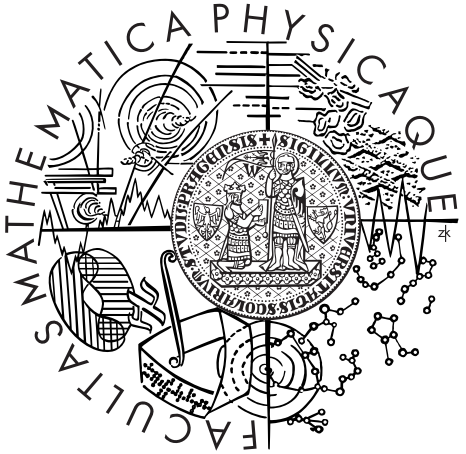
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

DIPLOMOVÁ PRÁCE



Miloslav Sobotka

Modulární a p-adické kódy

Katedra algebry

Vedoucí diplomové práce: RNDr. Jan Šťovíček, Ph.D.

Studijní program: Matematika

Studijní obor: Matematické metody informační bezpečnosti

Praha 2013

Děkuji vedoucímu své práce RNDr. Janu Šťovíčkovi, Ph.D., za vedení a cenné připomínky k práci.

Dále bych rád poděkoval rodině za podporu a trpělivost a snoubence Anně za to, že mi byla oporou.

Prohlašuji, že jsem tuto diplomovou práci vypracoval(a) 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 Praze dne 12. 4. 2012. Podpis autora

Název práce: Modulární a p-adické kódy

Autor: Bc. Miloslav Sobotka

Katedra: Katedra algebry

Vedoucí diplomové práce: RNDr. Jan Šťovíček, Ph.D., Katedra algebry, MFF UK

Abstrakt: Cílem práce bylo studium modulárních kódů nad okruhy $\mathbb{Z}_{p^e}$ a kódů p-adických. Motivací byla představa posloupnosti kódů nad do sebe vnořenými okruhy $\mathbb{Z}_{p^e}$, kdy kódy nad menšími okruhy mají tu vlastnost, že je lze získat z kódu nad vyšším okruhem operací modulo. Naopak při budování této posloupnosti volíme zdvihy tak, aby tato podmínka zůstala zachována. Tento koncept vede k celé řadě otázek týkajících se kvality zdvižených, či řekněme snížených kódů, od zachování parametrů kódů, přes samodualitu a cykličnost až po studium chování váhového výčtu.

Klíčová slova: modulární kód, p-adický kód, teorie invariantů, váhový výčet, MacWilliamsové identita

Title: Modular and p-adic codes

Author: Bc. Miloslav Sobotka

Department: Department of Algebra

Supervisor: RNDr. Jan Šťovíček, Ph.D., Department of Algebra, MFF UK

Abstract: The aim of this thesis was to study modular codes over rings $\mathbb{Z}_{p^e}$ and p-adic codes. The motivation was the idea of a sequence of codes over nested rings $\mathbb{Z}_{p^e}$, where the codes over smaller rings are obtained from the codes over larger rings using the modulo operation. Conversely, when constructing such a sequence we choose the lifts of the codes over smaller rings so that this condition is satisfied. This concept leads to a wide range of questions concerning the quality of the lifted or restricted codes, such as whether the parameters of the codes are preserved, whether lifted or restricted codes will be self-dual or cyclic, or what is the behavior of the weight enumeration with respect to lifting.

Keywords: modular code, p-adic code, theory of invariants, weight enumerator, MacWilliams identity

Obsah

Úvod

Studium kódů nad okruhy je poměrně mladou záležitostí. Na začátku devadesátých let minulého století způsobilo rozruch nalezení vztahu, přesněji řečeno zobrazení, které zobrazuje nelineární kód nad tělesem na lineární kód nad okruhem. Tento objev zveřejnili ve své práci [3] autoři Hammons, Kumar, Calderbank, Solé a Sloane. To vedlo k bouřlivému studiu kódů nad okruhy. Lineární kódy jsou totiž z praktického hlediska ve značné výhodě díky snadnějšímu kódování a dekódování. To je důvod, proč zůstávaly některé kódy nedoceněny, ačkoliv měly jinak dobré parametry. Jmenujme například Preparatovy a Kerdockovy kódy.

Hlavní motivací práce se stala představa vybraných modulárních kódů nad okruhy $\mathbb{Z}_{p^e}$, kdy $e \in \mathbb{N}$, jako nekonečné posloupnosti. Kódy do posloupnosti vybíráme tak, aby pro libovolné $e < f$, $e, f \in \mathbb{N}$, pro ně platilo, že pokud se podíváme na kód nad $\mathbb{Z}_{p^f}$ modulo p^e, dostaneme kód nad $\mathbb{Z}_{p^e}$. Namístě je pak řada otázek týkajících se zdvihu a ořezávání kódů. Jednou z nich je i otázka, co by se stalo, pokud bychom zvedli kód nekonečněkrát. Tato otázka vedla mimo jiné k zavedení definice p-adického kódu ve článku [4] autorů Sloaneho a Calderbanka. Autoři se v něm také zabývají studiem cyklických kódů. Samotné studium převádí na problém hledání ideálů ve faktorech Galoisových okruhů. Využívají podobného postupu, jaký se využívá při studiu cyklických kódů nad tělesem, které se převádí na studium ideálů faktorokruhu polynomů. Tímto článkem byla práce původně motivována. Nicméně v průběhu času se její těžiště posunulo spíše ke studiu samoduálních kódů, které vede ke konkrétnějším a zajímavějším výsledkům, jak je patrné i z následujícího krátkého představení jednotlivých kapitol.

Nejprve se budeme obecně zabývat modulárními kódy a jejich vztahem ke kódům p-adickým. Budeme hledat odpověď na otázku, co se stane při oříznutí či zdvihu modulárního kódu, a co se při tom děje se samodualitou. Také nalezneme ekvivalentní podmínku na existenci samoduálních modulárních a p-adických kódů.

Další zastávkou bude seznámení se s MacWilliamsové větou ve verzi pro okruhy a jejími důsledky. Jessie MacWilliamsová v roce 1962 dokázala, že váhový výčet kódu a výčet jeho duálu jsou pevně spjaty, že z jednoho lze jednoznačně určit druhý. MacWilliamsové identita, jak je také vztah nazýván, nám umožní aplikovat výsledky teorie invariantů. Z MacWilliamsové identity lze totiž vyčíst netriviální transformaci, vůči které musí být váhový výčet samoduálního kódu neměnný (invariantní). Tato, společně s dalšími případně vypozorovanými transformacemi, nám umožní zúžit okruh polynomů, které jsou vůči těmto transformacím invariantní. Tyto polynomy jsou zároveň potencionálními váhovými výčty samoduálních kódů. Ke každému invariantu totiž nemusí nutně existovat kód. Tímto problémem se ostatně mimo jiné zabývá kniha [12].

V poslední kapitole se daří propojit výsledky předchozích kapitol na konkrétním příkladu Hammingova rozšířeného binárního kódu. Ukážeme si na něm, že pokud budeme chtít zachovat při zvedání pro něj typické vlastnosti samodualitu a cykličnost, určíme tím jednoznačně podobu všech jeho zdvihů. Navíc za pomoci dokázané teorie nalezneme matice zdvižených kódů a určíme váhové výčty všech zdvihů.

Cílem práce bylo shromáždit a nastudovat dostupné články zabývající se té-

maty souvisejícími s teorií modulárních kódů. Dále z nich některé zajímavé vybrat a přehledně zpracovat. To vše ve srozumitelné podobě představit čtenáři. Snažil jsem se, aby byly podané důkazy dostatečně podrobné, aby bylo možné ověřit jejich platnost. Dále jsem se snažil o ucelenost a kompaktnost práce.

Výsledky v první podkapitole první kapitoly jsem převzal především z [6]. Věta 1.1.7 je vlastní. Část pojednávající o zvedání kódů vychází z výsledků uvedených v článku [14]. Vlastní jsou úvodní lemmata usnadňující práci s Euklidovými vahami. Dále jsou vlastní důkazy lemmat 1.2.4 a 1.2.5, jež jsem dokazoval na základě osnov uvedených v [14]. Postup při zpracování existence p-adických samoduálních kódů je rovněž přejat z [6]. Důkaz lemmatu 1.3.8 jsem dostudoval přes odkaz v článku [13] z článku [1] a přepracoval. Také důkazy lemmat 1.3.5, 1.3.9 a 1.3.10 jsou vlastní.

Původní důkaz MacWilliamsové identity v zobecněném znění pro okruhy se mi nedařilo dohledat. Inspiroval jsem se proto článkem [8], který dokazuje verzi pro tělesa způsobem, kdy je přímo vidět, proč by měla platit. Rozšíření pro modulární kódy je pak vlastní počin. Protože se však zobecněním důkaz stal méně čitelným a pochopitelným, uvádím důkazy obou verzí. Teorie invariantů je převzatá, zpracována především za pomoci zdrojů [11], [14], [15], [16].

Třetí kapitola je zčásti převzatá z [5], příklad je doplněn za využití [14] a [4].

Příklady jsou víceméně vlastní až na příklady související s teorií invariantů.

Z teorie čísel se předpokládá znalost Legendrova symbolu a jeho vlastností. Dále se bude předpokládat, že čtenář zná Henselovo lemma, například [2], str. 118, a že je mu znám okruh p-adických čísel.

Příprava

V úvodní podkapitole zadefinujeme základní pojmy, dokážeme jednoduché vztahy.

V celém textu p značí prvočíslo. Faktorokruh $\mathbb{Z}/p^e\mathbb{Z}$ budeme značit $\mathbb{Z}_{p^e}$, $\mathbb{Z}_{p^\infty}$ pak okruh p-adických celých čísel. Občas budeme společně značit $\mathbb{Z}_q$ modulární okruhy i okruh p-adických celých čísel, tedy $\mathbb{Z}_q = \mathbb{Z}_{p^e}$, kde $1 \leq e \leq \infty$.

Každý prvek konečného okruhu $\mathbb{Z}_{p^e}$ lze jednoznačně zapsat ve tvaru $\sum_{i=0}^{e-1} a_i p^i$, kde $0 \leq a_i < p$. Podobně každý prvek $\mathbb{Z}_{p^\infty}$ lze zapsat jako nekonečný součet $\sum_{i=0}^{\infty} a_i p^i$, opět $0 \leq a_i < p$. Charakteristika $\mathbb{Z}_{p^e}$ je p^e, okruh $\mathbb{Z}_{p^\infty}$ je charakteristiky 0.

Ať $\mathbb{Z}_q = \mathbb{Z}_{p^e}$, kde $1 \leq e \leq \infty$. Snadno lze ověřit, že množina $\mathbb{Z}_q^n$, $n \in \mathbb{N}$ tvoří $\mathbb{Z}_q$-modul. Libovolný jeho podmodul C budeme nazývat kódem. Obvykle se v literatuře definuje kód jako libovolná podmnožina $\mathbb{Z}_q^n$, podmodul $\mathbb{Z}_q^n$ se pak nazývá lineární kód. My se však budeme zabývat výhradně lineárními kódy, proto pod pojmem kód budeme rozumět vždy lineární kód. Hammingovou vahou kódového slova $c \in C$ budeme rozumět, jak je obvyklé, počet nenulových souřadnic, značíme ji $w(c)$. Minimální váha kódu je pak rovna minimální váze mezi vahami všech nenulových kódových slov. Pokud vezmeme $u, v \in \mathbb{Z}_q$, budeme vnitřním součinem u, v rozumět $[u, v] = \sum u_i v_i \pmod q$, v případě $q = p^\infty$ definujeme $[u, v] = \sum u_i v_i$.

Máme-li nenulový lineární kód C nad $\mathbb{Z}_{p^e}$, e konečné, lze generující matici kódu G převést pomocí elementárních řádkových úprav a pomocí vhodných permutací souřadnic do tvaru

$$\begin{pmatrix} p^0 I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & A_{0,e-1} & A_{0,e} \\ 0 & p^1 I_{k_1} & pA_{1,2} & pA_{1,3} & \cdots & pA_{1,e-1} & pA_{1,e} \\ 0 & 0 & p^2 I_{k_2} & p^2 A_{2,3} & \cdots & p^2 A_{2,e-1} & p^2 A_{2,e} \\ . & . & . & . & \cdots & . & . \\ 0 & 0 & 0 & 0 & \ldots & p^{e-1} I_{k_{e-1}} & p^{e-1} A_{e-1,e} \\ 0 & 0 & 0 & 0 & \ldots & 0 & p^e I_{k_e} \end{pmatrix}.$$

I_{k_i} značí identickou matici velikosti k_i. Platí $n = \sum_{i=0}^{e-1} k_i$. Takto upravenou matici po vynechání posledních k_e nulových (jsme v $\mathbb{Z}_{p^e}$) řádků nazveme generující maticí kódu ve standardizovaném tvaru a budeme ji značit G'. Typem matice G', případně typem kódu generovaného maticí G, budeme rozumět zápis

$$(1)^{k_0}(p)^{k_1}(p^2)^{k_2} \cdots (p^{e-1})^{k_{e-1}}(0)^{k_e}$$

nesoucí informaci o velikosti jednotlivých bloků matice. Pokud je k_i nulové, je zvykem v zápise vynechávat člen $(p^i)^{k_i}$.

Kód je tvořen lineárními kombinacemi řádků generující matice, v našem případě je možné, s přihlédnutím ke standardizované formě generující matice, každé slovo jednoznačně zapsat ve tvaru

$$(v_0, v_1, \ldots, v_{e-1})G',$$

kde vektor v_i je ze $\mathbb{Z}_{p^{e-i}}$ a má délku k_i. Počet kódových slov kódu s typem $(1)^{k_0}(p)^{k_1}(p^2)^{k_2} \cdots (p^{e-1})^{e-1}$ proto bude roven

$$|C| = (p^e)^{k_0}(p^{e-1})^{k_1}(p^{e-2})^{k_2} \ldots (p^1)^{k_{e-1}} = p^{(\sum_{i=1}^{e} i k_{e-i})}. \tag{1}$$

Lemma 0.0.1. *Ať M je matice $k \times n$ nad $\mathbb{Z}_{p^e}$ a ať je ve standardizovaném tvaru typu $(1)^{k_0}(p)^{k_1}(p^2)^{k_2}\cdots(p^{e-1})^{k_{e-1}}(p^e)^{k_e}$. Označme*

$$\mathrm{Ker}(M) = \{x \in \mathbb{Z}_{p^e} \mid Mx^T \equiv 0 \pmod{p^e}\}.$$

Potom $|\mathrm{Ker}(M)| = (1)^{k_0}(p)^{k_1}(p^2)^{k_2}\cdots(p^{e-1})^{k_{e-1}}(p^e)^{k_e}$.

Důkaz. Snadno si lze ověřit, že pokud $m \in \mathbb{N}$, $a \in \mathbb{Z}_{p^e}^m$, tak kongruence $p^l x^T \equiv 0 \pmod{p^e}$, $l \in \mathbb{N}_0$, má v $\mathbb{Z}_{p^e}^m$ celkem $\left(p^e/p^{e-l}\right)^m = (p^l)^m$ různých řešení.

Budeme hledat počet řešení v $\mathbb{Z}_{p^e}^n$ soustavy kongruencí zadaných maticí M. Protože elementární úpravy ani prohazování sloupců nemají na počet řešení vliv, lze předpokládat, že M je ve standardizovaném tvaru. Dostáváme soustavu

$$\begin{pmatrix} p^0 I_{k_0} & A_{0,1} & A_{0,2} & \cdots & A_{0,e-1} & A_{0,e} \\ 0 & p^1 I_{k_1} & pA_{1,2} & \cdots & pA_{1,e-1} & pA_{1,e} \\ 0 & 0 & p^2 I_{k_2} & \cdots & p^2 A_{2,e-1} & p^2 A_{2,e} \\ . & . & . & \cdots & . & . \\ 0 & 0 & 0 & \ldots & p^{e-1} I_{k_{e-1}} & p^{e-1} A_{e-1,e} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ . \\ x_n \end{pmatrix} \equiv 0 \pmod{p^e}.$$

Soustavu budeme řešit podobně jako soustavu lineárních rovnic. Podívejme se nejprve, jaké podmínky na řešení klade poslední blok matice (posledních k_{e-1} řádků). Označme x_{e-1}, x_e vektory proměnných délky k_{e-1}, respektive k_e, máme:

$$p^{e-1} I_{k_{e-1}} x_{e-1}^T + p^{e-1} A_{e-1,e} x_e^T \equiv 0 \pmod{p^e}.$$

Vektor x_e volíme libovolně ze $\mathbb{Z}_{p^e}^{k_e}$. Pak možností, jak dopočíst x_{e-1} je $(p^e/p^1)^{k_{e-1}} = (p^{e-1})^{k_{e-1}}$. Podobně v předposledním bloku můžeme volit z $(p^{e-2})^{k_{e-2}}$ vektorů. Stejně postupujeme až k prvnímu bloku. Dostáváme, že celkový počet různých řešení v $\mathbb{Z}_{p^e}$ je $(1)^{k_0}(p)^{k_1}(p^2)^{k_2}\cdots(p^{e-1})^{k_{e-1}}(p^e)^{k_e}$. □

Definujme duální kód k C jako $C^\perp = \{v \mid [u,v] = 0 \ \forall u \in C\}$, přičemž uvedeným vnitřním součinem se rozumí vnitřní součin příslušející okruhu, nad kterým je kód definován. Samoduálním kódem pak rozumíme kód C, že $C = C^\perp$.

Důsledek 0.0.2. *Ať C je kód nad $\mathbb{Z}_{p^e}$ typu $(1)^{k_0}(p)^{k_1}(p^2)^{k_2}\cdots(p^{e-1})^{k_{e-1}}$. Potom generující matici jeho duálního kódu $C^\perp$ lze převést na tvar*

$$\begin{pmatrix} p^{e-1}B_{e-1,e} & p^{e-1}I_{k_1} & 0 & 0 & 0 & 0 & 0 \\ . & . & . & . & \cdots & . & . \\ p^2 B_{2,e} & p^2 B_{2,e-1} & \ldots & p^2 B_{2,3} & p^2 I_{k_{e-2}} & 0 & 0 \\ pB_{1,e} & pB_{1,e-1} & \ldots & pB_{1,3} & pB_{1,2} & pI_{k_{e-1}} & 0 \\ B_{0,e} & B_{0,e-1} & \ldots & B_{0,3} & B_{0,2} & B_{0,1} & I_{k_e} \end{pmatrix}.$$

Dále platí $|C^\perp| = (p)^{k_1}(p^2)^{k_2}\cdots(p^{e-1})^{k_{e-1}}(p^e)^{k_e} = p^{(\sum_{i=1}^{e} i k_i)}$. Navíc $|C| \cdot |C^\perp| = (p^e)^n$ a $(C^\perp)^\perp = C$.

Důkaz. To, že lze generující matici duálu zapsat ve zmíněném tvaru plyne z důkazu lemmatu 0.0.1. Velikost již umíme z typu generující matice ve standardizovaném tvaru odvodit. Z $\sum_{i=0}^{e} k_i = n$ a z velikostí kódů plyne $|C| \cdot |C^\perp| = (p^e)^n$. Pokud tento vztah aplikujeme na $C^\perp$, dostaneme $|C^\perp| \cdot |(C^\perp)^\perp| = (p^e)^n$, tedy nutně $|C| = |(C^\perp)^\perp|$. Společně s $C \subseteq (C^\perp)^\perp$ dostáváme $(C^\perp)^\perp = C$. □

Důsledek 0.0.3. *Ať C je samoduální kód nad $\mathbb{Z}_{p^e}$. Potom $|C| = p^{en/2}$. Speciálně, pokud p^e není čtverec, nutně je n sudé.*

Důkaz. Přímý důsledek 0.0.2. □

Nyní se podíváme na kódy nad $\mathbb{Z}_{p^\infty}$, jinak také p-adické. Ať G je generující matice p-adického kódu. G' budeme značit její standardizovaný tvar, jehož dosáhneme opět permutací souřadnic a elementárními úpravami:

$$\begin{pmatrix} p^{m_0}I_{k_0} & p^{m_0}A_{0,1} & p^{m_0}A_{0,2} & p^{m_0}A_{0,3} & \cdots & p^{m_0}A_{0,b-1} & p^{m_0}A_{0,b} \\ 0 & p^{m_1}I_{k_1} & p^{m_1}A_{1,2} & p^{m_1}A_{1,3} & \cdots & p^{m_1}A_{1,b-1} & p^{m_1}A_{1,b} \\ . & . & . & . & \cdots & . & . \\ 0 & 0 & 0 & 0 & \cdots & p^{m_{b-1}}I_{k_{b-1}} & p^{m_{b-1}}A_{b-1,b} \end{pmatrix}, \quad (2)$$

kde $0 \leq m_0 < m_1 < \ldots < m_{b-1}$ a vhodné $b \in \mathbb{N}$. Sloupce budou opět tvořit bloky o velikostech $k_0, \ldots, k_b$, k_i nezáporné, $n = \sum_{i=0}^{b} k_i$. Říkáme, že matice G' stejně jako i kód, který generuje, je typu $(p^{m_0})^{k_0}(p^{m_1})^{k_1} \ldots (p^{m_{b-1}})^{k_{b-1}}$. Pokud je $m_0 > 0$, můžeme celý kód podělit p^{m_0}, protože $\mathbb{Z}_{p^\infty}$ je obor integrity. Budeme proto nadále předpokládat, že $m_0 = 0$. Nenulový kód nad $\mathbb{Z}_{p^\infty}$ obsahuje nekonečně slov.

1. Zvedání a ořezávání kódů, existence p-adických

Cílem této kapitoly je zjistit, co se děje s vlastností býti samoduálním kódem při ořezávání a při zdvihání samoduálního kódu. Dále dokážeme, pro které délky existuje samoduální p-adický kód, a naopak, jaké délky nutně musí být samoduální p-adický kód.

1.1 Pohled dolů, samodualita oříznutých kódů

Cíl: V této sekci se pokusíme zodpovědět otázku, co se stane se samoduálním kódem nad $\mathbb{Z}_{p^e}$, pokud se na něj podíváme modulo p^l, $l < e$, jako na kód nad $\mathbb{Z}_{p^l}$. Bude se jednat vůbec o kód? Zůstane zachována samodualita? A co se stane při stejném postupu s p-adickým samoduálním? Ukážeme si, že budeme-li na p-adický samoduální kód nahlížet modulo p^l, získáme opět samoduální kód. Narozdíl od modulárního samoduálního kódu, kdy tomu tak nutně být nemusí.

Lemma 1.1.1. *Ať C je p-adický kód. Pak $C^\perp$ je typu 1^k pro vhodné $k \in \mathbb{N}$.*

Důkaz. Stačí ukázat, že máme-li slovo v duálním kódu, které je násobkem p, bude duální kód obsahovat i slovo, které vznikne po jeho podělení p. Jinými slovy žádný řádek generující matice duálního kódu nebude násobkem p.

Ať $p^m u \in C^\perp$, tedy $[p^m u, v] = 0 \; \forall v \in C$. Využijeme, že $\mathbb{Z}_{p^\infty}$ je obor integrity a vlastností vnitřního součinu, dostáváme, $[p^m u, v] = p^m [u, v] = 0$ implikuje $[u, v] = 0 \; \forall v \in C$, tedy $u \in C^\perp$. □

Lemma 1.1.2. *Ať C je p-adický kód. Potom $C = (C^\perp)^\perp$ právě tehdy, když C je typu 1^k pro vhodné $k \in \mathbb{N}$.*

Důkaz. Ať C je typu 1^k. Z lemmatu 1.1.1 a linearity $C^\perp$ typu 1^{n-k}. Opětovná aplikace dává $(C^\perp)^\perp$ typu 1^k, nutně $(C^\perp)^\perp = C$. Naopak $(C^\perp)^\perp$ typu 1^k dle 1.1.1 a $C = (C^\perp)^\perp$. □

Důsledek 1.1.3. *Je-li C p-adický samoduální kód délky n, pak je typu $1^{n/2}$.*

Důkaz. Přímý důsledek 1.1.1. □

Zadefinujme ořezávací funkci $\Psi_f : \mathbb{Z}_{p^\infty} \to \mathbb{Z}_{p^f}$ takto

$$\Psi_f \left(\sum_{i=0}^{\infty} a_i p^i \right) = \sum_{i=0}^{f-1} a_i p^i.$$

Představíme-li si nekonečný p-adický zápis čísla ze $\mathbb{Z}_p^\infty$ (popřípadě celého vektoru), vidíme, že ořezávací funkce je obdoba modulení u celých čísel. Snadno lze ověřit, že se jedná o homomorfismus okruhů. Poznamenejme jen, že ořezávací funkce závisí na p, bylo by tedy vhodnější psát Ψ_{p^f}. Protože však nehrozí nedorozumění, budeme pro stručnost používat zkrácený zápis. Obdobně definujme ořezávací

funkci pro modulární okruhy. Ať $e, f \in \mathbb{N}$, $f \leq e$. Definujeme $\Psi_f^e : \mathbb{Z}_{p^e} \to \mathbb{Z}_{p^f}$ takto

$$\Psi_f^e \left(\sum_{i=0}^{e-1} a_i p^i \right) = \sum_{i=0}^{f-1} a_i p^i.$$

Je-li $v = (v_1, \ldots, v_n) \in \mathbb{Z}_{p^\infty}^n$, budeme zápisem $\Psi_f(v)$ rozumět vektor oříznutý po složkách, tedy $(\Psi_f(v_1), \ldots, \Psi_f(v_n))$ ze $\mathbb{Z}_{p^f}^n$. Obdobně pro Ψ_f^e.

Je-li H matice $k \times n$ nad p-adickými čísly, jejíž i-tý řádek je h_i, budeme zápisem $\Psi_f(H)$ rozumět matici $k \times n$, jejíž i-tý řádek je $\Psi_f(h_i)$. Obdobně pro Ψ_f^e.

Přirozenou otázkou je, zda oříznutím kódu získáme kód a co se stane s typem kódu. Protože se ořezávací funkce Ψ_f chová homomorfně, dostaneme zřejmě oříznutím p-adického či modulárního kódu kód. Typ zůstane zachován, pokud se v něm nebudou vyskytovat vyšší mocniny p než f-té, ty totiž Ψ_f zobrazí na 0. Shrňme tato pozorování do následujícího lemmatu jak pro modulární, tak p-adické kódy.

Lemma 1.1.4. *Ať C je kód s generující maticí G nad $\mathbb{Z}_{p^e}$, $1 \leq e \leq \infty$. Ať $f \in \mathbb{N}$, že $f < e$. Potom $G_f := \Psi_f^e(G)$ je generující matice kódu nad $\mathbb{Z}_{p^f}$. Je-li G' typu $(1)^{k_0}(p)^{k_1}(p^2)^{k_2} \cdots (p^{m-1})^{k_{m-1}}$, potom G'_f je typu $(1)^{k_0}(p)^{k_1}(p^2)^{k_2} \cdots (p^l)^{k_l}$, kde $l \in \mathbb{N}$ je největší mezi exponenty p vyskytujícími se v typu G' menšími než f.*

Důkaz. Vizte diskuze výše. □

Ať G je generující matice C. Zápisem $\Psi_f(C)$, případně $\Psi_f^e(C)$ budeme rozumět kód nad $\mathbb{Z}_{p^f}$ generovaný maticí $\Psi_f(G)$ případně $\Psi_f^e(G)$.

Lemma 1.1.5. *Ať C je samoduální kód nad $\mathbb{Z}_{p^e}$, $1 \leq e \leq \infty$. Ať $f \in \mathbb{N}$, že $f < e$. Potom platí $\Psi_f(C) \subseteq (\Psi_f(C))^\perp$.*

Důkaz. Protože C je samoduální, $\forall u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in C$ platí $[u, v] = 0$. Potom vnitřní součin v $\mathbb{Z}_{p^f}$ (počítáme tedy modulo p^f) libovolných dvou kódových slov oříznutého kódu je roven

$$[\Psi_f(u), \Psi_f(v)] \equiv \sum \Psi_f(u_i)\Psi_f(v_i) = \sum \Psi_f(u_i v_i) = \Psi_f\big(\sum u_i v_i\big) \equiv \Psi_f(0) = 0.$$

Vnitřní součin libovolných dvou kódových slov je tedy nulový. Proto $\Psi_f(C) \subseteq (\Psi_f(C))^\perp$. □

Následující lemma a poznámka zodpoví otázku, zda ořezávání p-adických a modulárních kódů zachovává vlastnost býti samoduálním kódem.

Věta 1.1.6 (Pohled dolů, p-adický)**.** *Je-li C p-adický samoduální kód, pak i $\Psi_e(C)$ je samoduální $\forall e \in \mathbb{N}$.*

Důkaz. Z lemmatu 1.1.5 víme $\Psi_e(C) \subseteq (\Psi_e(C))^\perp$. Aby byl kód samoduální, stačí proto zkontrolovat, že mimo něj není slovo kolmé na všechna kódová, tedy stačí ověřit $|\Psi_e(C)| = |(\Psi_e(C))^\perp|$. Z důsledku 1.1.3 plyne, že C je typu $1^{n/2}$, z 1.1.4 máme, že i $\Psi_e(C)$ je typu $1^{n/2}$, tedy $|\Psi_e(C)| = p^{en/2}$. Dále z důsledku 0.0.2 víme, že $|\Psi_e(C)| \cdot |(\Psi_e(C))^\perp| = p^{en}$, tedy nutně oba kódy mají stejný počet kódových slov a $\Psi_e(C) = (\Psi_e(C))^\perp$. □

Předchozí lemma říká, že ořízntím libovolného samoduálního p-adického kódu získáme samoduální. Obdobné tvrzení nebude platit pro libovolný modulární kód. Záleží na jeho typu. Uvažme jako příklad oříznutí nejmenšího samoduálního kódu nad $\mathbb{Z}_4$, kódu $\{0, 2\}$ délky 1. Jeho oříznutím totiž získáme nulový kód nad $\mathbb{Z}_2$ délky 1, který jistě není samoduální. Následující lemma nám poskytne ekvivalentní podmínku na to, aby kód a jeho oříznutí byly oba samoduální. Ukáže se, že je to ekvivalentní podmínce, že jsou typu 1^k. Protože jsou p-adické kódy nutně typu 1^k, je vidět, proč se oříznutím samodualita zachovává pro všechny p-adické samoduální a ne tak pro modulární samoduální.

Věta 1.1.7 (Pohled dolů, modulární)**.** *Ať C je samoduální kód nad $\mathbb{Z}_{p^e}$, $e \in \mathbb{N}$. Ať $f \in \mathbb{N}$, $f < e$. Potom $\Psi_f(C)$ je samoduální právě tehdy, když C je typu 1^k.*

Důkaz. Ať C je typu 1^k. Z lemmatu 0.0.3 máme $|C| = p^{en/2}$, speciálně tedy $k = n/2$. Z 1.1.5 víme $\Psi_f(C) \subseteq (\Psi_f(C))^\perp$. Abychom dokázali, že je samoduální, zbývá ověřit $|\Psi_f(C)| = |(\Psi_f(C))^\perp|$. Protože i $\Psi_f(C)$ musí být jedině typu $1^{n/2}$, můžeme spočítat velikost kódu i velikost jeho duálu. Obě vyjdou $p^{fn/2}$. Proto $\Psi_f(C)$ je samoduální.

Naopak předpokládejme, že C je samoduální kód nad $\mathbb{Z}_{p^e}$. Ať $f \in \mathbb{N}$, $f < e$ takové, že $\Psi_f(C)$ je také samoduální. Značme jej dále C'. Nechť kód C' je typu

$$(1)^{k_0}(p)^{k_1}(p^2)^{k_2} \cdots (p^{f-1})^{k_{f-1}}. \tag{1.1}$$

Typ kódu C pak můžeme zapsat

$$(1)^{k_0}(p)^{k_1}(p^2)^{k_2} \cdots (p^{f-1})^{k_{f-1}}(p^f)^{k_f}(p^{f+1})^{k_{f+1}} \cdots (p^{e-1})^{k_{e-1}}. \tag{1.2}$$

Pro jednoduchost nejprve předpokládejme, že typ kódu se oříznutím nezmění. To je ekvivalentní tomu, že obsahuje nejvýše $(f-1)$-ní mocninu p. Jinými slovy předpokládáme, že typ C i C' je shodně tvaru (1.1). Nyní velikost kódu C bude p^l, kde $l = \sum_{i=0}^{f-1} k_i(e-i)$. Podobně velikost kódu C' je rovna $p^{l'}$, kde $l' = \sum_{i=0}^{f-1} k_i(f-i)$. Protože oba jsou samoduální, dle 0.0.3 platí pro kód C rovnost $p^{en/2} = p^l$, tedy $en/2 = l$. Podobně pro C' dostaneme $fn/2 = l'$. Pokud první rovnost podělíme e a druhou f a rozepíšeme l a l', dostaneme rovnosti

$$\frac{n}{2} = k_0 \cdot 1 + k_1 \cdot \frac{e-1}{e} + k_2 \cdot \frac{e-2}{e} + \ldots + k_{f-1} \cdot \frac{e-f+1}{e}, \tag{1.3}$$

$$\frac{n}{2} = k_0 \cdot 1 + k_1 \cdot \frac{f-1}{f} + k_2 \cdot \frac{f-2}{f} + \ldots + k_{f-1} \cdot \frac{1}{f}. \tag{1.4}$$

Zlomek $(e-i)/e$ je ostře větší jak $(f-i)/f$ pro každé $i \in \{1, \ldots, f-1\}$, neboť $e > f$. To znamená, že pokud se v typu kódu vyskytuje nenulové k_i pro nějaké $i \in \{1, \ldots, f-1\}$, bude pravá strana rovnice (1.3) ostře větší jak pravá strana rovnice (1.4). Dostáváme spor $n/2 > n/2$. Nutně tedy v typu kódu je nejvyšší nenulový exponent k_0, proto je kód typu 1^k. Zbývá si rozmyslet, že obecně může být typ kódu C tvaru (1.2), nicméně ostrá nerovnost zůstane tím spíše zachována, spor. Dokázali jsme, že jsou-li dva samoduální kódy, kdy jeden je oříznutím druhého, jsou nutně typu 1^k.

□

Z právě dokázaného lemmatu mimo jiné plyne, že máme-li samoduální kód, který není typu 1^k, víme, že neexistuje žádné jeho oříznutí ani zdvih, který by byl rovněž samoduálním kódem. Z tohoto důvodu se dále omezíme jen na kódy typu 1^k.

1.2 Pohled nahoru, samodualita zdvižených kódů

Cíl: Pokusíme se odpovědět na obdobnou otázku, jako v předchozí části. Kdy lze zvednout samoduální kód na samoduální? Zdvihem kódu C_e nad Z_{p^e} přitom budeme rozumět kód C_f nad $\mathbb{Z}_{p^f}$, $f \in \mathbb{N}$, $f > e$, pro který platí $\Psi_e(C_f) = C_e$.

Odpovědí na úvodní otázku jsou věta 1.2.6 pro případ $p = 2$ a pro ostatní případy věta 1.2.7. Ukáže se, že v případě $p \neq 2$ lze zvednout libovolný samoduální kód typu 1^k. To však nebude platit pro $p = 2$. Můžeme například uvážit samoduální kód $00, 11$ nad $\mathbb{Z}_2$. Žádný z jeho zdvihů nad $\mathbb{Z}_4$ nebude samoduální, protože slovo 11 nelze zvednout tak, aby jeho vnitřní součin se sebou samým byl v $\mathbb{Z}_4$ nulový.

Po celou kapitolu budeme předpokládát typ kódu 1^k, proč, objasňuje diskuze za věta 1.1.7.

Nejprve se zaměřme na případ $p = 2$. Budeme potřebovat několik nových pojmů. Pro $u \in \mathbb{Z}_{p^e}$, $e \in \mathbb{N}$ definujeme Leeovu váhu jako

$$w_L(u) = \min\{u, |\mathbb{Z}_{p^e}| - u\},$$

Euklidovu váhu prvku jako

$$w_E(u) = (w_L(u))^2.$$

Pro $v \in \mathbb{Z}_{p^e}^n$, $e \in \mathbb{N}$ definujeme Euklidovu váhu vektoru

$$w_E(v) = \sum_{i=1}^{n} w_E(v_i).$$

Neformálně řečeno, Leeova váha prvku nám říká, jak daleko je prvek od nuly, Euklidova je jen jejím čtvercem. Poznamenejme, že v případě kódu nad $\mathbb{Z}_2$ jsou totéž Euklidova váha vektoru a Hammingova váha vektoru.

Gleason ve své proslulé větě (například [12], Th.2.5.1) dělí kódy nad tělesem do různých tříd. Třída Type I jsou binární kódy mající Hammingovy váhy všech slov dělitelné dvěma, ale už ne čtyřmi, třída Type II jsou binární kódy, jejichž všechna slova mají Hammingovy váhy dělitelné čtyřmi. Bývá zvykem kódům třídy Type II říkat dvojsudé. Pro modulární kódy, kdy $p = 2$, zavádíme podobnou terminologii, ovšem kódy budeme třídit dle toho, jakého mají největšího společného dělitele Euklidových vah všech slov. Obě definice nekolidují, potkávají se jen na třídě kódu nad $\mathbb{Z}_2$, ale tam je Euklidova a Hammingova váha totéž, tedy i definice dvojsudosti. Můžeme tedy modulární kódy nad $\mathbb{Z}_{2^e}$, jejichž největší společný dělitel Euklidovských vah slov je 2, nazývat Type I kódy, je-li to 4, budeme je nazývat Type II nebo také dvojsudé. Slova euklidovské váhy dělitelné čtyřmi budeme nazývat také dvojsudá.

Nejprve rozebereme případ $p = 2$.

Příklad 1. Pro představu, v tabulkách jsou uvedeny hodnoty w_L a w_E pro prvky okruhů $\mathbb{Z}_2$, $\mathbb{Z}_4$ a $\mathbb{Z}_8$.

$u \in \mathbb{Z}_2$	$w_L(u)$	$w_E(u)$	$u^2 \in \mathbb{Z}_2$
0	0	0	0
1	1	1	1

$u \in \mathbb{Z}_4$	$w_L(u)$	$w_E(u)$	$u^2 \in \mathbb{Z}_4$
0	0	0	0
1	1	1	1
2	2	4	0
3	1	1	1

$u \in \mathbb{Z}_8$	$w_L(u)$	$w_E(u)$	$u^2 \in \mathbb{Z}_8$
0	0	0	0
1	1	1	1
2	2	4	4
3	3	9	1
4	4	16	0
5	3	9	1
6	2	4	4
7	1	1	1

Abychom se vyhnuli nedorozumění, budeme horním indexem u značení váhy odkazovat na okruh, nad kterým váhu počítáme. Například váhu prvku $a \in \mathbb{Z}_{2^e}$ v okruhu $\mathbb{Z}_{2^e}$ budeme značit $w_E^e(a)$.

Následující vztah vystihuje zajímavé vztahy, jejichž platnost můžeme vypozorovat v předchozím příkladě.

Lemma 1.2.1. *Ať $a \in \mathbb{Z}_{2^e}$, $b \in \mathbb{Z}_{2^{e+1}}$, že $a = \Psi_e(b)$. Pak*

$$w_E^e(a) \equiv a^2 \equiv b^2 \pmod{2^{e+1}}. \tag{1.5}$$

Důkaz. První kongruence. Ať $a \in \mathbb{Z}_{2^e}$, že $a \leq 2^e/2$. Pak z definice Euklidovy váhy $w_E^e(a) = a^2$. Tím spíš $w_E^e(a) \equiv a^2 \pmod{2^{e+1}}$. Ať $a \in \mathbb{Z}_{2^e}$, že $a > 2^e/2$. Pak $w_E^e(a) = (2^e - a)^2 = 2^{2e} - a2^{e+1} + a^2 \equiv a^2 \pmod{2^{e+1}}$. Druhá kongruence. Ať $j \in \{0, 1\}$, že $b = a + j2^e$. Pak $b^2 = (a + j2^e)^2 \equiv a^2 \pmod{2^{e+1}}$. □

Právě dokázané lemma budeme v dalším textu hojně používat v případech, kdy nám bude stačit hodnota Euklidovy váhy $\bmod 2^{e+1}$. Lemma je velmi užitečné, těžko počítat s Euklidovými vahami přímo z definice.

V našem případě by dokonce postačilo definovat váhu pomocí vztahu 1.5, protože při práci s ní k ní budeme přistupovat vždy za pomocí tohoto vztahu.

Lemma 1.2.2. *Ať $a, a' \in \mathbb{Z}_{2^e}$ a $b, b' \in \mathbb{Z}_{2^{e+1}}$, že $a = \Psi_e(b), a' = \Psi_e(b')$. Ať 2^{e+1} dělí $w_E^e(a)$ i $w_E^e(a')$. Pak 2^{e+1} dělí i bb'.*

Důkaz. Z lemmatu 1.2.1 máme $a^2 \equiv b^2 \equiv 0 \pmod{2^{e+1}}$. Tedy $b^2 = k2^{e+1}$ pro vhodné $k \in \mathbb{N}$. Po odmocnění s využitím, že jsme v oboru celých čísel, máme $2^{\lceil \frac{e+1}{2} \rceil}$ dělí b. Analogicky $2^{\lceil \frac{e+1}{2} \rceil}$ dělí b'. Proto $2^{e+1} | bb'$. □

Euklidova váha zřejmě není lineární. Ukážeme, že v případě samoduálního kódu, $p = 2$, splňuje slabší podmínku.

Lemma 1.2.3. *Ať $a, b \in C$, kde $C \subseteq \mathbb{Z}_{2^e}^n$, $e \in \mathbb{N}$, je samoduální kód. Ať $w_E(a)$ i $w_E(b)$ jsou dělitelné 2^{e+1}. Potom i váha $w_E(a + b)$ je dělitelná 2^{e+1}.*

Důkaz. Ať $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$ splňují předpoklady věty. Z 1.2.1 máme

$$\begin{aligned} w_E(a) &\equiv \sum a_i^2 \equiv 0 \pmod{2^{e+1}}, \\ w_E(b) &\equiv \sum b_i^2 \equiv 0 \pmod{2^{e+1}}. \end{aligned}$$

Opět užijeme 1.2.1, tentokráte na jejich součet:

$$\begin{aligned} w_E(a+b) &\equiv \sum((a_i + b_i) \bmod 2^e)^2 \pmod{2^{e+1}} \\ &= \sum a_i^2 + \sum b_i^2 + 2\sum a_i b_i \pmod{2^{e+1}} \\ &= 2\sum a_i b_i \pmod{2^{e+1}}. \end{aligned}$$

Protože je kód samoduální, platí $[a, b] = 0$, což je z definice $\sum a_i b_i \equiv 0 \pmod{2^e}$. Jsme hotovi. □

Pro lepší orientaci budeme dále odkazovat dolním indexem kódu na okruh, nad kterým je definovaný. Například C_2 značí kód nad $\mathbb{Z}_{p^2}$. Protože se budeme zajímat vždy o jeden kód a jeho zdvihy, bude pak například C_1 značit $\Psi_1(C_2)$ a podobně.

Lemma 1.2.4. *Ať $e \in \mathbb{N}$ a C_e je samoduální kód nad $\mathbb{Z}_{2^e}$. Pak C_e lze zvednout na samoduální kód nad $\mathbb{Z}_{2^{e+1}}$ právě tehdy, když Euklidovské váhy všech slov kódu C_e jsou dělitelné 2^{e+1}.*

Důkaz. Zleva doprava. Ať C_{e+1} je samoduální zdvih kódu C_e, tedy $\Psi_e(C_{e+1}) = C_e$. Ať $a = (a_1, \ldots, a_n)$ je libovolné slovo C_e, ať $\bar{a} = (\bar{a_1}, \ldots, \bar{a_n}) \in C_{e+1}$ je jeho zdvih. Postupně použijeme samoduálnost kódu C_{e+1}, definici vnitřního součinu, lemma 1.2.1. Dostáváme:

$$0 \equiv [\bar{a}, \bar{a}] \equiv \sum \bar{a_i}^2 \equiv \sum a_i^2 \equiv \sum w_E^e(a_i) \equiv w_E^e(a) \pmod{2^{e+1}}.$$

Naopak. Ukážeme postup, jak vyrobit generující matici zdviženého kódu. Ať standardizovaný tvar generující matice kódu C_e je $G'_e = [I \ A_e]$. Kód C_e je dle předpokladu samoduální. Proto platí

$$A_e A_e^T + I \equiv 0 \pmod{2^e}. \tag{1.6}$$

Existuje tedy celočíselná matice J splňující $A_e A_e^T + I = 2^e J$. Poznamenejme, že (1.6) neříká nic jiného, než že vnitřní součin libovolných dvou řádků generující matice je nulový. Jinými slovy, že $C_e \subseteq C_e^\perp$.

Naším prvním cílem bude najít zvednutí matice A_e, značme ho A_{e+1}, aby splňovala

$$A_{e+1} A_{e+1}^T + I \equiv 0 \pmod{2^{e+1}}. \tag{1.7}$$

Hledejme binární matici M, aby platilo

$$(A_e + 2^e M)(A_e + 2^e M)^T + I \equiv 0 \pmod{2^{e+1}}.$$

Po roznásobení

$$A_e A_e^T + I + 2^e(MA_e^T + A_e M^T) \equiv 0 \pmod{2^{e+1}}. \tag{1.8}$$

Aby platila kongruence (1.8), stačí volit M, aby $MA_e^T + A_e M^T = J$, potom levá strana (1.8) bude $2^{e+1}J$.

Volme celočíselnou matici Q, aby splňovala

$$Q + Q^T \equiv J \pmod{2^{e+1}}.$$

Taková matice existuje, neboť J je zřejmě symetrická, to je vidět přímo z její definice, a na diagonále má 0 (mod 2). To platí díky tomu, že C_e obsahuje jen slova váhy dělitelné 2^{e+1}, tedy 2^{e+1} dělí prvky diagonály $2^e J$ a tedy 2 dělí prvky diagonály J.

Položme $M = Q(A_e^{-1})^T$. Pak dostáváme

$$\begin{aligned} 2^e(MA_e^T + A_e M^T) &= 2^e\left(Q(A_e^{-1})^T A_e^T + A_e(Q(A_e^{-1})^T)^T\right) \\ &\equiv 2^e(Q + Q^T) \pmod{2^{e+1}} \\ &\equiv 2^e J \pmod{2^{e+1}}. \end{aligned}$$

Položme tedy $A_{e+1} = (A_e + 2^e Q(A_e^{-1})^T) \bmod 2^{e+1}$ a máme splněný požadavek (1.7), proto kód C_{e+1} generovaný maticí $[I\ A_{e+1}]$ splňuje $C_{e+1} \subseteq (C_{e+1})^\perp$. Je i samoduální? Protože předpokládáme, že C je typu $1^{n/2}$, bude i jeho zdvih typu $1^{n/2}$. V přípravné kapitole jsme odvodili vzorce pro výpočet velikosti kódu i velikosti jeho duálu ze znalosti typu kódu. V našem případě vychází obě rovné $2^{(e+1)n/2}$. Tedy jsme dokázali $C_{e+1} = (C_{e+1})^\perp$. □

Příklad 2. Protože je důkaz konstrukční, vyzkoušejme si zdvihání na příkladu rozšířeného Hammingova kódu. Uvažme tedy binární kód C_1 generovaný maticí

$$G_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Po úpravě získáme

$$A_1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix},\ A_1 A_1^T = \begin{pmatrix} 3 & 2 & 2 & 2 \\ 2 & 3 & 2 & 2 \\ 2 & 2 & 3 & 2 \\ 2 & 2 & 2 & 3 \end{pmatrix}.$$

Volíme J, aby $2J = A_1 A_1^T + I$.

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

Za Q volíme celočíselnou matici splňující $Q + Q^T \equiv J \pmod 4$.

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

Spočteme A_1^{-1} a $(A_1^{-1})^T$

$$A_1^{-1} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}, \ (A_1^{-1})^T = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

Dopočteme $M = Q(A_1^{-1})^T$.

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

Matice $A_2 = (A_1 + 2M) \bmod 4$, tedy

$$A_2 = \begin{pmatrix} 3 & 2 & 3 & 3 \\ 1 & 3 & 1 & 0 \\ 3 & 1 & 2 & 1 \\ 0 & 3 & 3 & 3 \end{pmatrix}.$$

Kód C_1 jsme zdvihli na samoduální kód C_2 nad $\mathbb{Z}_4$ s generující maticí

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 3 & 2 & 3 & 3 \\ 0 & 1 & 0 & 0 & 1 & 3 & 1 & 0 \\ 0 & 0 & 1 & 0 & 3 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 3 & 3 & 3 \end{pmatrix}.$$

Generující matici jsme našli, ovšem můžeme vidět, že pokud bychom chtěli tento samoduální kód opět zvednout, nesplňují ani generující slova podmínku lemmatu. Jak upravit zdvih samoduálního kódu nad okruh $\mathbb{Z}_{2^{e+1}}$, aby měl váhy všech slov dělitelné 2^{e+2}, se dozvíme v konstrukčním důkazu následujícího lemmatu.

Lemma 1.2.5. *Ať $e \in \mathbb{N}$ a C_e je kód nad $\mathbb{Z}_{2^e}$ s Euklidovými vahami slov dělitelnými 2^{e+1}. Potom existuje samoduální zdvih C_{e+1} nad $\mathbb{Z}_{2^{e+1}}$ kódu C_e, že Euklidova váha libovolného jeho kódového slova je dělitelná 2^{e+2}.*

Důkaz. Ať C_e jako ve znění lemmatu. Z lemmatu 1.2.4 víme, že existuje zdvih kódu C_e, značme jej C_{e+1}, s generující matici ve standardizovaném tvaru $[I \ A_{e+1}]$. Pro přehlednější zápis důkazu budeme namísto A_{e+1} krátce psát A.

Budeme hledat zdvižení kódu C_e určené generující maticí $[I \ A']$ takové, aby $A'(A')^T + I$ měla na diagonále násobky 2^{e+2}. Odtud plyne, že libovolné kódové slovo má Euklidovu váhu dělitelnou 2^{e+2}. Pokud to není zřejmé, můžeme to dokázat podrobněji. Zřejmě $A'(A')^T + I$ má na diagonále násobky 2^{e+2} právě tehdy, když pro libovolný řádek $g = (g_1, \ldots, g_n)$ generující matice $[I \ A']$ je $\sum g_i^2$ dělitelná 2^{e+2}. Dle 1.2.1 je to ekvivalentní tomu, že Euklidova váha libovolného řádku generující matice je dělitelná 2^{e+2} a dle 1.2.3 má pak i každé kódové slovo váhu dělitelnou 2^{e+2}.

Nejprve ukážeme, že při volbě $A' = A - 2^e LA \bmod 2^{e+1}$ bude kód generovaný maticí $[I \ A']$ samoduální. To můžeme udělat podobně jako v lemmatu 1.2.4,

nejdříve ukážeme, že matice splňuje $A'(A')^T + I \equiv 0 \pmod{2^{e+1}}$, a dále, že velikosti kódu a kódu k němu duálního jsou shodně rovné $2^{(e+1)/2}$. Druhá podmínka je splněna díky tomu, že kód je typu $1^{n/2}$. První je také splněna, vizte rovnost (1.10).

Ať J je celočíselná matice, že $AA^T + I = 2^{e+1}J$. Rozepišme nyní

$$\begin{aligned} A'(A')^T &= (A - 2^e LA)(A^T - 2^e A^T L^T) \\ &= AA^T - 2^e AA^T L^T - 2^e LAA^T + 2^{2e} LAA^T L^T \\ &= AA^T + 2^{e+1}L - 2^{2e}L^2 - 2^{2e+1}(JL + LJ) + 2^{3e+1}LJL^T. \quad (1.9) \end{aligned}$$

Protože $e \geq 1$, platí

$$A'(A')^T \equiv AA^T \pmod{2^{e+1}}, \quad (1.10)$$

tedy kód generovaný maticí $[I\ A']$ je samoduální.

Nyní chceme volit chytře L, aby $A'(A')^T + I$ měla na diagonále násobky 2^{e+2}. Vyjádřeme s pomocí (1.9) $A'(A')^T + I$:

$$A'(A')^T + I = AA^T + I + 2^{e+1}L - 2^{2e}L^2 - 2^{2e+1}(JL + LJ) + 2^{3e+1}LJL^T.$$

Protože nás zajímají jen prvky na diagonále a navíc modulo 2^{e+2}, postačí, když budeme zkoumat jen $AA^T + I + 2^{e+1}L - 2^{2e}L^2$. Součet $JL + LJ$ má totiž na diagonále nuly modulo 2. Za to vděčíme symetričnosti L, J. Na pozici ii součinu LJ bude totiž vnitřní součin i-tého řádku L a i-tého řádku J, stejně tak i na pozici ii součinu JL. Tedy $2^{e+1}(JL + LJ)$ má 0 na diagonále modulo 2^{e+2}. Protože je $e \geq 1$, bude i $2^{3e+1}LJL^T$ kongruentní 0 modulo 2^{e+2}.

Nově tedy otázka zní, kdy má $AA^T + I + 2^{e+1}L - 2^{2e}L^2$ nulovou diagonálu modulo 2^{e+2}, ekvivalentně, kdy má

$$\frac{1}{2^{e+1}}(AA^T + I) + L - 2^{e-1}L^2$$

nulovou diagonálu modulo 2. Poznamenejme, že součet matic $AA^T + I$ lze dělit 2^{e+1} proto, že C_e má všechna slova váhy dělitelné 2^{e+1} a že druhé mocniny zdvižených souřadnic pak jsou rovny Euklidovým vahám (lemma 1.2.1).

Označme $B = 2^{-(e+1)}(AA^T + I) \bmod 2$. Hledáme L, aby $B + L - 2^{e-1}L^2$ měla na diagonále nuly modulo 2. Pro $e > 1$ se problém zjednoduší na hledání symetrické matice L, že $B + L$ má na diagonále 0 modulo 2, čehož lze jistě snadno dosáhnout. Ať tedy $e = 1$. Ať $B = (b_{ij})$. Uvažme případ, kdy počet jedniček na diagonále je sudý, tedy $\sum b_{ii} \equiv 0 \pmod 2$. Potom i počet nul je sudý, protože n je dělitelné 8 dle 2.2.1 a B je matice typu $(n/2) \times (n/2)$, tedy počet prvků na diagonále je jistě sudý. Nastavme matici L, aby měla všude jedničky. Pokud pro $i \in \{1, \ldots, n/2\}$ je $b_{ii} = 0$, přepišme i-tý řádek a i-tý sloupec nulami. Pak zřejmě na diagonále součtu $L - L^2$ na i-tém místě bude 0. Je-li $b_{ii} = 1$, bude i-tý řádek i i-tý sloupec obsahovat samé jedničky až na sudo přepsaných nul. Proto L^2 bude mít 0 na pozici ii a na ii-tém místě $L - L^2$ dostaneme jedničku modulo 2. Tedy v tomto případě umíme L nalézt.

Nyní ukážeme, že vždy nastane $\sum b_{ii} \equiv 0 \pmod 2$. Protože $n/2$ je sudé, ať $n/2 = 2m$. Připomeňme, že zkoumáme případ $e = 1$, tedy platí $AA^T \equiv -I \equiv 3I \pmod 4$. Pak $\det AA^T \equiv 3^{n/2} = 3^{2m} \equiv 1^m = 1 \pmod 4$. Proto platí

jedna z možností $\det AA^T \equiv 1 \pmod 8$, nebo $\det AA^T \equiv 5 \pmod 8$. Obecně platí, že determinant matice se rovná determinantu matice transponované. Proto $\det AA^T = (\det A)^2$. Ale 5 není čtverec modulo 8, tedy nutně

$$\det AA^T \equiv 1 \pmod 8. \tag{1.11}$$

Nyní vyjádříme $\det AA^T \pmod 8$ přímo z definice determinantu. B jsme definovali jako $B = 1/4(AA^T + I) \bmod 2$, což lze zapsat modulo 8:

$$4B + 3I \equiv AA^T \pmod 8$$

$$\begin{pmatrix} b_{11}+3 & & \\ & \ddots & \\ & & b_{2m,2m}+3 \end{pmatrix} \equiv AA^T \pmod 8.$$

Mimo diagonálu má matice buď 0 nebo 4. Proběhneme přes všechny permutace $\pi \in S_{2m}$ a podíváme se, jak vypadá pro každou z nich součin $b_{1,\pi(1)} \cdots b_{2m,\pi(2m)}$. Pokud součin obsahuje nějaký prvek mimo diagonálu, protože se jedná o permutaci, musí být alespoň dva mimo diagonálu. Potom jsou buď oba rovny 4 nebo je alespoň jeden nulový. Součin odpovídající dané permutaci je v takovém případě roven 0 mod 8. Jediný nenulový příspěvek proto bude mít součin neobsahující žádný prvek mimo diagonálu, tedy součin prvků diagonály. Upravme dále tento výsledek

$$\begin{aligned} \det AA^T &\equiv \prod_{i=1}^{2m}(4b_{ii}+3) \\ &\equiv (4b_{11}+3)(4b_{22}+3)\cdot \ldots \cdot (4b_{2m,2m}+3) \\ &\equiv 3^{2m} + 3^{2m-1}\cdot 4\sum_{i=1}^{2m} b_{ii} \\ &\equiv 1 + 12\sum_{i=1}^{2m} b_{ii} \\ &\equiv 1 + 4\sum_{i=1}^{2m} b_{ii} \pmod 8. \end{aligned} \tag{1.12}$$

Z (1.11) a (1.12) dostáváme $\sum b_{ii} \equiv 0 \pmod 2$. Důkaz dokončen. □

Poznamenejme, že v důkazu jsme použili jednu konkrétní volbu matice L takovou, aby splňovala požadované vlastností a dokázali jsme tak její existenci. Jinými jejími volbami, pokud budou splňovat požadované podmínky, lze získat různé zdvihy, pro které také platí znění lemmatu.

Příklad 3. Najděme samoduální zdvih, který lze dále zdvihat (tedy má váhy dělitelné 8), k binárnímu (Hammingovu) kódu C_1 generovanému maticí

$$G_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Při řešení příkladu 2 jsme zjistili, že kód C_1 lze zvednout na kód nad $\mathbb{Z}_4$ generovaný maticí

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 3 & 2 & 3 & 3 \\ 0 & 1 & 0 & 0 & 1 & 3 & 1 & 0 \\ 0 & 0 & 1 & 0 & 3 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 3 & 3 & 3 \end{pmatrix}.$$

Vidíme ovšem, že například kódové slovo na druhém řádku matice nemá váhu dělitelnou 8. Potřebný zdvih ale už umíme najít s využitím důkazu lemmatu 1.2.5. Nejprve potřebujeme znát $B = (1/2^{e+1})(A_2 A_2^T + I) \bmod 2$. Vychází

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

Protože má B na prvním a třetím místě diagonály 0, vezmeme matici se samými jedničkami, nahradíme první a třetí sloupec i řádek nulovým a získáme tak vyhovující matici L.

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

Za A' volíme $A_2 - 2LA_2$, tedy

$$A' = \begin{pmatrix} 3 & 2 & 3 & 3 \\ 3 & 3 & 1 & 2 \\ 3 & 1 & 2 & 1 \\ 2 & 3 & 3 & 1 \end{pmatrix}.$$

Nově jsme dostali samoduální zdvih kódu C_1 určený generující maticí

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 3 & 2 & 3 & 3 \\ 0 & 1 & 0 & 0 & 3 & 3 & 1 & 2 \\ 0 & 0 & 1 & 0 & 3 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 & 3 & 3 & 1 \end{pmatrix}.$$

Tento kód má generující slova váhy dělitelné osmi, dle lemmatu 1.2.3 jsou váhy všech slov dělitelné osmi. Tento zdvih je připraven k dalšímu zdvihnutí.

Věta 1.2.6. *Ať $e \in \mathbb{N}$ a C_e je samoduální kód nad $\mathbb{Z}_{2^e}$. Pak C_e lze zdvihnout na samoduální kód C_f nad $\mathbb{Z}_{2^f}$, $e < f \in \mathbb{N}$ právě tehdy, když Euklidovy váhy všech slov z C_e jou dělitelné 2^{e+1}. V takovém případě lze zdvih volit tak, aby Euklidovy váhy všech slov zdviženého kódu byly dělitelné 2^{f+1}. Speciálně lze takový kód zvednout na 2-adický samoduální.*

Důkaz. Plyne indukcí přímo z lemmat 1.2.4 a 1.2.5. Zdvih na p-adický získáme limitně. □

Věta 1.2.7. *Ať $p \neq 2$ a $e \in \mathbb{N}$. Samoduální kód nad $\mathbb{Z}_{p^e}$ lze zvednout na samoduální kód C_f nad $\mathbb{Z}_{p^f}$, $e < f \in \mathbb{N}$. Speciálně samoduální kód nad $\mathbb{Z}_{p^e}$ lze zvednout na samoduální nad $\mathbb{Z}_{p^\infty}$.*

Důkaz. Dokážeme zdvih kódu o jeden krok z e na $e+1$. Zbytek indukcí. Předpokládejme, že pro $e \in \mathbb{N}$ máme samoduální kód C_e určený maticí $G'_e = [I\ A_e]$. Platí tedy $A_e A_e^T + I \equiv 0 \pmod{p^e}$. Hledáme samoduální zdvih C_{e+1} nad $\mathbb{Z}_{p^{e+1}}$ určený maticí $[I\ A_{e+1}]$, kde A_{e+1} je tvaru $A_e + p^e M$ a splňuje $A_{e+1}A_{e+1}^T + I \equiv 0 \pmod{p^{e+1}}$. Potom bude platit $C_{e+1} \subseteq C_{e+1}^{\perp}$. Zdvižený kód opět podědí typ $1^{n/2}$, opět lze snadno výpočtem ověřit, že velikosti kódů C_{e+1} i $C_{e+1}^{\perp}$ jsou shodné.

Hledáme tedy A_{e+1} tvaru $A_e + p^e M$, kde M je vhodná matice prvků ze $\mathbb{Z}_p$. Značme J celočíselnou matici splňující $A_e A_e^T + I = p^e J$. Pak platí:

$$\begin{aligned} A_{e+1}A_{e+1}^T + I &\equiv A_e A_e^T + I + p^e(A_e M^T + M A_e^T) \\ &= p^e(J + A_e M^T + M A_e^T) \pmod{p^{e+1}}. \end{aligned}$$

Rádi bychom, aby $A_{e+1}A_{e+1}^T + I \equiv 0 \pmod{p^{e+1}}$, ekvivalentně tedy

$$J + A_e M^T + M A_e^T \equiv 0 \pmod{p}.$$

Snadno ověříme, že volba $M = \frac{1}{2} J A_e \bmod p$ vyhovuje této kongruenci. Stačí využít definice J a toho, že je symetrická.

$$\begin{aligned} J + A_e M^T + M A_e^T &= J + \frac{1}{2} A_e A_e^T J + \frac{1}{2} J A_e A_e^T \\ &\equiv J - \frac{1}{2} J - \frac{1}{2} J \\ &= 0 \pmod{p}. \end{aligned}$$

Volíme tedy $A_{e+1} = (I + \frac{1}{2} p^e J) A_e$. □

1.3 Existence p-adických samoduálních

Cíl: V této kapitole budeme zjišťovat, pro které délky existují samoduální p-adické kódy. Shrnutím dosažených výsledků je věta 1.3.1.

Věta 1.3.1. *Samoduální kód C nad $\mathbb{Z}_{p^\infty}$ délky n existuje, právě když*

(i) $8|n$ *pro případ* $p = 2$,

(ii) $2|n$ *pro případ* $p \equiv 1 \bmod (4)$,

(iii) $4|n$ *pro případ* $p \equiv 3 \bmod (4)$.

Případ (i).

Lemma 1.3.2. *Ať C je 2-adický samoduální kód délky n. Pak $8|n$.*

Důkaz. Ať C je samoduální kód nad $\mathbb{Z}_{2^\infty}$. Z 1.1.6 víme, že $\Psi_1(C)$ je samoduální. Zřejmě $\Psi_2(C)$ je jeho zdvih, opět samoduální, tedy dle 1.2.4 je $\Psi_1(C)$ dvojsudý. Ten musí mít délku dělitelnou 8 dle 2.2.1.

□

Lemma 1.3.3. *Ať $8|n$, $n \in \mathbb{N}$. Pak existuje samoduální 2-adický kód délky n.*

Důkaz. K dokázání existence samoduálního 2-adického délky 8 nám stačí existence samoduálního dvojsudého kódu a znalost věty 1.2.6. Zbytek plyne z toho, že k-násobným direktním součinem samoduálních kódů získáme samoduální kód délky kn. □

Dále se budeme věnovat případu (ii).

Lemma 1.3.4. *Ať $p \equiv 1 \pmod 4$, ať C je p-adický samoduální kód délky n. Pak $2|n$.*

Důkaz. Opět z 1.1.6 plyne, že C nad $\mathbb{Z}_{p^\infty}$ je samoduální implikuje $\Psi_1(C)$ samoduální. To je ovšem kód nad tělesem a je znám snadno ověřitelný fakt, že samoduální kódy nad konečnými tělesy existují jen pro sudé délky. □

Pro opačnou implikaci, tedy nalezení samoduálního p-adického kódu libovolné sudé délky nám díky větě 1.2.7 postačí najít samoduální kód odpovídající délky nad $\mathbb{Z}_p$. Pro konstrukci takového kódu využijeme následující lemma.

Lemma 1.3.5. *Ať p liché prvočíslo. Pak existuje $a \in \mathbb{Z}_p$, že $a^2 \equiv -1 \bmod p$, právě tehdy, když $p \equiv 1 \bmod 4$.*

Důkaz. Ať $p \equiv 1 \bmod 4$ a ať q je generátor $\mathbb{Z}_p^*$. Potom kongruence $x^4 - 1 = (x^2-1)(x^2+1) \equiv 0 \pmod p$ má právě tato čtyři řešení

$$1, -1, q^{\frac{p-1}{4}}, q^{3\frac{p-1}{4}}$$

Protože $1, -1$ jsou kořeny $x^2 - 1$, musí být $q^{(p-1)/4}, q^{3(p-1)/4}$ kořeny $x^2 + 1$. Stačí tedy volit a rovné jednomu z těchto dvou prvků.

Pro důkaz druhého směru ať p liché a ať $a \in \mathbb{Z}_p$, že $a^2 \equiv -1 \pmod 4$. Pak z Lagrangeovy věty

$$1 \equiv a^{p-1} \equiv (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}.$$

Aby kongruence mohly platit, nutně $(p-1)/2$ sudé, tedy $4|p-1$, tedy $p \equiv 1 \pmod 4$. □

Lemma 1.3.6. *Ať $p \equiv 1 \pmod 4$. Pak existuje samoduální p-adický kód libovolné sudé délky.*

Důkaz. Uvažme nejprve kód nad $\mathbb{Z}_p$ zadaný generující maticí $(1, a)$, kde a volíme tak, aby $a^2 \equiv -1 \bmod p$. To lze dle lemmatu 1.3.5. Dle věty 1.2.7 umíme tento kód zdvihnout na p-adický samoduální, značme jej C. Chceme-li ukázat existenci samoduálního pro n sudé, stačí vzít direktní součin $n/2$-krát kódu C, získáme samoduální p-adický délky n.

□

Důkaz případu (iii).

Lemma 1.3.7. *Ať $p \equiv 3 \pmod 4$, ať C je p-adický samoduální kód délky n. Pak $4|n$.*

Důkaz. Podobně jako v 1.3.4 stačí ukázat, že libovolný samoduální kód nad $\mathbb{Z}_p$ musí mít délku dělitelnou čtyřmi, to říká následující lemma 1.3.8. □

Lemma 1.3.8. *Ať $p \equiv 3 \pmod 4$. Samoduální kód nad $\mathbb{Z}_p$ má nutně délku dělitelnou* 4.

Důkaz. Protože se jedná zároveň o kód nad tělesem, nutně n sudé, ať $n = 2m$. Uvažme vektorový prostor $V = \mathbb{Z}_p^n$, s ortonormální bazí $v_1, \ldots, v_n$, kde v_i má na i-té pozici 1 jinak 0. Uvažme podprostor U, $U \subseteq U^\perp$, dimenze $n/2 = m$ s bazí $t_1, \ldots, t_m$, že $\forall i, j \in \{1, .2, \ldots, m\}$ je $[t_i, t_j] = 0$. Ukážeme, že existují vektory $a_1, \ldots, a_m$ prostoru V, že $t_1, a_1, t_2, a_2, \ldots, t_m, a_m$ tvoří ortogonální bázi V a dále, označíme-li B matici, která bude mít na řádcích tyto bázové vektory, bude platit

$$BB^T = \begin{pmatrix} 0 & 1 & & & & & & \\ 1 & 0 & & & & & & \\ & & 0 & 1 & & & & \\ & & 1 & 0 & & & & \\ & & & & \ddots & & & \\ & & & & & & 0 & 1 \\ & & & & & & 1 & 0 \end{pmatrix}, \tag{1.13}$$

přičemž nevypsané prvky jsou nulové. Ať U jako výše. Tvrzení dokážeme indukcí. Ať $k = m$. Označme W podprostor generovaný vektory $t_1, t_2, \ldots, t_{k-1}$. Pro každé $w \in W$ platí $[t_k, w] = 0$, tedy $t_k \in W^\perp$. Víme, že $t_k \notin W = (W^\perp)^\perp$, tedy není kolmý na všechny prvky $W^\perp$. Ať $v \in W^\perp$ je takový, že $[t_k, v] \neq 0$. Zřejmě dimenze prostoru generovaného t_k, v je 2. Označme $u = at_k + bv$, kde $a, b \in \mathbb{Z}_p, b \neq 0$. Potom $[t_k, u] = b[t_k, v]$. Protože je $[t_k, v] \neq 0$, volme b, aby $[t_k, u] = 1$. Při této volbě $[u, u] = 2a + b^2[v, v]$. Volme takové a, aby $[u, u] = 0$ (to lze, 2 je v $\mathbb{Z}_p$ invertibilní). Volme tedy $a_k = u$. Označme nyní W_k prostor generovaný t_k, a_k. W_k je kolmý na W, tedy $W \subseteq W_k^\perp$. Dimenze $W_k^\perp = n - 2$. Dosadíme-li $W_k^\perp$ namísto V a W namísto U, můžeme použít indukční předpoklad. Dostáváme tak, že lze volit bázi splňující (1.13).

V našem případě uvažujeme za V prostor $\mathbb{Z}_p^n$ a jako U samoduální kód C nad $\mathbb{Z}_p$ délky n. Umíme tedy získat bázi prostoru $\mathbb{Z}_p^n$ výše uvedených vlastností. Označme A matici přechodu od kanonické báze k bázi $t_1, a_1, t_2, a_2, \ldots, t_m, a_m$. Platí tedy $I = AB$. Dále $I = II^T = (AB)(AB)^T = ABB^TA^T$. Podívejme se na determinant levé a pravé strany. Máme $1 = \det I = (\det A)^2(\det B)^2$. Z lemmatu 1.3.5 víme, že -1 není čtverec v $\mathbb{Z}_p$ pro $p \equiv 3 \pmod 4$. Nutně $(\det A)^2 = (\det B)^2 = 1$. Dle (1.13) je determinant zároveň roven $(-1)^m$. Proto musí být m sudé a $4|n$. □

Pro důkaz druhé implikace případu (iii) budeme hledat samoduální kód délky 4 nad $\mathbb{Z}_p$. K tomu, jak později uvidíme, budeme potřebovat najít $a, b \in \mathbb{Z}_p$, že $a^2 + b^2 \equiv -1 \pmod p$. Než k jejich hledání přistoupíme, připomeňme si krátce Legendrův symbol a jeho základní vlastnosti.

Ať $a \in \mathbb{N}$ a p prvočíslo. Legendrovým symbolem nazýváme $\left(\frac{a}{p}\right)$. Ten je roven 1 v případě, že a je čtverec modulo p (existuje $b \in \mathbb{Z}_p$, že $b^2 \equiv a \pmod p$), hodnoty -1 nabývá v případě že a není čtverec (takové $b \in \mathbb{Z}_p$ neexistuje), a v případech, kdy je a, p soudělné, je roven 0. Je-li p liché prvočíslo, platí

$$\left(\frac{1}{p}\right) = 1, \quad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2},$$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Poznamenejme, že druhý vztah jsme dokázali v lemmatu 1.3.5. Dále platí

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Těleso $\mathbb{Z}_p$ obsahuje právě $\frac{p-1}{2}$ čtverců, $\frac{p-1}{2}$ prvků, jež nejsou čtverce, a nulu.

Obecně lze dokázat existenci a, b splňujících potřebnou kongruenci následovně.

Lemma 1.3.9. *Ať $p \equiv 3 \pmod 4$. Pak existuje $a, b \in \mathbb{Z}_p$, že $a^2 + b^2 \equiv -1 \pmod p$.*

Důkaz. Sporem. Ať takové a, b neexistují. Ekvivalentně lze říci, že neexistuje $A, B \in \mathbb{Z}_p$, že $A + B \equiv -1 \pmod p$ a $\left(\frac{A}{p}\right) = 1$, $\left(\frac{B}{p}\right) = 1$. Můžeme psát $B = tp - A - 1$ pro vhodné $t \in \mathbb{N}$. Potom, za využití vztahů a dosazení $p = 4k+3$, dostáváme

$$\begin{aligned}
\left(\frac{B}{p}\right) &= \left(\frac{tp - A - 1}{p}\right) \\
&= \left(\frac{-A - 1}{p}\right) \\
&= \left(\frac{-1}{p}\right)\left(\frac{A+1}{p}\right) \\
&= (-1)^{2k+1}\left(\frac{A+1}{p}\right) \\
&= -1 \cdot \left(\frac{A+1}{p}\right).
\end{aligned}$$

Tedy ekvivalentní podmínka na neexistenci vhodných a, b je, že neexistuje $A \in \mathbb{Z}_p$, že $\left(\frac{A}{p}\right) = 1$ a zároveň $\left(\frac{A+1}{p}\right) = -1$, jinými slovy, že neexistuje A, že A je čtverec a zároveň $A+1$ není čtverec. Lze si rozmyslet, že to splňuje jediné rozložení čtverců a nečtverců a sice $1, 2, \ldots, \frac{p-1}{2}$ by musely být nečtverce, $\frac{p+1}{2}, \ldots, p-1$ čtverce. Nicméně toto rozložení určitě poruší prvek 1, který je jistě čtverec, a dle 1.3.5 i prvek -1, který naopak čtverec není. Tedy vhodné rozložení neexistuje. □

Následující lemma jen upřesňuje, jak lze v některých případech volit sčítance. Pro důkaz existence však potřeba není.

Lemma 1.3.10. *Ať $p \equiv 3 \pmod 8$. Pak je možné volit $a = 1$ a existuje b, že $a^2 + b^2 \equiv -1 \pmod p$.*

Důkaz. Volíme-li $a = 1$, dostáváme

$$\begin{aligned}
1 + b^2 &\equiv -1 \pmod p \\
b^2 &\equiv -2 \pmod p.
\end{aligned}$$

Ekvivalentně se tedy můžeme ptát zda -2 ekvivalentně $p-2$ je čtverec modulo p. Za využití základních vztahů pro práci s Legendrovými symboly dostáváme

$$\begin{aligned}\left(\frac{-2}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) \\ &= (-1)^{(p-1)/2}(-1)^{(p^2-1)/8}.\end{aligned}$$

Po dosazení $p = 8k+3$ do exponentů dostaneme $\left(\frac{-2}{p}\right) = (-1)^{8k^2+10k+2} = 1$. Tedy víme, že existuje $b \in \mathbb{Z}_p$, že $1^2 + b^2 \equiv -1 \pmod{p}$. □

Lemma 1.3.11. *Ať $p \equiv 3 \bmod (4)$. Pak pro libovolné $n \in \mathbb{N}$, $4|n$, existuje samoduální p-adický kód.*

Důkaz. Budeme postupovat již známým způsobem. Ukažme existenci samoduálního kódu nad $\mathbb{Z}_p$, kde $p = 4k+3$. Ať a, b jako v lemmatu 1.3.9. Potom kód s generující maticí

$$\begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & -b & a \end{pmatrix}$$

je samoduální délky 4. Dle věty 1.2.7 lze tento kód zdvihnout na p-adický samoduální, značme ho C. Pro dokončení důkazu stačí při požadované délce n dělitelné čtyřmi vzít kód rovný direktnímu součinu $n/4$ kopií kódu C. □

Příklad 4. Uvažme například $\mathbb{Z}_{11}$. Chceme najít a, b splňující $a^2 + b^2 \equiv -1 \pmod{p}$. Nejprve spočítáme čtverce modulo 11. Z teorie čísel víme, že abychom dostali všechny čtverce, stačí umocnit $1, 2, \ldots, \frac{p-1}{2}$. V našem případě dostaneme po řadě $1, 4, 9, 5, 3$, po seřazení $1, 3, 4, 5, 9$. Vidíme na základě důkazu 1.3.9, že za a^2 takové, aby k němu existovalo b^2 čtverec, můžeme volit $1, 5, 9$, protože po nich následující číslo není čtverec. Tedy a můžeme volit $1, 10$ a tedy $a^2 = 1$, nebo za a volíme $4, 7$ a $a^2 = 5$, či a rovno $3, 8$ a a^2 bude 9. K nim bude po řadě možné volit b rovné $3, 8$, či $4, 7$, či $1, 10$.

Volme například $a = 4, b = 4$, dostáváme samoduální kód délky 4 nad $\mathbb{Z}_{11}$ s generující maticí

$$\begin{pmatrix} 1 & 0 & 4 & 4 \\ 0 & 1 & 7 & 4 \end{pmatrix}.$$

Alternativně bychom mohli důkazy lemmat 1.3.6 a 1.3.11 vést i následujícím způsobem. Namísto zdvihání celého kódu, budeme zvedat a případně a,b tak, aby podmínka na samoduálnost byla zachována i pro zvednutý kód. K důkazu prvního z jmenovaných by stačilo aplikovat Henselovo lemma, které pro $f(x)$ polynom nad $\mathbb{Z}_p$, že $f(a_1) \equiv 0 \bmod p$ a $f'(a_1) \not\equiv 0 \bmod p$, zaručuje existenci $a_e \in \mathbb{Z}_{p^e}$, že $a_e \equiv a_1 \bmod p$ a $f(a_e) \equiv 0 \bmod p^e$ pro $e > 1$. Limitně tedy můžeme najít $a_\infty \in \mathbb{Z}_{p^\infty}$, že $a_\infty \equiv a_1 \bmod p$ a $f(a_\infty) = 0$ v $\mathbb{Z}_{p^\infty}$. Za $f(x)$ volíme $x^2 + 1$, jeho derivace je po dosazení jakéhokoliv nenulového prvku nenulová, můžeme užít Henselovo lemma. Dostaneme $a_e \in \mathbb{Z}_{p^e}$, $e \in \mathbb{N} \cup \{\infty\}$, a kód generovaný maticí $(1, a_e)$ nad $\mathbb{Z}_{p^e}$ bude samoduální. V případě $p \equiv 3 \pmod 4$ ovšem potřebujeme zvednout prvky a i b zároveň. To Henselovo lemma neumožňuje. Nicméně postačí zvednout b na b a a dopočíst tak, aby vyhovovalo požadované kongruenci $x^2 + (b^2 + 1) \equiv 0 \pmod{p}$.

2. Teorie invariantů

Cíl: Cílem této kapitoly je obstojně vybudovat teorii invariantů v rozsahu potřebném pro studium invariantních polynomů. Motivací nám může být podkapitola 2.2, kde za pomoci teorie invariantů dokážeme, že samoduální dvojsudý kód musí mít délku dělitelnou 8.

Teorie invariantů obecně se zabývá studiem neměnného, invariantního. Ve spojení s kódy nás budou zajímat váhové výčty kódů. Váhovým výčtem kódu C délky n nazveme polynom

$$W_C(x,y) = \sum_{c\ \in C} x^{n-w(c)} y^{w(c)}.$$

Obvykle ho budeme zapisovat pomocí koeficientů A_i takto

$$W_C(x,y) = \sum_{i=0}^{n-1} A_i x^{n-i} y^i,$$

kde A_i je počet slov kódu s Hammingovou vahou rovnou i. Někdy se definuje rovněž jako polynom jedné proměnné ve tvaru

$$W_C(z) = \sum_{i=0}^{n} A_i z^i.$$

Definice v jedné a ve dvou proměnných jsou zřejmě ekvivalentní. Stačí dosadit $x = 1$ a $y = z$, naopak stačí, když za z dosadíme (y/x) a polynom přenásobíme x^n.

Poznamenejme, že tento váhový výčet se v literatuře nazývá Hammingův. Nese určitou informaci o vnitřním složení kódu. Informuje o tom, z jakých slov se skládá - kolik je slov určité váhy pro tu kterou Hammingovu váhu. Ačkoliv se zdá tato informace nepříliš cennou, ukážeme si, že silně omezí možnosti, jak mohou vypadat výčty samoduálních kódů.

Pro úplnost ještě dodejme, že se definují i jiné váhové výčty nesoucí silnější informaci. Například kompletní váhový výčet. Navolím-li si n prvků okruhu, nad kterým kód uvažuji, kompletní váhový výčet mi řekne počet kódových slov, která z nich mohu seskládat. Těmito se ovšem nebudeme zabývat. Pro bližší seznámení lze doporučit [14].

Příklad 5. Uvažme opět Hammingův kód s generující maticí G_1, vizte příklad 3. Vypíšeme-li si všech jeho šestnáct slov, snadno určíme, že jeho váhový výčet je

$$W_{h_8}(x,y) = x^8 + 14x^4y^4 + y^8. \tag{2.1}$$

Dalším zástupcem dvojsudého binárního kódu je rozšířený Golayův kód délky 24. Jeho váhový výčet, vizte příloha, je roven

$$W_{g_{24}}(x,y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}. \tag{2.2}$$

2.1 MacWilliamsové identita

Cíl: Jessie MacWilliams ve své disertační práci dokázala vztah, který dává do souvislosti váhový výčet kódu s výčtem jeho duálu. Přesněji, na základě znalosti výčtu kódu jsme schopni přímo určit váhový výčet jeho duálu. Tvrzení se dočkalo řady zobecnění, nás bude zajímat jeho podoba pro modulární kódy, kterou si v této sekci dokážeme.

Ať C je modulární kód nad $\mathbb{Z}_m$. Pak platí

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x + (m-1)y, x - y).$$

MacWilliamsové důkaz se opírá o výsledky teorie charakterů grupy, lze ho nalézt v [10]. Zobecnění pro modulární kódy poprvé publikoval ve své práci Klemm [9]. Názornější důkaz, kdy je vidět, proč identita platí, publikoval Honold [8]. Důkaz vedl jen pro kódy nad konečnými tělesy, my ho zobecníme pro kódy nad $\mathbb{Z}_{p^e}$. Přesto nejdříve projdeme důkaz pro tělesa, je snadnější a přehlednější. Poté si ukážeme odlišnosti pro kódy nad okruhy a pustíme se do obecnějšího důkazu.

Věta 2.1.1. *Ať $\mathbb{F}_q$ těleso, ať C je kód nad tělesem $\mathbb{F}_q$ délky n a dimenze k. Pak platí*

$$W_{C^\perp}(z) = \frac{1}{q^k} \left(1 + (q-1)z\right)^n W_C\left(\frac{1-z}{1+(q-1)z}\right).$$

Důkaz. Uvažme pro podmnožinu $S \subseteq \mathbb{F}_q^l$, $l \in \mathbb{N}$ polynom

$$B_S(z) = (1 + (q-1)z)^l W_S\left(\frac{1-z}{1+(q-1)z}\right),$$

kde $W_S = \sum_{i=0}^{n} A_i z^i$, A_i je počet prvků množiny S s Hammingovou vahou i. Chceme tedy dokázat, že $W_{C^\perp}(z) = B_C(z)/q^k$.

Bez újmy na obecnosti budeme předpokládat, že C je nerozložitelný, to jest, že nelze zapsat ve tvaru $C = C_1 \oplus C_2 = \{(c_1, c_2) \mid c_1 \in C_1 \wedge c_2 \in C_2\}$, kde C_1, C_2 jsou vhodné kódy. Pokud ano, platí rovněž $C^\perp = C_1^\perp \oplus C_2^\perp$, $W_C(z) = W_{C_1}(z) W_{C_2}(z)$ a $W_{C^\perp}(z) = W_{C_1^\perp}(z) W_{C_2^\perp}(z)$. Tedy stačí zkoumat nerozložitelné kódy.

Důkaz provedeme indukcí podle délky kódu. Snadno ukážeme platnost pro $n = 1$. Pro $n > 1$ provedeme projekci kódu C na prvních $n-1$ souřadnic. Dostaneme kód délky $n-1$, proto můžeme použít indukční předpoklad. Podobně postupujeme pro podkód C s nulovou poslední souřadnicí $C^0 = \{c = (c_1, c_2, \ldots, c_n) \in C \mid c_n = 0\}$. Budeme tak znát váhové výčty jejich duálních kódů. Pak už půjde jen o to, dohledat ke každému slovu z těchto duálních kódů vzor a podívat se, zda mělo poslední souřadnici nulovou nebo ne a to zohlednit při určování podoby váhového výčtu $C^\perp$.

Kódy délky 1 nad $\mathbb{F}_q$ jsou $\{0\}$ nebo celé $\mathbb{F}_q$. Platnost tvrzení lze snadno přímo ověřit. Předpokládejme $n > 1$. Ať C^0 jako výše, dále označme množinu slov s nenulovou poslední souřadnicí $C^\times = C \setminus C^0$. Uvažme projekci kódu

$$\begin{aligned} \pi &: C \longrightarrow \mathbb{F}_q^{n-1} \\ \pi &: (c_1, c_2, \ldots, c_{n-1}, c_n) \longrightarrow (c_1, c_2, \ldots, c_{n-1}). \end{aligned}$$

Lze si rozmyslet, že díky nerozložitelnosti a předpokladu $n > 1$ existuje k libovolnému prvku $\mathbb{F}_q^{n-1}$ nejvýše jeden vzor při zobrazení π a π je tedy prosté (připomeňme, že definiční obor π je C). Díky tomu platí následující rovnost:

$$\begin{aligned} W_{\pi(C)}(z) &= W_{\pi(C^0)}(z) + W_{\pi(C^\times)}(z) \\ &= W_{\pi(C^0)}(z) + \frac{W_{C^\times}(z)}{z}, \end{aligned}$$

přičemž jsme využili i toho, že $W_S(z) = W_{S_1}(z) + W_{S_2}(z)$ pro S_1, S_2 disjunktní podmnožiny S, že $S_1 \cup S_2 = S$. Za těchto podmínek i $B_S(z) = B_{S_1}(z) + B_{S_2}(z)$. Předchozí rozpis výčtu $W_{\pi(C)}(z)$ rovnou využijeme:

$$\begin{aligned} B_{\pi(C)}(z) &= (1+(q-1)z)^{n-1} W_{\pi(C)}\left(\frac{1-z}{1+(q-1)z}\right) \\ &= B_{\pi(C^0)}(z) + \frac{(1+(q-1)z)^n}{1-z} W_{C^\times}\left(\frac{1-z}{1+(q-1)z}\right) \\ &= B_{\pi(C^0)}(z) + \frac{B_{C^\times}(z)}{1-z}. \end{aligned} \tag{2.3}$$

Dále, protože je C nerozložitelný, existuje slovo s nenulovou poslední souřadnicí a protože je kód lineární nad tělesem, existuje slovo s 1 na n-té pozici. Označme nějaké takové $a = (a_1, a_2, \ldots, a_{n-1}, 1)$. Potom jistě $C = C^0 \oplus \{k \cdot a \mid k \in \mathbb{F}_q\}$.

Definujme

$$\begin{aligned} P &= \{(b', 0) \mid b' \in \pi(C)^\perp\} \\ Q &= \{(b', b_n) \mid b' \in \pi(C^0)^\perp \setminus \pi(C)^\perp,\ b_n \equiv -\sum_{i=1}^{n-1} a_i b_i \pmod q\}. \end{aligned}$$

Poznamenejme jen, že $(b', 0) \in P$ právě tehdy, když b' je kolmé na $\pi(C)$, to je právě tehdy, když $(b', 0)$ je kolmé na C (protože např. $a \in C$ má poslední souřadnici 1). Podobně, máme-li slovo $b \in Q$, tak $\pi(b)$ je kolmé na $\pi(C^0)$, tedy nutně b je kolmé na C^0. Dopočtením n-té, nenulové souřadnice jsme pak zajistili kolmost na celé C, neboť $C = C^0 \oplus \{k \cdot a \mid k \in \mathbb{F}_q\}$. Protože π je prosté, Q obsahuje právě slova kolmá na C s nenulovou poslední souřadnicí, proto skutečně platí $C^\perp = P \cup Q$.

Výčet duálního kódu pak je:

$$\begin{aligned} W_{C^\perp}(z) &= W_P(z) + W_Q(z) \\ &= W_{\pi(C)^\perp}(z) + z\left(W_{\pi(C^0)^\perp}(z) - W_{\pi(C)^\perp}(z)\right) \\ &= (1-z) W_{\pi(C)^\perp}(z) + z W_{\pi(C^0)^\perp}(z). \end{aligned}$$

Protože $\pi(C)$ i $\pi(C^0)$ jsou kódy délky $n-1$ a dimenze k respektive $k-1$, můžeme

užít indukční předpoklad. Zároveň využijeme rovnosti (2.3).

$$\begin{aligned} W_{C^\perp}(z) &= (1-z)W_{\pi(C)^\perp}(z) + zW_{\pi(C^0)^\perp}(z) \\ &= \frac{1-z}{q^k}B_{\pi(C)}(z) + \frac{z}{q^{k-1}}B_{\pi(C^0)}(z) \\ &= \frac{1}{q^k}\Big((1+(q-1)z)B_{\pi(C^0)}(z) + B_{C^\times}(z)\Big) \\ &= \frac{1}{q^k}\left(B_{C^0}(z) + B_{C^\times}(z)\right) \\ &= \frac{1}{q^k}B_C(z). \end{aligned}$$

□

Důkaz verze MacWilliamsové identity pro kódy nad okruhy $\mathbb{Z}_{p^e}$ založíme na stejné myšlence. V následujících příkladech se zaměříme na odlišnosti pro kódy nad okruhy $\mathbb{Z}_{p^e}$.

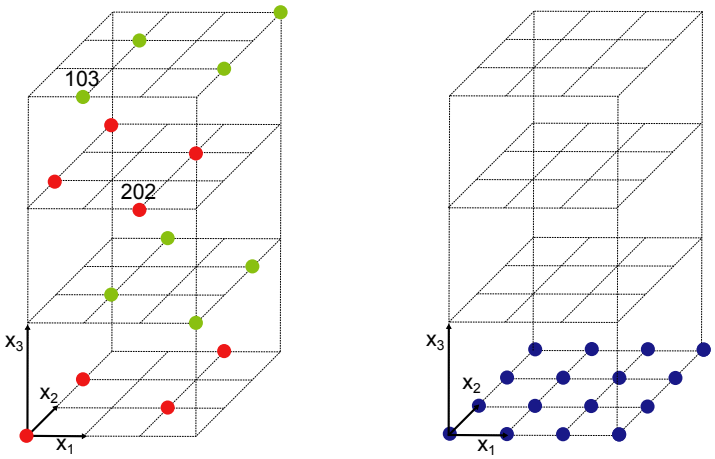
Příklad 6. V prvním příkladu se zamyslíme nad volbou $a \in C$ takového, aby $C^0 \oplus a\mathbb{Z}_{p^e} = C$. Připomeňme, že C^0 značí kódová slova s nulovou poslední souřadnicí. Uvažme kód nad $\mathbb{Z}_4$ generovaný maticí

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

Vidíme, že nejvyšší mocnina 2 dělící první řádek je 2^0, stejně tak i u druhého řádku, kód je tedy typu $(1)^2$. Matice ve standardizovaném tvaru:

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

Na obrázku 2.1 máme znázorněný prostor $\mathbb{Z}_3^3$, ve kterém jsou barevně vyznačena



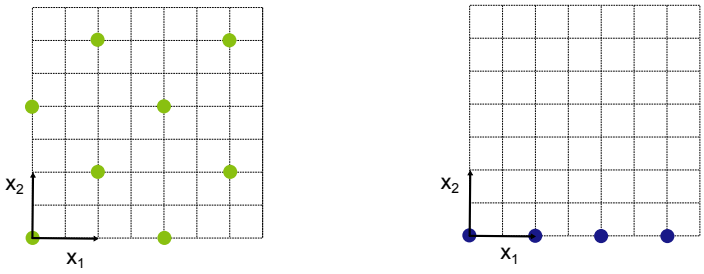
Obrázek 2.1: Zobrazení kódu generovaného maticí G a jeho projekce

slova kódu generovaného maticí G. Slovu (c_1, c_2, c_3) odpovídá bod (c_1, c_2, c_3).

Vidíme, že narozdíl od kódů nad tělesy nemůžeme a volit libovolně. Pokud bychom zvolili například $a = 202$, dostali bychom jen slova vyobrazená červeně. Jak tedy vybrat vhodné a? Zřejmě potřebujeme najít nejmenší vzdálenost mezi patry, ve kterých se vyskytují kódová slova. Hledáme tedy kódové slovo s nejnižší možnou p-valuací poslední souřadnice mezi všemi kódovými slovy. Nebo-li nejvyšší mocninu p, značme ji p^ν, že poslední souřadnice libovolného kódového slova je jí dělitelná. V našem případě je snadno vidět, že je to 2^0, tedy hledáme slovo, které má poslední souřadnici dělitelnou 2^0, ale již ne 2^1. Volme například $a = 103$.

Z obrázku dále vidíme, že π je prosté. To ale nemusí platit obecně. Uvažme například kód typu $(2)^1(4)^1$ nad $\mathbb{Z}_8$ s generující maticí (je již ve standardizovaném tvaru):

$$H = \begin{pmatrix} 2 & 2 \\ 0 & 4 \end{pmatrix}.$$



Obrázek 2.2: Zobrazení kódu generovaného maticí H a jeho projekce

Vidíme, že v tomto případu projekce prostá není. Pro potřeby důkazu se nám bude hodit znalost vztahu mezi $|C|$ a $|\pi(C)|$. Je-li kód typu $(1)^{k_0}(p^1)^{k_1}\cdots(p^{e-1})^{k_{e-1}}$, potom je jeho velikost $|C| = (p^e)^{k_0}(p^{e-1})^{k_1}(p^{e-2})^{k_2}\ldots(p^1)^{k_{e-1}}$. Odtud je vidět, že rovnost $|\pi(C)| = |C|$ nebude zachována právě tehdy, pokud kódy C a $\pi(C)$ budou různého typu. Proto projekce kódu generovaného G je prostá a kód generovaný H nikoliv. V prvním případě se totiž typ kódu projekcí nezměnil, ve druhém ano.

Nyní můžeme přistoupit k samotnému důkazu. Připomeňme pro jistotu, že v první kapitole jsme se v souvislosti se zdviháním a ořezáváním samoduálních kódů zabývali jen kódy typu 1^k. Nyní se zaměřujeme na kódy nad konkrétním okruhem, navíc ne nutně samoduální. Uvažujeme tedy obecný typ kódu.

Věta 2.1.2. *Ať C je modulární kód nad okruhem $\mathbb{Z}_{p^e}$ délky n s váhovým výčtem W_C. Potom při definici váhového výčtu v jedné proměnné platí*

$$W_{C^\perp}(z) = \frac{1}{|C|}\left(1 + (p^e - 1)z\right)^n W_C\left(\frac{1-z}{1+(p^e-1)z}\right).$$

Nebo, chceme-li zápis téhož při definici váhového výčtu ve dvou proměnných, můžeme ekvivalentně psát

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + (p^e - 1)y, x - y).$$

Důkaz. Důkaz provedeme stejně jako v předchozí větě indukcí dle délky kódu. Pro $S \subseteq \mathbb{Z}_{p^e}^l$, $l \in \mathbb{N}$ definujme

$$B_S(z) = (1 + (p^e - 1)z)^l W_S\left(\frac{1-z}{1+(p^e-1)z}\right),$$

kde W_S je váhový výčet množiny S. Chceme ukázat $W_{C^\perp}(z) = B_C(z)/|C|$.

$n = 1$. Podmnožina $C \subseteq \mathbb{Z}_{p^e}$ je kód právě tehdy, když je podgrupou $\mathbb{Z}_{p^e}$. V takovém případě existuje $m \in \mathbb{N}$, že $C \simeq \mathbb{Z}_{p^m}$. Jeho váhový výčet je roven $W_C(z) = 1 + (p^m - 1)z$. Duální kód $C^\perp$ k C je potom izomorfní $\mathbb{Z}_{p^{e-m}}$ a jeho váhový výčet zřejmě bude $W_{C^\perp}(z) = 1 + (p^{e-m} - 1)z$. Po krátké úpravě

$$\begin{aligned} B_C(z) &= (1 + (p^e - 1)z)\left(1 + (p^m - 1)\frac{1-z}{1+(p^m-1)z}\right) \\ &= p^m\left(1 + (p^{e-m} - 1)z\right). \end{aligned}$$

Protože $|C| = |\mathbb{Z}_{p^m}| = p^m$, zřejmě pro $n = 1$ tvrzení platí.

Dále ať $n > 1$. Označme $C^0 = \{c = (c_1, \ldots, c_n) \in C \mid c_n = 0\}$. Jak volit $a \in C$, aby $C = C^0 \oplus a\mathbb{Z}_{p^e}$? Připomeňme, že p-valuace v_p nenulového prvku je největší mocnina p, jež ho dělí, a $v_p(0) = \infty$. Označme $\nu \in \mathbb{N} \cup \{0\}$ nejmenší možnou p-valuaci poslední souřadnice mezi všemi kódovými slovy. Při takovéto volbě a je jedna inkluze splněna triviálně, pro druhou vezměme libovolné slovo $c = (c_1, \ldots, c_n) \in C$. Ať $c_n = p^{v_p(c_n)}c_n^*$, $a_n = p^\nu a_n^*$. Protože $\nu \leq v_p(c_n)$ a p nedělí c_n^* ani a_n^*, existuje $k \in \mathbb{N}$, že $k \cdot a_n = c_n$. Pak $(c_1, \ldots, c_n) - k(a_1, \ldots, a_n) \in C^0$. Druhá inkluze dokázána, tedy rovnost.

Definujme π, projekci kódu C:

$$\begin{aligned} \pi &: C \longrightarrow \pi(C) \subseteq \mathbb{Z}_{p^e}^{n-1} \\ \pi &: (c_1, c_2, \ldots, c_{n-1}, c_n) \longrightarrow (c_1, c_2, \ldots, c_{n-1}). \end{aligned}$$

π nemusí být prosté.

V dalším budeme používat $b' = (b_1, \ldots, b_{n-1})$. Definujme

$$\begin{aligned} P &= \{(b', 0) \mid b' \in \pi(C)^\perp\}, \\ Q_1 &= \{(b', b_n) \mid b' \in \pi(C^0)^\perp \setminus \pi(C)^\perp,\ b_n \in \mathbb{Z}_{p^e}, \text{že } [a, b] = 0\}, \\ Q_2 &= \{(b', b_n) \mid b' \in \pi(C)^\perp, b_n \in \mathbb{Z}_{p^e} \setminus \{0\}, \text{že } a_n b_n \equiv 0 \ (\mod p^e)\}. \end{aligned}$$

Chceme ukázat, že $C^\perp = P \cup Q$, kde $Q = Q_1 \cup Q_2$. Platí:

$$\begin{aligned} &\left(b = (b', b_n) = (b_1, \ldots, b_n) \in C^\perp\right) \Leftrightarrow \left(b \in (C^0)^\perp \wedge [b, a] = 0\right) \Leftrightarrow \\ &\Leftrightarrow \left(b' \in \pi(C^0)^\perp \ \wedge \ [b, a] = 0\right). \end{aligned} \tag{2.4}$$

První podmínku konjunkce splňují veškerá slova z P i Q. Pokud $b_n = 0$, je druhá podmínka splněna právě tehdy, když $[b', \pi(a)] = 0$, tedy konjunkce (2.4) je ekvivalentní podmínce $b' \in \pi(C)^\perp$ a tedy i ekvivalentní podmínce náležení množině P. Podobně je-li $b_n \neq 0$, je (b', b_n) slovo $C^\perp$ právě tehdy, když $[a, b] = 0$, a právě tyto případy Q pokrývá.

Nyní se zaměříme na váhové výčty P a Q. Pro P je to jednoduché: $W_P = W_{\pi(C)^\perp}$. U Q musíme nejdříve zjistit, kolik k nějakému b' můžeme dopočíst různých b_n. Pokud a přenásobíme $p^{e-\nu}$ dostaneme slovo s nulovou poslední souřadnicí, tedy $p^{e-\nu} \cdot a \in C^0$. Proto $\forall d \in \pi(C^0)^\perp$ platí

$$0 \ \equiv \ p^{e-\nu}[d, \pi(a)] \pmod{p^e}.$$

Odtud vidíme, že p^ν dělí $[d, \pi(a)]$ v $\mathbb{Z}_{p^e}$. Ačkoliv jsme nad okruhem, můžeme tedy vnitřní součin těchto prvků dělit. Fixujme $b_n = [b', \pi(a)]/p^\nu$. Pak $(b', b_n) \in C^\perp$. My chceme ale najít všechna řešení. Víme, že $b' \in (C^0)^\perp$, proto $\sum_{i=1}^{n-1} b_i a_i \equiv 0 \pmod{p^e}$, zároveň $\sum_{i=1}^{n} b_i a_i \equiv 0 \pmod{p^e}$, proto

$$\begin{aligned} a_n b_n = p^\nu a_n^* b_n &\equiv 0 \pmod{p^e} \\ a_n^* b_n &\equiv 0 \pmod{p^{e-\nu}}. \end{aligned}$$

Všechna x, aby $a_n^* x \equiv 0 \pmod{p^{e-\nu}}$ jsou tedy tato:

$$x = a_n^* b_n + t p^{e-\nu}, t \in \{1, 2, \ldots, p^\nu\}.$$

Podívejme se nejprve na Q_1. Každé slovo $b' \in \pi(C^0)^\perp \setminus \pi(C)^\perp$ má při zobrazení π celkem p^ν různých (nenulových) vzorů, proto

$$W_{Q_1}(z) = p^\nu z \left(W_{\pi(C^0)^\perp}(z) - W_{\pi(C)^\perp}(z) \right).$$

Podobně pro Q_2, $b' \in \pi(C)^\perp$ má $p^\nu - 1$ různých (nenulových) vzorů, proto

$$W_{Q_2}(z) = (p^\nu - 1) z W_{\pi(C)^\perp}(z).$$

Dostáváme:

$$\begin{aligned} W_{C^\perp}(z) &= (1 + (p^\nu - 1)z)\, W_{\pi(C)^\perp}(z) + z p^\nu \left(W_{\pi(C^0)^\perp}(z) - W_{\pi(C)^\perp}(z) \right) \\ &= (1 - z) W_{\pi(C)^\perp}(z) + z p^\nu W_{\pi(C^0)^\perp}(z). \end{aligned} \tag{2.5}$$

Dále π nemusí být prosté. Ať kód C je typu $(1)^{k_0}(p^1)^{k_1} \cdots (p^e)^{k_e}$ víme, že $|C| = (p^e)^{k_0}(p^{e-1})^{k_1}(p^{e-2})^{k_2} \ldots (p^1)^{k_{e-1}}$. Odtud je vidět, že rovnost $|\pi(C)| = |C|$ nebude zachována právě tehdy, pokud kódy C a $\pi(C)$ budou různého typu. Což nastane právě tehdy, když poslední řádek generující matice C ve standardizovaném tvaru bude dělitelný p^j pro nějaké $j < e$, $j \in \mathbb{N}$ (zřejmě j musí být nejvyšší nenulový index exponentu vyskytující se v typu kódu). V tomto případě $|C| = p^{e-j}|\pi(C)|$. Pokud je ovšem π prosté (definiční obor je C), je nejvyšší nenulový index exponentu vyskytující se v typu kódu k_e. Tedy opět platí $|C| = p^{e-j}|\pi(C)|$, protože $j = e$. Tedy obecně můžeme říct, že pro projekci π platí $|C| = p^{e-j}|\pi(C)|$, kde j voleno jako výše a jádro homomorfismu π je $|\mathrm{Ker}(\pi)| = p^{e-j}$. Dále víme, že $C = C^0 \oplus a$, kde $a_n = p^\nu a_n^*$. Proto $|C| = p^{e-\nu}|\pi(C^0)|$.

Ať $C^\times$ jsou slova kódu C s nenulovou poslední souřadnicí. Ať $c \in C^\times$. Homomorfismus π pošle $|\mathrm{Ker}(\pi)|$ slov z množiny $C^\times$ na $\pi(c)$, krom těch, kdy $\exists c^0 \in C^0$, že $\pi(c) = \pi(c^0)$. Potom jich bude o jedno méně, protože c^0 neleží v $C^\times$ ale v C^0. Tedy

$$W_{\pi(C^\times)}(z) = \frac{1}{|\mathrm{Ker}(\pi)|} \left(W_{C^0}(z) + \frac{W_{C^\times}(z)}{z} \right).$$

Odtud je navíc vidět, že $W_{\pi(C^\times)}(z) = W_{\pi(C)}(z)$, speciálně $|\pi(C^\times)| = |\pi(C)|$. Toto využijeme společně s rovností $W_{\pi(C^0)}(z) = W_{C^0}(z)$ v následujícím.

$$\begin{aligned} B_{\pi(C)}(z) &= (1 + (p^e - 1)z)^{n-1}\, W_{\pi(C)} \left(\frac{1 - z}{1 + (p^e - 1)z} \right) \\ &= \frac{(1 + (p^e - 1)z)^{n-1}}{|\mathrm{Ker}(\pi)|} \left(W_{C^0} \left(\frac{1 - z}{1 + (p^e - 1)z} \right) + \frac{W_{C^\times} \left(\frac{1-z}{1+(p^e-1)z} \right)}{\frac{1-z}{1+(p^e-1)z}} \right) \\ &= \frac{1}{|\mathrm{Ker}(\pi)|} \left(B_{\pi(C^0)}(z) + \frac{B_{C^\times}(z)}{1 - z} \right). \end{aligned} \tag{2.6}$$

Nyní už máme vše připraveno. Vezměme (2.5), na $W_{\pi(C)^\perp}(z)$ i na $W_{\pi(C^0)^\perp}(z)$ můžeme použít indukční předpoklad, protože se jedná o kódy délky $n-1$, poté rozepíšeme $B_{\pi(C)}(z)$ dle (2.6):

$$\begin{aligned} W_{C^\perp}(z) &= (1-z)W_{\pi(C)^\perp}(z) + zp^\nu W_{\pi(C^0)^\perp}(z), \\ &= (1-z)\frac{1}{|\pi(C)|}B_{\pi(C)}(z) + zp^\nu \frac{1}{|\pi(C^0)}B_{\pi(C^0)}(z) \\ &= \frac{1-z}{|\pi(C)|}\frac{1}{|\mathrm{Ker}(\pi)|}\left(B_{\pi(C^0)}(z) + \frac{B_{C^\times}(z)}{1-z}\right) + zp^\nu \frac{1}{|\pi(C^0)|}B_{\pi(C^0)}(z), \end{aligned}$$

využijeme vztahů $|C| = p^{e-\nu}|\pi(C^0)|$ a $|C| = p^{e-j}|\pi(C)| = |\mathrm{Ker}(\pi)||\pi(C)|$:

$$\begin{aligned} &= \frac{1}{|C|}\Big((1-z)B_{\pi(C^0)}(z) + B_{C^\times}(z) + p^e z B_{\pi(C^0)}(z)\Big) \\ &= \frac{1}{|C|}\Big((1+(p^e-1)z)B_{\pi(C^0)}(z) + B_{C^\times}(z)\Big) \\ &= \frac{1}{|C|}\Big(B_{C^0}(z) + B_{C^\times}(z)\Big) \\ &= \frac{1}{|C|}B_C(z). \end{aligned}$$

Důkaz hotov. □

2.2 Úvod do teorie invariantů

Cíl: Zadefinujeme okruh invariantů a blíže se stímto pojmem seznámíme na příkladu. Zároveň v něm uplatníme tvrzení, která v příští kapitole dokážeme. V rámci příkladu dokážeme, že samoduální dvojsudý kód má nutně délku dělitelnou 8.

Poznamenejme, že při studiu polynomů invariantních vůči působení nějaké konečné grupy se stačí zabývat podgrupami obecné lineární grupy. Každou grupu lze totiž zapsat jako podgrupu nějaké obecné lineární grupy. Uvažme okruh polynomů nad komplexními čísly v n nezávislých proměnných $\mathbb{C}[x_1, \ldots, x_n]$, dále ho budeme značit $\mathbb{C}[x]$. Značme $\mathrm{GL}(\mathbb{C}^n)$ obecnou lineární grupu $\mathbb{C}^n$, tedy grupu invertibilních matic $n \times n$ nad $\mathbb{C}$ neboli grupu automorfismů $\mathbb{C}^n$. Řekneme, že polynom $f \in \mathbb{C}[x]$ je invariant, případně invariantní vůči grupě transformací $G \subset \mathrm{GL}(\mathbb{C}^n)$, pokud pro každý prvek $A \in G$ platí $f(A(x)) = f(x)$. Snadno lze ověřit, že množina invariantů tvoří okruh. Okruh invariantů grupy G budeme značit $\mathbb{C}[x]^G$. Pro konečnou $G \subset \mathrm{GL}(\mathbb{C}^n)$ definujme Reynoldův operátor grupy G:

$$\begin{aligned} {}^*\colon \mathbb{C}[x] &\to \mathbb{C}[x]^G \\ f(x) &\mapsto \frac{1}{|G|}\sum_{A\in G} f(A(x)). \end{aligned} \tag{2.7}$$

Nebudeme značit, ke které grupě operátor přísluší, vždy to bude zřejmé z kontextu. Jedná se o jakési průměrování přes grupu. Lze snadno nahlédnout, že f^* je vždy invariantní vůči G a to z toho důvodu, že G je tvořena jen invertibilními prvky, proto pro libovolnou matici $B \in G$ platí

$$\frac{1}{|G|}\sum_{A\in G} f(AB(x)) = \frac{1}{|G|}\sum_{A\in G} f(A(x)).$$

To ospravedlňuje zadefinování Reynoldova operátoru jako zobrazení do okruhu invariantů. Také je zřejmě na. Poznamenejme, že obecně jakákoliv symetrická funkce přes grupu je vůči ní invariantní. Lze si rozmyslet, že Reynoldův operátor se také chová lineárně, platí $(f+g)^* = f^* + g^*$, $(cf)^* = cf^*$.

Uvažme polynom

$$f(x) = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} f_{(k_1,\ldots,k_n)} x_1^{k_1}\cdots x_n^{k_n} \in \mathbb{C}[x].$$

Nosičem polynomu je množina $\mathrm{Supp}(f) = \{(k_1,\ldots,k_n) \mid f_{(k_1,\ldots,k_n)} \neq (0,\ldots,0)\}$. Definujme váhu polynomu jako $\max\{\sum_{i=1}^n ik_i \mid (k_1,\ldots,k_n) \in \mathrm{Supp}(f)\}$. Definujme stupeň polynomu $\deg(f) = \max\{\sum_{i=1}^n k_i \mid (k_1,\ldots,k_n) \in \mathrm{Supp}(f(x))\}$. Pokud $f = 0$, definujeme $\deg(f) = -1$.

Dále o polynomu $f \in \mathbb{C}[x]$ řekneme, že je homogenní stupně $d, d \in \mathbb{N}_0$, pokud stupeň všech jeho monočlenů je shodně roven d. Příkladem homogenního polynomu stupně n může být váhový výčet (ve dvou proměnných) libovolného kódu délky n. Označme $\mathbb{C}[x]_d$ množinu homogenních polynomů stupně d. Zřejmě se jedná o grupu vzhledem ke sčítání. Dále platí $\mathbb{C}[x] = \mathbb{C}[x]_0 \oplus \mathbb{C}[x]_1 \oplus \mathbb{C}[x]_2 \oplus \cdots = \bigoplus_{i\geq 0} \mathbb{C}[x]_i$, přičemž $\mathbb{C}[x]_i \cdot \mathbb{C}[x]_j \subseteq \mathbb{C}[x]_{i+j}$.

Řekneme, že polynomy $f_1,\ldots,f_t \in \mathbb{C}[x]$ jsou algebraicky nezávislé nad $\mathbb{C}$, pokud neexistuje polynom $g(y) \in \mathbb{C}[y_1,\ldots,y_t]$, že $g(f_1,\ldots,f_t) = 0$ v $\mathbb{C}[x]$.

Příklad 7. MacWilliamsové identita klade podmínku na tvar váhového výčtu samoduálního kódu. Uvidíme, že toto omezení je překvapivě silné. V příkladu se zaměříme na binární samoduální dvojsudé kódy. Ukážeme, že za pomoci teorie, kterou vzápětí dokážeme, lze poměrně snadno odvodit možné stupně váhových výčtů. Dále určíme generátory okruhu invariantů.

Podívejme se, jak mohou váhové výčty binárního dvojsudého samoduálního kódu C vypadat. Protože je samoduální, platí $W_C(x,y) = W_{C^\perp}(x,y)$ a bude mít $2^{n/2}$ slov. Z 2.1.2 dostáváme, že

$$W_C(x,y) = \frac{1}{2^{n/2}} W_C(x+y, x-y). \tag{2.8}$$

Protože všechny váhy slov jsou dělitelné čtyřmi, bude $W_C(x,y)$ obsahovat jen mocniny y^4. To lze vystihnout požadavkem na výčet:

$$W_C(x,y) = W_C(x,iy). \tag{2.9}$$

Podmínky (2.8), (2.9) můžeme vyjádřit pomocí transformací T_1, T_2:

$$\begin{aligned} T_1 &: \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ T_2 &: \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}. \end{aligned}$$

Vůči těmto transformacím musí být váhový výčet dvojsudého samoduálu invariantní. Bude tedy invariantní i vůči jejich složení, tedy vůči $T_1T_2, T_1^2, \ldots$ a podobně. Jinými slovy je invariantní vůči podgrupě $\mathrm{GL}(\mathbb{C}^n)$ generované maticemi

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

Značme dále tuto grupu G_1. Grupa G_1 je konečná a má 192 prvků, vizte příloha. Zaměřme se na to, jak vypadá $\mathbb{C}[x]^{G_1}$.

Kolik je lineárně nezávislých homogenních invariantů stupně d? Označme jejich počet a_d. Ukážeme si, že k určení těchto počtů nám stačí znát prvky grupy G_1. Označíme-li mocninnou řadu $\Phi_{G_1}(\lambda) = a_0 + a_1\lambda + a_2\lambda^2 + \ldots$, ukážeme si (věta 2.3.6), že tato je rovna

$$\Phi_{G_1}(\lambda) = \frac{1}{|G_1|} \sum_{A \in G_1} \frac{1}{\det(I - \lambda A)}.$$

V našem případě dostaneme projitím G_1 a dosazení všech matic $I, T_1, T_2, \ldots$:

$$\Phi_{G_1}(\lambda) = \frac{1}{192} \left(\frac{1}{(1-\lambda)^2} + \frac{1}{1-\lambda^2} + \frac{1}{(1-\lambda)(1-i\lambda)} + \ldots \right).$$

Pokud bychom součet upravili, vizte příloha, dostaneme

$$\Phi_{G_1}(\lambda) = \frac{1}{(1-\lambda^8)(1-\lambda^{24})}.$$

Nyní si stačí uvědomit, že

$$\begin{aligned} 1 &= (1-\lambda^8)(1+\lambda^8+\lambda^{24}+\lambda^{32}+\ldots), \\ 1 &= (1-\lambda^{24})(1+\lambda^{24}+\lambda^{48}+\lambda^{72}+\ldots), \end{aligned}$$

tedy

$$\Phi_{G_1}(\lambda) = (1+\lambda^8+\lambda^{24}+\lambda^{32}+\ldots)(1+\lambda^{24}+\lambda^{48}+\lambda^{72}+\ldots).$$

Vidíme, že stupeň libovolného homogenního polynomu invariantního vůči působení G_1 je dělitelný 8. Tedy i stupeň váhového výčtu libovolného samoduálního kódu musí být dělitelný 8. Tedy samoduální dvojsudý kód musí mít délku dělitelnou 8.

V našem případě dokonce můžeme určit generující invarianty. Stačí se podívat na příklad 5. Oba kódy jsou dvojsudé, jeden je stupně 8, druhý 24. Pokud by byly jejich výčty algebraicky závislé, musel by existovat nenulový polynom

$$\sum_{(i,j)=(0,0)}^{(m,l)} a_{i,j} x^i y^j$$

nad $\mathbb{C}$ ve dvou proměnných, že

$$\sum_{(i,j)=(0,0)}^{(m,l)} a_{i,j} (W_{h_8})^i (W_{g_{24}})^j = 0.$$

Pro spor, ať takový existuje. Vezměme nejvyšší v něm vyskytující se mocninu x, ať je to x^{8r+24s}. Snadno nahlédneme, že koeficient tohoto členu bude roven přímo $a_{r,s}$, tedy $a_{r,s} = 0$. Spor. Výčty jsou tedy algebraicky nezávislé a proto je můžeme prohlásit za generátory $\mathbb{C}[x]^{G_1}$ dle lemmatu 2.3.7.

Shrňme si postup, jak určit okruh invariantů, v našem případě okruh polynomů, splňujících omezení daná třídou kódů a tedy okruh potenciálních váhových výčtů. Nejdříve, pokud to jde, vyjádříme vlastnosti, které kódy dané třídy musejí splňovat, pomocí transformací. U samoduálních kódů je to typicky transformace daná MacWilliamsové identitou. Poté se snažíme popsat okruh invariantů grupy generované těmito transformacemi. Typicky hledáme množinu invariantů generujících celý okruh, ale jak si ukážeme na závěr kapitoly, lze dokonce považovat jednoznačné vyjádření prvků okruhu invariantů.

Lemma 2.2.1. *Ať C je dvojsudý samoduální kód délky n nad $\mathbb{Z}_2$. Pak $8|n$.*

Důkaz. Vizte vypracování příkladu 7. □

2.3 Noetherové mez, Molienova posloupnost

Cíl: Tuto sekci můžeme rozdělit na dvě části. V první části budeme směřovat k důkazu lemmatu, které nám řekne, kterak najít generátory okruhu invariantů. Dále určíme horní hranici na jejich počet a také omezíme shora jejich stupeň. Tento odhad je však v některých případech velmi velkorysý. Proto ve druhé části zavedeme pojem Molienovy posloupnosti a dokážeme vztah, který nám umožní v některých případech zjistit, zda množina invariantů již generuje celý okruh.

K důkazu lemmatu 2.3.4 zabývajícího se omezeními na generátory budeme potřebovat jisté znalosti o symetrických polynomech, přesněji tvrzení, že každý symetrický polynom lze zapsat jen za pomoci mocninných sum omezeného stupně (lemma 2.3.2). Pokud je tento fakt čtenáři znám, může přejít rovnou k lemmatu 2.3.3.

Připomeňme, že rozumíme $x = (x_1, \ldots, x_n)$. Ať S_n značí symetrickou grupu permutací na n prvcích. Polynom $f \in \mathbb{C}[x]$ nazýváme symetrický, pokud je invariantní vůči působení grupy S_n, tedy pokud $f(\pi(x)) = f(x)\ \forall \pi \in S_n$. Množinu symetrických polynomů značme $\mathbb{C}[x]^{S_n}$. Dále ať z je proměnná nezávislá na $x_1, \ldots, x_n$. Položme

$$(z - x_1)(z - x_2) \cdot \cdots \cdot (z - x_n) = z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - \ldots (-1)^n \sigma_n.$$

Platí (Vietovy vztahy)

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + \cdots + x_n \\
\sigma_2 &= x_1x_2 + x_1x_3 + \ldots + x_2x_3 + \ldots + x_{n-1}x_n \\
\sigma_3 &= x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n \\
&\cdots \\
\sigma_n &= x_1x_2 \ldots x_n.
\end{aligned}$$

σ_i nazýváme i-tým elementárním symetrickým polynomem, $i = 1, \ldots, n$.

Lemma 2.3.1. *Ať $f(x) \in \mathbb{C}[x]^{S_n}$ je symetrický polynom v n proměnných stupně k. Potom existuje polynom $\varphi(x) \in \mathbb{C}[x]$ váhy k, že $f(x) = \varphi(\sigma_1(x), \ldots, \sigma_n(x))$.*

Důkaz. Důkaz provedeme indukcí podle počtu proměnných. Nejprve $n = 1$, ať $f(x_1) \in \mathbb{C}[x_1]$ symetrický polynom stupně k. Zřejmě $\sigma_1 = x_1$, proto $\varphi(\sigma_1) = \varphi(x_1) = f(x_1)$. Váha φ je rovna stupni f, tedy k.

Ať $n > 1$, předpokládejme, že tvrzení platí pro počet proměnných menších n. Opět použijeme indukci, tentokrát dle stupně d polynomu. Pro $d = 0$ netřeba rozvádět. Ať $d > 0$, předpokládejme tedy, že pro stupně menší d tvrzení platí. Ať $f(x) \in \mathbb{C}[x]$ je symetrický polynom stupně d. Pro $i = 1, \ldots, n-1$ je i-tý elementární polynom v $n-1$ proměnných roven $\sigma_i(x_1, \ldots, x_{n-1}, 0)$, kde σ_i je i-tý elementární polynom v n proměnných. Do f dosadíme $x_n = 0$ a jako na polynom v $n-1$ proměnných na něj můžeme použít indukční předpoklad. Dostáváme:

$$f(x_1, \ldots, x_{n-1}, 0) = \varphi(\sigma_1(x_1, \ldots, x_{n-1}, 0), \ldots, \sigma_{n-1}(x_1, \ldots, x_{n-1}, 0)).$$

Dle indukčního předpokladu zřejmě váha φ (před dosazením elementárních symetrických polynomů) bude menší rovna d, neboť po dosazení $x_n = 0$ se stupeň f může jen zmenšit. Označme

$$f'(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) - \varphi(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_{n-1}(x_1, \ldots, x_n)).$$

Snadno si lze rozmyslet, že dosazením elementárních symetrických polynomů za proměnné polynomu získáme symetrický polynom. Tedy

$$\varphi(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_{n-1}(x_1, \ldots, x_n))$$

jako polynom v $x_1, \ldots, x_n$ je symetrický. Protože symetrické polynomy tvoří okruh, je f' symetrický. Polynom φ před dosazením má váhu menší rovnou d. Připomeňme, že to znamená $\sum_{i=1}^{n-1} ik_i \leq d$ pro všechny monočleny $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ polynomu φ. Tedy po dosazení elementárních symetrických polynomů (kdy i-tý je stupně i), bude φ stupně menšího nebo rovného d. A protože f je stupně d, bude $\deg(f') \leq d$. Dále si uvědomme, že $f'(x_1, \ldots, x_{n-1}, 0) = 0$. Tedy x_n se vyskytuje ve všech členech f' a protože f' je symetrický, vyskytují se ve všech členech i $x_1, \ldots, x_{n-1}$. Proto můžeme vytknout celé σ_n, dostaneme $f'(x) = \sigma_n(x)g(x)$, kde g je nutně symetrický (jinak by f' nemohl být symetrický), $\deg(g) \leq d - n$. Můžeme na něj proto užít indukční předpoklad, dostaneme $g = \gamma(\sigma_1, \ldots, \sigma_n)$, kde $\gamma \in \mathbb{C}[x]$ s váhou menší rovnou $d - n$. Nyní

$$f = f' + \varphi(\sigma_1, \ldots, \sigma_{n-1}) = \sigma_n \gamma(\sigma_1, \ldots, \sigma_n) + \varphi(\sigma_1, \ldots, \sigma_{n-1}).$$

Na pravé straně jsme dostali hledaný polynom τ:

$$\tau(x_1, \ldots, x_n) = x_n \gamma(x_1, \ldots, x_n) + \varphi(x_1, \ldots, x_{n-1}).$$

Zbývá zkontrolovat váhu τ. Výše jsme odůvodnili, že stupeň $\varphi(\sigma_1, \ldots, \sigma_{n-1}) \leq d$, váha $\gamma(\sigma_1, \ldots, \sigma_n)$ menší rovna $d - n$, stupeň σ_n je n. Proto váha τ bude menší rovna d. Ale menší než d být nemůže, protože stupeň f je d a váha polynomu je vždy větší rovna jeho stupni. □

Lemma 2.3.2. *Ať $f(x) \in \mathbb{C}[x]^{S_n}$ je symetrický polynom. Pak existuje $\varphi(x) \in \mathbb{C}[x]$, že $f = \varphi(\rho_1, \ldots, \rho_n)$, kde ρ_k značí k-tou mocninnou sumu $x_1^k + \cdots + x_n^k$, $k = 0, 1, \ldots, n$.*

Důkaz. Pro potřeby důkazu zavedeme uspořádání $\prec$ monočlenů $x_1^{k_1} \cdots x_n^{k_n}$, shodného stupně $d = \sum k_i$. K tomu budeme potřebovat seřadit (přeskládat) dle velikosti koeficienty k_i. Označme $\lambda(k_1, \ldots, k_n)$ n-tici $(r_1, \ldots, r_n)$ takovou, že $r_1 \geq$

$r_2 \geq \ldots \geq r_n$ a že zároveň existuje permutace $\pi \in S_n$, že $\pi(k_1, \ldots, k_n) = (r_1, \ldots, r_n)$. Ať $\lambda(k_1, \ldots, k_n) = (r_1, \ldots, r_n)$, $\lambda(l_1, \ldots, l_n) = (s_1, \ldots, s_n)$. Pak definujeme $x_1^{k_1} \cdots x_n^{k_n} \prec x_1^{l_1} \cdots x_n^{l_n}$, pokud

$$\begin{cases} (r_1, \ldots, r_n) \neq (s_1, \ldots, s_n) \text{ a pro nejmenší i, že } r_i \neq s_i \text{ platí } r_i > s_i, \\ (r_1, \ldots, r_n) = (s_1, \ldots, s_n) \text{ a pro nejmenší i, že } k_i \neq l_i \text{ platí } k_i < l_i \end{cases}$$

Jedná se o úplné uspořádání. Můžeme tedy provést důkaz indukcí. Dle lemmatu 2.3.1 stačí předpokládat, že $f(x)$ je elementární symetrický polynom n proměnných. Tedy $\deg(f) = d \leq n$. Ať $f(x) = \sum_e f_e x_1^{e_1} \cdots x_n^{e_n}$, kde $e = (e_1, \ldots, e_n)$ běží přes $\mathrm{Supp}(f)$. Nechť $f_{(k_1,\ldots,k_n)} x_1^{k_1} \cdots x_n^{k_n} = \max \{f_e x_1^{e_1} \cdots x_n^{e_n} \mid e = (e_1, \ldots, e_n) \in \mathrm{Supp}(f)\}$ je maximální monočlen vzhledem k uspořádání $\prec$. To, že je $f(x)$ symetrický nám zaručuje $n \geq k_1 \geq k_2 \geq \cdots \geq k_n$. Jinak bychom permutovali dvojici souřadnic, která nám nerovnosti porušuje a protože je polynom symetrický, musí mít i po prohození souřadnic tentýž maximální člen, došli bychom ke sporu. Označme $g(x) = \rho_{k_1}(x) \cdots \rho_{k_n}(x)$, kde ρ_i je i-tá mocninná suma. Po rozmyšlení si, jak porovnává $\prec$ dojdeme k tomu, že maximální monočlen polynomu $g(x) = \sum_e g_e x_1^{e_1} \cdots x_n^{e_n}$ je právě $g_{(k_1,\ldots,k_n)} x_1^{k_1} \cdots x_n^{k_n}$. Položíme-li nyní

$$f'(x) = f(x) - \frac{f_{(k_1,\ldots,k_n)}}{g_{(k_1,\ldots,k_n)}} g(x),$$

dostaneme opět symetrický polynom ovšem s nižším maximálním monočlenem a zároveň stejným stupněm. □

Příklad 8. Uveďme příklad na porovnání pomocí $\prec$. Ať počet proměnných $n = 3$, stupeň monomů $d = 4$.

monočlen	k_1, k_2, k_3, k_4	$\lambda(k_1, k_2, k_3, k_4)$
x_1^4	4000	4000
x_4^4	0004	4000
$x_1^2 x_2^2$	2200	2200
$x_1 x_2 x_3^2$	1120	2110
$x_1 x_2 x_4$	1101	1110
$x_2 x_3 x_4$	0111	1110

Po porovnání:

$$x_4^4 \prec x_1^4 \prec x_1^2 x_2^2 \prec x_1 x_2 x_3^2 \prec x_2 x_3 x_4 \prec x_1 x_2 x_4.$$

Příklad 9. Ať $n = 2, d = 2$. Pomocí konstrukčního důkazu 2.3.2 zapišme polynom $x_1 x_2$ jako polynom v mocninných sumách $\rho_1(x_1, x_2) = x_1 + x_2$ a $\rho_2(x_1, x_2) = x_1^2 + x_2^2$. Polynom $x_1 x_2$ má jediný monočlen, tedy je maximální vzhledem k $\prec$, $k_1 = k_2 = 1$. Počítejme

krok	
1	$f = x_1x_2$ $g = \rho_{k_1}\rho_{k_2} = \rho_1\rho_1 = x_1^2 + 2x_1x_2 + x_2^2$ $f' = f - \frac{1}{2}g = -\frac{1}{2}(x_1^2 + x_2^2)$
2	porovnání: $x_2^2 \prec x_1^2$ $f = -\frac{1}{2}(x_1^2 + x_2^2)$ $g = \rho_2 = x_1^2 + x_2^2$ $f' = -\frac{1}{2}(x_1^2 + x_2^2) + \frac{1}{2}(x_1^2 + x_2^2) = 0$

Z průběhu výpočtu vidíme, že se nám podařilo polynom vyjádřit pomocí mocninných sum v tomto tvaru $x_1x_2 = 1/2(\rho_1^2 - \rho_2)$.

Pro $e = (e_1, \ldots, e_n) \in \mathbb{N}^n$ značme J_e invariant

$$J_e(x) = (x_1^{e_1} \cdots x_n^{e_n})^*,$$

kde * značí Reynoldův operátor grupy $G \subset \mathrm{GL}(\mathbb{C}^n)$. Pro $A \in G$, budeme $A(x_i)$ zkráceně značit $A((0, ..., 0, x_i, 0, ..., 0))$.

Lemma 2.3.3. *Ať $f(x) \in \mathbb{C}[x]^G$. Ať $f = \sum_e f_e x_1^{e_1} \cdots x_n^{e_n}$, kde $e = (e_1, \ldots, e_n)$ běží přes* Supp(f). *Invariant $f(x)$ lze zapsat pomocí invariantů $J_e(x)$ jako*

$$f(x) = \frac{1}{|G|} \sum_e f_e J_e(x),$$

kde $e = (e_1, \ldots, e_n)$ běží přes Supp(f).

Důkaz. Ať G je tvořena transformacemi $A_1, \ldots, A_{|G|}$. Protože je $f(x)$ invariant, je speciálně invariantní vůči *, tedy $f(x_1, \ldots, x_n) =$

$$\begin{aligned}
&= \frac{1}{|G|}\left(f(A_1(x_1), \ldots, A_1(x_n)) + \cdots + f(A_{|G|}(x_1), \ldots, A_{|G|}(x_n))\right) \\
&= \frac{1}{|G|}\sum_e f_e \left((A_1(x_1))^{e_1} \cdots (A_1(x_n))^{e_n} + \cdots + (A_{|G|}(x_1))^{e_1} \cdots (A_{|G|}(x_n))^{e_n}\right) \\
&= \frac{1}{|G|}\sum_e f_e J_e(x).
\end{aligned}$$

□

Nyní už můžeme přistoupit k důkazu Noetherové horní meze. Ukážeme, že pokud vezmeme všechny monomy, kdy každý bude mít celkový stupeň menší jak $|G|$, a zobrazíme je Reynoldovým operátorem, dostaneme generátory okruhu invariantních polynomů.

Věta 2.3.4 (Noetherové horní mez)**.** *Ať $\mathbb{C}[x]^G$ je okruh invariantů konečné grupy $G \subset \mathrm{GL}(\mathbb{C}^n)$. Potom $\mathbb{C}[x]^G$ je generovaný nejvýše $\binom{n+|G|}{n}$ invarianty, jejichž stupeň je shora omezený $|G|$. Jedna z možných množin generátorů je $\{J_e(x) \mid |e| \leq |G|\}$, kde $|e| = \sum_{i=1}^n e_i$.*

Důkaz. Lemma 2.3.3 nám říká, jak vyjádřit libovolný invariant pomocí invariantů $J_e(x)$, $e \in \mathrm{Supp}(f)$. Hodilo by se nám tedy ukázat, že libovolné $J_e(x)$ umíme vyjádřit pomocí těch z nich, kdy $|e| \leq |G|$. Pak bude platit $\mathbb{C}[x]^G = \mathbb{C}[\{J_e(x) \mid |e| \leq |G|\}]$.

Pro $e = (e_1, \ldots, e_n) \in \mathbb{N}^n$ označme $|e| = \sum_{i=1}^n e_i$. Uvažme takový invariant $J_t(x)$, kde $t = (t_1, \ldots, t_n)$ takové, že $|t| > |G|$.

Zaveďme nové proměnné $u_1, \ldots, u_n$ (nezávislé na $x_1, \ldots, x_n$). Definujme pro $k \in \mathbb{N}$

$$S_k = ((u_1 x_1 + \cdots + u_n x_n)^k)^*.$$

Pokud bychom umocnili vnitřní závorku na k a prohlédli si členy obdrženého polynomu, budou se zřejmě proměnné u_i a x_i vyskytovat v jednotlivých členech ve stejné mocnině. Pokud se na S_k budeme dívat jako na polynom v proměnných u_i (ty mimochodem nechá Reynoldův operátor nepozměněné), můžeme říct, že pro $e = (e_1, \ldots, e_n)$, $|e| = k$ bude mít $u_1^{e_1} \cdots u_n^{e_n}$ koeficient rovný $J_e(x)$ až na násobek kladným číslem.

Rozepišme dále $S_k =$

$$\frac{1}{|G|}\left((u_1 A_1(x_1) + \cdots + u_n A_1(x_n))^k + \ldots + (u_1 A_{|G|}(x_1) + \cdots + u_n A_{|G|}(x_n))^k\right).$$

Podívejme se nyní na S_k jako na polynom v $|G|$ proměnných

$$u_1 A_1(x_1) + \cdots + u_n A_1(x_n), \ldots, u_1 A_{|G|}(x_1) + \cdots + u_n A_{|G|}(x_n).$$

Vidíme, že S_k je k-tá mocninná suma těchto nových proměnných a můžeme použít větu 2.3.2 - existuje polynom φ nad $\mathbb{C}$ v $|G|$ proměnných, že

$$S_k = \varphi(S_1, \ldots, S_{|G|}). \tag{2.10}$$

Vezmeme-li množinu $J = \{J_e(x) \mid |e| \leq |G|\}$, najdeme v ní až na celočíselný násobek koeficienty všech S_e, $|e| \leq |G|$. Nyní toho využijeme a společně s vyjádřením (2.10) dostáváme, že koeficienty S_k jako polynomu v proměnných u_i můžeme vyjádřit jako polynomy s koeficienty z $\mathbb{C}$ a namísto proměnných bereme prvky J.

Máme-li tedy S_k, kde $k = |t|$, bude koeficient členu $u_1^{t_1} \cdots u_n^{t_n}$ až na násobek rovný $J_t(x)$. Výše jsme si ukázali, že S_k umím vyjádřit jako polynom nad $\mathbb{C}[J]$, tedy mimo jiné, že $J_t(x)$ je generován invarianty z J.

Pro dokončení důkazu už jen zbývá zjistit počet prvků v J. Podmínku $|e| \leq |G|$ splňuje $\sum_{i=0}^{|G|} \binom{n+i-1}{i} = \binom{n+|G|}{|G|}$ n-tic, které určují $\binom{n+|G|}{|G|}$ invariantů, jejichž stupeň je nejvýše $|G|$. □

Příklad 10. Uvažme grupu generovanou maticemi

$$A_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Polynom $f \in \mathbb{C}[x, y]$ je invariantní polynom vzhledem ke G_2 generované maticemi A_1, A_2 právě tehdy, je-li invariantní vůči A_1, A_2. Tedy $f \in \mathbb{C}[x, y]_2^G$ právě tehdy, je-li $f(x, y) = f(-x, y) = f(x, -y)$. Lze si rozmyslet, že tyto dvě podmínky budou splněny právě tehdy, když se v polynomu budou vyskytovat jen sudé exponenty

u mocnin x i y. Jinak by se měnila znaménka u jednotlivých monomů. Proto $\mathbb{C}[x,y]_2^G = \mathbb{C}[x^2,y^2]$, jinými slovy, x^2 a y^2 jsou hledané generátory $\mathbb{C}[x,y]_2^G$.

Nyní se pokusme najít generátory pomocí postupu z důkazu věty 2.3.4. G_2 je čtyřprvková grupa, obsahuje $I, -I, A_1, A_2$. Proto Reynoldův operátor grupy G_2 přiřadí polynomu f polynom

$$f^*(x,y) = 1/4(f(x,y) + f(-x,-y) + f(-x,y) + f(x,-y)).$$

Uvážíme všechny monomy v proměnných x, y s celkovým stupněm nepřevyšující 4. Působením Reynoldova operátoru se monomy x,y,xy,x^3,y^3,x^2y,xy^2,x^3y,xy^3 zobrazí na nulu. Monomy x^2,y^2,x^4,y^4,x^2y^2 působení Reynoldova operátoru nezmění. Platí tedy $\mathbb{C}[x,y]_2^G = \mathbb{C}[x^2,y^2,x^4,y^4,x^2y^2]$. Vidíme však, že také k nagenerování x^4,y^4,x^2y^2 postačí x^2, y^2. Proto $\mathbb{C}[x,y]_2^G = \mathbb{C}[x^2,y^2]$.

Na příkladu 10 jsme si mohli povšimnout, že věta 2.3.4 nám sice nabízí jednoduchý postup, jak najít generátory okruhu invariantů, nicméně poskytnutý odhad je velkorysý. Stačí si rozmyslet, jaký je horní odhad na počet invariantů generujících $\mathbb{C}[x]^{G_1}$ z příkladu 7. Na druhou stranu nutno podotknout, že existují grupy, pro které se odhad nabývá, tedy ho vylepšit nelze. Blíže vizte [15].

Z praktického pohledu by se nám obzvláště v případě větších grup hodilo rozpoznat, kdy nalezené invarianty již generují celý okruh, případně vybrat jen potřebné generátory, ve smyslu minimální množiny či, řekněme, báze. To je ostatně hlavní motivací pro zavedení Molienovy posloupnosti. Pomocí ní najdeme odpověď na otázku, kolik je lineárně nezávislých homogenních invariantů grupy pro daný stupeň.

Podobně jako $\mathbb{C}[x]$ můžeme i $\mathbb{C}[x]^G$ zapsat jako direktní sumu homogenních polynomů $\mathbb{C}[x]^G = \mathbb{C} \oplus \mathbb{C}[x]_1^G \oplus \mathbb{C}[x]_2^G \oplus \cdots = \bigoplus_{i\geq 0} \mathbb{C}[x]_i^G$, kde $\mathbb{C}[x]_i^G$ jsou homogenní invarianty grupy G stupně d.

Označme a_d počet lineárně nezávislých homogenních invariantů stupně d. Tyto invarianty tvoří bázi prostoru $\mathbb{C}[x]_d^G$. Jejich počet tedy odpovídá dimenzi $\mathbb{C}[x]_d^G$ jako vektorového prostoru nad $\mathbb{C}$.

Molienovou posloupností budeme rozumět zápis těchto dimenzí ve formě mocninné řady v následujícím tvaru

$$\Phi_G(\lambda) = a_0 + a_1\lambda + a_2\lambda^2 \ldots .$$

Ukážeme, že Molienova posloupnost je rovna průměru přes grupu inverzních hodnot charakteristických polynomů transformací, věta 2.3.6.

Nejprve pomocné lemma.

Lemma 2.3.5. *Ať $G \subset \mathrm{GL}(\mathbb{C}^n)$ konečná. Pak počet homogenních invariantů stupně 1 je roven*

$$a_1 = \frac{1}{|G|}\sum_{A\in G} \mathrm{Tr}(A).$$

Důkaz. Okruh homogenních polynomů stupně 1 v n proměnných, tedy polynomy $a_1x_1 + a_2x_2 + \ldots + a_nx_n$, $a_i \in \mathbb{C}$, můžeme ztotožnit s vektorovým prostorem $V = \mathbb{C}^n$. Zajímá nás dimenze podprostoru

$$V^G = \{v \in V \mid \forall A \in G : \ Av = v\}.$$

Označme

$$S = \frac{1}{|G|} \sum_{A \in G} A.$$

S jako zobrazení $S: V \to V^G$, $v \to S(v)$ je na, protože zřejmě každý invariant je invariantní i vůči S. Dále $S^2 = S$, protože aplikujeme-li S na polynom, dostaneme invariant a ten je invariantní vůči dalšímu působení S. S je tedy projekce, proto vlastní čísla S mohou být 0 případně 1. $\mathrm{Tr}(S)$ tak bude rovna násobnosti výskytu 1 ve vlastních číslech S, což odpovídá dimenzi vektorového prostoru V^G nad $\mathbb{C}$. Dostáváme $a_1 = \dim_{\mathbb{C}} V^G = \mathrm{Tr}(S) = \frac{1}{|G|} \sum \mathrm{Tr}(A)$. □

Věta 2.3.6 (Molienova)**.** *Ať $G \subset \mathrm{GL}(\mathbb{C}^n)$ konečná. Pak*

$$\Phi_G(\lambda) = \frac{1}{|G|} \sum_{A \in G} \frac{1}{\det(I - \lambda A)}.$$

Důkaz. Podobně jako v důkazu 2.3.5 můžeme ztotožnit $\mathbb{C}[x]_d$, okruh homogenních polynomů stupně d, s vektorovým prostorem $\mathbb{C}^m$, kde $m = \binom{n+d-1}{d}$, neboť právě tolik máme lineárně nezávislých homogenních monomů stupně d.

Uvažme ke každé lineární transformaci $A \in G$ transformaci $A^{[d]}$ vektorového prostoru $\mathbb{C}^m$, která je jednoznačně určena A. Narozdíl od A, která působí na $x_1, \ldots, x_n$, bude $A^{[d]}$ popisovat, jak se tato transformace projeví na monočlenech stupně d. Označme grupu $G^{[d]} = \{A^{[d]} \mid A \in G\}$.

Nyní a_d je rovno počtu lineárně nezávislých invariantů stupně 1 grupy $G^{[d]}$. Z předchozího lemmatu

$$a_d = \frac{1}{|G|} \sum_{A \in G} \mathrm{Tr}(A^{[d]}). \tag{2.11}$$

Jak vypadá stopa $A^{[d]}$? Označme $\alpha_1, \ldots, \alpha_n$ vlastní čísla matice A. Vlastní čísla $A^{[d]}$ pak jsou $\alpha_1^{d_1} \cdots \alpha_n^{d_n}$, kde $d = d_1 + \cdots + d_n$. Protože změna báze prostoru nezmění stopu matice, volme takovou bázi, aby tato vlastní čísla byla na diagonále $A^{[d]}$. Máme

$$\mathrm{Tr}(A^{[d]}) = \sum \alpha_1^{d_1} \cdots \alpha_n^{d_n}, \tag{2.12}$$

kde suma běží přes $(d_1, \ldots, d_n) \in \mathbb{N}^n$, že $d = \sum_{i=1}^n d_i$. Dále si povšimněme $(1 - \lambda\alpha) \cdot (1 + \lambda\alpha + (\lambda\alpha)^2 + \ldots) = 1$, tedy

$$\frac{1}{1 - \lambda\alpha} = \sum_{i=0}^{\infty} (\lambda\alpha)^i. \tag{2.13}$$

Dokončíme důkaz, vyjdeme z definice Molienovy posloupnosti, užijeme (2.11), (2.12), (2.13) a upravíme.

$$\begin{aligned}
\Phi_G(\lambda) &= \sum_{d=0}^{\infty} \dim{}_{\mathbb{C}}(\mathbb{C}[x]_d^G)\lambda^d \\
&= \sum_{d=0}^{\infty} \frac{1}{|G|} \sum_{A\in G} \mathrm{Tr}(A^{[d]})\lambda^d \\
&= \frac{1}{|G|} \sum_{A\in G} \sum_{d=0}^{\infty} \sum_{(d_1,\dots,d_n):d=\sum d_i} (\alpha_1^{d_1}\cdots\alpha_n^{d_n})\lambda^d \\
&= \frac{1}{|G|} \sum_{A\in G} \sum_{(d_1,\dots,d_n)} (\alpha_1^{d_1}\cdots\alpha_n^{d_n})\lambda^{d_1+\cdots+d_n} \\
&= \frac{1}{|G|} \sum_{A\in G} \prod_{i=1}^{n} \sum_{k=0}^{\infty} (\lambda\alpha_i)^k \\
&= \frac{1}{|G|} \sum_{A\in G} \prod_{i=1}^{n} \frac{1}{1-\alpha_i\lambda} \\
&= \frac{1}{|G|} \sum_{A\in G} \frac{1}{\det(I-\lambda A)}.
\end{aligned}$$

□

Následuje užitečné lemma, které říká, že pokud máme tip na generátory okruhu invariantů, které jsou algebraicky nezávislé a zároveň jejich stupně odpovídají mocninám ve jmenovateli Molienovy posloupnosti, jedná se již o generátory.

Lemma 2.3.7. *Ať $f_1,\dots,f_t \in \mathbb{C}[x]$ jsou homogenní polynomy algebraicky nezávislé nad $\mathbb{C}$, stupňů $d_1,\dots,d_t$. Uvažme okruh $P = \mathbb{C}[f_1,\dots,f_t]$. Označme P_i množinu homogenních polynomů z P stupně i. Pak platí*

$$\sum_{i=0}^{\infty} \lambda^i \dim{}_{\mathbb{C}} P_i = \frac{1}{(1-\lambda^{d_1})\cdots(1-\lambda^{d_t})}.$$

Důkaz. Označme $N_i = \{(i_1,\dots,i_t) \in \mathbb{N}^t \mid i_1d_1+\cdots+i_td_t = d\}$, $i \in \mathbb{N}$. Protože jsou $f_1,\dots,f_t$ algebraicky nezávislé, je $\{f_1^{i_1}\cdots f_t^{i_t} \mid (i_1,\dots,i_t) \in N_i\}$ báze P_i. Protože $1 = (1-\lambda^{d_i})(1+\lambda^{d_i}+\lambda^{2d_i}+\dots)$, platí

$$\begin{aligned}
\frac{1}{(1-\lambda^{d_1})\cdots(1-\lambda^{d_t})} &= \frac{1}{(1-\lambda^{d_1})}\cdots\frac{1}{(1-\lambda^{d_t})} \\
&= \left(\sum_{i_1=0}^{\infty}\lambda^{i_1d_1}\right)\cdots\left(\sum_{i_t=0}^{\infty}\lambda^{i_td_t}\right) \\
&= \sum_{i=0}^{\infty} \sum_{(i_1,\dots,i_t)\in N_i} \lambda^i \\
&= \sum_{i=0}^{\infty} |N_i|\lambda^i \\
&= \sum_{i=0}^{\infty} \dim{}_{\mathbb{C}} P_i(\lambda)^i.
\end{aligned}$$

□

Potud jsme dokázali všechna tvrzení užitá v příkladu 7. Nicméně, co se týká struktury okruhu invariantů, jednalo se o speciální případ. Okruh invariantů je zde zároveň polynomiálním okruhem, kdy namísto proměnných uvažujeme generující polynomy. To obecně neplatí. Podívejme se na příklad 11. Ten není polynomiálním okruhem. Důvodem je algebraická závislost generujících invariantů. Uvážíme-li obecně generátory $f_1, \ldots, f_t$ okruhu invariantů $\mathbb{C}[x]^G \subset \mathbb{C}[x]$, platí $\mathbb{C}[x]^G = \mathbb{C}[f_1, \ldots, f_t]$. Vezměme ideál I okruhu $\mathbb{C}[x]^G$ tvořený polynomy $g \in \mathbb{C}[y_1, \ldots, y_t]$ splňujícími $g(f_1, \ldots, f_t) = 0$. Tento ideál tedy postihuje všechny algebraické závislosti polynomů $f_1, \ldots, f_t$. Potom platí $\mathbb{C}[x]^G \cong \mathbb{C}[f_1, \ldots, f_t]/I$.

Dalším přirozeným cílem, který bychom mohli sledovat, pokud by nás blíže zajímala teorie invariantů, by bylo ukázat, že okruh invariantů $\mathbb{C}[x]^G$ je Cohen-Macaluay okruh. To dle definice znamená, že lze volit invarianty $f_1, \ldots, f_t$ algebraicky nezávislé a $g_1, \ldots, g_l$ z $\mathbb{C}[x]^G$ takové, že

$$\mathbb{C}[x]^G = \oplus_{i=1}^{l} g_i \mathbb{C}[f_1, \ldots, f_t].$$

Tento rozklad se nazývá Hironakova dekompozice. Z věty 2.3.7 víme, jakého tvaru je Molienova posloupnost okruhu $\mathbb{C}[f_1, \ldots, f_t]$. Protože $\mathbb{C}[x]^G$ je direktní suma g_i-násobků tohoto okruhu, lze si rozmyslet, že platí

$$\Phi_G(\lambda) \;=\; \sum_{i=1}^{l} \lambda^{\deg g_i} \frac{1}{\prod_{j=1}^{t}(1-\lambda^{\deg f_j})} = \frac{\sum_{i=1}^{l} \lambda^{\deg g_i}}{\prod_{j=1}^{t}(1-\lambda^{\deg f_j})}. \qquad (2.14)$$

Příklad 11. Uvažme grupu $G_3 = \{I, -I\}$. Polynom $f(x,y) = \sum a_{ij} x^i y^j \in \mathbb{C}[x,y]$ je invariantní ke G_3 právě tehdy, když $f(x,y) = f(-x,-y)$. Lze si snadno rozmyslet, že tato podmínka není splněna právě tehdy, pokud se v polynomu vyskytuje s nenulovým koeficientem člen $x^i y^j$, kde $i+j$ liché. Tedy každý invariantní polynom lze zapsat jako polynom v proměnných x^2, xy, y^2, jinými slovy $\mathbb{C}[x,y]^{G_3} = \mathbb{C}[x^2, xy, y^2]$. Polynomy x^2, xy, y^2 jsou ovšem algebraicky závislé, platí $x^2y^2 - (xy)^2 = 0$. Hironakova dekompozice okruhu invariantů je dle [14]

$$\mathbb{C}[x,y]^{G_3} = \mathbb{C}[x^2, y^2] \oplus xy\mathbb{C}[x^2, y^2].$$

Z (2.14) dostáváme, že

$$\Phi_{G_3}(\lambda) = \frac{1+\lambda^2}{(1-\lambda^2)^2}.$$

K tomuto výsledku vede i užití věty 2.3.6, což lze snadno ověřit.

Příklad 12. Podívejme se dále na samoduální modulární kód C sudé délky n nad $\mathbb{Z}_{p^e}$, $e \in \mathbb{N}$. Z důsledku 0.0.3 víme, že $|C| = p^{en/2}$. Můžeme tedy dle 2.1.2 psát:

$$W_C(x,y) \;=\; \frac{1}{p^{en/2}} W_C(x + (p^e - 1)y, x - y).$$

Protože n dle předpokladu sudé, platí

$$W_C(x,y) \;=\; W_C(-x,-y).$$

Dostáváme transformace, vůči kterým je váhový výčet kódu C invariantní:

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \frac{1}{\sqrt{p^e}} \begin{pmatrix} 1 & p^e-1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$
$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Značme G_4 grupu generovanou maticemi

$$A = \frac{1}{\sqrt{p^e}} \begin{pmatrix} 1 & p^e-1 \\ 1 & -1 \end{pmatrix}, -I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Ta je podgrupou $\mathrm{GL}(\mathbb{C}^2)$, výpočty proto probíhají v charakteristice 0. Protože platí $A^2 = (-I)^2 = I$, je snadno vidět, že grupu tvoří čtyři prvky $A, -I, -A, I$. Spočtěme Molienovu posloupnost pro G_4 dle 2.3.6.

$$\begin{aligned} \Phi_{G_4}(\lambda) &= \frac{1}{|G_4|} \sum_{B \in G_4} \frac{1}{\det(I - \lambda B)} \\ &= \frac{1}{4}\left(\frac{1}{1-\lambda^2} + \frac{1}{1-\lambda^2} + \frac{1}{(1-\lambda)^2} + \frac{1}{(1+\lambda)^2} \right) \\ &= \frac{1}{(1-\lambda)^2(1+\lambda)^2} \\ &= \frac{1}{(1-\lambda^2)^2}. \end{aligned}$$

Z tvaru $\Phi_{G_4}(\lambda)$ můžeme vyčíst, že pokud najdeme dva homogenní algebraicky nezávislé polynomy invariantní vůči G_4 stupně 2, máme generující polynomy $\mathbb{C}[x,y]^{G_4}$ dle 2.3.7.

Připomeňme, že obrazem polynomu f pomocí Reynoldova operátoru * grupy G, vizte (2.7), získáme polynom f^*, který je vůči G invariantní. Navíc z lemmatu 2.3.4 víme, že při hledání generujících invariantů se stačí v našem případě omezit na obrazy monomů celkového stupně $\leq |G_4| = 4$. Náhodně spočteme pár kandidátů na generátory, například

$$\begin{aligned} (y^2)^* &= \frac{x^2 - 2xy + (p^e+1)y^2}{2p^e}, \\ (xy)^* &= \frac{x^2 + 2(p^e-1)xy - (p^e-1)y^2}{2p^e}. \end{aligned}$$

Tyto invarianty nejsou, řekněme, v pěkném tvaru, ale protože nás zajímají generátory coby bázové vektory prostoru $\mathbb{C}[x,y]^{G_4}$, můžeme namísto těchto získaných invariantů uvážit jejich nenulovou lineární kombinaci, či násobek komplexním číslem. Položme proto

$$\begin{aligned} u_1 &= 2\big((xy)^* + (p^e-1)(y^2)^*\big) = x^2 + (p^e-1)y^2, \\ u_2 &= \frac{1}{2}\big(2p^e(y^2)^* - u_1\big) = y^2 - xy. \end{aligned}$$

S těmito se již bude pracovat lépe. Protože jde o lineární kombinace invariantů a invarianty tvoří okruh, jedná se o invarianty. Nicméně poznamenejme, že pokud

bychom potřebovali testovat polynom na invarianci, stačí zkontrolovat, zda $f = f^*$.

Algebraickou nezávislost, tedy neexistenci nenulového polynomu $a(z_1, z_2) \in \mathbb{C}[z_1, z_2]$, že $a(u_1, u_2) = 0$, lze dokázat snadno porovnáním vedoucích členů v proměnné x polynomů u_1, u_2. V prvním případě x^2, ve druhém xy. Položme $a(u_1, u_2) = \sum a_{i,j} u_1^i u_2^j$. Lze si rozmyslet, že aby měl po roznásobení vedoucí člen v proměnné x nulový koeficient, musí být nulový odpovídající koeficient polynomu a. Tedy polynom $a(u_1, u_2)$ bude nulový právě tehdy, když bude nulový polynom a. Proto jsou u_1, u_2 algebraicky nezávislé. Ukázali jsme $\mathbb{C}[x, y]^{G_4} = \mathbb{C}[u_1, u_2]$.

Důsledek 2.3.8. *Ať C je samoduální modulární kód sudé délky nad $\mathbb{Z}_{p^e}$, $e \in \mathbb{N}$. Pak jeho váhový výčet $W_C(x, y) \in \mathbb{C}[x^2 + (p^e - 1)y^2, y^2 - xy]$.*

Důkaz. Vizte vypracování příkladu 12. □

3. Váhové výčty zdvižených kódů

Cíl: V této kapitole budeme studovat změnu váhového výčtu při zdvižení kódu. Budeme se zabývat jen zdvihy samoduálních kódů, které půjde zvednout na p-adické samoduální, tedy kódy typu 1^k. Hlavní věta této kapitoly nám řekne, jak se změní při zvednutí d-tý člen váhového výčtu, kde d je minimální vzdálenost kódu. Společně s teorií invariantů nám tato znalost umožní v případě Hammingova kódu určit váhový výčet libovolného zdvihu. Tím završíme kapitolu i celý text.

3.1 Výpočet koeficientu A_d

Ať C_∞ je lineární kód nad $\mathbb{Z}_{p^\infty}$ s generující maticí G typu 1^k. O matici H řekneme, že je paritní, pokud $c \cdot H^T = 0$ právě tehdy, když c je kódové. Poznamenejme, že násobení probíhá vždy nad okruhem, nad nímž je kód definován. Oříznutí $\Psi_e(C_\infty)$ budeme krátce značit C_e, $e \in \mathbb{N}$. Dále budeme používat zkrácený zápis $G_e = \Psi_e(G)$ a podobně $H_e = \Psi_e(G)$ pro generující, případně paritní matici kódu C_e. Minimální vzdáleností kódu budeme rozumět nejmenší z Hammingových vah nenulových kódových slov. Minimální vzdálenost kódu C budeme značit $d(C)$.

Dokažme několik pomocných lemmat. Platnost prvního z nich lze snadno nahlédnout.

Lemma 3.1.1. *Ať $0 < f \leq e < \infty$ a M je matice p-adických čísel. Potom*

$$p^{e-f}\Psi_f(M) \equiv p^{e-f}\Psi_e(M) \pmod{p^e}.$$

Důkaz. Mějme M ze znění. Pak

$$\begin{aligned} \Psi_f(M) &\equiv \Psi_e(M) \pmod{p^f} \\ p^{e-f}\Psi_f(M) &\equiv p^{e-f}\Psi_e(M) \pmod{p^e}. \end{aligned}$$

□

Lemma 3.1.2. *Ať $0 < f < e < \infty$. Potom*

(i) $p^{e-f}C_f \subset C_e$

(ii) $\mathrm{Ker}\Psi_f^e = p^f C_{e-f}$

Důkaz. Ať $c \in C_f$, jinými slovy $cH_f^T \equiv 0 \pmod{p^f}$. Ekvivalentně lze kongruenci přepsat jako $p^{e-f}cH_f^T \equiv 0 \pmod{p^e}$. Užijeme lemma 3.1.1 a dostaneme $p^{e-f}cH_e^T \equiv 0 \pmod{p^e}$, jinými slovy $p^{e-f}c \in C_e$.

Homomorfismus Ψ_f^e mi zobrazí na nulu slovo z C^e právě tehdy, pokud bude násobkem p^f. Budeme se tedy ptát, kdy c tvaru $c = p^f c_1$ je v C_e. Využijeme opět

lemma 3.1.1, přičemž za f ze znění lemmatu dosadíme $e-f$. Získáme tak kongruenci $p^f H_{e-f}^T \equiv p^f H_e^T \pmod{p^e}$, kterou využijeme v následující šňůře ekvivalencí:

$$\begin{aligned} c \in C^e &\Leftrightarrow p^f c_1 H_e^T \equiv 0 \pmod{p^e} \\ &\Leftrightarrow p^f c_1 H_{e-f}^T \equiv 0 \pmod{p^e} \\ &\Leftrightarrow c_1 H_{e-f}^T \equiv 0 \pmod{p^{e-f}} \\ &\Leftrightarrow c_1 \in C_{e-f} \\ &\Leftrightarrow c \in p^f C_{e-f}. \end{aligned}$$

□

Důsledek 3.1.3. *Ke každému slovu kódu C^f existuje slovo kódu C^e shodné Hammingovy váhy. Váhový výčet C^{e-f} je roven váhovému výčtu* $\mathrm{Ker}\Psi_f^e$.

Důkaz. Přímý důsledek 3.1.2. □

Lemma 3.1.4 (Vztah mezi vzdálenostmi.)**.** *Ať C_∞ je p-adický kód. Pak*

(i) $\forall e \in \mathbb{N} : d(C_e) = d(C_1)$

(ii) $d(C_\infty) \geq d(C_1)$.

Důkaz. Chceme $\forall e \in \mathbb{N} : d(C_e) = d(C_1)$. Ať $0 < f < e < \infty$. Pro každé slovo z C_f existuje slovo z C_e shodné váhy, říká důsledek 3.1.3. Proto platí $d(C_e) \leq d(C_1)$. Pro druhou nerovnost předpokládejme pro spor, že $e+1 \in \mathbb{N}$ je nejmenší takové, že $d(C_{e+1}) < d(C_1)$. Ať $c \in C_{e+1}$ nenulové, že $w(c) < d(C_1)$. Potom $0 \leq w(\Psi_e(c)) \leq w(c) < d(C)$. Nutně $\Psi_e(c)$ je nulové slovo kódu C_e tedy je násobkem p^e. Ať $c = p^e c_1$. Z 3.1.2 (ii) dostáváme $\mathrm{Ker}\Psi_e^{e+1} = p^e C_1$, tedy c_1 je slovo C_1. Protože c je nenulové v C_{e+1}, nutně c_1 nenulové v C_1. Tedy $0 < w(c_1) = w(c) < d(C_1)$, spor.

Chceme $d(C_\infty) \geq d(C_1)$. Pro spor uvažme nenulové slovo $c \in C_\infty$, že $w(c) < d(C_1)$. Volme dostatečně velké $e \in \mathbb{N}$, aby $w(\Psi_e(c)) = w(c)$, to jistě lze. Potom $w(\Psi_e(c)) < d(C_1)$, spor. □

Pro zjednodušení značení budeme dále značit minimální vzdálenost libovolného konečného zdvihu $d = d(C_1) = d(C_e)$, $e \in \mathbb{N}$, minimální vzdálenost p-adického kódu pak $d_\infty = d(C_\infty)$.

Ať $x = (x_1, \ldots, x_n)$ vektor délky n a ať $S \subseteq \{1, \ldots, n\}$. Označme $s = |S|$. Potom definujeme x_S jako vektor délky s, který dostaneme vyškrtáním souřadnic vektoru x, jejichž index není v S. Pokud bychom chtěli x_S definovat formálně, ať $S = \{i_1, \ldots, i_s\}$, kdy navíc volíme značení prvků S tak, aby $i_k < i_l$ pro $k < l$. Pak j-tá souřadnice x_S je rovna x_{i_j}, $j \in \{1, \ldots, s\}$.

Dále ať $y = (y_1, \ldots, y_s)$. Potom y^S budeme značit vektor délky n, který získáme z y doplněním 0 na souřadnice mimo S. Formálně $y^S = (z_1, \ldots, z_n)$, kde $z_{i_j} = y_j$ pro $j \in \{1, \ldots, s\}$ a $z_j = 0$ pro $j \notin S$.

Ať M je matice $k \times n$ a S jako výše. Maticí M_S budeme rozumět matici vzniklou z M vyškrtáním řádků s indexy mimo S. Formálně, je-li m_i, $i \in \{1, \ldots, k\}$ i-tý řádek matice M, tedy $M = (m_i)_{i=1}^k$, potom $M_S = (m_{i_j})_{j=1}^s$, přičemž i_j opět probíhá prvky S seřazené vzestupně.

Ať x vektor délky $n \in \mathbb{N}$. Definujme $\mathrm{Supp}(x) = \{i \in \{1, \ldots, n\} \mid x_i \neq 0\}$. Zřejmě platí následující lemma:

Lemma 3.1.5. *Ať C je kód s paritní maticí H. Ať x je kódové slovo váhy s a ať $S = \mathrm{Supp}(x)$. Potom $H_S(x_S)^T = 0$. Naopak, je-li $H_S y^T = 0$, potom y^S je kódové slovo a jeho váha je rovna váze y.*

Důkaz. Plyne přímo z definice. □

Umluvme značení v souvislosti s typem matice p-adického kódu. Budeme rozumět $p^\infty = 0$. Ačkoliv to vypadá nepřirozeně, jde o obdobu značení u modulárních kódů, kdy pro kód nad $\mathbb{Z}_{p^e}$ je $p^e = 0$. Dále jsme definovali standardizovaný tvar matice jen pro matici generující. Bezpochyby můžeme do standardizovaného tvaru převést libovolnou matici, stejně jako lze hovořit o jejím typu. Obojí tak budeme dále používat.

Lemma 3.1.6. *Uvažme p-adický kód C_∞ s paritní maticí H. Ať $D \subseteq \{1, \ldots, n\}$, že $|D| = d$, kde d je minimální vzdálenost $C_1 = \Psi_1(C_\infty)$. Potom H'_D je typu $(1)^{d-1}(p^j)^1$ pro nějaké $j \in \mathbb{N}_0^\infty$.*

Důkaz. Protože C_1 má minimální vzdálenost d, bude každých $d-1$ sloupců matice $\Psi_1(H)$ lineárně nezávislých nad $\mathbb{Z}_p$. Proto každá matice tvořená $d-1$ sloupci $\Psi_1(H)$ bude mít standardizovaný tvar $\binom{I_{d-1}}{0}$. Nyní si stačí rozmyslet, že po libovolném zvednutí zůstanou prvky na diagonále invertibilní a tudíž po úpravě do standardizovaného tvaru získáme opět matici $\binom{I_{d-1}}{0}$. Pokud budeme zdvihat do nekonečna, dostaneme, že i H'_D je tohoto tvaru. Přidáním dalšího sloupce tak získáme matici ve standardizovaném tvaru typu $(1)^{d-1}(p^j)^1$ pro nějaké $j \in \mathbb{N}_0^\infty$. □

Pro $j \in \mathbb{N}_0^\infty$ označme P_j počet různých d prvkových podmnožin $D \subseteq \{1, \ldots, n\}$, že standardizovaný tvar H_D je typu $(1)^{d-1}(p^j)^1$. Poznamenejme, že P_j je závislý jen na paritní matici C_∞.

Věta 3.1.7. *Ať C_e je kód nad $\mathbb{Z}_{p^e}$. Pak počet A_e^d kódových slov váhy rovné minimální vzdálenosti kódu d je roven*

$$A_e^d = \sum_{j=1}^{e-1} P_j(p^j - 1) + (p^e - 1)\sum_{j \geq e} P_j + (p^e - 1)P_\infty. \tag{3.1}$$

Důkaz. Ať C_∞ je p-adický kód, že $\Psi_e(C_\infty) = C_e$, a ať H je jeho paritní matice, $H_e = \Psi_e(H)$ pak paritní matice C_e.

Označme $A_e^d = \{c \in C_e \mid w(c) = d\})$ množinu všech kódových slov C_e s váhou rovnou minimální vzdálenosti kódu. Pro $D \subseteq \{1, \ldots, n\}$, $|D| = d$ označme

$$C_e^D = \{y^D \mid 0 \neq y \in \mathbb{Z}_{p^e}^d \wedge y \in \mathrm{Ker}\,((H_e)_D)\}$$

Lze si rozmyslet, že by A_d^e mělo být rovno disjunktnímu sjednocení $\bigcup C_e^D$ přes $D \subseteq \{1, \ldots, n\}$, $|D| = d$. Pro jistotu uvedeme pečlivější odůvodnění. Nejprve $A_e^d \subseteq \bigcup C_e^D$. Ať h_i je i-tý řádek H_e. Platí $c \in A_e^d$ právě tehdy, když je slovo kódové, tedy $[h_i, c] = 0\ \forall i \in$ Supp (c), a má váhu d, tedy $|$ Supp $(c)| = d$. Stačí volit $D =$ Supp (c).

Dále chceme $A_e^d \supseteq \bigcup C_e^D$. Ať $D \subseteq \{1, \ldots, n\}$, že $|D| = d$, ať $y \in C_e^D$. Protože každých $d-1$ sloupců H_e je lineárně nezávislých (modulo p^e), musí být $w(y) = d$, tedy i $w(y^D) = d$. Zřejmě y^D kódové, druhá inkluze dokázána.

Ukážeme, že sjednocení je disjunktní. K tomu stačí dokázat, že žádné slovo (všechna jsou nenulová) nemůže být započteno dvakrát. Pro spor ať existují D_1, D_2, různé d-prvkové podmnožiny $\{1, \ldots, n\}$, a $y_1 \in C_e^{D_1}$, $y_2 \in C_e^{D_2}$, že $y_1^{D_1} = y_2^{D_2}$. Opět využijeme, že $d-1$ sloupců H_e nemůže být lineárně závislých a tedy $w(y_1) = w(y_2) = d$. To společně s $y_1^{D_1} = y_2^{D_2}$ dává, že obě slova mají stejný počet stejných nenulových souřadnic, na kterých se rovnají, proto se musí rovnat $D_1 = D_2$ i $y_1 = y_2$.

Pro dokončení stačí nasčítat $|C_e^D|$ pro všechna vyhovující D. Ať H'_D je typu $(1)^{d-1}(p^j)^1$. Zřejmě pro $0 < j < e$ je i $(H_e)'_D$ typu $(1)^{d-1}(p^j)^1$. Pro $e \leq j$ je typu $(1)^{d-1}(0)^1$. V tomto případě platí $|C_e^D| = |\mathrm{Ker}(H_D)| - 1$. Užijeme větu 0.0.1. Pro $0 < j < e$ dostaneme $|C_e^D| = p^j - 1$. Pro $j \geq e$ a $j = \infty$ pak $|C_e^D| = p^e - 1$. □

Důsledek 3.1.8. *Ať $e \in \mathbb{N}$. Pak*

$$A_{e+1}^d - A_e^d \;=\; \left(P_\infty + \sum_{j \geq e+1} P_j\right)(p^{e+1} - p^e). \tag{3.2}$$

Důkaz. Aplikujeme na A_{e+1}^d a A_e^d výsledek věty 3.1.7. □

Následuje důležitý výsledek. Pokud C_1 a C_2 mají stejný počet slov váhy d, pak libovolný zdvih bude mít tentýž počet slov váhy d.

Lemma 3.1.9. *Ať $A_1^d = A_2^d$. Potom $A_1^d = A_e^d$ pro libovolné $e \in \mathbb{N}$.*

Důkaz. Dosadíme do (3.2) pro $e = 1$, dostaneme $A_2^d - A_1^d = \left(P_\infty + \sum_{j \geq 2} P_j\right)(p^2 - p)$. Z předpokladu lemmatu je $A_2^d - A_1^d = 0$. Protože $p^2 - p$ je jistě nenulové, musí být $P_\infty + \sum_{j \geq 2} P_j = 0$. Protože všechny sčítance jsou nezáporné, nutně $P_j = 0$ pro $j \geq 2$ a $j = \infty$. Po dosazení těchto hodnot do rovnice (3.1) pro obecné $e \geq 2$, dostaneme $A_e^d = P_1(p-1)$. Tentýž výsledek získáme z rovnice (3.1) pro volbu $e = 1$. Tedy $A_e^d = A_1^d$ pro $e \in \mathbb{N}$. □

Následující lemma nám říká, že pokud máme kód dostatečně zdvižený, je A_e^d polynomiální funkcí v p^e s koeficienty nezávislými na e. Pokud navíc $P_\infty = 0$, jsou si počty kódových slov váhy d dostatečně zdvižených kódů rovny.

Lemma 3.1.10. *Označme $N = \max\{j \in \mathbb{N} \mid P_j \neq 0\}$. Potom*

(i) Je-li $e > N$, platí $A_e^d = ap^e + b$, kde a, b nezávisí na e.

(ii) Je-li $e \geq N$ a $P_\infty = 0$, platí $A_e^d = A_N^d$.

Důkaz. Stačí položit $a = P_\infty$ a $b = -P_\infty + \sum_{j=1}^N P_j(p^j - 1)$ a užít 3.1.7.

Ať $e \geq N$. Dosadíme do (3.1) hodnoty pro e, získáme $A_e^d = \sum_{j=1}^N P_j(p^j - 1)$. Tatáž rovnice pro N dává $A_N^d = P_N(p^N - 1) + \sum_{j=1}^{N-1} P_j(p^j - 1)$. □

Budeme-li znát koeficienty a, b z 3.1.10, umíme z podmínky (i) určit počet kódových slov váhy d libovolného dostatečně vysokého zdvihu kódu. Hodilo by se nám tedy jednoduše rozpoznat, kdy je $P_\infty = 0$.

Lemma 3.1.11. *Ať C_∞ je p-adický kód s minimální vzdáleností d_∞ a minimální vzdáleností oříznutého kódu d. Pak platí $P_\infty = 0 \Leftrightarrow d_\infty > d$.*

Důkaz. Ať C_∞ p-adický kód a H jeho paritní matice. Ať $D \subseteq \{1,\ldots,n\}$, že $|D| = d$. Předpokládejme, že $P_\infty = 0$, tedy všechny matice H'_D budou typu $(1)^{d-1}(p^j)^1$ pro nějaké $j \geq 0$. Protože $\mathbb{Z}_{p^\infty}$ je obor integrity, bude $\mathrm{Ker}(H_D) = \{0\}$. Tedy neexistuje slovo kódu C_∞ váhy d, proto $d_\infty > d$.

Opačně. Ať $d_\infty > d$. Pro spor ať existuje $D \subseteq \{1,\ldots,n\}$, $|D| = d$, že H'_D typu $(1)^{d-1}(0)^1$. Potom ale existuje slovo kódu C_∞ váhy d, spor. □

Následující věta je zobecněním lemmatu 3.1.10. Říká, že od určité hranice mají zdvihy stejný počet kódových slov váhy j, kde $d \leq j < d_\infty$.

Věta 3.1.12. *Ať C_∞ je p-adický kód a $C_e = \Psi_e(C_\infty)$ pro $e \in \mathbb{N}$. Potom existuje $N \in \mathbb{N}$, že pro každé $e \geq N, e \in \mathbb{N}$ a $j \in \mathbb{N}$, $d \leq j < d_\infty$ platí $A^j_e = A^j_N$. Navíc platí, že každé kódové slovo z C_e váhy j je tvaru $p^{e-N}c$, kde $c \in C_N$ váhy j.*

Důkaz. Ať H je paritní matice kódu C_∞. Označme $K \subseteq \mathbb{N}$, že $m \in K \Leftrightarrow \exists S \subseteq \{1,\ldots,n\}, d \leq |S| < d_\infty$, že H'_S má v typu p^m. Označme $N = 1 + \max K$. Pro úplnost poznamenejme, že v žádném typu se dle 3.1.11 nebude vyskytovat p^∞, neboť $d < d_\infty$.

Označme B^j_e počet slov kódu C_e váhy menší rovné j. Platí tedy $A^j_e = B^j_e - B^{j-1}_e$. Stačí ukázat, že $B^j_e = B^j_N$ a $B^{j-1}_e = B^{j-1}_N$ pro $e \geq N$. Pak bude $A^j_e = A^j_N$. Zřejmě platí

$$\begin{aligned} B^j_N &= \Big| \bigcup_{|S|=j} \{y^S \mid y \in \mathrm{Ker}(H_N)_S\} \Big| \\ B^j_e &= \Big| \bigcup_{|S|=j} \{y^S \mid y \in \mathrm{Ker}(H_e)_S\} \Big|. \end{aligned}$$

Nevyloučili jsme totiž, že by souřadnice s indexy z S nemohly být nulové. Pokud ukážeme $|\mathrm{Ker}(H_N)_S| = |\mathrm{Ker}(H_e)_S|$, bude platit $B^j_N = B^j_e$. Lemma 0.0.1 nám říká, že stačí ukázat, že $(H_N)'_S$ a $(H_e)'_S$ jsou stejného typu. Platí $p^m \not\equiv 0 \pmod{p^N}$ pro všechna m z K, tedy všechna m, jež se mohou vyskytnou v typu matice. Tedy Ψ_N v tomto případě nezmění typ matice. Tím je dokázána první část věty.

Platí $y \in \mathrm{Ker}((H_N)_S)$ právě tehdy, když $(H_N)_S \cdot y^T \equiv 0 \pmod{p^N}$, to nastane právě, když $p^{e-N}(H_N)_S \cdot y^T \equiv 0 \pmod{p^e}$, což je dle 3.1.1 právě tehdy, když $p^{e-N}(H_e)_S \cdot y^T \equiv 0 \pmod{p^e}$. □

3.2 Váhové výčty zdvihu Hammingova kódu

Cíl: Naposledy se zaměříme na Hammingův rozšířený binární kód. Ukážeme si, že věta 3.1.12 je nástroj dostatečně silný pro určení všech koeficientů váhového výčtu jeho libovolného zdvihu.

Hammingův kód navíc nebudeme zvedat libovolně, ale budeme si vybírat cyklický zdvih. Cyklický kód nad okruhem se definuje obdobně jako cyklický kód nad tělesem. Kód C délky n nad okruhem nazýváme cyklický, pokud pro každé $c = (c_1,\ldots,c_n) \in C$ platí $(c_2,\ldots,c_n,c_1) \in C$. Cyklické kódy délky n nad tělesem $\mathbb{F}$ lze ztotožnit s ideály faktorokruhu

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

Podobně cyklické kódy délky n nad okruhem $\mathbb{Z}_{p^e}$ odpovídají právě ideálům faktorokruhu

$$\mathbb{Z}_{p^e}[x]/(x^n - 1).$$

Značme C_1 Hammingův binární kód generovaný maticí

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

Kód C_1 lze reprezentovat jako hlavní ideál okruhu $\mathbb{Z}_2[x]/(x^7 - 1)$ generovaný ireducibilním polynomem $f_1 = x^3 + x^2 + 1$. Polynom f_1 lze dle jednoznačně zvednout na ireducibilní polynom $f_2 \in \mathbb{Z}_4[x]$. Výpočtem, vizte příloha, získáme $f_2 = x^3 + 2x^2 + x + 3$. Podobným způsobem můžeme získat f_e, $e \in \mathbb{N}$. Jak ale získat odpovídající faktor rozkladu nad p-adickými čísly? Označme 2-adické číslo

$$\alpha = \frac{1 + \sqrt{-7}}{2},$$

ve 2-adickém zápisu

$$\alpha = 0110010111111001110011011\ldots.$$

Snadno lze ověřit, že α splňuje rovnost

$$\alpha^2 - \alpha + 2 = 0. \tag{3.3}$$

Roznásobíme-li následující součin a upravíme-li ho za využití (3.3)

$$(x-1)(x^3 + \alpha x^2 + (\alpha - 1)x - 1)(x^3 - (\alpha - 1)x^2 - \alpha x - 1),$$

získáme $x^7 - 1$. Zřejmě se tedy jedná o jednoznačně určený rozklad $x^7 - 1$ na ireducibilní polynomy v $\mathbb{Z}_{2^\infty}$. Nás zajímá především člen $x^3 + \alpha x^2 + (\alpha - 1)x - 1$, neboť

$$f_e = x^3 + \Psi_e(\alpha)x^2 + \Psi_e(\alpha - 1)x - 1$$

Proto je zdvih C_e Hammingova rozšířeného binárního kódu generovaný maticí $\Psi_e(G_\infty)$, kde

$$G_\infty = \begin{pmatrix} 1 & \alpha & \alpha - 1 & -1 & 0 & 0 & 0 & 1 \\ 0 & 1 & \alpha & \alpha - 1 & -1 & 0 & 0 & 1 \\ 0 & 0 & 1 & \alpha & \alpha - 1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 1 & \alpha & \alpha - 1 & -1 & 1 \end{pmatrix}$$

a nekonečný zdvih, tedy kód nad $\mathbb{Z}_{2^\infty}$, je generován maticí G_∞. Zřejmě tyto kódy jsou samoduální. To lze zjistit snadno spočtením vnitřního součinu generujících slov kódu C_∞ se sebou samými a navzájem. Samodualita oříznutých kódů plyne z 1.1.6.

Minimální vzdálenost kódů C_e, $e \in \mathbb{N}$ je 4. Minimální vzdálenost kódu C_∞ je 5. Nabývají ji slova na řádcích generující matice. Zbývá odůvodnit, že není menší, v našem případě rovna 4. Ať pro spor $d_\infty = 4$. Z lemmatu 3.1.11 víme, že to je ekvivalentní podmínce, že $P_\infty > 0$. To dle definice znamená, že existuje čtveřice

sloupců paritní matice kódu C_∞, která je po převedení do standardizovaného tvaru typu $(1)^{d-1}(p^\infty)^1$, tedy $(1)^3(0)^1$. To je zřejmě ekvivalentní tomu, že tato podmatice má hodnost 3. V případě samoduálního kódu lze za paritní matici volit generující matici. Libovolná podmatice 4×4 generující matice G_∞ má však lineárně nezávislé sloupce a řádky. Spor. Tedy $d_\infty = 5$.

Z 2.3.8 plyne, že

$$W_{C_e} = \sum_{i=0}^{4} c_i u_1^i u_2^{4-i}, \tag{3.4}$$

kde $u_1 = x^2 + (p^e - 1)y^2, u_2 = y^2 - xy$. Dále lze spočíst, vizte příloha, že váhový výčet kódu C_2 je

$$x^8 + 14x^4y^4 + 112x^3y^5 + 112xy^7 + 17y^8,$$

tedy $A_2^4 = A_1^4 = 14$. To implikuje dle lemmatu 3.1.9, že $A_e^4 = 14$ pro libovolné $e \in \mathbb{N}$. Nulové kódové slovo je právě jedno,tedy $A_0^e = 1$. Minimální vzdálenost kódu je 4, tedy $A_1^e = A_2^e = A_3^e = 0$. Dostáváme

$$W_{C_e} = 1 + 14x^4y^4 + \sum_{i=5}^{8} A_i x^{8-i} y^i. \tag{3.5}$$

Vyjádření (3.4) a (3.5) váhového výčtu si musí být rovny. Porovnáním koeficientů u jednotlivých členů postupně dostaneme řešení soustavy:

$$\begin{aligned} c_4 &= A_0 = 1 \\ c_3 &= A_1 = 0 \\ c_2 &= 4(p^e + 1) \\ c_1 &= 8(p^e + 1) \\ c_0 &= 2(p^e - 6)^2 - 36. \end{aligned}$$

Po dosazení do (3.4) a roznásobení dostáváme seznam koeficientů:

$$\begin{aligned} A_1 &= 1 \\ A_2 &= 0 \\ A_3 &= 0 \\ A_4 &= 14 \\ A_5 &= 56(p^e - 2) \\ A_6 &= 28(p^{2e} - 6p^e + 8) \\ A_7 &= 8(p^{3e} - 7p2e + 21p^e - 22) \\ A_8 &= p^{4e} - 8p^{3e} + 28p^{2e} - 56p^e + 49. \end{aligned}$$

S využitím vypracované teorie jsme si tedy ukázali na příkladě Hammingova rošířeného binárního kódu, jak určit jeho zdvihy tak, aby byly cyklické. Dále jsme si ukázali, jaký bude tvar matice libovolného zdvihu. Nakonec jsme plně určili váhový výčet libovolného zdvihu.

Závěr

V práci jsme se zabývali studiem modulárních a p-adických kódů. Především jsme na ně nahlíželi jako na posloupnost kódů nad okruhy $\mathbb{Z}_{p^e}$, $e \in \mathbb{N}$. Kód nad větším okruhem je v jistém slova smyslu zpřesněním kódu nad menším okruhem. Limitně takto dojdeme ke kódu p-adickému. Zajímali jsme se o kvalitu oříznutých a zvednutých kódů - zůstanou-li samoduální, a co se stane s váhovým výčtem. Naučili jsme se, jak najít cyklický zdvih. Pro bližší zkoumání váhového výčtu jsme pak úspěšně využívali výsledky teorie invariantů.

Při zpracování bylo třeba nejdříve projít dostupné články s podobnou tematikou a získat přehled o publikovaných výsledcích. Ukázalo se, že mnoho autorů se vydává cestou zobecňování známých tvrzení a to stylem případ od případu zvlášť, což vede k zahlcení a znepřehlednění dostupných výsledků. Přesto se podařilo vybrat smysluplná témata tak, aby na sebe navazovala a vzájemně se doplňovala, a dojít tak ke konkrétním a pestrým výsledkům. Těžiště práce se postupně ustálilo na studiu modulárních a p-adických samoduálních kódů.

Velkou pozornost jsem věnoval zpracování důkazů, aby byly přehledné a ověřitelné. Obzvláště v první kapitole, bylo potřeba důkazy na základě osnov uvedených v článcích rozpracovat do srozumitelného tvaru. Dále jsem se snažil dohledávat důkazy odkazované a bylo-li třeba, dokázat je za pomoci známé teorie, byť třeba ve slabší, pro naše účely však postačující verzi. Doprovodné příklady byly voleny tak, aby vedly k lepší orientaci v probíraném tématu. V některých případech zároveň přinesly užitečné výsledky.

Uveďme na závěr několik směrů, kterým by se mohlo studium dále ubírat. První z nich je již zmiňované zobecňování výsledků pro obecnější třídy kódů. Důležitým mezníkem v tomto směru je kniha [12] od Nebeové, Rainse, Sloane, kde jsou autoři po zavedení hutného formalismu schopni pokrýt při studiu zároveň různorodé třídy kódů. Sjednocují a zobecňují tak pohled na kódy nad okruhy. Sám Sloane považuje tuto knihu za završení své práce v této oblasti. Také se jim daří odpovědět na některé důležité otázky. Zmiňme například obecnější obdobu Gleasonovy věty. Dalším bezesporu zajímavým výsledkem je tvrzení, že za určitých podmínek jsou váhové výčty určité třídy kódů prvky určitého okruhu invariantů a naopak, tento okruh je generován váhovými výčty kódů z této třídy kódů. Což není samozřejmé. Pro libovolný invariant tak existuje kód s váhovým výčtem, který je tomuto invariantu rovný.

Zpracování okruhů invariantů v práci se neobešlo bez kompromisu. Téma je zpracováno pro naše účely v dostatečném rozsahu a hloubce. Nicméně jsme se nedostali k jednoznačné klasifikaci okruhů invariantů. K tomu by bylo třeba zavést Noetherové normalizační lemma pro stupňované okruhy, definovat Cohen-Macaluayovy okruhy, nastudovat jejich vlastnosti a ukázat, že okruhy invariantů jsou Cohen-Macaluayovy. Přímo z definice těchto okruhů je pak zřejmé, jak volit generující invarianty, aby byl zápis jednoznačný. Pokoušel jsem se toto téma zpracovat v duchu uvedených zásad, ale bylo by příliš rozsáhlé a vzhledem k našemu zaměření nepříliš přínosné. Pokud však čtenáře zajímá, lze doporučit [11] a především [15]. V této literatuře najdeme také odpověď na otázku, kdy je okruh invariantů zároveň polynomiálním okruhem, kdy za proměnné uvažujeme generátory okruhu.

Další možností je zabývat se touto oblastí z hlediska algoritmického a výpočetního. Například hledání báze okruhů invariantů. Zde lze rovněž doporučit [15]. Neobejdeme se ovšem bez znalosti Gröbnerových bází.

Z praktického hlediska je nevyřešeným problémem hledání vhodných dekódovacích algoritmů pro modulární kódy. Využit se nabízí pro kódy nad $\mathbb{Z}_4$, které by šly teoreticky použít pro čtyřstavovou modulaci typu QPSK. Blíže k tomuto tématu [7].

Související oblastí je také teorie mříží a ortogonálních polí, kdy dokonce pojmy a výsledky z těchto oborů odpovídají pojmům a výsledkům teorie kódů nad okruhy. Blíže například [14], kapitola 14.

Seznam použité literatury

[1] E. Artin, *Geometric algebra*, Interscience Publishers, 1957.

[2] L. Barto, D. Stanovský, *Počítačová algebra*, MatfyzPress, 2011.

[3] A. R. Calderbank, A. R. Hammons, P. V. Kumar, N. J. A. Sloane, P. Solé, *A linear construction for certain Kerdock and Preparata codes*, 1993.

[4] A. R. Calderbank, N. J. A. Sloane, *Modular and p-adic cyclic codes*, Designs, Codes and Cryptography, 6, 21-35, 2003.

[5] S. T. Dougherty, S. Y. Kim, Y. H. Park, *Lifted Codes and their weight enumerators*, Discrete Mathematics 305, Elsevier, 2005.

[6] S. T. Dougherty, Y. H. Park, *Codes over the p-adic integers*, Design, codes and cryptography. Springer, 2006.

[7] M. Greferath, *An introduction to ring-linear coding theory*, Gröbner bases, coding, and cryptography, Springer, 2009.

[8] T. Honold, *A proof of MacWilliams identity*, Journal of Geometry, Vol. 57 , 1996.

[9] M. Klemm, *Über die Identität von MacWilliams für die Gewichtsfunktion von Codes*, Archiv Math. 49 1987.

[10] F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.

[11] J. Müller, *Invariant theory of finite groups*, preprint, 2004.

[12] G. Nebe, E. M. Rains, N. J. A. Sloane, *Self-dual codes and invariant theory*, Springer, 1993.

[13] V. Pless, *On the uniqueness of the Golay codes*, Journal of combinatorial theory 5, 1968.

[14] E. M. Rains, N. J. A. Sloane, *Self-dual codes and invariant theory*, Handbook of coding theory Elsevier, 1998.

[15] B. Sturmfels, *Algorithms in invariant theory*, Springer, New York, 1993.

[16] B. L. van der Waerden, *Modern algebra*, 1949.

Seznam použitých symbolů

p	prvočíslo
$\mathbb{Z}_{p^e}$	modulární okruh $\mathbb{Z}/p^e\mathbb{Z}$
$\mathbb{Z}_{p^\infty}$	okruh p-adických celých čísel
C	kód (vždy lineární)
$\|C\|$	počet kódových slov, velikost kódu
$C^\perp$	duální kód ke kódu C
C_e	e-tý zdvih kódu C_1, $e \in \mathbb{N}$
C_∞	p-adický kód
w	Hammingova váha
w_L	Leeova váha
w_E	Euklidova váha
$[\ ,\ ]$	vnitřní součin
n	délka kódu
d	minimální vzdálenost
G	generující matice kodu
G'	generující matice G převedená do standardizovaného tvaru
I_k	jednotková matice $k \times k$
$\mathrm{GL}(\mathbb{C}^n)$	množina invertibilních matic $n \times n$ nad komplexními čísly
$\mathbb{C}[x]_i$	množina homogenních polynomů nad $\mathbb{C}$ stupně i
$\mathbb{C}[x]^G$	okruh invariantů grupy G
$\Phi_G(\lambda)$	Molienova posloupnost okruhu invariantů $\mathbb{C}[x]^G$
Ψ_e	ořezávací funkce (do $\mathbb{Z}_{p^e}$)
$\Psi_e(C)$	oříznutí kódu C
$W_C(x, y)$	váhový výčet kódu C
$\mathbb{N}$	množina přirozených čísel $\{1, 2, 3, \ldots\}$
$\mathbb{N}_0$	množina $\mathbb{N} \cup \{0\}$
$\mathbb{N}_0^\infty$	množina $\mathbb{N} \cup \{0, \infty\}$
Tr	stopa matice
$J_e(x)$	$x_1^{e_1} \cdots x_n^{e_n}$ pro pro $e = (e_1, \ldots, e_n) \in \mathbb{N}^n$
*	Reynoldův operátor

Přílohy

Pro práci s kódy i grupami transformací jsem používal program MAGMA dostupný na adrese http://magma.maths.usyd.edu.au/ a nezbývá, než ho vřele doporučit.

Výpočet váhového výčtu rozšířeného Golayova kódu G_{24} pro příklad 5.

```
-------
Vstup:
-------
W_G24<x,y>:=HammingWeightEnumerator(GolayCode(GF(2),true));
W_G24;
-------
Výstup:
-------
x^24 + 759*x^16*y^8 + 2576*x^12*y^12 + 759*x^8*y^16 + y^24
```

Dotaz na konečnost grupy generované transformacemi T_1, T_2 v příkladu 7, výpočet její velikosti. Výpočet Molienovy posloupnosti této grupy.

```
-------
Vstup:
-------
R<x> := PolynomialRing(Rationals());
K<a,i> := NumberField([x^2 - 1/2, x^2 + 1]);
G:=MatrixGroup<2,K|[1,0, 0,i],[a,a, a,-a] >;
IsFinite(G);
Order(G);
Phi<t> := MolienSeries(G);
Phi;
-------
Výstup:
-------
true
192
1/(t^32 - t^24 - t^8 + 1)
```

Výpočet váhového výčtu kódu C_2 z podkapitoly 3.2.

```
-------
Vstup:
-------
C2 := LinearCode<IntegerRing(4), 8 |
    [1,2,1,3,0,0,0,1],
    [0,1,2,1,3,0,0,1],
    [0,0,1,2,1,3,0,1],
    [0,0,0,1,2,1,3,1]>;
```

```
W_C2<x,y> := HammingWeightEnumerator(C2);
W_C2;
-------
Výstup:
-------
x^8 + 14*x^4*y^4 + 112*x^3*y^5 + 112*x*y^7 + 17*y^8
```

Výpočet Henselova liftu polynomu f_1 z podkapitoly 3.2.

```
-------
Vstup:
-------
e:=2;
R<x> := PolynomialRing(Integers());
f := x^7 - 1;
R1<x> := PolynomialRing(Integers(2));
faktory_f := [w[1]:w in Factorization(R1!f)];
faktory_f;
R2<x> := PolynomialRing(Integers(2^e));
HenselLift(f, faktory_f, R2);
-------
Výstup:
-------
[
    x + 1,
    x^3 + x + 1,
    x^3 + x^2 + 1
]
[
    x + 3,
    x^3 + 2*x^2 + x + 3,
    x^3 + 3*x^2 + 2*x + 3
]
```