistě $YG^T = 0$, proto

$$Y(xG)^T = (YG^T)x^T = 0.$$

($\Leftarrow$) Ukážeme, že množina $M = \{x \in R^n \mid Yx^T = 0\}$ je rovna $(C^\perp)^\perp$. Platí

$$(C^\perp)^\perp = \left\{x \in R^n \mid [yY, x] = yYx^T = 0 \text{ pro všechna } y \in R^{\mathrm{rank}(C^\perp)}\right\}.$$

Inkluze $M \subseteq (C^\perp)^\perp$ je zřejmá. Druhá inkluze plyne z toho, že za y volíme pro $i = 1, \ldots, \mathrm{rank}(C^\perp)$ postupně $e_i \in R^n$, kde na i-té pozici je jednička a jinde nuly. Dostaneme tak rovnost $Yx^T = 0$ po jednotlivých rovnicích v řádcích. Zbývá ukázat $(C^\perp)^\perp = C$. Inkluze $(C^\perp)^\perp \supseteq C$ je zřejmá z první implikace. Navíc C a $(C^\perp)^\perp$ mají stejný typ z Tvrzení 2.4, proto z Věty 2.2 existuje bijekce $(C^\perp)^\perp \simeq C$. Celkově dostaneme rovnost $(C^\perp)^\perp = C$. □

Matici H z výstupu Algoritmu 6 nazýváme proto kontrolní maticí kódu C ve standardním tvaru. Podobně jako u standardní generující matice G můžeme sloučit jednotlivé bloky v řádcích matice H a dostat tak zkrácený tvar

$$H = \begin{pmatrix} B_0 \\ uB_1 \\ u^2B_2 \\ \vdots \\ u^{m-1}B_{m-1} \end{pmatrix}.$$

Vynecháním generátorů maximálního ideálu z matice H obdržíme matici B:

$$B = \begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ \vdots \\ B_{m-1} \end{pmatrix}.$$

Z Tvrzení 2.1 víme, jak vypadá generující matice kódu $\overline{(C : u^i)}$. Nyní se zaměříme na kontrolní matici tohoto kódu. Kontrolní matice kódu $\overline{(C : u^i)}$ je generující matice kódu $\overline{(C : u^i)}^{\perp}$. Z důkazu Tvrzení 2.4 víme, že

$$\overline{(C : u^i)}^{\perp} = \overline{(C^{\perp} : u^{m-i-1})} = \overline{(D : u^{m-i-1})},$$

kde H generuje D. Jako důsledek předchozích tvrzení dostáváme tvary kontrolních matic torzních kódů.

Důsledek 2.6. *Mějme kód C nad R délky n typu $(k_0, \ldots, k_{m-1})$ a hodnosti k. Nechť je $0 \leq i \leq m-1$. Ať e je součet prvních $m-i$ složek z vektoru čísel $(n-k, k_{m-1}, \ldots, k_1)$. Pak $\overline{(C : u^i)}$ má kontrolní matici $\overline{B}_{(m-i-1)}$, která vznikne vybráním prvních e řádků z B a následného uplatnění kanonické projekce na každý řádek.*

$$\overline{B}_{(m-i-1)} = \begin{pmatrix} \overline{B_0} \\ \overline{B_1} \\ \vdots \\ \overline{B}_{m-i-1} \end{pmatrix}.$$

2.4 Volné kódy

Připomeňme definici, že lineární kód C nad R je volný, pokud je volný jako R-podmodul. Volné kódy mají velmi významné postavení pokud vzdálenosti kódových slov měříme Hammingovou metrikou, jak objasníme v příští kapitole. Pro lepší porozumění volným kódům uvádíme následující charakterizaci volných kódů, která rozšiřuje tvrzení v [24, Proposition 3.13].

Tvrzení 2.7. *Mějme netriviální lineární kód C nad R délky n typu $(k_0, \ldots, k_{m-1})$ a hodnosti k. Ať G resp. H je generující resp. kontrolní matice kódu C ve standardním tvaru. Pak následující podmínky jsou ekvivalentní.*

1. *Kód C je volný.*
2. $\operatorname{rank}(C) = k_0$.
3. *Matice G má tvar $G = (I \mid Q)$, pro nějakou matici $Q \in R^{k \times (n-k)}$.*
4. $\overline{C} = \overline{(C : u^{m-1})}$.
5. *Matice $\overline{G}$ je generující matice $\overline{C}$.*
6. *Matice $\overline{H}$ je kontrolní matice $\overline{C}$.*

7. *Lineární kód $C^\perp$ je volný.*

8. $\mathrm{rank}(C) + \mathrm{rank}(C^\perp) = n$.

Důkaz. (1. $\Rightarrow$ 2.) Volný kód C je z definice izomorfní R^k. Dle Věty 2.2 je $C \simeq \bigoplus_{i=0}^{m-1} u^i R^{k_i}$. Proto $k_0 = \mathrm{rank}(C)$.
(2. $\Rightarrow$ 3.) Jelikož $k_0 = \mathrm{rank}(C)$, musí typ kódu C být $(k_0, 0, \ldots, 0)$. Odtud zmíněný tvar matice G.
(3. $\Rightarrow$ 4.) Matice $\overline{G}$ generuje $\overline{C}$ i $\overline{(C : u^{m-1})}$ z Tvrzení 2.1. Proto se tyto kódy rovnají.
(4. $\Rightarrow$ 5.) Z Tvrzení 2.1 je

$$k_0 = \dim_{\mathbb{F}} \overline{C} = \dim_{\mathbb{F}} \overline{(C : u^{m-1})} = \sum_{j=0}^{m-1} k_j.$$

Proto C má typ $(k_0, 0, \ldots, 0)$. Z dalšího použití Tvrzení 2.1 vyplývá, že generující maticí $\overline{C} = \overline{(C : u^{m-1})}$ je $\overline{G}$.
(5. $\Rightarrow$ 6.) Jelikož $\overline{G}$ je generující matice (speciálně neobsahuje nulový řádek), nesmí matice G obsahovat řádek, který by byl násobkem u. Proto C má typ $(k_0, 0, \ldots, 0)$. Z Důsledku 2.6 pro $i = 0$ plyne, že kontrolní matice $\overline{C}$ je $\overline{H}$.
(6. $\Rightarrow$ 7.) Jelikož $\overline{H}$ je generující matice kódu $\overline{C}^\perp$ (speciálně neobsahuje nulový řádek), tak v matici H neexistuje řádek, který je násobkem u. Proto dle Tvrzení 2.4 je $C^\perp$ typu $(n - k_0, 0, \ldots, 0)$. Z Věty 2.2 je $C^\perp \simeq R^{n-k_0}$, a proto volný.
(7. $\Rightarrow$ 8.) Jelikož $C^\perp$ je izomorfní $R^{\mathrm{rank}(C^\perp)}$ tak Věta 2.2 implikuje, že složky počínaje druhou v typu $C^\perp$ budou nulové. Z Tvrzení 2.4 je $C^\perp$ typu $(n - k, 0, \ldots, 0)$ a hodnosti $n - k_0$. Proto $k = k_0$. Proto $\mathrm{rank}(C^\perp) = n - \mathrm{rank}(C)$.
(8. $\Rightarrow$ 1.) Z tvrzení 2.4 Máme

$$\mathrm{rank}(C) = n - \mathrm{rank}(C^\perp) = n - n + k_0 = k_0.$$

Tedy kód C je typu $(k_0, 0, \ldots, 0)$, a proto z Věty 2.2 je $C \simeq R^{k_0}$. To znamená, že C je volný. □

Kapitola 3

Váhy a izometrie

Zavedené značení a předpoklady pro řetězcový okruh R používáme i nadále. Maximální ideál R je M, M je generován u a prvek u má stupeň nilpotence m. Zbytkové těleso R/M má q prvků a značíme ho $\mathbb{F}$ či $\mathbb{F}_q$. Pruhem označujeme kanonickou projekci $R \to \mathbb{F}$.

V této kapitole studujeme vlastnosti lineárních kódů nad R vzhledem k Hammingově a homogenní váze. Popisujeme rozšířené Grayovo zobrazení, které překládá lineární kódy nad R na kódy nad $\mathbb{F}$. V textu jsme čerpali zejména z [25] a [17].

Jako doplňující literaturu o homogenních váhách odkážeme na [16], kde je možno nalézt hlubší výsledek o charakterizaci homogenních vah na Frobeniově okruhu pomocí generujícího charakteru. My se omezíme na situaci nad R. Motivační příklad v sekci 3.3 je předveden pro kvaternární kódy. Další podrobnosti týkající se kvaternárních kódů a jejich obrazů při Grayově zobrazení je možné nalézt v [29]. Informace k Reed-Mullerovým kódům lze nalézt v [1, sekce 5.4].

3.1 Váhy, homogenní váha

K okruhu R nyní přidejme určité zobrazení, které bude jistým způsobem ohodnocovat (vážit) prvky tohoto okruhu. Váhovou funkcí na abecedě (v našem případě okruhu) R myslíme libovolné zobrazení $w : R \to \mathbb{Q}$ splňující $w(0) = 0$, kde $\mathbb{Q}$ je těleso racionálních čísel.

Uveďme některé důležité příklady vah pro různé okruhy. Leeova a Euklidova váha je převzata z [27, str. 10]. Homogenní váha na R je převzata z [17]. Písmeno r bude označovat prvek příslušného okruhu, p prvočíslo a e přirozené číslo.

- Hammingova váha pro obecný okruh

$$w_H(r) = \begin{cases} 0 & \text{pokud } r = 0, \\ 1 & \text{pokud } r \neq 0. \end{cases}$$

- Leeova váha na $\mathbb{Z}_{p^e}$ je $w_L(r) = \min\{r, p^e - r\}$.

- Euklidova váha na $\mathbb{Z}_{p^e}$ je $w_E(r) = (w_L(r))^2$.

- Homogenní váha pro řetězcový okruh R s indexem nilpotence $m \geq 2$.

$$w_h(r) = \begin{cases} q^{m-2}(q-1) & \text{pokud } r \in R \setminus u^{m-1}R, \\ q^{m-1} & \text{pokud } r \in u^{m-1}R \setminus \{0\}, \\ 0 & \text{pokud } r = 0. \end{cases}$$

Zastavme se na chvíli u homogenní váhy. V obecné poloze pro konečný okruh byla poprvé uvedena v disertační práci I. Constantinescuové [7]. Následující definice je převzata z [16, Definition 1.1]

Definice. *Homogenní váha w na konečném okruhu S je váhová funkce taková, že platí:*

1. *Pokud pro $x, y \in S$ platí $xS = yS$, pak $w(x) = w(y)$.*
2. *Existuje nezáporné $l \in \mathbb{Q}$, že $\sum_{a \in xS} w(a) = l \cdot |xS|$ pro všechna nenulová $x \in S$.*

Vlastně jsme nadefinovali pravou homogenní váhu. Analogicky se definuje levá homogenní váha pro nekomutativní okruhy. Jelikož pracujeme s komutativními okruhy, tak přívlastky u homogenní váhy nerozlišujeme. Konstantu l nazýváme průměrnou hodnotou homogenní váhy w.

Nyní zde podáme elementární důkaz (tj. bez odkazování na hlubší poznatky ohledně Frobeniových okruhů), že výše definovaná váha w_h na R je vskutku homogenní.

Pozorování 3.1. *Výše zavedená váha w_h na R s indexem nilpotence $m \geq 2$ je homogenní s průměrnou hodnotou $l = q^{m-2}(q-1)$.*

Důkaz. Ověřme přímo definici homogenní váhy.
1. Mějme $x, y \in R$ takové, že $xR = yR$. Dle Tvrzení 1.2 existuje $i \in \{0, \ldots, m\}$, že $xR = yR = u^iR$. Jelikož x, y generují stejný ideál, liší se až na násobek invertibilního prvku, přičemž $R^* = R \setminus uR$ dle Tvrzení 1.2. Proto pomocí Algoritmu 3 rozložíme x, y na $x = u^i r$, $y = u^i s$, kde $r, s \in R^*$. Připomeňme, že $0 \in R$ rozkládáme v duchu Algoritmu 3 jako $u^m \cdot 1$. Definici w_h pro takto rozložené x pak můžeme ekvivalentně upravit na

$$w_h(x) = \begin{cases} q^{m-2}(q-1) & \text{pokud } i = 0, \ldots, m-2, \\ q^{m-1} & \text{pokud } i = m-1, \\ 0 & \text{pokud } i = m. \end{cases}$$

Konkrétní hodnoty závisí na i, který je v rozkladu x a y stejný. Proto $w_h(x) = w_h(y)$.

2. Mějme libovolné $0 \neq x \in R$. Existuje $i \in \{0, \ldots, m-1\}$, že $xR = u^iR$. Z Důsledku 1.6 víme, že $|u^iR| = q^{m-i} \neq 0$. Vyčísleme průměrnou hodnotu:

$$l = \frac{1}{|xR|} \sum_{a \in xR} w_h(a) = \frac{1}{q^{m-i}} \sum_{a \in u^iR} w_h(a).$$

Sumu rozdělíme a použijeme $w_h(0) = 0$. Dostaneme tak

$$\frac{1}{q^{m-i}} \sum_{a \in u^iR} w_h(a) = \frac{1}{q^{m-i}} \left(\sum_{a \in u^iR \setminus u^{m-1}R} w_h(a) + \sum_{a \in u^{m-1}R \setminus \{0\}} w_h(a) \right).$$

Dosadíme hodnoty váhové funkce w_h a využijeme Důsledek 1.6

$$\frac{1}{q^{m-i}}\left(\sum_{a\in u^i R\setminus u^{m-1}R} w_h(a)+\sum_{a\in u^{m-1}R\setminus\{0\}} w_h(a)\right)=$$
$$=\frac{1}{q^{m-i}}\left(q(q^{m-i-1}-1)q^{m-2}(q-1)+(q-1)q^{m-1}\right).$$

Poslední výraz pak dále můžeme upravit jako

$$\frac{q-1}{q^{m-i}}\left((q^{m-i-1}-1)q^{m-1}+q^{m-1}\right)=\frac{(q-1)q^{m-1}q^{m-i-1}}{q^{m-i}}=q^{m-2}(q-1).$$

□

Je známo (viz [16]), že až na volbu průměrné hodnoty existuje na Frobeniově okruhu homogenní váha jednoznačně. Proto se také často v literatuře předpokládá místo obecné homogenní váhy $w(x)$ s průměrnou hodnotou l normalizovaná váha $l^{-1}\cdot w(x)$, která má již průměrnou hodnotu 1.

Nakonec vidíme, že klasická Hammingova váha na konečném tělese $\mathbb{F}_q$ je homogenní s průměrnou hodnotou $(q-1)/q$. Pokud uvážíme w_h na řetězcovém okruhu $\mathbb{Z}_4$ dostaneme Leeovu váhu w_L a její průměrná hodnota je rovna jedné.

Libovolnou váhovou funkci w na R pak můžeme rozšířit na $w : R^n \to \mathbb{Q}$ předpisem

$$w(x_1,\ldots,x_n)=\sum_{i=1}^{n} w(x_i).$$

Každá takováto váha pak indukuje vzdálenost mezi $x, y \in R^n$ takto $d(x,y) := w(x-y)$. Minimální vzdálenost kódu C indukovaná váhovou funkcí w je definována jako

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

a minimální váha kódu C jako

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

Předpokládejme, že kód C je lineární. Pro $x \neq y \in C$ je $d(x,y) = w(x-y)$ a $0 \neq x-y \in C$, protože C je aditivní grupa. Pro lineární kód C, libovolnou váhu w a její indukovanou vzdálenost d tedy zřejmě nastává:

$$d(C)=w(C).$$

Díky předchozím definicím můžeme měřit vlastnosti kódů. Zejména schopnost opravovat chyby. Čím větší je vzdálenost mezi kódovými slovy, tím je větší šance na správnou detekci chyb a jejich následné opravení.

Pokud budeme chtít zdůraznit příslušnou váhu, tak ji zapíšeme jako dolní index. Např. pro Hammingovu váhu máme $w_H(x)$, $w_H(C)$, $d_H(C)$ a pro homogenní váhu na R máme $w_h(x)$, $w_h(C)$, $d_h(C)$. Značení vah je stejné jako v příkladech na začátku sekce.

3.2 Hammingova váha a projekce

Nyní vybudujeme potřebné značení související s Hammingovou váhou, které budeme potřebovat v následující větě. Mějme $x = (x_1, \ldots, x_n) \in R^n$. Nosič prvku x je $\operatorname{supp}(x) = \{i \mid x_i \neq 0\}$. Nosič kódu C je

$$\operatorname{supp}(C) = \{\operatorname{supp}(c) \mid 0 \neq c \in C\}.$$

Minimální nosič kódu C je

$$S(C) = \{M \mid M \in \operatorname{supp}(C), \forall L \in \operatorname{supp}(C), L \subseteq M \Rightarrow M = L\}.$$

Nyní směřujeme k porovnání minimální vzdáleností kódu a jeho torzních kódů nad řetězcovým okruhem. Ukážeme, že vzhledem k Hammingově metrice má lineární kód C nad R velmi podobné vlastnosti jako kód $\overline{(C : u^{m-1})}$ nad $\mathbb{F}$.

R-modul $u^{m-1}R^n$ je také vektorovým prostorem nad $\mathbb{F}$. Násobení vektoru $u^{m-1}x \in u^{m-1}R^n$ skalárem $r \in \mathbb{F}$ definujme jako $su^{m-1}x$, kde $s \in R$ takové, že $\overline{s} = r$. Následující lemma s větou je uvedeno v [25, Lemma 4.1, Theorem 4.2].

Lemma 3.2. *Zobrazení $\omega : u^{m-1}R^n \to \mathbb{F}^n$ definované předpisem $\omega(u^{m-1}x) = \overline{x}$ je izomorfismus vektorových prostorů nad $\mathbb{F}$. Navíc ω zachovává Hammingovy váhy a nosiče, tj. pro $x \in R^n$ platí:*

1. $w_H(u^{m-1}x) = w_H(\omega(u^{m-1}x))$.
2. $\operatorname{supp}(u^{m-1}x) = \operatorname{supp}(\omega(u^{m-1}x))$.

Důkaz. Ověřme, že ω je homomorfismus. Mějme $x, y \in R^n$, $r \in \mathbb{F}$ a $s \in R$ takové, že $\overline{s} = r$.

$$\omega(u^{m-1}x + u^{m-1}y) = \omega(u^{m-1}(x+y)) = \overline{x+y} = \overline{x} + \overline{y} = \omega(u^{m-1}x) + \omega(u^{m-1}y),$$

$$\omega(r \cdot u^{m-1}x) = \omega(su^{m-1}x) = \overline{sx} = r\overline{x} = r\omega(u^{m-1}x).$$

Předpokládejme, že $\overline{x} = \overline{y}$. To znamená, že $x - y \in uR$, a tedy $u^{m-1}x - u^{m-1}y = 0$. Proto je ω prosté. Navíc z Důsledku 1.6 vyplývá, že $|u^{m-1}R^n| = q^n = |\mathbb{F}^n|$. Homomorfismus ω je tedy vskutku bijektivní.

Nulové pozice vektoru $u^{m-1}x$ jsou tam, kde složky $x = (x_1, \ldots, x_n)$ jsou násobkem u, protože $u^m = 0$. To jsou však přesně pozice, kde má projekce $\overline{x}$ nulové složky. Nosiče jsou stejné, a proto i Hammingovy váhy se zachovávají $w_H(u^{m-1}x) = |\operatorname{supp}(u^{m-1}x)| = |\operatorname{supp}(\overline{x})| = w_H(\overline{x})$. □

Hammingova váha je úzce spjata s nosičem. Pro lineární kód C je $d_H(C) = w_H(C) = \min_{L \in S(C)} |L|$. Pokud dva lineární kódy mají stejné minimální nosiče, tak mají stejnou i minimální Hammningovu vzdálenost. Poznamenejme, že pro C lineární je $C \cap u^i R^n$ také lineární, kde $i = 0, \ldots, m$.

Nyní odvodíme vztah mezi minimálním nosičem kódu a minimálním nosičem jistého torzního kódu a dostaneme důležitý výsledek týkající se minimální vzdálenosti kódu a jeho projekce.

Věta 3.3 (Minimální vzdálenost a nosič)**.** *Mějme nenulový lineární kód C nad R délky n.*

1. *Platí* $S(C) = S(C \cap u^{m-1}R^n)$ *a* $d_H(C) = d_H(C \cap u^{m-1}R^n)$.

2. *Platí* $S(C) = S(\overline{(C : u^{m-1})})$ *a* $d_H(C) = d_H(\overline{(C : u^{m-1})})$.

3. *Pokud* $\overline{C} \neq \{0\}$, *pak* $d_H(C) \leq d_H(\overline{C})$.

4. *Pokud* $\overline{C} \neq \{0\}$ *a* C *je volný, pak* $d_H(C) = d_H(\overline{C})$.

Důkaz. 1. Dokážeme, že $S(C) = S(D)$ pro $D = C \cap u^{m-1}R^n$. Nejdříve ukážeme inkluzi $S(C) \subseteq S(D)$. Mějme $c \in C$ takové, že $\mathrm{supp}(c) \in S(C)$. Máme

$$\mathrm{supp}(c) \supseteq \mathrm{supp}(uc) \supseteq \cdots \supseteq \mathrm{supp}(u^j c) \supseteq \cdots \supseteq \mathrm{supp}(\underbrace{u^m c}_{=0}) = \emptyset.$$

Vezměme $j \in \mathbb{N} \cup \{0\}$ největší možné tak, že $u^j c \neq 0$. Jelikož je C uzavřen na násobení prvkem u, tak $u^j c \in C$. Pak z minimality plyne $\mathrm{supp}(c) = \mathrm{supp}(u^j c)$. Z $u^{j+1}c = 0$ plyne $c \in u^{m-j-1}R^n$. Tedy víme $u^j c \in D$. Protože $D \subseteq C$ a $\mathrm{supp}(u^j c) = \mathrm{supp}(c) \in S(C)$, tak jistě také $\mathrm{supp}(c) = \mathrm{supp}(u^j c) \in S(D)$.

Dokažme druhou inkluzi $S(C) \supseteq S(D)$. Mějme $d \in D$ takové, že $\mathrm{supp}(d) \in S(D)$. Jelikož $D \subseteq C$, tak $\mathrm{supp}(d) \in \mathrm{supp}(C)$. Postupujme sporem a předpokládejme, že $\mathrm{supp}(d) \notin S(C)$. Pak existuje $h \in C$, že $\mathrm{supp}(h) \in S(C)$ a $\mathrm{supp}(h) \subsetneq \mathrm{supp}(d)$ jsou do sebe ostře vřazeny. Již z dokázané inkluze víme, že $S(C) \subseteq S(D)$. Tudíž existuje $g \in D$, že

$$\mathrm{supp}(g) = \mathrm{supp}(h) \subsetneq \mathrm{supp}(d).$$

To je ale spor s tím, že $d \in S(D)$. Tím jsme dokázali rovnost $S(C) = S(D)$. Odtud ihned plyne výsledek pro minimální vzdálenost příslušných kódů.

2. Nejdříve si uvědomíme, že $C \cap u^{m-1}R^n = u^{m-1}(C : u^{m-1})$. Pravá strana je množina všech takových $u^{m-1}x \in R^n$, kde $x \in (C : u^{m-1})$, proto $u^{m-1}x \in C$. Tedy jsou to taková kódová slova C, která jsou zároveň tvaru $u^{m-1}R^n$. Nyní využijeme zobrazení ω z Lemmatu 3.2 a dostaneme

$$\omega(C \cap u^{m-1}R^n) = \omega(u^{m-1}(C : u^{m-1})) = \overline{(C : u^{m-1})}.$$

Z Lemmatu 3.2 také víme, že ω zachovává nosič, tj.

$$S(C \cap u^{m-1}R^n) = S(\omega(C \cap u^{m-1}R^n)) = S(\overline{(C : u^{m-1})}).$$

Použitím bodu 1. máme

$$S(C) = S(C \cap u^{m-1}R^n) = S(\overline{(C : u^{m-1})}).$$

Odtud máme i výsledek pro minimální vzdálenost příslušných kódů.

3. Z bodu 2. víme, že $d_H(C) = d_H(\overline{(C : u^{m-1})})$. Dostáváme tak řetězec nerovností:

$$d_H(C) = d_H(\overline{(C : u^{m-1})}) \leq d_H(\overline{(C : u^{m-2})}) \leq \cdots \leq d_H(\overline{(C : u^0)}) = d_H(\overline{C}),$$

neboť víme, že

$$\overline{(C : u^{m-1})} \supseteq \overline{(C : u^{m-2})} \supseteq \cdots \supseteq \overline{(C : u^0)} = \overline{C}.$$

Počet kódových slov v kódech v tomto řetězci neroste, a tudíž se minimální vzdálenost nemůže zmenšovat.

4. Z druhého bodu máme $d_H(C) = d_H(\overline{(C : u^{m-1})})$. Pro volný kód C z Tvrzení 2.7 platí $\overline{(C : u^{m-1})} = \overline{C}$. Tudíž $d_H(C) = d_H(\overline{(C : u^{m-1})}) = d_H(\overline{C})$. □

Připomeňme, že podmínku na volnost kódů C v posledním bodu vyslovené věty jsme charakterizovali v Tvrzení 2.7. Právě dokázaná věta má mnoho zajímavých důsledků, proto přidáme k jednotlivým bodům komentáře. První bod Věty 3.3 lze zobecnit. Pro každé $i = 0, \ldots, m-1$ totiž platí

$$S(C) = S(C \cap u^i R^n), \quad d_H(C) = d_H(C \cap u^i R^n).$$

Pro $i = 0, \ldots, m-2$ stačí ve znění za kód C dosadit kód $C \cap u^i R^n$ a následně využít 1. bod pro již dokázanou situaci $i = m-1$. Dostaneme tak

$$S(C \cap u^i R^n) = S(C \cap u^i R^n \cap u^{m-1} R^n) = S(C \cap u^{m-1} R^n) = S(C).$$

Z linearity C pak samozřejmě také $d_H(C) = d_H(C \cap u^i R^n)$.

Předpokládejme, že C je typu $(k_0, \ldots, k_{m-1})$. Pokud bychom určovali $d_H(C)$ hrubou silou, pomůže nám druhý bod Věty 3.3 zmenšit prohledávaný prostor. Připomeňme, že nemusíme procházet všechny různé dvojice z C (tj. $\binom{|C|}{2}$ porovnání), ale z linearity postačí najít nenulové kódové slovo s nejmenší vahou (tedy $|C| - 1$ porovnání). Již z předchozích kapitol víme, že

$$|\overline{(C : u^{m-1})}| = q^{\dim_{\mathbb{F}} \overline{(C:u^{m-1})}} = q^{\sum_{i=0}^{m-1} k_i},$$

zatímco

$$|C| = q^{\sum_{i=0}^{m-1} (m-i) k_i}.$$

Druhý bod Věty 3.3 tak redukuje hledání minimálního nenulového slova v C na hledání minimálního nenulového slova v $\overline{(C : u^{m-1})}$, což při velkém m má vliv na reálnou dobu běhu algoritmu, i když se stále jedná o exponenciální časovou složitost.

Nejdůležitější pro nás nadále bude třetí bod Věty 3.3. Proto zde uvedeme alternativní důkaz faktu, že pro C lineární takové, že $\overline{C} \neq \{0\}$ je $d_H(C) \leq d_H(\overline{C})$. Důležitým krokem bude opět použití Lemmatu 3.2.

Alternativní důkaz 3. bodu ve Větě 3.3. Pro každý prvek $0 \neq r \in R$ z Tvrzení 1.7 existuje jednoznačně $i = 0, \ldots, m-1$, že $r = su^i$, kde $s \in R^*$. Může nastat, že v minimálním slově $x = (x_1, \ldots, x_n) \neq 0$ vzhledem k Hammingově váze jsou dvě různé složky takové, že jedna je tvaru ru^i a druhá je tvaru su^j, kde $i \neq j$ a $r, s \in R^*$?

$$x = (\ldots, ru^i, \ldots, su^j, \ldots) \in C.$$

Bez újmy na obecnosti předpokládejme, že $i < j$. Uvažme prvek

$$u^{m-i} x = (\ldots, ru^m, \ldots, su^{m-i+j}, \ldots).$$

Složka ru^m je nulová a zároveň je $0 \neq u^{m-i} x \in C$, což je spor s minimalitou.

Všechna minimální slova x mají ve složkách stejné mocniny u. Ať číslo $i = 0, \ldots, m-1$ je největší možné, že $x = u^i y$, kde $y \in (R^* \cup \{0\})^n$. Pak z definice je

$$y \in (C : u^i) \subseteq (C : u^{m-1}).$$

Platí $\overline{C} \subseteq \overline{(C : u^{m-1})}$, a proto $d_H(\overline{C}) \geq d_H(\overline{(C : u^{m-1})})$. Jistě $w_H(y) = w_H(\overline{y})$, protože $R^* = R \setminus uR$ z Tvrzení 1.2. Ukážeme, že $w_H(\overline{y}) = w_H(\overline{(C : u^{m-1})})$. Sporem předpokládejme, že existuje $d \in (C : u^{m-1})$ takové, že $\overline{d} \neq 0$ a zároveň platí $w_H(\overline{d}) < w_H(\overline{y})$. Jelikož $\overline{d} \neq 0$, není d násobkem u, a proto $u^{m-1}d \neq 0$. S využitím Lemmatu 3.2 a rovnosti $w_H(y) = w_H(x)$ dostáváme:

$$w_H(\underbrace{u^{m-1}d}_{\in C\setminus\{0\}}) = w_H(\overline{d}) < w_H(\overline{y}) = w_H(y) = w_H(x).$$

Jelikož x bylo takové, že $w_H(x) = w_H(C)$, máme spor. Odtud obdržíme:

$$d_H(C) = w_H(x) = w_H(y) = w_H(\overline{y}) = d_H(\overline{(C : u^{m-1})}) \leq d_H(\overline{C}).$$

□

Poslední bod Věty 3.3 vlastně říká, že volné kódy dosahují nejlepší možné minimální Hammingovy vzdálenosti. To není však všechno: obsahují také více slov při stejné délce, hodnosti a minimální vzdálenosti než kódy, které volné nejsou. Vezměme nenulový kód C nad R typu $(k_0, \ldots, k_{m-1})$ s délkou n, který není volný (dle Tvrzení 2.7 existuje $k_i > 0$ pro nějaké $i = 1, \ldots, m-1$) se zkrácenou standardní generující maticí

$$G = \begin{pmatrix} A_0 \\ uA_1 \\ u^2A_2 \\ \vdots \\ u^{m-1}A_{m-1} \end{pmatrix}.$$

Uvažme kód D nad R generovaný touto maticí (umazali jsme z G mocniny u):

$$A = \begin{pmatrix} A_0 \\ A_1 \\ A_2 \\ \vdots \\ A_{m-1} \end{pmatrix}.$$

Kód D je volný délky n, a proto $d_H(D) = d_H(\overline{D})$. Matice $\overline{A}$ je generující matice kódu $\overline{D}$ a zároveň z Tvrzení 2.1 generuje i $\overline{(C : u^{m-1})}$. Tedy $\overline{D} = \overline{(C : u^{m-1})}$. Dvojí aplikací Věty 3.3 dostáváme

$$d_H(D) = d_H(\overline{D}) = d_H(\overline{(C : u^{m-1})}) = d_H(C).$$

Jistě také $\operatorname{rank}(C) = \operatorname{rank}(D)$. Kód D je typu $(\sum_{i=0}^{m-1} k_i, 0, \ldots, 0)$. Z Důsledku 2.3 je

$$q^{\sum_{i=0}^{m-1}(m-i)k_i} = |C| < |D| = q^{m\sum_{i=0}^{m-1}k_i}.$$

V [25, Remarks 4.4] je poznamenáno, že Věta 3.3 se dá zobecnit i pro nelineární kódy C uzavřené na násobení prvkem u. To však není pravda. Uveďme protipříklad pro první bod, kde se tvrdí, že $d_H(C) = d_H(C \cap u^{m-1}R^n)$. Uvažme pro $2 \leq j \in \mathbb{N}$ kód K_j nad $\mathbb{Z}_4$, jehož slova jsou

$$\begin{array}{ll} (\overbrace{1,1,\ldots,1}^{j\times},2) & \\ (1,1,\ldots,1,0) & \\ (2,2,\ldots,2,0) & \in K_j \cap 2\mathbb{Z}_4^{j+1} \\ (0,0,\ldots,0,0) & \in K_j \cap 2\mathbb{Z}_4^{j+1} \end{array}$$

Kód K_j je uzavřen na násobení $u = 2$ a

$$d_H(K_j) = 1 < j = d_H(K_j \cap 2\mathbb{Z}_4^{j+1}).$$

Jelikož obecně $C \supseteq C \cap u^{m-1}R^n$, tak zřejmě $d_H(C) \leq d_H(C \cap u^{m-1}R^n)$. Jak vidíme z příkladu, nerovnost může být ostrá. Protipříklad lze zobecnit tak, že lze vždy za jistých předpokladů nalézt nadkód C, pro který bude tato nerovnost ostrá, jak formálně napíšeme v následující větě. Shrneme zde také výsledky inspirované Větou 3.3, které pro takové kódy C platí.

Věta 3.4 (Nelineární verze Věty o minimální vzdálenosti a nosiči)**.** *Mějme obecně nelineární kód C nad R délky n a $i \in \{0, \ldots, m-1\}$ takové, že C je uzavřen na násobení prvkem u^i.*

1. *Pokud $i = 1$, tak platí $S(C) = S(C \cap u^{m-1}R^n)$ a $S(C) = S(\overline{(C : u^{m-1})})$.*
2. *Předpokládejme, že $i = 1$, index nilpotence u je $m \geq 2$ a $n \geq 4$. Nechť $d_H(C \cap u^{m-1}R^n) > 1$. Pak existuje kód $\hat{C} \supseteq C$ nad R délky n, který je také uzavřen na násobení prvkem u takový, že zároveň*

$$\begin{aligned} d_H(\hat{C}) &< d_H(\hat{C} \cap u^{m-1}R^n), \\ d_H(\hat{C}) &< d_H(\overline{(\hat{C} : u^{m-1})}). \end{aligned}$$

3. *Předpokládejme, že $i = m - 1 - j$ pro nějaké $j \in \{0, \ldots, m-1\}$. Pokud $C \cap u^{m-1}R^n$ a $\overline{(C : u^j)}$ jsou neprázdné množiny různé od $\{0\}$, pak*

$$d_H(C) \leq d_H(\overline{(C : u^j)}).$$

Důkaz. 1. Lze použít důkaz o minimálních nosičích 1. a 2. bodu z Věty 3.3 beze změny.

2. Pokud je přímo $d_H(C) < d_H(C \cap u^{m-1}R^n)$, stačí vzít $\hat{C} = C$. Ať toto nenastane. Uvažme nejdříve případ, kdy existuje $0 \neq x \in C \cap u^{m-1}R^n$ takové, že $w_H(x) < n$. Pak vytkneme z x prvek u^{m-1}. To uděláme třeba provedením Algoritmu 3 na každou nenulovou složku x (0 nerozkládáme a interpretujeme ji jako 0 nikoliv jako u^m). Najdeme tedy takové $y \in (R^* \cup \{0\})^n$, že $x = u^{m-1}y$. Máme tak $w_H(y) = w_H(x) < n$. Ať y_i je nulová složka y. Definujme $z = (z_1, \ldots, z_n) \in R^n$ jako $z_j = y_j$ pro $j \in \{1, \ldots, n\} \setminus \{i\}$ a $z_i = u^{m-1}$. Přenásobením u se y, z převede na stejný prvek.

$$\begin{matrix} y \\ z \end{matrix} \overset{\cdot u}{\to} uy \overset{\cdot u}{\to} \cdots \overset{\cdot u}{\to} u^{m-2}y \overset{\cdot u}{\to} u^{m-1}y = x.$$

Definujme $\hat{C} = C \cup \{y, z, uy, u^2y, \ldots, u^{m-2}y\}$. Důležité je, že $d_H(y, z) = 1$ a navíc $C \cap u^{m-1}R^n = \hat{C} \cap u^{m-1}R^n$. Dostáváme tak

$$d_H(\hat{C}) = 1 < d_H(C \cap u^{m-1}R^n) = d_H(\hat{C} \cap u^{m-1}R^n).$$

Zbývající případ je, když pro všechny nenulové $x \in C \cap u^{m-1}R^n$ je $w_H(x) = n$. Definujme $y = (1, 1, 0, 0, \ldots, 0)$, $z = (1, 1, u^{m-1}, 0, \ldots, 0)$. Přenásobením u se y, z převede na stejný prvek.

$$\begin{matrix} y \\ z \end{matrix} \overset{\cdot u}{\to} uy \overset{\cdot u}{\to} \cdots \overset{\cdot u}{\to} u^{m-2}y \overset{\cdot u}{\to} u^{m-1}y = (u^{m-1}, u^{m-1}, 0, \ldots, 0).$$

Položme $\hat{C} = C \cup \{y, z, uy, u^2y, \ldots, u^{m-1}y\}$. Opět $d_H(\hat{C}) = 1$. Dále známe vzdálenost $d_H(u^{m-1}y, 0) = 2$. Pokud $C \cap u^{m-1}R^n$ obsahuje nenulové slovo c s vlastností $d_H(u^{m-1}y, c) = 1$, musí se c od $(u^{m-1}, u^{m-1}, 0, \ldots, 0)$ lišit v jedné souřadnici. Jelikož $n \geq 4$, tak musí být jedná složka c nulová, což je spor s tím, že $w_H(c) = n$. Proto

$$d_H(\hat{C}) = 1 < d_H(\hat{C} \cap u^{m-1}R^n).$$

S využitím Lemmatu 3.2 máme pro $u^{m-1}x, u^{m-1}x \in \hat{C}$ následující:

$$d_H(u^{m-1}x, u^{m-1}y) = w_H(u^{m-1}(x-y)) = w_H(\overline{x-y}) = w_H(\overline{x} - \overline{y}) = d_H(\overline{x}, \overline{y}).$$

Proto platí $d_H(\hat{C} \cap u^{m-1}R^n) = d_H(\overline{(\hat{C} : u^{m-1})})$.

3. Důkaz tohoto bodu ve Větě 3.3 stačí mírně upravit. Triviálně $C \supseteq C \cap u^{m-1}R^n$. Navíc zobrazení ω zachovává vzdálenosti mezi kódy $C \cap u^{m-1}R^n$ a $\overline{(C : u^{m-1})}$. Proto

$$d_H(C) \leq d_H(C \cap u^{m-1}R^n) = d_H(\overline{(C : u^{m-1})}).$$

Ukážeme, že $\overline{(C : u^{m-1})} \supseteq \overline{(C : u^j)}$. Mějme $x \in (C : u^j)$, čili $u^j x \in C$. Z uzavřenosti na násobení u^{m-1-j} máme $u^{m-1-j}u^j x = u^{m-1}x \in C$, to znamená $x \in (C : u^{m-1})$. Po aplikaci projekce je $\overline{x} \in \overline{(C : u^{m-1})}$. Proto

$$d_H(C) \leq d_H(\overline{(C : u^{m-1})}) \leq d_H(\overline{(C : u^j)}).$$

□

3.3 Grayovo zobrazení

Důsledkem 3. bodu Věty 3.3 je nepříliš příznivý fakt, že lineární kódy nad řetězcovým okruhem neposkytují lepší minimální vzdálenosti než kódy nad tělesem vzhledem k Hammingově váze. Lze totiž vždy přejít k projekčnímu kódu a dostat tak stejnou nebo větší minimální vzdálenost.

Nabízí se proto otázka, zda kódy nad okruhem přinášejí vůbec nějakou výhodu oproti klasickým kódům nad tělesem. Takové výhody skutečně existují. Jedna z nejdůležitějších je popis nelineárních kódů nad tělesem pomocí lineárních nad okruhem. Jako motivaci nastíníme základní myšlenky s kódy nad $\mathbb{Z}_4$. Leeovu váhu w_L prvků ze $\mathbb{Z}_4$ již známe:

$$\begin{aligned} w_L(0) &= 0 \\ w_L(1) &= 1 \\ w_L(2) &= 2 \\ w_L(3) &= 1 \end{aligned}$$

Zaveďme Grayovo zobrazení $\phi : \mathbb{Z}_4 \to \mathbb{F}_2^2$ jako:

$$\begin{aligned} 0 &\mapsto (0,0) \\ 1 &\mapsto (0,1) \\ 2 &\mapsto (1,1) \\ 3 &\mapsto (1,0) \end{aligned}$$

Zřejmě lze bijekci ϕ rozšířit po složkách na bijekci $\phi : \mathbb{Z}_4^n \to \mathbb{F}_2^{2n}$. Značení ϕ jsme přetížili a používáme ho i pro rozšířenou verzi. Zobrazení ϕ navíc zachovává váhy i vzdálenosti mezi $(\mathbb{Z}_4^n, w_L)$ a $(\mathbb{F}_2^{2n}, w_H)$. Tento fakt dokážeme později v obecnějším nastavení. Zobrazení s touto vlastností nazýváme izometrie, což v tomto textu chápeme jako synonymum pro Grayovo zobrazení. Grayovo zobrazení ϕ nám tak překládá kód C nad okruhem $\mathbb{Z}_4$ na binární kód B (nad konečným tělesem $\mathbb{Z}_2$) dvojnásobné délky následovně:

$$B = \phi(C) = \{\phi(c) \mid c \in C\}.$$

I když je kód C lineární, jeho binární obraz B lineární být nemusí, protože ϕ není lineární. Avšak minimální Leeova vzdálenost kódu C je rovna Hammingově minimální vzdálenosti kódu B, tedy $d_L(C) = d_H(B)$. Některé nelineární kódy např. Kerdockovy nebo Preparatovy kódy, které obsahují alespoň dvakrát více kódových slov než lineární kódy při stejné délce a minimální vzdálenosti, se podařilo popsat zmíněnou metodou jako obrazy Grayova zobrazení $\mathbb{Z}_4$-lineárních kódů (viz [4]). To má rozhodující roli pro popis těchto jinak špatně uchopitelných kódů a pro dekódovací algoritmy. Nyní celou myšlenku zobecníme pro řetězcový okruh R, což znamená najít vhodné zobecněné Grayovo zobrazení. Zobecnit dále Grayovo zobrazení na obecný konečný okruh je otevřený problém.

Připomeňme značení, že R/M je q-prvkové těleso $\mathbb{F}$, kde M je maximální ideál generovaný u. Uvažme vektor samých jedniček $I \in \mathbb{F}^q$:

$$I = \underbrace{(1, \ldots, 1)}_{q\times}.$$

Dále mějme vektor $F \in \mathbb{F}^q$ obsahující všechny prvky z $\mathbb{F}$. Např. pro t primitivní prvek tělesa $\mathbb{F}$ (tj. generátor cyklické grupy $\mathbb{F}^*$), můžeme jednoduše psát

$$F = (0, 1, t, t^2, \ldots, t^{q-2}).$$

Pro zkrácení zápisu budeme používat Kroneckerův součin (značíme symbolem $\otimes$), což je speciální případ tenzorového součinu. Pro $x = (x_1, \ldots, x_n) \in \mathbb{F}^n$, $y = (y_1, \ldots, y_m) \in \mathbb{F}^m$ ho definujme jako

$$x \otimes y = (xy_1, xy_2, \ldots, xy_n) \in \mathbb{F}^{m\times n}.$$

Výsledek Kroneckerova součinu dvou vektorů můžeme chápat jako matici, nebo jako vektor, který vznikl zapsáním složek součinu za sebe. Obecně je např. přirozené ztotožnit výsledek součinu

$$\underbrace{x \otimes y \otimes \cdots \otimes x}_{m-1\times}$$

s vektorem z $\mathbb{F}^{q^{m-1}}$. Kroneckerův součin je nekomutativní, a tudíž takovýto výpočet provádíme postupně zprava doleva.

Připomeňme, že m značí index nilpotence prvku u. Předpokládáme, že $m > 1$. Pomocí vektorů I a F definujme $c_i \in \mathbb{F}^{q^{m-1}}$ pro $i = 0, \ldots, m-1$ následovně:

$$c_i = \delta_{i,0} \otimes \delta_{i,1} \otimes \cdots \otimes \delta_{i,m-2},$$

kde $\delta_{i,j}$ znamená:

$$\delta_{i,j} = \begin{cases} F & \text{pokud } i = j, \\ I & \text{pokud } i \neq j. \end{cases}$$

Pro lepší přehlednost vektory c_i ještě vypíšeme:

$$\begin{array}{rcccccccccccc}
c_0 & = & F & \otimes & I & \otimes & I & \otimes & I & \otimes & \cdots & \otimes & I \\
c_1 & = & I & \otimes & F & \otimes & I & \otimes & I & \otimes & \cdots & \otimes & I \\
c_2 & = & I & \otimes & I & \otimes & F & \otimes & I & \otimes & \cdots & \otimes & I \\
\vdots & = & \vdots & & \vdots & & \vdots & & \ddots & & \cdots & & \\
\vdots & = & \vdots & & \vdots & & \vdots & & \vdots & & \ddots & & \\
c_{m-2} & = & I & \otimes & I & \otimes & I & \otimes & \cdots & \otimes & \cdots & \otimes & F \\
c_{m-1} & = & I & \otimes & I & \otimes & I & \otimes & \cdots & \otimes & \cdots & \otimes & I
\end{array}$$

Vektory $c_0, \ldots, c_{m-1}$ generují vektorový prostor nad $\mathbb{F}$, který nyní označíme jako K. Důležité je, že tyto vektory jsou bází K. Lineární nezávislost dokážeme v samostatném pozorování.

Pozorování 3.5. *Výše definované vektory $c_0, \ldots, c_{m-1}$ jsou lineárně nezávislé v $\mathbb{F}^{q^{m-1}}$ nad $\mathbb{F}$.*

Důkaz. Nechť P je matice postupně s řádky $c_0, \ldots, c_{m-1}$. Z P vybereme určité sloupce tak, abychom dostali regulární čtvercovou matici o rozměrech $m \times m$. Víme, že libovolný řádek c matice P je tvaru

$$c = a_1 \otimes \cdots \otimes a_{m-1},$$

kde $a_i \in \mathbb{F}^q$. Konkrétní vyjádření a_i sice známe, ale zatím není důležité, a navíc by učinilo zápis méně přehledným. Jednotlivé složky c budeme indexovat prvky tělesa $\mathbb{F}$. Složka indexovaná $J = (j_1, \ldots, j_{m-1}) \in \mathbb{F}^{m-1}$ je rovna

$$c_J = (a_1)_{j_1} \cdot (a_2)_{j_2} \ldots (a_{m-1})_{j_{m-1}},$$

kde $(a_i)_j$ je j-tá složka vektoru a_i. Vybereme z P sloupce, které jsou indexovány kanonickou bází $\{e_1, \ldots, e_{m-1}\}$ v $\mathbb{F}^{m-1}$ a nulovým vektorem $o \in \mathbb{F}^{m-1}$. Vektor e_i má na i-té pozici prvek $1 \in \mathbb{F}$ a všude jinde nuly. Nyní si uvědomíme, jak jsou jednotlivé a_i v řádcích definovány (buď je to I nebo F). Uspořádejme F tak, aby $(F)_0 = 0$ a $(F)_1 = 1$. Vybereme tak tuto podmatici o rozměrech $m \times m$:

$$\begin{array}{r} \\ c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{m-2} \\ c_{m-1} \end{array}
\begin{array}{c}
\begin{array}{ccccccc} e_1 & e_2 & e_3 & \cdots & e_{m-1} & o \end{array} \\
\begin{pmatrix}
1 & 0 & 0 & \cdots & 0 & 0 \\
0 & 1 & 0 & \cdots & 0 & 0 \\
0 & 0 & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1 & 0 \\
1 & 1 & 1 & \cdots & 1 & 1
\end{pmatrix}
\end{array}$$

Vidíme, že je shora v odstupňovaném tvaru, a proto je regulární. □

Připomeňme značení, že $T \subseteq R$ je množina, jejichž prvky modulo M tvoří reprezentanty tříd faktorokruhu R/M. Navíc předpokládáme, že $0 \in T$. Z Tvrzení 1.4 víme, že pro každé $r \in R$ existují jednoznačně $r^{(0)}, \ldots, r^{(m-1)} \in T$ tak, že $r = \sum_{i=0}^{m-1} u^i r^{(i)}$. Zobrazení $\phi : R \to \mathbb{F}^{q^{m-1}}$ definujme jako

$$\sum_{i=0}^{m-1} u^i r^{(i)} \mapsto \sum_{i=0}^{m-1} c_i \overline{r^{(i)}}.$$

Nahlédneme, že ϕ je prosté. Mějme $r \neq s \in R$ s rozklady

$$r = \sum_{i=0}^{m-1} u^i r^{(i)} \neq \sum_{i=0}^{m-1} u^i s^{(i)} = s.$$

Z Tvrzení 1.4 jsou tyto $r^{(i)}, s^{(i)} \in T$ jednoznačně určeny. Musí proto existovat $i \in \{0, \ldots, m-1\}$, že $r^{(i)} \neq s^{(i)}$. Z definice T pak $\overline{r^{(i)}} \neq \overline{s^{(i)}}$. Z Pozorování 3.5 jsou výše definované vektory c_i nezávislé, a tudíž lineární kombinace $\sum_{i=0}^{m-1} c_i \overline{r^{(i)}} \neq \sum_{i=0}^{m-1} c_i \overline{s^{(i)}}$ budou rozdílné.

Chceme dokázat, že ϕ je vskutku zobecněné Grayovo zobrazení pro řetězcový okruh R. Nad konečným tělesem ponecháme Hammingovu vzdálenost a řetězcové okruhy vybavíme homogenní vzdáleností.

Uvažme opět lineární kód K nad $\mathbb{F}$ generovaný vektory $c_0, \ldots, c_{m-1}$. Tyto vektory jsou z Pozorování 3.5 lineárně nezávislé, a proto je kód K dimenze m a délky q^{m-1}. Z definice ϕ vidíme, že $\phi(R) = K$ a $\phi : R \to K$ je bijekce. Nejdříve se zaměřme na váhové rozdělení kódu $K = \phi(R)$.

K důkazu využijeme poznatek z klasické teorie samoopravných kódů nad tělesem, že vektory $c_0, \ldots, c_{m-1}$ jsou vlastně bází Reed-Mullerova kódu prvního řádu $\mathrm{RM}_q(1, m-1)$ nad tělesem $\mathbb{F}_q$ (viz [17]), a tedy $K = \mathrm{RM}_q(1, m-1)$. Reed-Mullerovy kódy jsou dobře prozkoumány a je známo (viz [17]), že nenulová kódová slova $\mathrm{RM}_q(1, m-1)$ mají Hammingovu váhu $q^{m-2}(q-1)$ nebo q^{m-1}. Posledně zmíněnou váhu nabývají pouze nenulové násobky c_{m-1}.

Pro usnadnění značení v dalších důkazech použijme tentokrát I jako vektor q^{m-1} jedniček z $\mathbb{F}$. Následující tvrzení a věta s důsledkem vychází z [17].

Tvrzení 3.6. *Prosté zobrazení $\phi : R \to \mathbb{F}^{q^{m-1}}$ zachovává váhy v následujícím smyslu:*

$$w_h(r) = w_H(\phi(r)) \text{ pro } r \in R.$$

Důkaz. Zaměřme se na to, jaké jsou Hammingovy váhy kódových slov z $K = \mathrm{RM}_q(1, m-1)$. Jistě z prostoty ϕ platí $\phi(0) = 0$ a 0 je jediné slovo s váhou 0. Vektor c_{m-1} je vlastně vektor I a má tedy váhu $w_H(c_{m-1}) = q^{m-1}$. Celkem K jistě obsahuje $q-1$ vektorů s váhou q^{m-1} (jsou to nenulové $\mathbb{F}$-násobky c_{m-1}). Prvky ideálu $u^{m-1}R$ jsou tvaru $u^{m-1}r$, kde $r \in R$ rozložíme ve smyslu Tvrzení 1.4 jako $r = \sum_{i=0}^{m-1} u^i r^{(i)}$. Pak $u^{m-1}r = u^{m-1}r^{(0)}$, protože $u^m = 0$. Máme tedy $\phi(u^{m-1}r) = c_{m-1}r^{(0)}$, kde $c_{m-1} = I$. Proto $u^{m-1}R \setminus \{0\}$ o mohutnosti $q-1$ (viz Důsledek 1.6) se zobrazí právě na slova Hammingovy váhy q^{m-1}.

Jelikož $\phi : R \to K$ je bijekce, nezbývá nic jiného než, že se $R \setminus u^{m-1}R$ zobrazí na slova Hammingovy váhy $q^{m-2}(q-1)$ a těch zbývá $q^m - q$. Výsledky ohledně rozdělení vah v K jsme shrnuli do Tabulky 3.1.

Z toho, jak je w_h definované vidíme, že ϕ zachovává váhy, tj. $w_h(r) = w_H(\phi(r))$ pro $r \in R$. □

počet slov	w_H	vzor ϕ
$q^m - q$	$q^{m-2}(q-1)$	$R \setminus u^{m-1}R$
$q-1$	q^{m-1}	$u^{m-1}R \setminus \{0\}$
1	0	0

Tabulka 3.1: Váhové rozdělení kódu K

Z důkazu je pro další postup důležité, že ϕ zachovává váhy a samotné váhové rozdělení tohoto kódu s příslušnými vzory ϕ v R v Tabulce 3.1.

Vraťme se na chvíli k definici w_h. Kromě toho, že splňuje definici homogenní váhy, nebylo zřejmé, k čemu ji lze nadále využít. Ve světle předchozího tvrzení se na ni můžeme dívat jako na technické řešení, aby ϕ zachovávalo váhy. Konkrétní hodnoty w_h na R lze pro naše účely definovat až zde z posledních dvou sloupců Tabulky 3.1.

Směřujeme k dokázání rovnosti $w_h(r-s) = w_H(\phi(r) - \phi(s))$ pro $r, s \in R$. Argumentaci rozdělíme do tří kroků. I když nemusí být ϕ lineární, tak přesto platí následující rovnosti.

Věta 3.7 (Grayovo zobrazení)**.** *Pro $a, r, s \in R$ platí:*

1. $\phi(u^{m-1}a + s) = \phi(u^{m-1}a) + \phi(s)$.
2. $w_H(\phi(r-s)) = w_H(\phi(r) - \phi(s))$.
3. $d_h(r,s) = d_H(\phi(r), \phi(s))$.

Důkaz. 1. Ať $a = \sum_{i=0}^{m-1} u^i a^{(i)}$, $s = \sum_{i=0}^{m-1} u^i s^{(i)}$. Pak $u^{m-1}a = u^{m-1}a^{(0)}$, protože $u^m = 0$. Aplikujme ϕ a dostaneme

$$\phi(u^{m-1}a) = c_{m-1}\overline{a^{(0)}},$$

$$\phi(s) = c_0\overline{s^{(0)}} + \cdots + c_{m-1}\overline{s^{(m-1)}}.$$

Na druhou stranu

$$u^{m-1}a + s = s^{(0)} + \cdots + u^{m-2}s^{(m-2)} + u^{m-1}(s^{(m-1)} + a^{(0)}).$$

Z toho vidíme

$$\phi(u^{m-1}a + s) = c_0\overline{s^{(0)}} + \cdots + c_{m-2}\overline{s^{(m-2)}} + c_{m-1}\overline{(s^{(m-1)} + a^{(0)})}.$$

Jelikož platí $\overline{s^{(m-1)} + a^{(0)}} = \overline{s^{(m-1)}} + \overline{a^{(0)}}$ stačí porovnat obě strany dokazovaného výrazu a dostaneme rovnost.

2. V Tabulce 3.1 jsou uvedené jednotlivé možnosti pro Hammingovu váhu kódu $\phi(R)$. Pro $r = s$ platí tento bod triviálně. Nenulové slovo $\phi(r-s)$ má buď váhu q^{m-1} a je to vlastně násobek I, nebo má váhu $q^{m-2}(q-1)$. Stačí proto dokázat tuto ekvivalenci:

$$\phi(r-s) \text{ je násobek } I \iff \phi(r) - \phi(s) \text{ je násobek } I.$$

($\Rightarrow$) Pokud $\phi(r-s)$ je násobek I, tak $r-s \in u^{m-1}R$ a tedy existuje $b \in R$, že $r = u^{m-1}b + s$. Pišme

$$\phi(r) - \phi(s) = \phi(u^{m-1}b + s) - \phi(s) = \phi(u^{m-1}b) + \phi(s) - \phi(s) = \phi(u^{m-1}b).$$

Při rozepisování jsme použili první bod a vektor $\phi(r) - \phi(s)$ je tak násobek I.
($\Leftarrow$) Ať $\phi(r) - \phi(s)$ je násobek I. Pak nutně $\phi(r) - \phi(s) = \phi(u^{m-1}b)$ pro nějaké $b \in R$. Použitím prvního bodu dostáváme

$$\phi(r) = \phi(u^{m-1}b) + \phi(s) = \phi(u^{m-1}b + s).$$

Z toho, že $\phi : R \to \phi(R)$ je bijekce, musí nastat $r = u^{m-1}b+s$, a tak $r-s = u^{m-1}b$. Vskutku tedy je $\phi(r-s)$ násobek I.

3. S využitím druhého bodu a toho, že ϕ zachovává váhy (viz Tvrzení 3.6) tak již dostáváme:

$$d_h(r,s) = w_h(r-s) = w_H(\phi(r-s)) = w_H(\phi(r) - \phi(s)) = d_H(\phi(r), \phi(s)).$$

□

Zobrazení ϕ tedy zachovává váhy (viz Tvrzení 3.6) i vzdálenosti (viz poslední bod předchozí Věty 3.7). Vrátíme-li se zpět k motivačnímu příkladu nad $\mathbb{Z}_4$, zjistíme, že naše Grayovo zobrazení se shoduje s uvedeným Grayovým zobrazením pro $\mathbb{Z}_4$ a jak jsme již zmínili, tak i w_h se v tomto případě shoduje s w_L. Máme totiž pro $\mathbb{Z}_4$ toto nastavení $u = 2$, $m = 2$, $F = (0,1)$, $I = (1,1)$ a z toho dopočteme $c_0 = (0,1)$, $c_1 = (1,1)$. Grayovo zobrazení $\phi : \mathbb{Z}_4 \to \mathbb{F}_2^2$ má tuto podobu:

$$\begin{aligned}
0 = 2^0 \cdot 0 + 2 \cdot 0 &\overset{\phi}{\mapsto} (0,1) \cdot 0 + (1,1) \cdot 0 = (0,0) \\
1 = 2^0 \cdot 1 + 2 \cdot 0 &\overset{\phi}{\mapsto} (0,1) \cdot 1 + (1,1) \cdot 0 = (0,1) \\
2 = 2^0 \cdot 0 + 2 \cdot 1 &\overset{\phi}{\mapsto} (0,1) \cdot 0 + (1,1) \cdot 1 = (1,1) \\
3 = 2^0 \cdot 1 + 2 \cdot 1 &\overset{\phi}{\mapsto} (0,1) \cdot 1 + (1,1) \cdot 1 = (1,0)
\end{aligned}$$

Nyní ϕ rozšíříme na R^n. Nejdříve rozepíšeme $(x_1, \ldots, x_n) \in R^n$ takto:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum_{i=0}^{m-1} u^i x_1^{(i)} \\ \vdots \\ \sum_{i=0}^{m-1} u^i x_n^{(i)} \end{pmatrix} = \sum_{i=0}^{m-1} u^i \begin{pmatrix} x_1^{(i)} \\ \vdots \\ x_n^{(i)} \end{pmatrix} = \sum_{i=0}^{m-1} u^i x^{(i)}.$$

V poslední rovnosti jsme pouze využili značení $x^{(i)} = (x_1^{(i)}, \ldots, x_n^{(i)})^T$ a předpokládáme, že $x_i^{(0)}, \ldots, x_i^{(m-1)} \in T$ mají stejný význam jako v Tvrzení 1.4. Nyní máme dostatek znalostí a značení pro rozšířené zobrazení $\phi : R^n \to \mathbb{F}^{q^{m-1}n}$, které zavedeme po složkách jako $\phi(x_1, \ldots, x_n) = (\phi(x_1), \ldots, \phi(x_n))$. Opět používáme stejné označení ϕ pro zobrazení na R i R^n.

$$\phi \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum_{i=0}^{m-1} c_i \overline{x_1^{(i)}} \\ \vdots \\ \sum_{i=0}^{m-1} c_i \overline{x_n^{(i)}} \end{pmatrix} = \sum_{i=0}^{m-1} c_i \otimes \begin{pmatrix} \overline{x_1^{(i)}} \\ \vdots \\ \overline{x_n^{(i)}} \end{pmatrix} = \sum_{i=0}^{m-1} c_i \otimes \overline{x^{(i)}}.$$

Vidíme, že rozšířené ϕ má předpis:

$$(x_1, \ldots, x_n) \mapsto \sum_{i=0}^{m-1} c_i \otimes \overline{x^{(i)}}.$$

Jelikož jsme rozšířili prosté zobrazení na více složek, bude výsledné zobrazení opět prosté. Hlavním úkolem je nyní dokázat, že rozšířené Grayovo zobrazení ϕ je izometrie.

Důsledek 3.8 (Rozšířené Grayovo zobrazení)**.** *Nechť je $m \geq 2$. Potom zobrazení $\phi : R^n \to \mathbb{F}^{q^{m-1}n}$ definované výše je prostým Grayovým zobrazením z (R^n, d_h) do $(\mathbb{F}^{q^{m-1}n}, d_H)$. Pro kód C nad R délky n proto platí:*

$$d_h(C) = d_H(\phi(C)).$$

Důkaz. Důkaz máme proveden pro jednu složku z Věty 3.7 o Grayově zobrazení, tj. $w_h(r - s) = w_H(\phi(r) - \phi(s))$ pro $r, s \in R$. Tento fakt snadno rozšíříme pro $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in R^n$, neboť platí:

$$\begin{aligned} d_h(x, y) = w_h(x - y) = \sum_{i=1}^{n} w_h(x_i - y_i) = \sum_{i=1}^{n} w_H(\phi(x_i) - \phi(y_i)) = \\ = w_H(\phi(x) - \phi(y)) = d_H(\phi(x), \phi(y)). \end{aligned}$$

□

Kapitola 4

Konstrukce kódů

Tato kapitola inspirována články [11] a [17]. Po celou dobu kapitoly používáme zavedené značení a předpoklady pro řetězcový okruh R. Jeho maximální ideál M je generovaný u o indexu nilpotence m. Zbytkové těleso R značíme $\mathbb{F}$ či $\mathbb{F}_q$, pokud chceme zdůraznit jeho mohutnost q. Pruhem označujeme kanonickou projekci R do $\mathbb{F}$. Jako obvykle je C lineární kód nad R.

4.1 Shrnutí předchozí kapitoly

Zopakujme nejdříve několik základních faktů z předchozí kapitoly. Grayovo zobrazení ϕ je prosté, a tudíž máme stejný počet kódových slov kódu C i jeho obrazu $\phi(C)$. Důležité parametry každého kódu zapíšeme za sebou takto: (n, M, d)-kód znamená kód délky n, mohutnosti M a minimální vzdálenosti d (vzhledem k zvolené váze). Popř. jsou možné některé další varianty zápisu, když nějaký parametr vynecháme jako (n, M)-kód apod.

Mějme (n, M, d)-kód nad R, kde d je minimální homogenní vzdálenost kódu. Zobrazením tohoto kódů pomocí ϕ dostaneme $(q^{m-1}n, M, d)$-kód nad $\mathbb{F}$, kde d je nyní myšleno vzhledem k Hammingově váze (Důsledek 3.8).

$$(n, M, d)\text{-kód } C \text{ nad } R \text{ s } w_h \xrightarrow{\phi} (q^{m-1}n, M, d)\text{-kód } \phi(C) \text{ nad } \mathbb{F} \text{ s } w_H.$$

Chceme z lineárních kódů nad R zkonstruovat a popsat (obecně) nelineární kódy nad $\mathbb{F}$ s dobrými parametry. Dobré parametry v tomto kontextu znamenají, co nejlepší schopnost opravovat chyby (velké d) při co největší mohutnosti kódu (velké M).

4.2 Zvednutí kódu

V této sekci vycházíme z článku [11]. Mějme lineární kód D nad $\mathbb{F}$. Z řetězcového okruhu R zkonstruujeme další řetězcové okruhy. Pro $e \in \{1, \ldots, m\}$ definujme faktorokruh

$$R_e = R \,/\, \langle u^e \rangle ,$$

což je opět řetězcový okruh s maximálním ideálem generovaný u o indexu nilpotence e. Platí totiž, že faktorokruh řetězcového okruhu je opět řetězcový. Okruh R má ideály

$$R \supseteq uR \supseteq \cdots \supseteq u^m R.$$

Pak okruh R_e má ideály

$$R_e \supseteq uR_e \supseteq \cdots \supseteq u^e R_e.$$

Dle Tvrzení 1.4 nosná množina R je

$$R = \left\{ \sum_{i=0}^{m-1} u^i r^{(i)} \mid r^{(i)} \in T \right\},$$

kde $T \subseteq R$ taková, že prvky T modulo M jsou reprezentanti rozkladových tříd R/M. Navíc $0 \in T$. Proto za reprezentanty faktorokruhu R_e volíme

$$R_e = \left\{ \sum_{i=0}^{e-1} u^i r^{(i)} \mid r^{(i)} \in T \right\}.$$

Ať $f \in \{1, \ldots, m\}$ takové, že $e \leq f$. Zaveďme ořezávací funkci $\Psi_e^f : R_f \to R_e$ předpisem:

$$\Psi_e^f \left(\sum_{i=0}^{f-1} u^i r^{(i)} \right) = \sum_{i=0}^{e-1} u^i r^{(i)}.$$

Zobrazení Ψ_e^f je homomorfismem okruhů. Ořezávací funkci jako obvykle také rozšíříme po složkách na n složek (či na matice). Postupným ořezáváním (ve směru šipek) okruhu R dostaneme reprezentanty okruhů R_f

$$R = R_m \overset{\Psi_f^m}{\to} R_f \overset{\Psi_e^f}{\to} R_e \overset{\Psi_1^e}{\to} R_1 = \mathbb{F}.$$

Pokud máme vnoření $\mathbb{F} \subseteq R$ jako např. u okruhu $R = \mathbb{Z}_2[x]/\langle x^3 \rangle$, kde nosná množina $\mathbb{F}$ je $\{0, 1\}$, je přirozené vzít přímo $T = \mathbb{F}$. Zobrazení Ψ_1^e je pak projekce na $\mathbb{F}$, kterou značíme pruhem. Podobně můžeme chápat inkluzi nosných množin $\mathbb{Z}_p \subseteq \mathbb{Z}_{p^e}$, i když $\mathbb{Z}_p$ není podtěleso v $\mathbb{Z}_{p^e}$, protože není uzavřená na sčítání. V tomto případě volíme $T = \{0, \ldots, p-1\}$.

Naopak proti směru šipek budeme okruhy a kódy zvedat. Obecněji můžeme začít s nějakým nekonečným řetězcovým okruhem, třeba okruhem formálních řad $\mathbb{F}[[x]]$ v proměnné x nad $\mathbb{F}$ s maximálním ideálem $\langle x \rangle$. Po drobném rozšíření definice ořezávací funkce postupně dostáváme tyto řetězcové okruhy

$$\mathbb{F}[[x]] \overset{\Psi_f^\infty}{\to} \mathbb{F}[x]/\langle x^f \rangle \overset{\Psi_e^f}{\to} \mathbb{F}[x]/\langle x^e \rangle \overset{\Psi_1^e}{\to} \mathbb{F}[x]/\langle x \rangle = \mathbb{F}.$$

Zvedání kódu nad okruhem R_e na kód nad okruhem R_f můžeme pak definovat takto. Ať e,$f \in \{1, \ldots, m\}$, kde $e \leq f$. Mějme okruh R a z něho odvozené okruhy R_e, R_f jako výše. Řekneme, že kód D nad R_e délky n se zvedne na kód C nad R_f délky n, pokud $D = \Psi_e^f(C)$. Pro nás bude nejdůležitější případ, kdy zvedáme kód nad $\mathbb{F}$ na kód nad R.

Definice (Zvednutí kódu)**.** *Řekneme, že kód D nad $\mathbb{F}$ se zdvihne na kód C nad R, pokud $D = \overline{C}$.*

Kód C také nazýváme zdvihnutím kódu D. Předpokládejme, že máme generující matici V kódu D nad $\mathbb{F}$ (bez újmy na obecnosti můžeme předpokládat, že je v odstupňovaném tvaru) a nějakou matici W nad R s vlastností $V = \overline{W}$. Pak

W je generující matice C. Naopak neplatí, že pokud W je generující matice, tak i V musí být generující matice. Např. pro $R = \mathbb{Z}_4$, $\mathbb{F} = \mathbb{Z}_2$ s maticemi:

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

je oříznutá matice W rovna

$$\overline{W} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix},$$

Z toho je patrné, že musíme vynechat R-lineárně závislé řádky. Po vynechání nulového řádku z $\overline{W}$ nastane rovnost.

Mějme generující matici V netriviálního kódu D o rozměrech $k \times n$. Navíc můžeme předpokládat, že V je v odstupňovaném tvaru. Generující matici zvednutého kódu W (mající stejné rozměry jako V) v tomto případě dostaneme tak, že předepíšeme řádky W. Pro každý i-tý řádek w_i, v_i matic W a V musí platit, že $\overline{w_i} = v_i$.

Takových matic W existuje mnoho, a tedy W není určeno jednoznačně. Každý invertibilní prvek $\mathbb{F}$ (tzn. nenulový) se zvedne na invertibilní prvek v R z Tvrzení 1.2.

Jak pak pro předepsanou W zvedneme konkrétní slovo $d \in D$? Nejdříve d vyjádříme vzhledem k bázi D, což jsou řádky matice V (ty značíme v_i). Tedy existují jednoznačně $s_1, \ldots, s_k \in \mathbb{F}$ tak, že $d = \sum_{i=1}^{k} s_i v_i$. Zvolme $t_1, \ldots, t_k \in R$, že $\overline{t_i} = s_i$ pro všechna $i = 1, \ldots, k$. Zdvih tohoto slova je pak $c = \sum_{i=1}^{k} t_i w_i$, protože

$$\overline{c} = \overline{\sum_{i=1}^{k} t_i w_i} = \sum_{i=1}^{k} \overline{t_i w_i} = \sum_{i=1}^{k} s_i v_i = d.$$

Celý postup shrneme do Algoritmu 7.

Algoritmus 7 Zdvihnutí slova

Vstup: $d \in D$, generující matice V kódu D nad $\mathbb{F}$, generující matice W kódu C nad R, který je zvednutím D.

Výstup: $c \in C$ takové, že $\overline{c} = d$.

$v_1, \ldots, v_k \leftarrow$ postupně řádky V

Nalezni souřadnice $s_1, \ldots, s_k \in \mathbb{F}$ vektoru d vzhledem k bázi $v_1, \ldots, v_k$.

Zvol $t_1, \ldots, t_k \in R$ takové, že $\overline{t_i} = s_i$ pro všechna $i = 1, \ldots, k$.

$w_1, \ldots, w_k \leftarrow$ postupně řádky W

Vrať $c = \sum_{i=1}^{k} t_i w_i$ jako výstup.

Zvednutí některých kódů podobných cyklickým kódům je ještě jednodušší, jak je popsáno v [25, str. 4]. Identifikujeme-li kódová slova délky n s koeficienty polynomů z $R[x]$ stupně menšího než n, některé kódy lze pak popsat jako ideály $R[x]/\langle f \rangle$. Přehled názvosloví kódů převzaté z [25, Remarks 4.8] pro různá f uvedeme v Tabulce 4.1.

Vždy pro jednoduchost předpokládáme, že $f \in R[x]$ je takový, že $\overline{f}$ je bezčtvercový. Bezčtvercovost polynomu $\overline{f}$ znamená, že pokud pro $g \in \mathbb{F}[x]$ polynom g^2 dělí $\overline{f}$, pak nutně g je invertibilní. V okruhu $R[x]$ není obecně jednoznačná faktorizace na ireducibilní faktory. Pokud ale předpokládáme, že $\overline{f}$ je bezčtvercový,

Třída kódů	f
Cyklické kódy	$x^n - 1$
Negacyklické kódy	$x^n + 1$
Konstacyklické kódy	$x^n + a$, kde $a \in R \setminus \{0\}$

Tabulka 4.1: Přehled názvosloví tříd kódů

tak jistou jednoznačnost (rozkladu na základní ireducibilní faktory) dostaneme. Tento fakt zformulujeme jako variantu Henselova lemmatu. Důkaz lze najít v [24, Theorem 2.7]. Neinvertibilní polynom $f \in R[x]$ nazveme základní ireducibilní, pokud f je ireducibilní nad R a zároveň $\overline{f}$ je ireducibilní nad $\mathbb{F}$.

Lemma (Henselovo)**.** *Nechť $f \in R[x]$ je monický polynom takový, že $\overline{f}$ je bezčtvercový. Pak f se jednoznačně (až na pořadí) rozkládá na po dvou nesoudělné základní ireducibilní monické polynomy.*

Další úvahy provedeme pouze pro cyklické kódy. Pro ostatní třídy v Tabulce 4.1 lze postupovat analogicky. Místo generující matice cyklického kódu D uvažme generující polynom g. AŤ tedy je $f = x^n - 1$. Předpokládejme, že n není dělitelný charakteristikou $\mathbb{F}$, a proto $x^n - 1$ je bezčtvercový polynom v $\mathbb{F}[x]$. Z Henselova lemmatu pak plyne, že pro každý monický dělitel $g \in \mathbb{F}[x]$ polynomu $x^n - 1$ existuje jednoznačně určený monický polynom $h \in R[x]$ takový, že $\overline{h} = g$ a zároveň h dělí $x^n - 1$ v $R[x]$. Kód generovaný polynomem h je zvednutí kódu generovaného g.

Shrňme dílčí otázky při konstrukci pomocí zdvihání v kontextu, který jsme naznačili v úvodu kapitoly.

1. Volba lineárního kódu D nad $\mathbb{F}$.
2. Vybrání konkrétního zvednutí kódu D na lineární kód C nad R.
3. Aplikace Grayova zobrazení ϕ na C.
4. Určení či odhad $d_H(\phi(C))$.

Kromě třetího bodu není na otázky jasná odpověď. Za kód D volíme dobře prozkoumané kódy. Typicky se používají Golayovo kódy či QR kódy.

Pokud je D cyklický, tak odpadají problémy s volbou zdvihu (druhý bod), neboť je jednoznačně určen. Poslední otázkou se zabýváme v následující sekci.

4.3 Minimální homogenní vzdálenost

Zdůrazněme, že odhady na $d_h(C)$ nám vypovídají z Důsledku 3.8 o minimální Hammingově vzdálenosti obrazu, protože $d_h(C) = d_h(\phi(C))$. Uvažme, že známe pouze délku a mohutnost kódu C. Plotkinův odhad lze zobecnit na Frobeniovy okruhy vybavené homogenní vahou. Tvrzení uvedeme bez důkazu, neboť nedává příliš omezující horní odhad na $d_h(C)$. Důkaz je možné nalézt v [16, Proposition 2.1]. V případě řetězcového okruhu jsme za průměrnou hodnotu w_h dosadili hodnotu $(q^{m-2})(q-1)$, kterou jsme spočítali v Pozorování 3.1.

Tvrzení (Plotkinův odhad)**.** *Mějme (obecně nelineární) netriviální (n, M)-kód C nad okruhem R. Pak*

$$d_h(C) \leq \frac{M}{M-1} n(q^{m-2})(q-1).$$

Dostáváme tak vlastně odhad minimální Hammingovy váhy ϕ-obrazu:

$$d_H(\phi(C)) = d_h(C) \leq \frac{M}{M-1} n(q^{m-2})(q-1).$$

Plotkinův odhad je však většinou velmi nadhodnocený. Pokud známe $d_H(C)$, můžeme odhadnout $d_h(C)$ i zdola a horní mez zpřesnit. Následující tvrzení je volně inspirováno [28, Proposition 3.2].

Tvrzení 4.1. *Mějme lineární (n, M)-kód C nad okruhem R. Ať $P \subseteq C$ je taková množina, že pro každé $x \in P$ platí, že $w_H(x) = w_H(C)$. Pak*

$$q^{m-2}(q-1)d_H(C) \leq d_h(C) \leq \min_{x \in P} w_h(x) \leq q^{m-1} d_H(C)$$

Důkaz. Mějme $x \in P$. Hammingova váha udává počet nenulových pozic v x. Je zřejmé, že neexistuje $0 \neq y \in C$, pro které $d_H(y) < d_H(x)$, neboť by to byl spor s minimalitou v definici P. Zároveň nenulové složky x mohou nabývat nejmenší hodnotu $q^{m-2}(q-1)$ vzhledem k homogenní váze. Tím je dokázán dolní odhad.

Vezměme opět $x \in P$. Jistě $d_h(C) \leq d_h(x)$, neboť $d_h(C)$ je minimum. Každá nenulová složka x má homogenní váhu nejvýše q^{m-1}. Tím jsou dokázány horní odhady. □

Znalost minimálních nenulových slov vzhledem k Hammingově váze nám pomůže aproximovat horní mez $d_h(C)$. Odvození prvků P pro obecný kód C je složité, a proto si mnohdy vystačíme s případem, kdy P je pouze náš odhad na množinu minimálních nenulových slov (např. slova s minimálním nosičem z náhodně vybrané podmnožiny $C \setminus \{0\}$). Obecně ale neplatí, že by $\min_{x \in T} w_h(x) = d_h(C)$. Uvažme kód generovaný matici

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

nad $\mathbb{Z}_4$. Tedy $\mathbb{Z}_4 / \langle 2 \rangle = \mathbb{Z}_2$. Násobky prvního řádku matice jsou:

$$(0,0,0,0,0),$$
$$(2,2,0,0,0).$$

Násobky druhého řádku jsou:

$$(0,0,0,0,0),$$
$$(0,0,1,1,1),$$
$$(0,0,2,2,2),$$
$$(0,0,3,3,3).$$

Množina minimálních slov vzhledem k Hammingově váze je $S = \{(2,2,0,0,0)\}$, neboť ostatní lineární kombinace mají váhu alespoň 3. Avšak pro kódové slovo $c = (0,0,1,1,1) \notin P$ je

$$3 = d_h(c) < \min_{x \in S} w_h(x) = 4.$$

Proto v Tvrzení 4.1 nelze pomocí minimálních slov aproximovat $w_h(C)$ zezdola. Rozdíl horní a dolní meze je

$$q^{m-1}d_H(C) - q^{m-2}(q-1)d_H(C) = (q^{m-1} - q^{m-2}(q-1))d_H(C) = q^{m-2}d_H(C).$$

Pokud uvážíme R s $m = 2$ a s libovolným zbytkovým tělesem $\mathbb{F}$, bude předchozí rozdíl nejmenší možný, a to $d_H(C)$. Hammingova váha totiž na rozdíl od homogenní měří pouze nenulové pozice bez ohledu na to, jaký je na nenulové pozici prvek. Abychom toto vyrovnali, můžeme minimalizovat rozdíl nenulových vah v předpisu pro homogenní váhu. To nastává přesně pro $m = 2$ a předpisy w_h pro nenulové prvky se pak liší pouze o jedna.

Obecně můžeme použít odhady z Tvrzení 4.1 následovně. Zdvihneme-li nenulový (volný) lineární kód D nad $\mathbb{F}$ se známou $d_H(D)$ na volný kód C nad R tak víme, že $d_H(C) = d_H(D)$ z Věty 3.3. Pak můžeme použít Tvrzení 4.1 a dostaneme odhad na $d_h(C)$.

Nejčastěji, pokud je to výpočetně možné, se $d_h(C)$ určí přímo hrubou silou. Uvedené výsledky demonstrujeme na komplexních příkladech ternárního Golayova kódu z [17, str. 2523] a binárního Golayova kódu [12]. Je známo, že

$$g = -1 + x^2 - x^3 + x^4 + x^5 \in \mathbb{Z}_3[x]$$

je generující polynom ternárního Golayova $(11, 3^6, 5)$-kódu vzhledem k Hammingově váze. Dle Henselova lemmatu existuje jednoznačně určený polynom h takový, že $\overline{h} = g$ a h dělí $x^{11} - 1$ v $\mathbb{Z}_9[x]$. Takový polynom je

$$h = -1 - 3x + x^2 - x^3 - 2x^4 + x^5 \in \mathbb{Z}_9[x].$$

Pracujeme tedy nad řetězcovým okruhem $\mathbb{Z}_9$, kde zbytkové těleso je $\mathbb{Z}_9/\langle 3\rangle = \mathbb{Z}_3$. Uvažme lineární $(11, 9^6)$-kód, který je generován h a přidejme k jeho generující matici sloupec samých 5. Výsledný $(12, 9^6)$-kód nad $\mathbb{Z}_9$ označme jako C. Jedná se o takové rozšíření původního kódu, kde pro každé rozšířené kódové slovo $x = (x_1, \ldots, x_n) \in C$ je součet složek $\sum_{i=1}^{n} x_i = 0 \pmod 9$. Autoři článku [17] určili hrubou silou, že $d_H(C) = 6$ a $d_h(C) = 15$. Pokusme se bez této znalosti co nejlépe odhadnout $d_h(C)$. Plotkinův odhad dává

$$d_h(C) \leq \frac{9^6}{9^6 - 1} \cdot 12 \cdot 2 = \frac{1594323}{66430} \approx 24.$$

Minimální vzdálenost $d_H(C) = 6$ je pro rozšířený Golayův kód dobře známý. Hrubé odhady z Tvrzení 4.1 potom dávají

$$12 \leq d_h(C) \leq 18.$$

Pokud však uvážíme slovo

$$x = (8, 6, 1, 8, 7, 1, 0, 0, 0, 0, 0, 5) \in C,$$

což je vlastně první řádek generující matice kódu C (záporné složky jsme převedli na kladné). Pak platí $d_H(x) = 7$ a $d_h(x) = 15$. I přesto, že x není minimální slovo vzhledem k Hammingově váze, x je minimální vzhledem k homogenní váze a dává tak nejlepší možný horní odhad na $d_h(C)$. Tudíž jsme zlepšili horní odhad na

$$12 \leq d_H(\phi(C)) \leq 15.$$

Použitím Grayova zobrazení obdržíme $(36, 3^{12}, 15)$ kód $\phi(C)$ nad $\mathbb{F}_3$. Kód $\phi(C)$ je navíc nelineární. Uvažme první a druhý řádek generující matice

$$x = (8, 6, 1, 8, 7, 1, 0, 0, 0, 0, 0, 5) \in C,$$

$$y = (0, 8, 6, 1, 8, 7, 1, 0, 0, 0, 0, 5) \in C.$$

Vektor $\phi(x + y) - \phi(x) - \phi(y)$ má Hammingovu váhu 9. Jelikož $d_H(\phi(C)) = 15$, tak

$$\phi(x + y) - \phi(x) - \phi(y) \notin \phi(C).$$

Jelikož C je lineární, tak $x + y \in C$. To znamená, že kód $\phi(C)$ není uzavřen na lineární kombinace, a proto je nelineární. Článek [17], kde je uvedena tato konstrukce, je z roku 1999. Tvrdí se zde, že v té době není znám ternární $(36, 3^{12})$ kód, který by měl větší minimální vzdálenost. V prosinci 2001 je do Grasslovy tabulky lineárních kódů [15] zadán ternární lineární kód mající stejné parametry, který vznikl propíchnutím některých souřadnic jistého rozšíření ternárního QR kódu (viz [15]).

Analogicky lze postupovat pro binární Golayův $(23, 2^{12}, 7)$-kód (viz [12]), který je generován

$$g = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11} \in \mathbb{Z}_2[x].$$

Generující polynom lze opět dle Henselova lemmatu jednoznačně zvednout na polynom $h \in \mathbb{Z}_8[x]$. Rozšiřme kód generovaný h tak, že přidáme sloupce paritních symbolů k jeho generující matici. Výsledný kód má parametry $(24, 8^{12}, 24)$ vzhledem k homogenní váze. Minimální homogenní vzdálenost určili autoři [12] hrubou silou. Zobrazením pomocí ϕ obdržíme $(96, 2^{36}, 24)$-kód vzhledem k Hammingově váze. Obdobně jako v minulém příkladě je v [12] ukázáno, že tento obraz je nelineární. Nejlepší známý lineární binární kód stejné délky a mohutnosti má dle Grasslovy tabulky [15] minimální vzdálenost rovnu 20.

4.4 Testování

Máme již připravený aparát pro převádění lineárních kódů nad R na kódy nad $\mathbb{F}$ pomocí Grayova zobrazení (viz Důsledek 3.8). Cílem testování je nalézt lineární kód nad R s co největší minimální homogenní vzdálenosti při co největší mohutnosti kódu. Náš přístup k tomuto problému bude založen na náhodném (resp. pseudonáhodném) generování.

Existují však i jiné možnosti. Stejného cíle lze dosahovat například pomocí lexikografických kódu (viz [18]), kde kód se konstruuje hladovým algoritmem s předem zadanou minimální vzdáleností, který navíc zaručuje i linearitu. Bohužel, časová i prostorová složitost tohoto algoritmu je exponenciální (procházíme a ukládáme slova z R^n). Další možností je použití heuristických algoritmů. Na stránce [32] J. Zwanzgera je uvedena databáze vygenerovaných kódů nad různými řetězcovými okruhy. Článek, který by se podrobněji zabýval touto konstrukcí se nám ale nepodařilo nalézt.

Nyní popíšeme průběh testování, který jsme implementovali v programu Mathematica [30]. Zaveďme diskrétní náhodnou veličinu X na $R\backslash\{0\}$ s pravděpodobnostním rozdělením $P[X = r] = p_r$, kde samozřejmě $\sum_{r \in R\backslash\{0\}} p_r = 1$. Generující matici V lineárního kódu nad R jsme vytvářeli pomocí Algoritmu 8.

Algoritmus 8 Konstrukce generující matice

Vstup: nezáporná $p_r \in \mathbb{R}$ pro $r \in R \setminus \{0\}$ taková, že $\sum_{r \in R\setminus\{0\}} p_r = 1$. Dále $k < n \in \mathbb{N}$.
Výstup: generující matice V lineárního kódu nad R délky n a hodnosti k.

1: Dle pravděpodobnostního rozdělení $P[X = r] = p_r$ na $R \setminus \{0\}$ vygeneruj náhodně nezávisle prvky $a_1, \ldots, a_{n-k}$ z $R \setminus \{0\}$.
2: Za posloupnost prvků $a_1, \ldots, a_{n-k}$ přidej $k - 1$ nul.
3: Těchto dohromady $n - 1$ prvků z R označme jako $v \in R^{n-1}$.
4: Vytvoř cirkulantní matici V o rozměrech $k \times (n - 1)$ určenou prvním řádkem v.
5: Přidej na konec matice V sloupec samých 1.
6: Vrať V jako výstup.

Cirkulantní matice je tvořena pravými cyklickým posuny prvního řádku. Matice V na výstupu vypadá takto:

$$V = \begin{pmatrix} a_1 & a_2 & \ldots & a_{n-k} & 0 & \ldots & 0 & 0 & 1 \\ 0 & a_1 & a_2 & \ldots & a_{n-k} & 0 & \ldots & 0 & 1 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ldots & 0 & 1 \\ 0 & \ldots & 0 & a_1 & a_2 & \ldots & a_{n-k} & 0 & 1 \\ 0 & \ldots & 0 & 0 & a_1 & a_2 & \ldots & a_{n-k} & 1 \end{pmatrix},$$

kde prvky $a_1, \ldots, a_{n-k}$ jsou vygenerovány v prvním kroku algoritmu. Z odstupňovaného tvaru matice V ihned vidíme, že V je vskutku generující maticí. Tedy V generuje lineární kód C délky n a hodnosti k. Nyní dokážeme nutnou i postačující podmínku, kdy je C volný.

Tvrzení 4.2. *Mějme matici V z výstupu Algoritmu 8 o rozměrech $k \times n$. Předpokládejme, že $k > 1$. Lineární kód nad R generovaný V označme C. Pak C je volný právě tehdy, když existuje $1 \leq i \leq n - k$ takové, že $a_i \in R^*$.*

Důkaz. ($\Rightarrow$) Důkaz provedeme nepřímo. Předpokládejme, že $a_i \notin R^*$ pro každé $1 \leq i \leq n - k$. Z Tvrzení 1.2 jsou všechna a_i z uR. Prohoďme první a poslední sloupec v matici V. Výslednou matici označme $\tilde{V}$. Odečtením prvního řádku $\tilde{V}$ od ostatních vynulujeme složky pod 1 v jejím prvním sloupci (přitom první řádek zůstává nezměněn). Ideál uR je jistě uzavřen na sčítání a na násobení prvkem z R, a tudíž všechny složky upravené matice kromě složky v prvním řádku a sloupci (to je totiž 1) jsou z uR. Algoritmus 5 puštěný na takto upravenou matici vrátí standardní tvar G, pro který existuje $j \in \{1, \ldots, m - 1\}$, že $k_j > 0$. Tudíž dle Tvrzení 2.7 není C volný.

($\Leftarrow$) Vezměme $1 \leq i \leq n - k$ nejmenší číslo takové, že $a_i \in R^*$. Jsme v situaci

$$V = \left(\begin{array}{cc|ccccc|ccc} a_1 & \ldots & a_i & \ldots & a_{n-k} & 0 & \ldots & 0 & 0 & 1 \\ 0 & a_1 & \ldots & a_i & \ldots & a_{n-k} & 0 & \ldots & 0 & 1 \\ \vdots & \ldots & \ddots & \ddots & \ddots & \ddots & \ddots & \ldots & 0 & 1 \\ 0 & \ldots & 0 & a_1 & \ldots & a_i & \ldots & a_{n-k} & 0 & 1 \\ 0 & \ldots & 0 & 0 & a_1 & \ldots & a_i & \ldots & a_{n-k} & 1 \end{array}\right).$$

Zaměřme se na na zvýrazněnou podmatici, jejíž diagonála obsahuje samé prvky a_i. Označme ji W. Na matici V budeme provádět ekvivalentními úpravy

tak, aby podmatice W se přeměnila na jednotkovou matici. Dále pak tuto jednotkovou matici propermutujememe na začátek matice V. Permutačně ekvivalentními úpravami jsme z V obdrželi standardní tvar generující matice tvaru $(I \mid Q)$ pro nějakou matici Q. Z Tvrzení 2.7 pak vyplyne, že generovaný kód je volný.

Nejdříve si všimněme, že prvky pod hlavní diagonálou W jsou všechny neinvertibilní v R a na hlavní diagonále W jsou invertibilní v R. Postupujme odzadu a vynulujme hodnoty v posledním sloupci podmatice W nad prvkem a_i, tím že budeme přičítat násobek posledního řádku k ostatním (poslední řádek se nemění). Vhodný násobek vždy nalezneme, neboť a_i je invertibilní. Ukážeme, že i po těchto úpravách zůstávají prvky pod hlavní diagonálou W neinvertibilní a na hlavní diagonále W zůstávají invertibilní.

Z Tvrzení 1.2 jsou neinvertibilní prvky z uR a invertibilní z $R \setminus uR$. Složky posledního řádku W bez prvku a_i vynásobené prvkem z R zůstávají tak v uR. Přičteme-li prvek z uR k prvku z uR obdržíme opět prvek z uR. Tudíž pod diagonálou matice W zůstávají neinvertibilní prvky. Naopak přičtením prvku $s \in uR$ k prvku $r \in R \setminus uR$ je výsledkem prvek z $R \setminus uR$, neboť

$$\overline{s + r} = \overline{s} + \overline{r} = \overline{r} \neq 0.$$

Tudíž na hlavní diagonále W zůstávají invertibilní prvky.

Indukčně můžeme pokračovat předposledním řádkem atd. až dostaneme na místě W shora odstupňovanou matici. Na diagonále vždy zůstávají po ekvivalentních úpravách invertibilní prvky a pod ní neinvertibilní. Snadno proto můžeme vynulovat prvky pod diagonálou a vynásobit řádky příslušnými inverzními prvky, abychom tak dostali na místě W jednotkovou matici, jak jsme potřebovali. □

Průchodem všech kódových slov C stanovíme minimální homogenní vzdálenost a dopočítáme parametry obrazu $\phi(C)$. V průběhu testování Algoritmus 8 vícekrát opakujeme a popř. měníme na začátku hodnoty p_r, kde $r \in R \setminus \{0\}$. Osvědčilo se volit hodnoty p_r rovnoměrně či s zdůrazněním prvků, které nabývají na R největší homogenní váhy. Např. pro $\mathbb{Z}_4$ jsme používali rozdělení $p_1 = 1/3$, $p_2 = 1/3$, $p_3 = 1/3$ nebo rozdělení $p_1 = 1/4$, $p_2 = 1/2$, $p_3 = 1/4$.

Tento způsob generování se osvědčil. Jednak na základě našich pokusů dává lepší výsledky než po náhodném vygenerování celé matice, jelikož nám stačí náhodně vygenerovat jen část prvního řádku matice a navíc při náhodném generování celé matice může vzniknout situace, kdy jeden řádek matice je lineární kombinací ostatních. Tvar matice z Algoritmu 8 je cirkulantní matice, což má souvislost s cyklickými kódy, s přidaným „paritním“ sloupcem. Takovýto tvar V jsme zvolili, neboť v literatuře se často v tomto tvaru objevují generující matice zajímavých kódů (např. [12, 17]).

Nyní uvedeme pozorování, s jehož pomocí budeme porovnávat naše vygenerované kódy. Ukážeme, že pokud existuje kód nad konečným tělesem s minimální Hammingovou vzdáleností d, tak jsme schopni zkonstruovat lineární kód nad řetězcovým okruhem, jehož minimální homogenní vzdálenost nabývá dolní hranice z Tvrzení 4.1.

Pozorování 4.3. *Mějme nenulový (n, q^k, d)-kód D nad $\mathbb{F}_q$ vzhledem k w_H. Potom:*

1. *Existuje volný* $(n, q^{mk}, q^{m-2}(q-1)d)$*-kód nad* R *vzhledem k* w_h.

2. *Existuje* $(q^{m-1}n, q^{mk}, q^{m-2}(q-1)d)$*-kód nad* $\mathbb{F}_q$ *vzhledem k* w_H.

Důkaz. Generující matici X kódu D vybereme tak, aby obsahovala v prvním svém řádku vektor $x \in \mathbb{F}_q^n$ s Hammingovou váhou d. Dle Steinitzovy věty o výměně (rozšíříme lineárně nezávislou množinu $\{x\}$ na bázi D o některé generátory D) lze takovou X nalézt. V matici případně X permutujeme sloupce tak, abychom dostali ve složce v prvním řádku a sloupci nenulový prvek. Následně takto upravenou matici převedeme do (zdola) odstupňovaného tvaru, přičemž první řádek x se neměnní. Výslednou matici označme Y.

Zvolme množinu reprezentantů $T \subseteq R$ o mohutnosti q tak, aby po aplikaci kanonické projekce jsme dostali všechny prvky $\mathbb{F}_q$ a zároveň $0 \in T$. Zvednutí invertibilního prvku $\mathbb{F}$ (tzn. nenulového) je invertibilní v R z Tvrzení 1.2. Uvažme $k \times n$ matici W nad R takovou, že obsahuje pouze složky z T a $Y = \overline{W}$. Jelikož má W na hlavní diagonále invertibilní prvky, můžeme ekvivalentními úpravami převést W do standardního tvaru $(I_k \mid Q)$ pro nějakou Q. Kód generovaný W označme C.

Kód C z tvaru standardní generující matice je z Tvrzení 2.7 volný o mohutnosti $|R|^{\mathrm{rank}(C)} = q^{mk}$ (viz Důsledek 1.6). Protože $\overline{C} \neq \{0\}$, je $d_H(C) = d$ dle Věty 3.3. Z Tvrzení 4.1 použijeme dolní odhad a dostaneme $q^{m-2}(q-1)d \leq d_h(C)$. Pro všechna $0 \neq t \in T$ je váha $w_h(t) = q^{m-2}(q-1)$, neboť $t \notin uR$. Výše zmíněný řádek x z X se tedy zdvihne na řádek s homogenní vahou $q^{m-2}(q-1)d$. Proto $d_h(C) = q^{m-2}(q-1)d$.

Druhý bod je snadným důsledkem prvního bodu a Důsledku 3.8. □

Výsledky testování pro $R = \mathbb{Z}_4$ jsou uvedeny v Tabulce 4.2 a pro $R = \mathbb{Z}_9$ v Tabulce 4.3. Nejlepší získané kódy z testování opakováním Algoritmu 8 zapisujeme do tabulky jako kódy C. Jejich délka je n, M je mohutnost kódu, $\log_{q^m} M$ je jejich hodnost (uvedené kódy C jsou volné) a d_h je zkratka pro $d_h(C)$. Stejný význam sloupců nacházíme i ve sdružení sloupců pod kódem $\phi(C)$, kde akorát d_H je zkrácení $d_H(\phi(C))$. Konkrétní předpis ϕ závisí na konkrétním R a je uveden před Tvrzením 3.6. Jednotlivé parametry $\phi(C)$ jsou spočítány z parametrů C použitím Důsledku 3.8.

V Pozorování 4.3 bereme za D nejlepší známý lineární kód délky n a dimenze $\log_{q^m} M$, kde M je mohutnost C, z Grasslovy tabulky kódů [15], abychom v rámci tohoto pozorování dosáhli nejlepších možných minimální vah. Jednotlivé minimální homogenní váhy této konstrukce z Pozorování 4.3 jsou znázorněny ve sloupci „Konstr. 4.3“. Délka a hodnost kódu z konstrukce v Pozorování 4.3 je stejná jako u kódu C (viz první dvě nejlevější hodnoty ve stejném řádku), proto zapisujeme do tabulek pouze údaj o minimální homogenní váze kódu, který opět značíme jako d_h.

Kódy nad $\mathbb{Z}_4$ v Tabulce 4.2 jsme navíc srovnávali s databází $\mathbb{Z}_4$ kódů [2]. V ní jsou uloženy kvaternární kódy nalezené zejména algoritmem PDG (angl. progressive dimension growth) nebo aplikací inverzního Grayova zobrazení na známé binární lineární kódy. V databázi [2] neexistuje lineární kód, který by měl lepší parametry než lineární kódy uvedené v Tabulce 4.2. Navíc jsme našli lineární kódy, které mají větší minimální homogenní vzdálenost než kódy při stejné délce a mohutnosti uvedené v databázi [2]. Tyto kódy byly posléze do databáze [2] přidány. Generující matice přidaných kódů lze nalézt v příloze na str. 63.

Zbývá vysvětlit použité zkratky v poznámkách u kódů C a $\phi(C)$. Popisek „nový“ se nachází pouze u kódů C v Tabulce 4.2 a znamená, že daný kód má vetší minimální homogenní vzdálenost než lineární kódy v databázi [2] se stejnou délkou i mohutností. Takto označené kódy byly do této databáze dodatečně vloženy.

Poznámka „JNL“ se vyskytuje u kódů $\phi(C)$ a je zkrácením neformálního „jako nejlepší lineární“ a znamená, že kód $\phi(C)$ má stejné parametry jako nejlepší lineární kód nad $\mathbb{F}$ v Grasslově tabulce kódů [15].

Poznámka „LNL“ se vyskytuje u kódů $\phi(C)$ a je zkrácením neformálního „lepší než lineární“ a znamená, že kód $\phi(C)$ má vetší minimální vzdálenost než jako nejlepší lineární kód nad $\mathbb{Z}_2$ v Grasslově tabulce kódů [15] se stejnou délkou a mohutností.

Poznámka „OPT“ se vyskytuje u kódů $\phi(C)$ a je zkrácením přívlastku „optimální“ a znamená, že žádný jiný nelineární kód mající délku a minimální vzdálenost jako $\phi(C)$ nemůže mít větší mohutnost než právě $\phi(C)$. Odhady na nelineární kódy nad $\mathbb{F}$ byly převzaty z [3].

4.5 Shrnutí testování

Algoritmus 8 poskytuje jednoduchý postup, jak konstruovat lineární kódy nad R. Záznamy z Tabulek 4.2 a 4.3 shromažďují některé zajímavé kódy získané touto metodou. Lineárně jsme popsali mnoho kódů nad konečným tělesem, které mají parametry jako nejlepší lineární (u kódu $\phi(C)$ mají poznámku JNL). Pro lepší přehlednost zavedeme značení, že matice $V(n, M, d_h)$ z výstupu Algoritmu 8 generuje lineární kód délky n, mohutnosti M a minimální homogenní vzdálenosti d_h. Grayovy obrazy lineárních kódů nad $\mathbb{Z}_4$ generované maticemi $V(7, 4^3, 6)$ a $V(8, 4^4, 6)$ mají parametry dokonce lepší něž jakýkoli binární lineární kód o stejné délce a mohutnosti.

$$V(7,4^3,6) = \begin{pmatrix} 1 & 2 & 1 & 3 & 0 & 0 & 1 \\ 0 & 1 & 2 & 1 & 3 & 0 & 1 \\ 0 & 0 & 1 & 2 & 1 & 3 & 1 \end{pmatrix},$$

$$V(8,4^4,6) = \begin{pmatrix} 1 & 3 & 2 & 3 & 0 & 0 & 0 & 1 \\ 0 & 1 & 3 & 2 & 3 & 0 & 0 & 1 \\ 0 & 0 & 1 & 3 & 2 & 3 & 0 & 1 \\ 0 & 0 & 0 & 1 & 3 & 2 & 3 & 1 \end{pmatrix}.$$

Zároveň žádný jiný nelineární binární kód mající stejnou délkou a minimální Hammingovou vzdálenost, ale větší mohutnost, neexistuje. Lineární kód nad $\mathbb{Z}_4$ generovaný $V(8, 4^4, 6)$ má parametry stejné jako známý oktakód (viz [29, Example 3.4]), jehož Grayův obraz je snad ještě známější Nordstrom-Robinsonův kód.

Vygenerované kódy nad $\mathbb{Z}_4$ jsme dále srovnávali s databází kvaternárních kódů [2]. Algoritmem 8 jsme obdrželi několik kódů s lepšími parametry, než které jsou v uvedené v [2] (jsou označeny jako nové). Jejich generující matice jsou uvedeny v příloze na str. 63. Úzkým hrdlem testování je určování minimální vzdálenosti kódů hrubou silou, což má exponenciální časovou složitost vzhledem k hodnosti kódů. Jistě by bylo zajímavé provést testování na mohutnějších a delších kódech, které jsme z výpočetního hlediska nemohli provést.

Kód C				Konstr. 4.3	Kód $\phi(C)$			
n	$\log_4 M$	d_h	Pozn.	d_h	n	$\log_2 M$	d_H	Pozn.
7	3	6		4	14	6	6	LNL, OPT
8	4	6		4	16	8	6	LNL, OPT
9	4	6		4	18	8	6	JNL
9	5	4		4	18	10	4	JNL
10	2	9		6	20	4	9	
10	4	6		4	20	8	6	
10	5	6		4	20	10	6	JNL
10	6	4		3	20	12	4	JNL
11	4	8	nový	5	22	8	8	JNL
11	5	6		4	22	10	6	
11	7	4		3	22	14	4	JNL
12	3	10	nový	6	24	6	10	JNL
12	4	8		6	24	8	8	JNL
12	5	6		4	24	10	6	
13	3	11	nový	7	26	6	11	
13	5	8		5	26	10	8	JNL
13	6	6		4	26	12	6	
14	4	10	nový	7	28	8	10	
14	5	8		6	28	10	8	
14	6	8	nový	5	28	12	8	JNL
15	2	14		10	30	4	14	
15	4	12		8	30	8	12	JNL
15	5	10		7	30	10	10	
15	6	8		6	30	12	8	
16	6	9	nový	6	32	12	9	
16	7	8		6	32	14	8	JNL
17	5	11	nový	8	34	10	11	
17	6	10		7	34	12	10	
17	7	8		6	34	14	8	
18	5	12		8	36	10	12	
18	6	10		8	36	12	10	
19	5	13	nový	8	38	10	13	
19	7	10		8	38	14	10	
20	6	12		8	40	12	12	
20	7	10		8	40	14	10	

Tabulka 4.2: Přehled některých vygenerovaných kódů nad $\mathbb{Z}_4$ s ϕ obrazy

	Kód C		Konstr. 4.3		Kód $\phi(C)$		
n	$\log_9 M$	d_h	d_h	n	$\log_3 M$	d_H	Pozn.
5	3	6	4	15	6	6	JNL
6	2	11	8	18	4	11	JNL
8	2	15	12	24	4	15	JNL
8	3	12	10	24	6	12	
8	4	10	8	24	8	10	
9	2	18	12	27	4	18	JNL
9	3	15	12	27	6	15	JNL
10	3	15	12	30	6	15	
10	4	12	12	30	8	12	
11	2	21	16	33	4	21	JNL
11	3	18	14	33	6	18	JNL
11	4	15	12	33	8	15	
12	1	27	24	36	2	27	JNL
12	2	24	18	36	4	24	JNL
13	2	24	18	39	4	24	
13	3	21	18	39	6	21	
13	4	18	14	39	8	18	
14	2	27	20	42	4	27	JNL
14	3	22	18	42	6	22	
14	4	19	16	42	8	19	
15	2	29	22	45	4	29	JNL
15	3	24	18	45	6	24	
15	4	21	18	45	8	21	
16	2	31	24	48	4	31	JNL
16	3	26	20	48	6	26	
16	4	23	18	48	8	23	
16	5	19	18	48	10	19	
17	2	33	24	51	4	33	JNL
17	3	28	22	51	6	28	
17	4	24	20	51	8	24	
17	5	21	18	51	10	21	
18	2	35	26	54	4	35	
18	3	30	24	54	6	30	
18	4	26	22	54	8	26	

Tabulka 4.3: Přehled některých vygenerovaných kódů nad $\mathbb{Z}_9$ s ϕ obrazy

Závěr

V této práci jsme uvedli základy teorie samoopravných kódů nad konečnými komutativními řetězcovými okruhy. Ve stručnosti shrneme základní linii myšlenek abstrahovaných ze všech kapitol dohromady.

Nejdříve jsme představili potřebný aparát k práci s řetězcovými okruhy. Posléze jsme studovali strukturu lineárních kódů nad konečnými řetězcovými okruhy. Hlavní výsledek z Věty 3.3 nám však říká, že z pohledu Hammingovy váhy nemají tyto kódy lepší parametry než klasické lineární kódy nad konečným tělesem. V kontextu Věty 3.3 se může zdát, že zobecnění kódů nad tělesem na řetězcové okruhy není potřeba. Pokud začneme vážit jednotlivá kódová slova jinou vahovou funkci, v našem případě homogenní váhou, situace se změní. V podkapitole 3.3 představujeme koncept zobecněného Grayova zobrazení pro řetězcové okruhy, který dodává těmto kódům znova na atraktivitě. Je totiž možné lineárně popsat nelineární kódy, které můžou mít parametry lepší než nejlepší lineární kódy. Tímto faktem jsme byli motivováni provést v poslední kapitole testování a hledat tak lineární kódy nad řetězcovým okruhem s co nejlepšími parametry jejich Grayova obrazu.

Zdrojů, které souvisí se studiem tématu práce je velmi mnoho. Orientace je o to složitější, že teorie často v této oblasti vzniká postupným zobecňováním. To je např. znatelné u konceptu Grayova zobrazení, které je v literatuře častokrát zkoumáno jen pro konkrétní třídy řetězcových okruhů. Naším cílem bylo proto vybrat vhodnou výchozí literaturu pro toto téma, která je dostatečně obecná a zároveň poskytuje užitečnou teorii.

Snažili jsme se o největší možnou kompaktnost práce. Jelikož jsme větší prostor v práci vymezili teorii kódů, některé hlubší výsledky jsme v teorii řetězcových okruhů přímo v textu nedokazovali. Ukázalo se, že by bylo potřeba zavést poměrně rozsáhlý teoretický aparát, který by se nikde jinde v práci nevyužil. Místo toho jsme mohli hlouběji prozkoumat minimální vzdálenosti kódů a zobecněné Grayovo zobrazení. Navíc zde popsaná témata týkající se kódů vyžadují pouze základní poznatky z teorie řetězcových okruhů.

Vygenerované kódy v poslední kapitole dávají mnoho zajímavých výsledků. Úzké hrdlo testování je určování minimální homogenní vzdálenosti hrubou silou. Vygenerované kódy o velké hodnosti nemohly být z výpočetního hlediska podrobeny dalším testům (mohutnost kódů roste exponenciálně vzhledem k hodnosti). Bylo by jistě zajímavé otestovat naši uvedenou konstrukci pro delší a mohutnější kódy a také pro jiné třídy řetězcových okruhů.

Seznam použité literatury

[1] E. F. Assmus and J. D. Dey. *Designs and their Codes*. Number 103. Cambridge University Press, 1992.

[2] N. Aydin and T. Asamov. The Z4 database, 2007 [cit. 2014-04-03]. Dostupné z: `http://www.asamov.com/Z4Codes/CODES/ShowCODESTablePage.aspx`.

[3] M. Best, A. Brouwer, F. MacWilliams, A. Odlyzko, and N. Sloane. Bounds for binary codes of length less than 25. *IEEE Transactions on Information Theory*, 24(1):81–93, 1978.

[4] A. R. Calderbank, A. R. Hammons, P. V. Kumar, N. J. A. Sloane, and P. Solé. A linear construction for certain Kerdock and Preparata codes. *Bulletin of the American Mathematical Society*, 29(2):218–222, 1993.

[5] W. E. Clark and D. A. Drake. Finite chain rings. In *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*, volume 39, pages 147–153. Springer, 1973.

[6] W. E. Clark and J. J. Liang. Enumeration of finite commutative chain rings. *Journal of Algebra*, 27(3):445–453, 1973.

[7] I. Constantinescu. *Lineare Codes über Restklassenringen ganzer Zahlen und ihre Automorphismen bezüglich einer verallgemeinerten Hamming-Metrik*. Disertační práce, Technische universität München, 1995.

[8] H. Q. Dinh, S. R. López-Permouth, and S. Szabo. On the structure of cyclic and negacyclic codes over finite chain rings. *Codes over Rings, e-Proc. of the CIMPA Summer School, Turkey*, pages 18–29, 2008.

[9] S. T. Dougherty, J. L. Kim, and H. Kulosman. MDS codes over finite principal ideal rings. *Designs, Codes and Cryptography*, 50(1):77–92, 2009.

[10] S. T. Dougherty, J. L. Kim, and H. Liu. Constructions of self-dual codes over finite commutative chain rings. *International Journal of Information and Coding Theory*, 1(2):171–190, 2010.

[11] S. T. Dougherty, H. Liu, and Y. H. Park. Lifted codes over finite chain rings. *Mathematical Journal of Okayama University*, 53(1):39–53, 2011.

[12] I. M. Duursma, M. Greferath, S. N. Litsyn, and S. E. Schmidt. A $\mathbb{Z}_8$ - linear lift of the binary Golay code and a nonlinear binary (96, 2^{37}, 24)-code. *Information Theory, IEEE Transactions on*, 47(4):1596–1598, 2001.

[13] C. Flaut. Cyclic codes over some special rings. *Bull. Korean Math. Soc*, 50(5):1513–1521, 2013.

[14] T. G. Gazaryan. An example of non-isomorphic commutative chain rings. *Russian Mathematical Surveys*, 47(3):174–175, 1992.

[15] M. Grassl. Bounds on the minimum distance of linear codes and quantum codes, 2007 [cit. 2014-04-03]. Dostupné z: `http://www.codetables.de`.

[16] M. Greferath and M. E. O'Sullivan. On bounds for codes over Frobenius rings under homogeneous weights. *Discrete mathematics*, 289(1):11–24, 2004.

[17] M. Greferath and S. E. Schmidt. Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code. *Information Theory, IEEE Transactions on*, 45(7):2522–2524, 1999.

[18] K. Guenda, T. A. Gulliver, and S. A. Sheikholeslam. Lexicodes over rings. *Designs, Codes and Cryptography*, pages 1–15, 2012.

[19] T. Honold and I. Landjev. Linear codes over finite chain rings. *The Electronic Journal of Combinatorics*, 7(1):R11, 1999.

[20] J. Horáček. Grupové okruhy v teorii kódů. Bakalářská práce, Univerzita Karlova v Praze, Matematicko-fyzikální fakulta, 2012.

[21] X. Hou. Lattice of ideals of the polynomial ring over a commutative chain ring. *arXiv preprint arXiv:1308.0727*, 2013.

[22] E. Kleinfeld et al. Finite Hjelmslev planes. *Illinois Journal of Mathematics*, 3(3):403–407, 1959.

[23] G. H. Norton. On minimal realization over a finite chain ring. *Designs, Codes and Cryptography*, 16(2):161–178, 1999.

[24] G. H. Norton and A. Sălăgean. On the structure of linear and cyclic codes over a finite chain ring. *Applicable algebra in engineering, communication and computing*, 10(6):489–506, 2000.

[25] G. H. Norton and A. Salagean. On the Hamming distance of linear codes over a finite chain ring. 2001.

[26] Y. H. Park. Modular independence and generator matrices for codes over $\mathbb{Z}_m$. *Designs, codes and Cryptography*, 50(2):147–162, 2009.

[27] M. Sobotka. Modulární a p-adické kódy. Diplomová práce, Univerzita Karlova v Praze, Matematicko-fyzikální fakulta, 2013.

[28] P. Sole and V. Sison. Bounds on the minimum homogeneous distance of the p^r-ary image of linear block codes over the Galois ring $\mathrm{GR}(p^r, m)$. *IEEE transactions on information theory*, 53(6):2270–2273, 2007.

[29] Z. X. Wan and C. H. Wan. *Quaternary codes*. World Scientific Publishing Co., Inc., 1998.

[30] Inc. Wolfram Research. *Mathematica, Version 8.0*. Wolfram Research, Inc., Champaign, Illinois, 2010.

[31] J. A. Wood. Foundations of linear codes defined over finite modules: the extension theorem and the MacWilliams identities. *Codes Over Rings (Ankara, 2008), Ser. Coding Theory Cryptol*, 6:124–190, 2009.

[32] J. Zwanzger. A table for good linear codes over chain rings constructed by Heurico II, 2009 [cit. 2014-04-04]. Dostupné z: `http://www.mathe2.uni-bayreuth.de/20er/codedb/index.html`.

Seznam tabulek

3.1 Rozdělení vah kódu K 42

4.1 Přehled názvosloví tříd kódů 48
4.2 Přehled některých vygenerovaných kódů nad $\mathbb{Z}_4$ 56
4.3 Přehled některých vygenerovaných kódů nad $\mathbb{Z}_9$ 57

Příloha

Generující matice lineárních kódů nad $\mathbb{Z}_4$ z výstupu Algoritmu 8, které byly přidány do databáze kódů [2]. V kulatých závorkách za V je postupně uvedena délka, mohutnost a minimální homogenní vzdálenost kódu, který je generován příslušnou maticí.

$$V(11,4^4,8) = \begin{pmatrix} 3 & 1 & 3 & 2 & 3 & 2 & 1 & 0 & 0 & 0 & 1 \\ 0 & 3 & 1 & 3 & 2 & 3 & 2 & 1 & 0 & 0 & 1 \\ 0 & 0 & 3 & 1 & 3 & 2 & 3 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 3 & 1 & 3 & 2 & 3 & 2 & 1 & 1 \end{pmatrix}$$

$$V(12,4^3,10) = \begin{pmatrix} 1 & 2 & 2 & 1 & 1 & 3 & 1 & 2 & 1 & 0 & 0 & 1 \\ 0 & 1 & 2 & 2 & 1 & 1 & 3 & 1 & 2 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 & 2 & 1 & 1 & 3 & 1 & 2 & 1 & 1 \end{pmatrix}$$

$$V(13,4^3,11) = \begin{pmatrix} 1 & 1 & 3 & 2 & 3 & 1 & 3 & 3 & 2 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 3 & 2 & 3 & 1 & 3 & 3 & 2 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 3 & 2 & 3 & 1 & 3 & 3 & 2 & 1 & 1 \end{pmatrix}$$

$$V(14,4^4,10) = \begin{pmatrix} 3 & 2 & 3 & 1 & 3 & 3 & 2 & 1 & 3 & 3 & 0 & 0 & 0 & 1 \\ 0 & 3 & 2 & 3 & 1 & 3 & 3 & 2 & 1 & 3 & 3 & 0 & 0 & 1 \\ 0 & 0 & 3 & 2 & 3 & 1 & 3 & 3 & 2 & 1 & 3 & 3 & 0 & 1 \\ 0 & 0 & 0 & 3 & 2 & 3 & 1 & 3 & 3 & 2 & 1 & 3 & 3 & 1 \end{pmatrix}$$

$$V(14,4^6,8) = \begin{pmatrix} 3 & 1 & 2 & 1 & 3 & 3 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 3 & 1 & 2 & 1 & 3 & 3 & 3 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 3 & 1 & 2 & 1 & 3 & 3 & 3 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 3 & 1 & 2 & 1 & 3 & 3 & 3 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 3 & 1 & 2 & 1 & 3 & 3 & 3 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 3 & 1 & 2 & 1 & 3 & 3 & 3 & 1 & 1 \end{pmatrix}$$

$$V(16,4^6,9) = \begin{pmatrix} 1 & 2 & 2 & 3 & 3 & 2 & 1 & 2 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 2 & 2 & 3 & 3 & 2 & 1 & 2 & 3 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 2 & 2 & 3 & 3 & 2 & 1 & 2 & 3 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 2 & 2 & 3 & 3 & 2 & 1 & 2 & 3 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 2 & 3 & 3 & 2 & 1 & 2 & 3 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 3 & 3 & 2 & 1 & 2 & 3 & 1 & 1 \end{pmatrix}$$

$$V(17,4^5,11) = \begin{pmatrix} 1 & 2 & 3 & 3 & 1 & 2 & 3 & 2 & 3 & 1 & 2 & 3 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 2 & 3 & 3 & 1 & 2 & 3 & 2 & 3 & 1 & 2 & 3 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 2 & 3 & 3 & 1 & 2 & 3 & 2 & 3 & 1 & 2 & 3 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 2 & 3 & 3 & 1 & 2 & 3 & 2 & 3 & 1 & 2 & 3 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 3 & 3 & 1 & 2 & 3 & 2 & 3 & 1 & 2 & 3 & 1 \end{pmatrix}$$

$$V(19,4^5,13)=\begin{pmatrix}
2&3&1&1&2&1&3&2&2&2&3&1&2&3&0&0&0&0&1\\
0&2&3&1&1&2&1&3&2&2&2&3&1&2&3&0&0&0&1\\
0&0&2&3&1&1&2&1&3&2&2&2&3&1&2&3&0&0&1\\
0&0&0&2&3&1&1&2&1&3&2&2&2&3&1&2&3&0&1\\
0&0&0&0&2&3&1&1&2&1&3&2&2&2&3&1&2&3&1
\end{pmatrix}$$