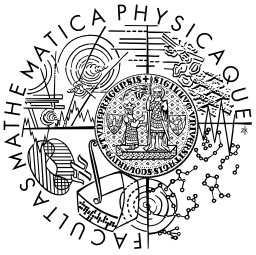

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Kateřina Bžatková

Viditelně ireducibilní polynomy

Katedra algebry

Vedoucí bakalářské práce:	Mgr. Vítězslav Kala, Ph.D.
Studijní program:	Matematika
Studijní obor:	Matematika pro informační technologie

Praha 2019

Prohlašuji, že jsem tuto bakalářskou 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 má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

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

Ráda bych poděkovala svému vedoucímu Víťovi za pomoc při psaní práce, cenné připomínky a rady na konzultacích.

Název práce: Viditelně ireducibilní polynomy

Autor: Kateřina Bžatková

Katedra: Katedra algebry

Vedoucí bakalářské práce: Mgr. Vítězslav Kala, Ph.D., katedra algebry

Abstrakt: Práce se zabývá ireducibilitou polynomů nad konečnými tělesy. Článek Evan M. O'Dorney, Visibly irreducible polynomials over finite fields, při dokazování ireducibility používá viditelně ireducibilního rozkladu VID, což je rozklad, ze kterého lze ireducibilitu snadno vyčíst. V práci podrobně zpracujeme výsledky z tohoto článku. Dále zobecníme definici VID ze zmiňovaného článku vynecháním podmínky na některé stupně polynomů.

Klíčová slova: ireducibilní polynomy, viditelně ireducibilní rozklad,
působení grupy na množině

Title: Visibly irreducible polynomials

Author: Kateřina Bžatková

Department: Department of algebra

Supervisor: Mgr. Vítězslav Kala, Ph.D., department of algebra

Abstract: Thesis is focused on the irreducibility of polynomials over finite fields. Paper Evan M. O'Dorney, Visibly irreducible polynomials over finite fields, when prooving irreducibility uses visibly irreducible decomposition VID, which is type of decomposition easily determinating irreducibility. In the thesis we analyse in detail results from this paper. Furthermore we generalize the definition of VID from mentioned paper by omitting a condition on any degree of polynomials.

Keywords: irreducible polynomials, visibly irreducible decomposition,
group action

Obsah

Úvod

Ireducibilita polynomů je často zkoumané téma. Především nad konečnými tělesy se poznatky mohou využít například v kryptografii a jiných oblastech.

Uveďme článek autora Evan M. O'Dorney, Visibly irreducible polynomials over finite fields [1], ve kterém se na prokazování ireducibility polynomů podívali odlišným způsobem. Místo testování ireducibility hrubou silou se snažili najít takový rozklad, ze kterého je ireducibilita vidět okamžitě. Tato práce ze zmiňovaného článku vychází, zobecňuje jimi používanou definici a rozšiřuje tak některé věty a lemmata, které se ve článku nachází.

Nejdříve ukažme, jak takové rozklady vypadají. Uveďme jako příklad x^2+x+1, což je ireducibilní kvadratický polynom nad tělesem $\mathbb{F}_2$. Polynom přepíšeme do tvaru

$$f_1(x) = x^2 + x + 1 = (x)^2 + (x + 1)$$

Kvadratický polynom je ireducibilní, pokud není dělitelný žádným lineárním polynomem, tedy pokud nemá žádný kořen. Nad $\mathbb{F}_2$ můžeme mít konkrétně dva kořeny 0, 1. Hned vidíme, že 0 je kořenem prvního sčítance, ale nikoli druhého a naopak 1 je kořenem druhého, ale není kořenem prvního.

Pro stejný polynom můžeme takovýchto vyjádření napsat více.

$$f_1(x) = (x + 1)^2 + (x)$$
$$f_1(x) = (x)(x + 1) + 1$$

Opět 0, 1 jsou kořeny pouze jednoho ze sčítanců, tedy celkově nemohou být kořeny polynomu $f_1(x)$.

Pro polynomy stupně 4 je takové vyjádření složitější.

$$f(x) = x^4 + x + 1 = (x)^4 + (x + 1)$$

Je sice vidět, že polynom nemá žádný kořen, ale to nám ireducibilitu ještě nezaručuje, protože $f_2(x)$ se může rozkládat na dva ireducibilní kvadratické polynomy.

Předpokládejme, že víme, že $x^2 + x + 1$ je jediný ireducibilní polynom nad $\mathbb{F}_2$.

$$f_2(x) = x(x + 1)(x^2 + x + 1) + 1$$

Nyní už vidíme, že ani žádný kvadratický polynom nedělí $f_2(x)$ a tedy, že $f_2(x)$ je skutečně ireducibilní.

Jako další příklad zmíníme opět kvadratický polynom, ale tentokrát nad tělesem $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$.

$$f_3(x) = (1 + \alpha)x^2 + x + 1 = x(x - \alpha) + \alpha(x - 1)(x - \alpha - 1)$$

Z rozkladu je patrné, že 0, α jsou kořeny pouze prvního sčítance a 1, $\alpha + 1$ jsou kořeny pouze druhého sčítance, tedy celkově polynom nemá žádný kořen a je ireducibilní.

Takovými pěknými rozklady, ze kterých lze snadno vyčíst ireducibilitu, se bude tato práce zabývat.

Jak už vypovídá název, celá práce se zaměřuje polynomy nad konečnými tělesy, proto první kapitolu budeme věnovat právě jim. Ze skript Konečná tělesa [2] a ze skript Základy algebry [3], zmíníme pár definic a tvrzení, které budeme nadále v práci využívat.

Ve druhé kapitole zmíníme pojem viditelně ireducibilní rozklad VID, což bude přesně rozklad motivovaný příklady výše. Dále uvedeme větu, která bude určovat pro které polynomy rozklady VID existují.

Hned v další kapitole výrazně omezíme parametry polynomů, pro které mohou rozklady VID existovat. Parametry polynomů tady myslíme jejich stupně a tělesa nad kterými jsou polynomy definovány.

Při nacházení rozkladů VID se budeme snažit rozdělit polynomy do skupin, aby se dokazování existence VID zjednodušilo. Budeme k tomu využívat část algebry zabývající se působením grupy na množině. V našem případě půjde o grupu regulárních matic na množině homogenních forem. Homogenní formy jsme zvolili proto, že působení se na homogenních formách se lépe zkoumá.

Třetí kapitola se proto zabývá homogenními formami a jejich korespondencí s polynomy v jedné proměnné.

Ve čtvrté kapitole se zaměříme na grupu regulárních matic a následně její faktorgrupu Γ. Ukážeme, že k hledání rozkladu VID nám stačí zkoumat právě jen působení faktorgrupy. Zjistíme, že rozdělení polynomů, respektive homogenních forem, do výše zmíněných skupin odpovídá nalezení Γ orbit.

Poslední část bude věnována nalezení a sestavování rozkladů VID. Budeme se snažit postupovat co nejvíc obecně a využívat k tomu všech poznatků z předchozích kapitol.

1. Konečná tělesa

V první kapitole ze skript Konečná tělesa [2] shrneme základní pojmy a tvrzení, které budeme v této v práci dále potřebovat.

1.1 Konečná tělesa a jejich podtělesa

Tvrzení 1 (O existenci a jednoznačnosti konečných těles)**.**

- *Každé konečné těleso má p^n prvků, kde p je prvočíslo a n je přirozené číslo.*
- *Pro každé prvočíslo p a přirozené číslo n existuje těleso s $q = p^n$ prvky.*
- *Libovolná dvě tělesa s p^n prvky jsou izomorfní.*

Poznámka. Těleso s q prvky značíme $\mathbb{F}_q$.

Definice 2 (podtěleso)**.** *Těleso $\mathbb{K}$ nazýváme podtělesem tělesa $\mathbb{F}$, pokud $\boldsymbol{K}$ je podmnožinou $\boldsymbol{F}$ a operace $+,\cdot$ se v tělesech $\mathbb{K}$ a $\mathbb{F}$ shodují. Značíme $\mathbb{K} \leq \mathbb{F}$.*

Tvrzení 3. *[O podtělesech konečných těles]Každé podtěleso tělesa $\mathbb{F}_{p^n}$ má p^m prvků pro nějaké m dělící n. Pro každé $m|n$ existuje právě jedno podtěleso tělesa $\mathbb{F}_{p^n}$, které má p^m prvků (a je tvořeno právě prvky $a \in \mathbb{F}_{p^n}$ pro něž $a^{p^m} = a$).*

Uveďme jeden příklad, který tvrzení 3 přímo využívá.

Příklad 4. *Všechna podtělesa $\mathbb{F}_{2^{30}}$ jsou $\mathbb{F}_2$, $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^5}$, $\mathbb{F}_{2^6}$, $\mathbb{F}_{2^{10}}$, $\mathbb{F}_{2^{15}}$, $\mathbb{F}_{2^{30}}$.*

1.2 Algebraický uzávěr

V této sekci zmíníme pojmy algebraické rozšíření, uzavřené těleso a algebraický uzávěr.

Definice 5 (algebraicky uzavřené těleso)**.** *Těleso $\mathbb{F}$ je algebraicky uzavřené, pokud každý polynom $\in \mathbb{F}[x]$ má v $\mathbb{F}$ kořen.*

Poznámka. Indukcí lze snadno dokázat, že pokud je $\mathbb{F}$ algebraicky uzavřené těleso, potom se každý nekonstantní polynom nad $\mathbb{F}$ rozkládá na lineární členy.

Příklad 6.

- *$\mathbb{R}$ není algebraicky uzavřené těleso, protože polynom x^2+1 nemá v $\mathbb{R}$ kořen.*
- *Ze základní věty algebry plyne, že $\mathbb{C}$ je algebraicky uzavřené.*
- *Žádné konečné těleso nemůže být algebraicky uzavřené.*
  Označíme-li $a_1, \ldots, a_n$ jeho prvky, pak polynom $(x - a_1) \cdot \cdots \cdot (x - a_n) + 1$ nemá v tomto tělese kořen.

Pokud k tělesu přidáme přidáme jakýkoliv prvek, dostaneme obecně jeho rozšíření. Nás dále budou zajímat ty případy, kdy přidáme pouze algebraické prvky.

Definice 7 (algebraické rozšíření tělesa)**.** *Mějme tělesová rozšíření $\mathbb{S} \geq \mathbb{F}$. Řekneme, že $\mathbb{S}$ je algebraické rozšíření $\mathbb{F}$, pokud všechny prvky v $\mathbb{S}$ jsou algebraický nad $\mathbb{F}$. (tj. každý prvek v $\mathbb{S}$ je kořenem nějakého polynomu z $\mathbb{F}[x]$).*

Definice 8 (algebraický uzávěr)**.** *Algebraickým uzávěrem tělesa $\mathbb{F}$ rozumíme jeho algebraické rozšíření, které je navíc algebraicky uzavřené.*

Poznámka. Algebraický uzávěr tělesa $\mathbb{F}$ značíme $\bar{\mathbb{F}}$.

Příklad 9.

- $\mathbb{C}$ *je algebraickým uzávěrem* $\mathbb{R}$.
- $\mathbb{C}$ *není algebraickým uzávěrem* $\mathbb{Q}$*, protože např. prvek* π *není kořenem žádného polynomu nad* $\mathbb{Q}$.

Poznámka. Algebraický uzávěr existuje pro každé těleso $\mathbb{F}$ a zároveň každé jeho dva algebraické uzávěry jsou $\mathbb{F}$- izomorfní.

Konkrétně nás bude zajímat algebraický uzávěr konečného tělesa.

Tvrzení 10. *Nechť $\mathbb{F}_q$ je konečné těleso a m je přirozené číslo. Pak existuje ireducibilní polynom $f(x) \in \mathbb{F}_q[x]$ stupně m.*

Tvrzení 11. *Kořenové rozšíření konečného tělesa $\mathbb{F}_q$ určené ireducibilním polynomem $f(x)$ je rozkladovým rozšířením $\mathbb{F}_q$ určeným $f(x)$. Speciálně $\mathbb{F}_{q^m}$ je rozkladové rozšíření $\mathbb{F}_q$ určené libovolným ireducibilním polynomem $f(x) \in \mathbb{F}_q[x]$ stupně m.*

Důsledek 12. *Pro každé $m \in \mathbb{N}$ a těleso $\mathbb{F}_q$ platí, že $\mathbb{F}_{q^m} \leq \bar{\mathbb{F}}_q$.*

Příklad 13. *Mějme tělesa $\mathbb{F}_q, \mathbb{F}_{q^2}, \ldots, \mathbb{F}_{q^m}$. Díky důsledku víme, že to jsou podtělesa tělesa $\bar{\mathbb{F}}_q$. Položme $N = NSN(1, \ldots, m)$. $\mathbb{F}_{q^N}$ je opět podtěleso $\bar{\mathbb{F}}_q$ a díky tvrzení 3 víme, že pro všechna $i = 1, \ldots, m$ platí, že $\mathbb{F}_{q^i}$ je podtěleso $\mathbb{F}_{q^N}$.*

Dále budeme potřebovat spočítat velikost sjednocení těles.

Poznámka. Díky lemmatu tělesa $\mathbb{F}_q, \mathbb{F}_{q^2}, \ldots, \mathbb{F}_{q^m}$ umíme mezi sebou uspořádat ve vztahu podtěleso, nadtěleso. Při počítaní velikosti sjednocení má cenu uvažovat jen tělesa, které jsou maximálními prvky tohoto uspořádání, protože prvky všech jejich podtěles jsou v nich už obsaženy.

Nyní budeme postupovat podle principu inkluze a exkluze. Vezmeme tělesa, která jsou maximálními prvky zmíněného uspořádání a sečteme počty prvků těchto těles. Dále odečteme prvky, které leží v průniku každých dvou z nich, protože jsme je započítali dvakrát. Potom přičteme prvky které leží v průniku každých třech z nich atd.

Uveďme konkrétní příklad.

Příklad 14. *Mějme tělesa $\mathbb{F}_q, \mathbb{F}_{q^2}, \ldots, \mathbb{F}_{q^6}$. Spočtěme, že $N = NSN(1, \ldots, 6) = 60$. Už víme, že pro $i = 1, \ldots, 6$ jsou $\mathbb{F}_{q^i}$ podtělesa $\mathbb{F}_{q^6}$0. Z tvrzení 3 také víme, že $\mathbb{F}_q \leq \{\mathbb{F}_{q^2}, \mathbb{F}_{q^3}, \mathbb{F}_{q^5}\}$, $\mathbb{F}_{q^2} \leq \{\mathbb{F}_{q^4}, \mathbb{F}_{q^6}\}$, $\mathbb{F}_{q^3} \leq \mathbb{F}_{q^6}$. Velikost sjednocení spočteme podle předchozí poznámky.*

$$\left| \bigcup_{i=1}^{6} \mathbb{F}_{2^i} \right| = \mathbb{F}_{2^4} + \mathbb{F}_{2^5} + \mathbb{F}_{2^6} - \mathbb{F}_{2^2} - \mathbb{F}_2 - \mathbb{F}_2 + \mathbb{F}_2 = 106$$

2. Viditelně ireducibilní tvar polynomu

Jak jsme už naznačili v úvodu, naším cílem bude elegantně prokázat ireducibilitu polynomů. Pro daný polynom f se budeme snažit najít vhodný rozklad na součet jiných polynomů, aby z rozkladu bylo vidět, že f je skutečně ireducibilní.

Konkretní příklad takového rozkladu jsme už ukázali v úvodu, uveďme obecnou definici.

Definice 15 (viditelně ireducibilní rozklad)**.** *Nechť q je mocnina prvočísla, $r \geq 2$, f je polynom stupně $d \geq 2$ nad konečným tělesem $\mathbb{F}_q$.*
Potom součet $f_1(x) + ... + f_r(x) = f(x)$, kde $\deg f_i \leq d$, $f_i \in \mathbb{F}_q[x]$, nazveme viditelně ireducibilní rozklad (VID)*, pokud je splněna následující podmínka:*

(VID-1) Každý ireducibilní polynom $p(x)$ stupně nejvýše $d/2$ dělí všechny až na právě jeden $f_i(x)$.

Poznámka. Z definice přímo plyne několik pozorování:

- pro všechny $p(x)$ z podmínky (VID-1) platí, že $p(x) \nmid f(x)$, neboli $f(x)$ je ireducibilní polynom
- aspoň jeden z polynomů f_i musí být stupně právě d, jinak by ani součet $f = f_1 + \cdots + f_r$ nemohl být stupně d
- definice 15 připouští, že součet $f_1 + \cdots + f_r$ je VID, jen pokud i tento součet je stupně právě d.

Jestliže aspoň mají dva polynomy stupeň právě d, pak přesto může může nastat, že jejich součet bude stupně $< d$ (protože součet jejich vedoucích koeficientů se může rovnat 0).

Příklad 16. *Počítejme nad tělesem $\mathbb{Z}_5$.*

- $f_1(x) + f_2(x) = 3x(x+1)(x+2) + 2(x+3)^2(x+4)$.
  Po roznásobení $f_1(x) + f_2(x) = 3x^3 + 4x^2 + x + 2x^3 + x + 2 = 4x^2 + 2x + 2$ dostaneme polynom stupně 2. Tedy $\deg(f_1 + f_2) < \deg f_1, \deg f_2$. Tedy $f_1(x) + f_2(x)$ není VID.
- $f_3(x) + f_4(x) = 3x(x+1)(x+2) + (x+3)^2(x+4)$.
  Nyní po roznásobení $f_3(x) + f_4(x) = 3x^3 + 4x^2 + x + x^3 + 3x + 1 = 4x^3 + 4x^2 + 4x + 1$ dostaneme polynom stupně 3. Navíc vidíme, že $f_3(x) + f_4(x)$ splňuje podmínku VID-1, Tedy $f_3(x) + f_4(x)$ je VID.

Obecně tedy není zaručeno, že součet $f_1 + \cdots + f_r$, kde $\deg f_i \leq d$, přestože splňuje podmínku (VID-1), je skutečně VID. Proto se v úvodu článku [1] uvádí druhá definice, která sice připouští rozkladů méně, ale stupeň výsledného součtu f je vidět okamžitě.

Definice 17 (silný viditelně ireducibilní rozklad)**.** *Nechť je q mocnina prvočísla, $r \geq 2$, f je polynom stupně $d \geq 2$ nad konečným tělesem $\mathbb{F}_q$.*
Potom součet $f_1(x) + ... + f_r(x) = f(x)$, $\deg f_i \leq d$, $f_i \in \mathbb{F}_q[x]$, nazveme silný viditelně ireducibilní rozklad (VID-S)*, pokud jsou splněny následující podmínky:*

(VID-1) Každý ireducibilní polynom $p(x)$ stupně nejvýše $d/2$ dělí všechny až na právě jeden $f_i(x)$.

(VID-2) Právě jeden polynom $f_i(x)$ má stupeň d. Ostatní členy mají stupeň menší než d.

V této práci se ovšem zaměříme na definici 15. Následující věta je zobecněnější verzí věty 1 z článku [1] právě proto, že se odkazuje na obecnější definici VID a říká nám, pro které polynomy dokážeme jejich viditelně ireducibilní rozklad najít. Důkaz následující věty bude jedním z hlavních výsledků této práce.

Věta 18.

(a) Pokud (q,d) je jedna z následujících dvojic, potom pro každý ireducibilní polynom nad konečným tělesem $\mathbb{F}_q$ stupně d existuje VID,

- *(2,2), (3,2), (4,2)*
- *(2,3), (3,3), (4,3), (5,3)*
- *(2,4)*
- *(2,5)*
- *(2,6)*
- *(2,7)*

(b) Pro (q,d) = (3,5) platí, že právě polovině ireducibilních polynomů stupně 3 nad tělesem $\mathbb{F}_5$ odpovídá VID.

(c) Pro všechny ostatní dvojice (q,d) platí, že žádný ireducibilní polynom stupně d nad $\mathbb{F}_q$ nemá odpovídající VID.

3. Omezení dvojic (q,d)

V dokazování věty 18 začneme částí c). Pomocích následujících lemmat ukážeme, že seznam dvojic (q,d), pro které existují polynomy s rozkladem VID, je omezený. Lemmata jsou obdobou lemmat z první kapitoly článku [1], avšak pro naši obecnější definici mají trochu odlišné znění .

Lemma 19. *Nechť je q mocnina prvočísla, $r \geq 2$ a $f_1(x) + \cdots + f_r = f(x)$ je VID stupně d nad konečným tělesem $\mathbb{F}_q$. Potom:*

$$dr \geq (r-1)\left|\bigcup_{n=1}^{\lfloor d/2 \rfloor} \mathbb{F}_{q^n}\right| \tag{3.1}$$

Poznámka. Sjednocení konečných těles uvažujeme v algebraickém uzávěru $\bar{\mathbb{F}}_q$. V první kapitole jsme uvedli poznámku a příklad, jak velikost sjednocení spočítat.

Důkaz. Nechť $\xi \in \mathbb{F}_{q^n}$, $1 \leq n \leq \lfloor d/2 \rfloor$ a m_ξ jeho monický minimální polynom nad $\mathbb{F}_q$. Stupeň minimálního polynomu je roven algebraickému stupni rozšíření, tedy:

$$\deg(m_\xi) = |\mathbb{F}_q(\xi) : \mathbb{F}_q| \leq n \leq \lfloor d/2 \rfloor$$

Z definice minimálního polynomu musí být m_ξ ireducibilní, tedy podle podmínky VID-1 musí dělit všechny až na právě jeden z polynomů $f_1,\ldots,f_r$. Odtud ξ je minimálně $(r-1)$ násobný kořen polynomu $f_1 \cdots f_r$.

Uvažujme všechny možné n a všechny možné prvky $\xi \in \mathbb{F}_{q^n}$, potom $f_1 \cdots f_r$ má minimálně $(r-1)\left|\bigcup_{n=1}^{\lfloor d/2 \rfloor} \mathbb{F}_{q^n}\right|$ kořenů. Stupeň polynomu $f_1 \cdots f_r$ je podle definice VID maximálně $d \cdot r$.

Protože stupeň polynomu je větší nebo roven počtu kořenů polynomu, dostáváme následující nerovnost: $dr \geq (r-1)\left|\bigcup_{n=1}^{\lfloor d/2 \rfloor} \mathbb{F}_{q^n}\right|$.

□

Pokud pro polynom stupně d nad tělesem $\mathbb{F}_q$ existuje rozklad VID, potom q, d musí splňovat nerovnost (3.1). Následující lemma udává, pro které dvojice (q,d) nerovnost platí.

Lemma 20. *Nechť q je mocnina prvočísla, $r \geq 2$. Žádné jiné dvojice (q,d), než které určuje věta 18(a),(b), nerovnost*

$$dr \geq (r-1)\left|\bigcup_{n=1}^{\lfloor d/2 \rfloor} \mathbb{F}_{q^n}\right|$$

nesplňují.

Důkaz. Nerovnost převedeme do tvaru:

$$d\left(\frac{r}{r-1}\right) \geq \left|\bigcup_{n=1}^{\lfloor d/2 \rfloor} \mathbb{F}_{q^n}\right|$$

Po vynechání členů ve sjednocení až na člen, kde $n = \lfloor d/2 \rfloor$ dostaneme:

$$d\left(\frac{r}{r-1}\right) \geq \left|\mathbb{F}_{q^{\lfloor d/2 \rfloor}}\right| = q^{\lfloor d/2 \rfloor}$$

Nechť $r_1 \leq r_2$, potom $\frac{r_1}{r_1-1} \geq \frac{r_2}{r_2-1}$. Protože zároveň $r \geq 2$:

$$\begin{aligned} 2d = d\left(\frac{2}{2-1}\right) \geq d\left(\frac{r}{r-1}\right) \geq q^{\lfloor d/2 \rfloor} \\ \Rightarrow 2d \geq q^{\lfloor d/2 \rfloor} \end{aligned} \tag{3.2}$$

Protože q je mocnina prvočísla, máme $q \geq 2$ a platí:

$$2d \geq q^{\lfloor d/2 \rfloor} \geq 2^{\lfloor d/2 \rfloor} \tag{3.3}$$

Nyní dokážeme určit základní odhad pro d.
Položme $d = 2k + \varepsilon,\ k \in \mathbb{N},\ \varepsilon \in \{0,1\}$

$$\begin{aligned} 2d &\geq 2^{\lfloor d/2 \rfloor} \\ 2(2k+\varepsilon) &\geq 2^k \end{aligned}$$

- $\epsilon = 0,\ 4k \geq 2^k \Rightarrow k \leq 4 \Rightarrow d \leq 8$
- $\epsilon = 1,\ 4k + 2 \geq 2^k \Rightarrow k \leq 4 \Rightarrow d \leq 9$

Odtud vidíme, že nerovnost (3.3) je splněna pouze pro $d \leq 9$.

Všimneme si, že pár možností můžeme hned vyloučit. Detailněji si rozepíšeme dva případy.

- Případ $d = 9$.
  $18 = 2d \geq |\mathbb{F}_{q^3} \cup \mathbb{F}_{q^3}| = q^3 + q^4 - q \geq 8 + 16 - 2 = 22$. Což je spor, proto $d \neq 9$.
- Stejným způsobem rozvedeme případ $d = 8$.
  $16 = 2d \geq |\mathbb{F}_{q^3} \cup \mathbb{F}_{q^4}| = q^3 + q^4 - q \geq 8 + 16 - 2 = 22$. Opět spor, $d \neq 8$.

$\Rightarrow 2 \leq d \leq 7$ (z definice VID $d \neq 1$).

Z rovnice (3.2) vyjádříme q, čímž dostaneme podmínku pro q v závislosti na d.

$$q \leq d^{\frac{1}{\lfloor d/2 \rfloor}}$$

Dosadíme jednotlivé hodnoty d a spočítáme konktrétní vyhovující dvojice (q,d).

d	$q \leq 2d^{\frac{1}{\lfloor d/2 \rfloor}}$	q
2	$q \leq 4^1$	2,3,4
3	$q \leq 6^1$	2,3,4,5,$\emptyset$
4	$q \leq 8^{\frac{1}{2}}$	2
5	$q \leq 10^{\frac{1}{2}}$	2,3
6	$q \leq 12^{\frac{1}{3}}$	2
7	$q \leq 14^{\frac{1}{3}}$	2

Možnost $d = 3,\ q = 6$ je neplatná, protože q značí velikost konečného tělesa, což musí být vždy p^k, pro p prvočíslo, $k \in \mathbb{N}$. Dostali jsme přesně dvojice jako ve větě 18.

□

Tímto je dokázána část c) věty 15, protože lemma 20 nám všechny ostatní dvojice, než které jsou uvedeny v částech a), b) věty 18 vylučuje.

4. Homogenní formy

Od polynomů jedné proměnné přejdeme k homogenním formám. Jak už jsme zmiňovali v úvodu bude s nimi lépe pracovat při zkoumání působení grupy regulárních matic.

Dále ukážeme jakým způsobem si polynomy a homogenní formy odpovídají a jak lze mezi nimi přecházet.

Definice 21 (Homogenní forma)**.** *Nechť $n, d, r \in \mathbb{N}$. Řekneme, že F je homogenní forma stupně d v n proměnných $X_1, \ldots, X_n$, jestliže*

$$F = \sum_{i=1}^{r} F_i,$$

$$kde\ F_i = konst \prod_{j=1}^{n} {X_j}^{k_j},\ \deg(F_i) = \sum_{j=1}^{r} k_j = d,\ \forall i = 1, \ldots r.$$

Neboli, homogenní forma má všechny nenulové členy stejného stupně d.

Příklad 22. *$X^4 + 3XY^3 + Y^4$ je homogenní forma ve dvou proměnných, která má stupeň* 4.

K důkazu věty 15 budeme využívat homogenní formy ve dvou proměnných, proto se nadále budeme zabývat pouze jimi.

Definice 23 (Ireducibilní homogenní forma)**.** *Homogenní forma $F(X,Y)$ je ireducibilní, jestliže nelze rozložit na součin jiných homogenních forem stupně aspoň* 1.

Poznámka. Forma $F(X,Y) = 3(X + Y)$ je ireducibilní, protože ji dělí pouze konstanta.

Mezi polynomy jedné proměnné a homogenními formami ve dvou proměnných dokážeme snadno přecházet pomocí následujících zobrazení.

Definice 24 (Homogenizace)**.** *Nechť $d \in \mathbb{N}$. Potom homogenizace polynomu polynomu $f(x)$ na homogenní formu stupně d je zobrazení:*
$f(x) \mapsto F(X,Y) = Y^d f\left(\frac{X}{Y}\right)$

Poznámka. Z definice vyplývá, že polynom $f(x)$ musí být stupně nejvýše d, jinak by totiž výsledná homogenní forma měla v některých členech jako proměnné zlomky.

Definice 25 (Dehomogenizace)**.** *Dehomogenizace homogenní formy na polynom $f(x)$ je zobrazení: $F(X,Y) \mapsto f(x) = F(x,1)$*

Poznámka.

- Stupeň $f(x)$ je roven nejvyšší mocnině u proměnné X v $F(X,Y)$.

- Každý polynom $f(x)$ stupně nejvýše d se *homogenizací* zobrazí na homogenní formu $F(X,Y)$ stupně právě d. Tato forma se následnou dehomogenizací zobrazí zpátky na polynom $f(x)$.
- Obě zobrazení jsou dobře definovaná, tedy jednoznačná.

Odtud vidíme, že homogenizace a dehomogenizace jsou navzájem inverzní zobrazení a mezi homogenními formami stupně d a polynomy v jedné proměnné stupně nejvýše d existuje bijekce.

Homogenizace, která zachovává stupeň, tedy polynom stupně d zobrazí na formu stupně d, zachovává dokonce ireducibilitu.

Lemma 26. *Nechť polynom $f(x)$ stupně d se homogenizací se zobrazí na formu $F(X,Y)$ také stupně d. Potom $f(x)$ je ireducibilní $\Leftrightarrow$ $F(X,Y)$ je ireduciblní.*

Důkaz. "$\Rightarrow$" Předpokládejme, že $f(x)$ není ireducibilní, $f(x) = f_1(x) \cdots f_r(x)$. Potom $F(X,Y) = F_1(X,Y) \cdots F_r(X,Y)$, kde $F_i(X,Y)$ vznikne homogenizací $f_i(x)$.
"$\Leftarrow$" Nechť $F(X,Y)$ není ireducibilní, tedy $F(X,Y) = F_1(X,Y) \cdots F_r(X,Y)$. Potom $f(x) = f_1(x) \cdots f_1(x)$, kde $f_i(x)$ vznikne dehomogenizací $F_i(X,Y)$. Nyní by mohlo pro nějaké i nastat, že $f_i(x) = 1$. Potom by nebylo jasné, že $f(x)$ není ireducibilní. Jenže to nastane jen v případě, že některá z forem $F_i(X,Y) = Y^k$, tedy pokud $Y|F(X,Y)$. Potom by ale v $F(X,Y)$ neexistovala forma X^d a tedy $f(x)$ by nebylo stupně d.

□

Předpoklad, že homogenizace zachovává stupeň je nezbytný, protože by forma $F(X,Y)$ byla dělitelná Y.

Ve druhé kapitole jsme zavedli rozklad VID, pro homogenní formy definujme ekvivalentní rozklad HVID.

Definice 27 (homogenní tvar HVID)**.** *Nechť q je mocnina prvočísla, $r \geq 2$, $F(X,Y)$ je homogenní forma stupně $d \geq 2$ nad konečným tělesem $\mathbb{F}_q$.*
Potom součet $F_1(X,Y) + ... + F_r(X,Y) = F(X,Y)$, $F_i \in \mathbb{F}_q(X,Y)$, $degF_i = d$, nazveme homogenní tvar viditelně ireducibilní rozkladu (HVID)*, pokud je splněna následující podmínka:*

(HVID-1) Pro každou ireducibilní homogenní formu $P(X,Y)$ tž. $P(X,Y) \neq Y$ stupně nejvýše $d/2$ existuje právě jedno j tž. $P(X,Y) \nmid F_j(X,Y)$ a zároveň pro všechna $i \neq j$ platí, že $P(X,Y) \mid F_i(X,Y)$.

(HVID-2) Lineární forma $Y \nmid F(X,Y)$

Poznámka. Z definice přímo vyplývá, že $P(X,Y) \nmid F(X,Y)$ pro všechny $P(X,Y)$ ireducibilní homogenní formy stupně nejvýše $d/2$. Tedy HVID je skutečně ireducibilní homogenní forma.

Lineární forma $P(X,Y) = Y$ se dehomogenizací zobrazí na $p(x) = 1$. Pokud forma Y dělí F_i stupně d, znamená to, že po dehomogenizaci F_i dostaneme polynom $f_i(x)$ stupně $< d$.

Pokud by i lineární forma Y musela splňovat podmínku HVID-1, potom by rozklad $f_1 + \cdots + f_r = f(x)$ nutně splňoval podmínku VID-2. To ale v naší definici VID nevyžadujeme, proto i $P(X,Y) = Y$ v podmínce HVID-1 chybí.

Odtud plyne užitečné lemma.

Lemma 28. *Mějme homogenní formu $F(X,Y)$, který dostaneme homogenizací polynomu $f(x)$. Definice HVID je stavěna tak, aby VID polynomu $f(x)$ odpovídalo po homogenizaci HVID formy $F(X,Y)$ a naopak.*

Ve druhé kapitole jsme také zmínili definici VID-S, ve 2. kapitole článku [1] je k ní uvedena ekvivalentní definice HVID-S pro homogenní formy.

Definice 29 (homogenní tvar HVID-S)**.** *Nechť q je mocnina prvočísla, $r \geq 2$, $F(X,Y)$ je homogenní forma stupně $d \geq 2$ nad konečným tělesem $\mathbb{F}_q$.*
Potom součet $F_1(X,Y) + ... + F_r(X,Y) = F(X,Y)$, $F_i \in \mathbb{F}_q(X,Y)$, $degF_i = d$, nazveme homogenní tvar viditelně ireducibilní rozkladu (HVID-S)*, pokud je splněna následující podmínka:*

(HVID-S1) Pro každou ireducibilní homogenní formu $P(X,Y)$ stupně nejvýše $d/2$ existuje právě jedno j tž. $P(X,Y) \nmid F_j(X,Y)$ a zároveň pro všechna $i \neq j$ platí, že $P(X,Y) \mid F_i(X,Y)$.

5. Grupové působení na množinu homogenních forem

V této kapitole se zaměříme na grupu regulárních matic $GL_2(\mathbb{F}_q)$ a především její faktorgrupu $PGL_2(\mathbb{F}_q)$. Budeme zkoumat její působení na množinu homgenních forem, což nám pomůže ke zjednodušení důkazu věty 18.

5.1 Působení faktorgrupy $PGL_2(\mathbb{F}_q)$

Začneme zmíněním definic z algebry.

Definice 30 (Působením grupy G na množině X)**.** *rozumíme homomorfismus*

$$\pi\colon \boldsymbol{G} \to \boldsymbol{S}_X,$$
kde $\boldsymbol{S}_X$ *je permutační grupa na množině* X*.*

Neboli homomorfismus π přiřadí každému prvku $g \in \mathbf{G}$ nějakou permutaci σ, kde σ je permutace na prvcích množiny X.

Poznámka. Hodnotu permutace $\pi(g)$ na prvku $x \in X$ (neboli $\pi(g)(x)$) obvykle značíme krátce $g(x)$.

Připomeňmě ještě jeden pojem z lineární algebry. Regulární matice je čvercová matice, která má všechny sloupce lineárně nezávislé .

Definice 31 (Lineární grupa $GL_n(\mathbb{F}_q)$)**.**
$GL_2(\mathbb{F}_q) = (\{M : M$ *je regulární matice* $n \times n$ *nad tělesem* $\mathbb{F}_q\}, \cdot\ , {}^{-1}, I_n)$.

Konktrétně nás bude zajímat její faktorgrupa.

Definice 32 (Faktorgrupa Γ)**.**
$\Gamma = PGL_2(\mathbb{F}_q) = GL_2(\mathbb{F}_q)/Z(\mathbb{F}_q^*)$, *kde* $Z(\mathbb{F}_q^*)$ *je multiplikativní grupa skalárních matic* $\{\alpha I_2,\ \alpha \in \mathbb{F}_q^*\}$.

Poznámka. Velikost grupy Γ dokážeme spočítat.
Nejprve vyjádříme počet prvků grupy $GL_2(\mathbb{F}_q)$, což jsou regulární matice nad $\mathbb{F}_q$ o rozměrech 2×2. Pro první sloupec máme $q^2 - 1$ možností, protože první sloupec nesmí být nulový. Pro druhý sloupec nám zbývá $q^2 - q$ možností, protože aby matice byla regulární, nesmí být druhý sloupec q-násobkem prvního. Odtud $|GL_2(\mathbb{F}_q)| = (q^2-1)(q^2-q)$. Dále víme,že $\left|Z(\mathbb{F}_q^*)\right| = q - 1$. Potom

$$|\Gamma| = |GL_2(\mathbb{F}_q)| \,/\, |Z(\mathbb{F}q^*)| = \frac{(q^2-1)(q^2-q)}{q-1} = q(q-1)(q+1) \tag{5.1}$$

.

Všimneme si, že dvě matice M, N jsou ve stejné rozkladové třídě této faktorgrupy, pokud $M = \alpha N$ pro nějaké $\alpha \in \mathbb{F}_q^*$.

Definice 33. *[Působení grupy $GL_2(\mathbb{F}_q)$ na množině homogenních forem]*
Nechť $M \in GL_2(\mathbb{F}_q)$, $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $F(X,Y)$ je homogenní forma. M působí na $F(X,Y)$ následovně:
$M(F(X,Y)) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} (F(X,Y)) = F(\alpha X + \gamma Y, \beta X + \delta Y)$.

Uveďme ještě jednu definici.

Definice 34. *[Působení grupy $GL_2(\mathbb{F}_q)$ na množině prvků tělesa $\mathbb{F}_{q^d}$]*
Nechť $M \in GL_2(\mathbb{F}_q)$, $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $\xi \in \mathbb{F}_{q^d}$. M působí na ξ následovně:
$M(\xi) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} (\xi) = \frac{\delta\xi - \gamma}{-\beta\xi + \alpha}$.

Na příkladě ukážeme jakým způsobem si obě definice odpovídají.

Příklad 35. *Mějme $M \in GL_2(\mathbb{F}_q)$, $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ a $F = (X - \xi Y)$ homogenní formu, která má prvek ξ za kořen. Podíváme se na působení matici M na formu F.*

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} (X - \xi Y) = (\alpha X + \gamma Y - \xi(\beta X + \delta Y))$$
$$= (\alpha - \xi\beta)X + (\gamma - \delta\xi)Y = (\alpha - \xi\beta)(X + \tfrac{\gamma - \xi\delta}{\alpha - \xi\beta} Y)$$

Vidíme, že forma F se zobrazila na $(\alpha - \xi\beta)(X - \xi Y)$, kde $(\alpha - M(\xi)\beta)$ je konstanta v $\mathbb{F}_{q^d}$. Tedy $M(\xi)$ je kořenem $M(x - \xi Y)$, neboli působení Γ zobrazuje kořeny forem opět na kořeny jejich obrazů.

Poznámka.

- Skalární matice αI_2 zobrazí $F(X,Y)$ na $\alpha F(X,Y)$.
- Nechť M,N jsou dvě matice ze stejné rozkladové třídy faktorgrupy Γ. Potom $M = \alpha N$, pro nějaké $\alpha \in \mathbb{F}_q^*$. Nechť $N(F(X,Y)) = F(\bar{X},\bar{Y})$, potom $M(F(X,Y)) = \alpha F(\bar{X},\bar{Y})$.

Důsledek 36. *Matice ze stejné rozkladové třídy faktorgrupy Γ zobrazí homogenní formu $F(X,Y)$ na skalární násobky jiné formy $F(\bar{X},\bar{Y})$.*

5.2 Množina ireducibilních forem $\mathcal{I}(q,d)$

Definice 37. *$\mathcal{I}(q,d)$ je množina všech monických ireducibilních homogenních forem stupně d nad $\mathbb{F}_q$.*

Množina $\mathcal{I}(q,d)$ zahrnuje všechny ireducibilní homogenní formy až na jejich násobky konstantou z $\mathbb{F}_q$.

Definice 38. *$\mathcal{M}(q,d)$ je množina všech monických ireducibilních polynomů v jedné proměnné stupně d nad $\mathbb{F}_q$.*

Lemma 39.
Nechť $d \geq 2$. Množina $\mathcal{I}(q,d)$ je v bijekci s množinou $\mathcal{M}(q,d)$.

Důkaz. Uvažujme homogenizaci $h : \mathcal{M}(q,d) \to \mathcal{I}(q,d)$,
tž. $f(x) \mapsto F(X,Y) = Y^d f(\frac{X}{Y})$.

Homogenizace $f(x) \mapsto F(X,Y) = Y^d f(\frac{X}{Y})$ je dobře definovaná a zřejmě $F(X,Y)$ je stupně d. Z lemmatu 26 plyne, že $F(X,Y)$ je ireducibilní. Navíc protože $f(x)$ je monický, tak i $F(X,Y)$ je monická forma. Odtud plyne, že h je dobře definované.

$F_1 \neq F_2 \Rightarrow Y^d f_1(\frac{X}{Y}) \neq Y^d f_2(\frac{X}{Y}) \Rightarrow f_1(x) \neq f_2(x)$. Odtud plyne, že h je prosté.

Nechť $F(X,Y) \in \mathcal{I}(q,d)$. Víme, že $F(X,Y)$ se dehomogenizací zobrazí jednoznačně na $f(x)$ stupně nejvýše d. Polynom $f(x)$ je zřejmě monický a z lemmatu 26 plyne, že pokud je $f(x)$ stupně d, pak je i ireducibilní. Zbývá dokázat, že $f(x)$ je stupně právě d. $F(X,Y)$ je ireducibilní forma stupně $d \geq 2$, proto nesmí její člen s nejvyšším koeficientem u X obsahovat Y, jinak by $F(X,Y) = Y \cdot G(X,Y)$. Protože $F(X,Y)$ je stupně d, její člen s nejvyšším koeficientem u X musí být X^d, proto $f(x)$ je také stupně d, tedy $f(x) \in \mathcal{M}(q,d)$.

$\Rightarrow h$ je bijekce.

□

Poznámka. Předpoklad $d \geq 2$ je nezbytný, protože ireducibilní lineární forma Y se dehomogenizací zobrazí na polynom 1 stupně 0.

Tohoto lemmatu využijeme při dokazování věty 18. Pokud forma $F(X,Y)$ z $\mathcal{I}(q,d)$ má tvar HVID, potom zřejmě všechny její skalární násobky $Q(X,Y)$ mají také tvar HVID. Podle lemmatu 28 z minulé kapitoly víme, že všechny polynomy jedné proměnné, které vzniknou dehomogenizací forem $Q(X,Y)$ mají tvar VID.

Místo toho abychom pro každý ireducibilní polynom v jedné proměnné stupně d hledali tvar VID, budeme pro každou formu náležející $\mathcal{I}(q,d)$ hledat HVID.

Velikost $\mathcal{I}(q,d)$ umíme určit podle tvrzení ze skript Konečných těles [2]. Aplikací Möbiovy inverzní formule z 5.kapitoly dostaneme následující vzorec:

$$|\mathcal{I}(q,d)| = \begin{cases} \frac{1}{d}\sum_{k|d} \mu(k) q^{d/k}, & d \leq 2 \\ q+1, & d = 1 \end{cases} \tag{5.2}$$

kde $\mu(k)$ je Möbiova funkce:

$$\mu(k) = \begin{cases} 1, & k = 1 \\ (-1)^m, & k \text{ je součin různých } m \text{ prvočísel} \\ 0, & p^2 | k \text{ pro nějaké } p \end{cases}$$

Z minulé sekce připomeňme faktorgrupu $\Gamma = PGL_2(\mathbb{F}_q)$, na kterou se můžeme dívat jako na grupu všech regulárních matic až na násobky konstantou z $\mathbb{F}_q^*$.

V předchozí sekci jsme také vysvětlili, jak grupa $GL_2(\mathbb{F}_q)$ působí na množině všech homogenních forem. Podle důsledku 36, víme, že dvě matice ze stejné třídy

faktorgrupy Γ zobrazí formu F na formy F_1,F_2, kde jedna je násobkem druhé. Tedy obě jsou násobkem jediné formy v $\mathcal{I}(q,d)$.Místo působení $GL_2(\mathbb{F}_q)$ na $\mathcal{I}(q,d)$ tedy stačí uvažovat působení Γ na $\mathcal{I}(q,d)$.

Ukážeme, kdy Γ nemění ireducibilitu forem a zachovává HVID.

Lemma 40. *Nechť $\gamma \in \Gamma$, $F(X,Y) \in \mathcal{I}(q,d)$. Potom $F(X,Y)$ je ireducibilní právě tehdy, když $\gamma(F(X,Y))$ je ireducibilní.*

Důkaz. Nechť $F(X,Y)$ není ireducibilní, tedy $F(X,Y) = G(X,Y)H(X,Y)$, kde $G(X,Y)$, $H(X,Y) \in \mathcal{I}(q,d)$. Potom $\gamma(F(X,Y)) = \gamma(G(X,Y))\gamma(H(X,Y))$.

Naopak předpokládejme, že $\gamma(F(X,Y))$ není ireducibilní, tedy $\gamma(F(X,Y)) = G(X,Y)H(X,Y)$, kde $G(X,Y)$, $H(X,Y) \in \mathcal{I}(q,d)$. Protože γ je regulární matice, existuje k ní inverzní matice γ^{-1}. Potom $F(X,Y) = \gamma^{-1}\gamma(F(X,Y)) = \gamma^{-1}(G(X,Y))\gamma^{-1}(H(X,Y))$.

□

Působení grupy Γ na množině $\mathcal{I}(q,d)$ tedy zachovává ireducibilitu. Se zachováváním existence tvaru HVID je to složitější. Připomeňme definici 51 HVID, ze článku [1]. Potom pro působení Γ na $\mathcal{I}(q,d)$ platí navíc následující lemma.

Lemma 41. *Nechť $\gamma \in \Gamma$, $F(X,Y) \in \mathcal{I}(q,d)$. Potom pro $F(X,Y)$ existuje tvar HVID-S právě tehdy, když pro $\gamma(F(X,Y))$ existuje tvar HVID-S .*

Důkaz. Nechť $F(X,Y)$ má tvar HVID-S. Tedy $F(X,Y) = F_1(X,Y) + \cdots F_r(X,Y)$ a platí že všechny ireducibilní formy $P(X,Y)$ stupně nejvýše $\lfloor d/2 \rfloor$, dělí všechny až na právě jeden sčítanec F_i.

Působením γ dostaneme, že $\gamma(F(X,Y)) = \gamma(F_1(X,Y)) + \cdots \gamma(F_r(X,Y))$, a platí, že všechny formy $\gamma(P(X,Y))$, dělí všechny až na právě jeden sčítanec γF_i. Jak víme z předchozího lemmatu, působení Γ zachovává ireducibilitu, tedy $\gamma P(X,Y)$ je opět ireducibilní forma stupně nejvýše $\lfloor d/2 \rfloor$. Tedy všechny formy $P(X,Y)$ splňují podmínku HVID-S1 a tedy opět $\gamma F(X,Y)$ má tvar HVID-S.

□

Na konci důkazu se využívá, že $\gamma(P(X,Y))$ opět splňuje podmínku HVID-S1. Může sice nastat, že $\gamma(P(X,Y)) = Y$, což ale v případě definice HVID-S nevadí. Pokud bychom uvažovali obecnější definici HVID, potom by pro $\gamma(P(X,Y)) = Y$ podmínka HVID-1 být splněna nemusela a $\gamma(F(X,Y))$ by nebylo HVID.

Působení grupy Γ na množině $\mathcal{I}(q,d)$ zachovává tvary HVID-S, z čehož plyne důležitý důsledek.

Důsledek 42. *Jestliže $F(X,Y) \in \mathcal{I}(q,d)$ má odpovídající HVID-S, pak všechny $Q(X,Y) \in \mathcal{I}(q,d)$ náležející Γ-orbitě prvku $F(X,Y)$ mají též HVID-S.*

Tím se nám podstatně zlehčuje důkaz věty 15. Odteď víme, že nám stačí najít HVID-S pro jednu homogenní formu v každé Γ-orbitě. Potom HVID-S existuje pro všechny formy v $\mathcal{I}(q,d)$. Zároveň definice HVID je obecnější definice HVID-S. Tedy pokud pro formu existuje HVID-S, pak jistě existuje i HVID.

5.3 Počet Γ-orbit množiny $\mathcal{I}(q,d)$

Díky předchozí sekci víme, že se nám bude hodit určit orbity Γ v množině $\mathcal{I}(q,d)$. Prvním krokem bude zjistit jejich počet pro konkrétní dvojice (q,d). Nejdříve zmíníme další definici z algebry.

Definice 43 (Grupa afinní transformace přímky $GA_1(\mathbb{F}_q)$)**.**
$GA_1(\mathbb{F}_q) = \{\gamma : \gamma(x) = ax + b,\ a \in \mathbb{F}_q^*,\ b \in \mathbb{F}_q\}$, *kde* $x \in \mathbb{F}_{q^d}$, $d \in \mathbb{N}$

Lemma 44. *Grupa* $GA_1(\mathbb{F}_q)$ *fixuje lineární formu* $Y \in \mathcal{I}(q,1)$ *a je podgrupou grupy* Γ.

Důkaz. Nechť $\mathcal{A}$ je podgrupa grupy Γ taková, že matice náležející do $\mathcal{A}$ fixují lineární formu Y. Neboli, $\mathcal{A} = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mid \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} Y = Y \right\}$.
Z definice působení grupy víme, že $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} (F(X,Y)) = F(\alpha X + \gamma Y, \beta X + \delta Y)$.
Pro $F(X,Y) = Y$ dostáváme podmínku $\beta X + \delta Y = Y \Rightarrow \beta = 0,\ \delta = 1$.
$\Rightarrow \mathcal{A} = \left\{ \begin{pmatrix} \alpha & 0 \\ \gamma & 1 \end{pmatrix} \right\}$.
Mějme libovolnou matici $M \in \mathcal{A}$, $M = \begin{pmatrix} \alpha & 0 \\ \gamma & 1 \end{pmatrix}$. Všimneme si, že $\alpha \neq 0$, protože jinak by M nebyla regulární. Potom z definice?? víme, že $M(\xi) = \frac{\xi - \gamma}{\alpha}$. Položme pro $a,b \in \mathbb{F}_q$, $a = \frac{1}{\alpha}$, $b = -\frac{\gamma}{\alpha}$. Potom $\alpha = \frac{1}{a}$, $\gamma = -\frac{b}{a}$. (Odtud získáváme podmínku $a \in \mathbb{F}_q^*$). Po dosazení dostáváme, že $M(\xi) = a\xi + b$. Tedy jsme jednoznačně našli $g \in GA_1(\mathbb{F}_q)$, tž. $M(\xi) = g(\xi)$. Odtud $GA_1(\mathbb{F}_q) \simeq \mathcal{A}$, protože matice M i prvek ξ jsou libovolné. Tedy $GA_1(\mathbb{F}_q)$ je podgrupa Γ fixující formu Y.

□

Definice 45. *Grupa* Γ *působí jednoduše tranzitivně na množině* X*, pokud* $\forall\ a, b \in X\ \exists\ \gamma \in \Gamma : \gamma(a) = b$.

Speciálně, $GA_1(\mathbb{F}_q)$ působí jednoduše tranzitivně na $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$, jestliže $\forall\ a, b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q\ \exists g \in GA_1(\mathbb{F}_q) : g(a) = b$.

Lemma 46.

(a) Grupa $GA_1(\mathbb{F}_q)$ *působí jednoduše tranzitivně na* $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

(b) Γ *působí jednoduše tranzitivně na* $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$

Důkaz.
(a) $GA_1(\mathbb{F}_q) = \{g : g(x) = ax+b, a \in \mathbb{F}_q^*, b \in \mathbb{F}_q\}$, tedy vidíme, že $|GA_1(\mathbb{F}_q)| = q\ (q-1)$ a zároveň si všimneme, že $|\mathbb{F}_{q^2} \setminus \mathbb{F}_q| = q^2 - q = q\ (q-1)$ a tedy

$$|GA_1(\mathbb{F}_q)| = |\mathbb{F}_{q^2} \setminus \mathbb{F}_q| \tag{5.3}$$

Nyní dokážeme, že $\forall \xi \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ je stabilizátor G_ξ triviální, neboli identita. Nechť $\xi \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ a $g \in GA_1(\mathbb{F}_q)$ leží ve stabilizátoru prvku ξ. Tedy $g(\xi) =$

$a\xi + b = \xi$.
Mějme τ generátor $Gal(\mathbb{F}_{q^2}/\mathbb{F}_q)$, tedy víme, že τ fixuje všechny prvky $\mathbb{F}_q$.

$$g(\tau(\xi)) = a\tau(\xi) + b = \tau(a)\tau(\xi) + \tau(b) = \tau(a\xi + b) = \tau(g(\xi)) = \tau(\xi)$$

Odtud vidíme, že g fixuje také $\tau(\xi)$.
$\xi \neq \tau(\xi)$, protože $\xi \notin \mathbb{F}_q$ a zároveň τ je generátor $Gal(\mathbb{F}_{q^2}/\mathbb{F}_q)$. Afinní zobrazení, které fixuje dva různé prvky, musí být identita.

Z algebry víme, že pro konečnou grupu platí:

$$|GA_1(\mathbb{F}_q)| = |G_\xi| \cdot |[\xi]|\,,$$

kde G_ξ je stabilizátor prvku ξ, $[\xi]$ je orbita obsahující ξ.
$|G_\xi| = 1$, jelikož do G_ξ náleží jen identita. Také zřejmě platí, že $|[\xi]| \leq |\mathbb{F}_{q^2} \setminus \mathbb{F}_q|$.
Odtud a z rovnosti 5.3 dostáváme:

$$\begin{gathered} |\mathbb{F}_{q^2} \setminus \mathbb{F}_q| = |GA_1(\mathbb{F}_q)| = |[\xi]| \leq |\mathbb{F}_{q^2} \setminus \mathbb{F}_q| \\ \Rightarrow |[\xi]| = |\mathbb{F}_{q^2} \setminus \mathbb{F}_q| \end{gathered}$$

Zjistili jsme, že $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ obsahuje jen jednu orbitu a tedy že $GA_1(\mathbb{F}_q)$ působí na $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ jednoduše tranzitivně.

(b) Z poznámky 5.1 víme, že $|\Gamma| = q(q-1)(q+1)$.
Zároveň $|\mathbb{F}_{q^3} \setminus \mathbb{F}_q| = q^3 - q = q(q-1)(q+1)$.

$$\Rightarrow |\Gamma| = |\mathbb{F}_{q^3} \setminus \mathbb{F}_q| \tag{5.4}$$

Podobně jako v bodě a) dokážeme, že stabilizátor každého prvku je pouze idetita. Nechť $\xi \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$, $\gamma \in \Gamma$, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ je stabilizátor prvku ξ. Potom podle definice?? víme, že $\frac{d\xi - c}{-b\xi + a} = \gamma\,(\xi) = \xi$.

Mějme τ generátor $Gal(\mathbb{F}_{q^3}/\mathbb{F}_q)$, tedy víme, že τ fixuje všechny prvky $\mathbb{F}_q$.

$$\gamma(\tau(\xi)) = \frac{d\tau(\xi) - c}{-b\tau(\xi) + a} = \frac{\tau(d)\tau(\xi) - \tau(c)}{-\tau(b)\tau(\xi) + \tau(a)} = \tau\left(\frac{d\xi - c}{-b\xi + a}\right) = \tau(\xi).$$

Stejně se vyjádří:

$$\gamma(\tau^2(\xi)) = \tau^2(\xi)$$

Protože τ je generátor $Gal(\mathbb{F}_{q^3}/\mathbb{F}_q)$ a $\xi \notin \mathbb{F}_q$, jsou $\xi, \tau(\xi), \tau^2(\xi)$ tři různé prvky.

Nyní dokážeme, že γ už musí být nutně identita. Nechť $x \in \mathbb{F}_{q^3}$ a γ fixuje x. Potom

$$\begin{gathered} \gamma(x) = \tfrac{ax+b}{cx+d} = x \\ \Rightarrow cx^2 + dx - ax - b = 0 \end{gathered}$$

Tedy x musí být kořenem kvadratického polynomu. Ty jsou nejvýše dva, ale γ fixuje tři různé prvky, proto polynom $cx^2 + dx - ax - b$ musí být triviálně 0. Tedy $c = b = 0,\ d = a$, zároveň γ náleží faktorgrupě Γ, proto $\gamma = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Z rovnice (5.4) a podobně jako v bodě a) dostáváme:

$$|\mathbb{F}_{q^3} \setminus \mathbb{F}_q| = |\Gamma| = |[\xi]| \leq |\mathbb{F}_{q^3} \setminus \mathbb{F}_q|$$
$$\Rightarrow |[\xi]| = |\mathbb{F}_{q^3} \setminus \mathbb{F}_q|$$

Zjistili jsme, že $\mathbb{F}_{q^3}/\mathbb{F}_q$ obsahuje pouze jednu $\Gamma-$orbitu a tedy Γ působí na $\mathbb{F}_{q^3}/\mathbb{F}_q$ jednoduše tranzitivně.

□

Poznámka. Pro všechny prvky $a,b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ existuje $\gamma \in GA_1(\mathbb{F}_q)$, tž. $\gamma(a) = b$. Z lemmatu 44 víme, že $GA_1(\mathbb{F}_q)$ je podgrupou grupy Γ. Tedy zřejmě pro všechny $a,b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ existuje $\gamma \in \Gamma$, tž. $\gamma(a) = b$. Neboli také Γ působí na $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ tranzitivně.

Lemma 47. *Nechť $\xi \in \mathbb{F}_{q^d}$, polynom $f \in \mathbb{F}_q[x]$, $\gamma \in \Gamma$. Potom ξ je kořen $f \Leftrightarrow \gamma(\xi)$ je kořenem polynomu $\gamma(f)$.*

Důkaz. Nechť $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Z definice působení Γ na množině forem víme, že:

$$\gamma(X - \xi Y) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} (X - \xi Y) = (aX + cY) - \xi(bX + dY) =$$
$$= (a - b\xi)X + (c - d\xi)Y = (a - b\xi)\left(X - \left(\tfrac{d\xi - c}{a - b\xi}\right) Y\right).$$

Podle definice 34$\gamma(\xi) = \frac{d\xi - c}{a - b\xi}$ a $(a - b\xi)$ je konstanta v $\mathbb{F}_{q^d}$. Tedy, $\gamma(X - \xi Y) = c(X - \gamma(\xi)Y)$, kde $c \in \mathbb{F}_{q^d}$.

Odtud po dehomogenizaci formy $(X - \xi Y)$, dostáváme, že $\gamma(x - \xi) = c(x - \gamma(\xi))$.

Uvažujme polynom f, který má kořen $\xi \in \mathbb{F}_{q^d}$. Tedy $f = (x - \xi)h$, kde $h \in \mathbb{F}_q[x]$. Protože působení γ na polynomy je homomorfismus, $\gamma(f) = \gamma(x - \xi)\gamma(h) = c(x - \gamma(\xi))\gamma(h)$. Tedy $\gamma(\xi)$ je kořenem polynomu $\gamma(f)$.

Naopak nechť $\gamma(\xi)$ je kořenem $\gamma(f)$. Protože γ je regulární matice, existuje k ní inverzní matice γ^{-1}. Už jsme dokázali, že potom platí $\gamma^{-1}\gamma(\xi)$ je kořenem $\gamma^{-1}\gamma(f)$. Neboli ξ je kořenem f.

□

Lemma 48. *Pokud $d = 2$ nebo 3, pak množina $\mathcal{I}(q,d)$ obsahuje jen jednu Γ-orbitu.*

Důkaz. Položme $d = 2$ nebo 3. Mějme polynomy $f, g \in \mathcal{M}(q,d)$. Protože f, g jsou ireducibilní, nemají kořeny v $\mathbb{F}_q$. Pokud $d = 2$, pak jejich kořeny leží v $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Pokud $d = 3$, pak jejich kořeny leží v $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$, v $\mathbb{F}_{q^2}$ ani ležet nemůžou, protože $\mathbb{F}_{q^2}$ není podtělesem $\mathbb{F}_{q^3}$.

Uvažujme α, která je kořenem f, β, která je kořenem g. Z lemmatu 46 a poznámky za ním víme, že Γ působí na $\mathbb{F}_q^d \setminus \mathbb{F}_q$ tranzitivně (protože $d = 2, 3$), neboli existuje $\gamma \in \Gamma$, tž. $\gamma(\alpha) = \beta$.

Z předchozího lemmatu 47 plyne, že $\gamma(\alpha)$ je kořenem $\gamma(f)$. Potom β je kořenem g a zároveň $\gamma(f)$. Polynomy $\gamma(f)$, g jsou ireducibní, tedy oba jsou pro prvek β minimální nad $\mathbb{F}_q$. Polynomy $g, \gamma(f)$ jsou tedy stejné až na násobek konstantou. ($g \in \mathcal{M}(q,d)$ je monický, ale $\gamma(f)$ být monický nemusí), tedy $\gamma(f) = c.g$, kde $c \in \mathbb{F}_q$. Odtud vyplývá, že Γ působí i na $\mathcal{M}(q,d)$ tranzitivně.

Díky Lemmatu 39 $\mathcal{M}(q,d)$ je v bijekci s $\mathcal{I}(q,d)$. Γ proto působí tranzitivně i na $\mathcal{I}(q,d)$. Jinými slovy pokud $d = 2,3$, pak $\mathcal{I}(q,d)$ obsahuje pouze jednu Γ- orbitu.

□

Lemma 49.
Pokud je $d \geq 3$, pak pro každou $F(X,Y) \in \mathcal{I}(q,d)$ je stabilizátor Γ_F cyklická grupa řádu dělícího d.

Důkaz. Nechť f je polynom, který vznikl dehomogenizací formy F. Potom stabilizátor $\Gamma_F = \Gamma_f$. Protože F je ireducibilní, je i polynom f ireducibilní. Z tvzení 11 z první kapitoly víme, že rozkladové nadtěleso polynomu f je $\mathbb{F}_{q^d}$ a je rovno kořenovému nadtělesu určeného jedním kořenem polynomu f. Tedy mějme a kořen polynomu f, pak $\mathbb{F}_{q^d} = \mathbb{F}_q(a)$.

Nyní uvažujme Galoisovu grupu $G = Gal(\mathbb{F}_q(a)/\mathbb{F}_q)$, což je grupa všech homomorfismů, který permutují prvky $\mathbb{F}_q(a)$ a zároveň zachovávají prvky z $\mathbb{F}_q$. Tedy tyto homomorfismy jsou jednoznačně určeny zobrazením prvku a.

Vezměme libovolný prvek $g \in \Gamma_f$, tedy $g(f) = f$. Rozložme polynom f na lineární členy nad $\mathbb{F}_q^d$, neboli $f = c(x - a_1) \cdots (x - a_d)$. Potom $g(f) = g(c(x - a_1) \cdots (x - a_d)) = \phi(c)(x - \phi(a_1) \cdots (x - \phi(a_d)$, odtud vidíme, že g musí zachovávat $c \in \mathbb{F}_q$ a permutovat kořeny náležející $\mathbb{F}_{q^d}$. Nechť BÚNO $a = a_1$, a položme $\bar{\phi}(a) = \phi(a)$. Potom $\bar{\phi}$ je určeno jednoznačně a je prvkem Galoisovy grupy G.

Uvažujme tedy zobrazení ψ z grupy stabilizátoru Γ_f do grupy G, které prvku g přiřadí právě zobrazení $\bar{\phi}$. Zřejmě ψ je homomorfismem.

Nyní se budeme snažit ověřit, že ψ je prosté, tedy, že jde dokonce o vnoření do grupy G. K tomu potřebujeme určit jádro ψ.

Jádro ψ je množina všech $g \in \Gamma_f$, tž. $\psi(g) = id$. Neboli $\psi(g) = \bar{\phi} = id$. Chceme ověřit, že takové g je už nutně pouze jednotková matice.

Máme tedy, že $\bar{\phi}(a) = g(a) = a$. Rozepíšeme tento vztah podle definice 34,

$g(a) = \frac{\delta a - \gamma}{-\beta a + \alpha} = a$. Odtud dostáváme kvadratickou rovnici $\beta a^2 - \alpha a + \delta a - \gamma = 0$, neboli, že a je kořenem kvadratického polynomu. Protože a je kořen polynomu f, který je navíc ireducibilní, musí být f také minimálním polynomem a nad $\mathbb{F}_q$. Stupeň f je minimálně 3, což je ve sporu s tím, že a je kořenem kvadratického polynomu. Tedy $\beta a^2 - \alpha a + \delta a - \gamma$ musí být triviálně nulový polynom a tedy $\beta = \gamma = 0$, $\alpha = \delta$. Protože g leží ve faktorgrupě Γ, $\alpha = \delta = 1$. Odtud tedy získáváme, že g je jednotková matice.

Zjistili jsme, že v jádru ψ leží pouze identita, tedy ψ je prostý homomorfismus, a proto $\Gamma_f \simeq Im(\psi)$. Grupa G je cyklická řádu d, potom z Lagrangeovy věty víme, že $Im(\psi)$ a Γ_f jsou cyklické grupy řádu dělícího d.

□

Lemma 49 nám umožňuje napsat odhad pro velikost Γ-orbit. Faktorgrupa Γ je konečná a tedy z algebry víme že $\forall f \in \mathcal{I}(q,d)$ platí následující rovnost:

$$|[f]| = \frac{|\Gamma|}{|\Gamma_f|} \geq \frac{|\Gamma|}{NSD(|\Gamma|, d)} \tag{5.5}$$

Nerovnost plyne z toho, že $|\Gamma_f|$ dělí d (z Lemmatu 49) a zároveň dělí $|\Gamma|$, tedy $|\Gamma_f| \leq NSD(|\Gamma|, d)$.

Konkrétně rozepíšeme dva případy:

- $(q,d) = (2,4)$
  Z rovnosti (5.1) víme že $|\Gamma| = 6$. Z odhadu (5.5) dostáváme, že $|[f]| \geq 3$, $\forall f \in \mathcal{I}(2,4)$. Podle vzorce 5.2 je $|\mathcal{I}(2,4)| = 3$. Odtud je zřejmé, že $\mathcal{I}(2,4)$ obsahuje právě jednu Γ- orbitu.

- $(q,d) = (2,5)$
  Opět $|\Gamma| = 6$ a z odhadu (5.5) dostáváme, že velikost každé Γ- orbity je nejméně 6. Podle vzorce 5.2 je $|\mathcal{I}(2,5)| = 6$. Tedy také $\mathcal{I}(2,5)$ obsahuje právě jednu Γ-orbitu.

Nyní se zaměříme na zbývající případy z věty 18 a), kdy $(q,d) = (2,6), (2,7)$.
Z vzorce 5.2 dostáváme, že $|\mathcal{I}(2,6)| = 9$, $|\mathcal{I}(2,7)| = 18$. Opět $|\Gamma| = 6$. Proto platí, že $|\mathcal{I}(2,6)| > |\Gamma|$, $|\mathcal{I}(2,7)| > |\Gamma|$.

Protože v jedné orbitě může náležet nejvýše $|\Gamma|$ prvků, musí $\mathcal{I}(2,6)$ i $\mathcal{I}(2,7)$ obsahovat orbity aspoň dvě.
Případ (3,5) rozebereme později.
Celou tuto sekci o počtu Γ-orbit můžeme shrnout do následujícího důsledku.

Důsledek 50.

(a) Pokud $d = 2,3$, nebo $(q,d) = (2,4), (2,5)$, množina $\mathcal{I}(q,d)$ obsahuje jen jednu Γ-orbitu,

(b) Ve všech ostatních případech obsahuje množina $\mathcal{I}(q,d)$ aspoň dvě Γ-orbity.

5.4 Působení $GA_1(\mathbb{F}_q)$ na $\mathcal{I}(q,d)$

Na konci sekce 5.2 jsme ukázali, že působení Γ zachovává rozklady HVID-S. Ukážeme, že působení $GA_1(\mathbb{F}_q)$ zachovává dokonce rozklady HVID.

Podle lemmatu 44 je $GA_1(\mathbb{F}_q)$ podgrupou Γ, která fixuje lineární formu Y. Tento fakt nám umožní upravit lemma 41, aby zahrnovalo definici HVID.

Lemma 51. *Nechť $\gamma \in GA_1(\mathbb{F}_q)$, $F(X,Y) \in \mathcal{I}(q,d)$. Potom pro $F(X,Y)$ existuje tvar HVID právě tehdy, když pro $\gamma(F(X,Y))$ existuje tvar HVID.*

Důkaz. Nechť $F(X,Y)$ má tvar HVID. Tedy $F(X,Y) = F_1(X,Y) + \cdots F_r(X,Y)$ a až na formu Y, tak pro všechny ireducibilní formy $P(X,Y)$ stupně nejvýše $\lfloor d/2 \rfloor$, platí, že dělí všechny až na právě jeden sčítanec F_i.

Působením γ dostaneme, že $\gamma(F(X,Y)) = \gamma(F_1(X,Y)) + \cdots \gamma(F_r(X,Y))$, a platí, že kromě formy $\gamma(Y)$, tak všechny formy $\gamma(P(X,Y))$, dělí všechny až na právě jeden sčítanec $\gamma(F_i)$. Působení Γ zachovává ireducibilitu, tedy $\gamma(P(X,Y))$ je opět ireducibilní forma stupně nejvýše $\lfloor d/2 \rfloor$. Zároveň $GA_1(\mathbb{F}_q)$ fixuje formu Y, tedy $\gamma(Y) = Y$. Tedy všechny formy $P(X,Y)$ kromě Y splňují podmínku HVID-1 a tedy opět $\gamma(F(X,Y))$ má tvar HVID.

□

Z lemmatu 46 víme, že $GA_1(\mathbb{F}_q)$ působí tranzitivně na $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$, neboli podle dalšího lemmatu 48 $GA_1(\mathbb{F}_q)$ působí tranzitivně na $\mathcal{I}(q,d)$. Tedy v případě, kdy $d = 2$, platí, že pokud jsme našli pro jednu formu HVID, pak pro všechny formy ležící ve stejné orbitě také existuje HVID.

6. Konstrukce HVID

V této kapitole popíšeme postup jak sestavit HVID (pro připomenutí VID pro homogenní formy) pro formy náležející $\mathcal{I}(q,d)$, kde (q,d) je jakákoliv dvojice z věty 18.

Značení
V této kapitole budeme všechny lineární homogenní formy značit L, kvadratické formy Q a kubické formy C.

Pro připomenutí, aby součet homogenních forem $F = F_1 + \cdots + F_r$, kde každá forma F_i je stupně právě d, byl HVID, musí být splněny následující dvě podmínky:
(HVID -1) Každá ireducibilní homogenní forma $P(X,Y)$ stupně nejvýše $\lfloor d/2 \rfloor$ musí dělit všechny až na právě jednu formu F_i. Tuto podmínku nemusí splňovat jedna speciální forma $P(X,Y) = Y$.
(HVID-2) $Y \nmid F$.

Nejdříve sestavíme HVID pro konkrétní případ.

Příklad 52. $(q,d) = (4,3),\ r = 2$

- *Ireducibiní homogenní formy stupně nejvýše $\lfloor d/2 \rfloor$ jsou všechny lineární formy nad $\mathbb{F}_4$. Těch je pět podle vzorce 5.2. Označme je L_1, L_2, L_3, L_4, L_5, konkrétně to jsou formy X, $X+Y$, $X+\alpha Y$, $X+\alpha Y+Y$, Y. Předpokládejme, že chceme, aby i forma Y podmínku HVID-1 splňovala.*

- *$r = 2$, tedy $F = F_1 + F_2$. Protože stupeň žádné formy F_i nemůže překročit 3 musíme lineární formy uspořádat následovně:*
  $F_1 + F_2 = L_1L_2 + L_3L_4L_5$

- *Aby i forma F_1 měla stupeň právě 3, musíme do prvního členu přidat ještě jednou L_1, nebo L_2 (nikoli L_3, L_4, L_5, protože potom by nebyla splněna podmínka 1.).*
  Dostáváme tvar HVID : $cL_1^2L_2 + L_3L_4L_5$, kde $c \in \mathbb{F}^*$.

- *Nyní stačí za L_i dosadit konkrétní homogenní formy a za α hodnotu z $\mathbb{F}^*$. Tímto dostaneme konkrétní HVID. V dosazování máme více možností a tedy tímto způsobem získáme více HVID, např:*
  $F = (\alpha+1)X^2(X+Y) + (X+\alpha Y)(X+Y\alpha+Y)Y$

Pokud lineární formu Y v některých členech vynecháme, můžeme dostat jiný tvar rozkladu HVID. Později uvidíme, že $cL_1^2L_2 + L_3L_4L_5$ skutečně není jediný tvar HVID pro formy náležející $\mathcal{I}(4,3)$.

Pokusíme se co nejvíce obecně popsat jak pro jakoukoliv dvojici (q,d) nalézt všechny možné tvary HVID. Pro tento účel uvedeme pár definic, které nám pomůžou ve vytvoření formálního tvaru HVID.

Nejprve upustíme od podmínky pro HVID a definujeme obecně formální tvar homogenního součtu.

Definice 53 (Formální tvar homogenního součtu)**.** *Formální tvar homogenního součtu stupně d je suma:*

$$\mathfrak{S} = \sum_{i=1}^{r} \alpha_i \left(\prod_{j=1}^{s_i} \mathfrak{B}_{i,j} \right)$$

produktů formálních forem $\mathfrak{B}_{i,j}$, která splňuje dvě podmínky:

1. *ke každé formě $\mathfrak{B}_{i,j}$ je přiřazen stupeň formy $\deg \mathfrak{B}_{i,j} \in \mathbb{N}$, přičemž pokud mají dvě formy stejný stupeň, pak mohou být ekvivalentní.*
2. *$\sum_{j=1}^{s_i} \deg \mathfrak{B}_{i,j} = d$.*

Příklad 54. *Pro $(q,d) = (2,2)$, $r = 3$ máme například tyto formální tvary:*
$\mathfrak{S}_1 = L_1L_2 + Q_1 + Q_2$
$\mathfrak{S}_2 = L_1^2 + Q_1 + Q_2$
$\mathfrak{S}_3 = L_1L_2 + L_2L_3 + L_1^2$

Poznámka. Dvě homogenní formy nazveme ekvivalentní, pokud jedna je skalárním násobkem druhé.

Definice 55 (Instance formálního tvaru)**.** *Instance $\mathfrak{I}$ formálního tvaru $\mathfrak{S}$ homogenního součtu nad tělesem $\mathbb{F}$ je suma*

$$\mathfrak{I} = \sum_{i=1}^{r} \alpha_i \left(\prod_{j=1}^{s_i} F_{i,j} \right)$$

kde F_i jsou konkrétní homogenní formy nad $\mathbb{F}$ příslušného stupně, které nahrazují formální formy z formálního tvaru $\mathfrak{S}$.

- *ekvivalentní formální formy jsou nahrazeny ekvivalentními homogenními formami*
- *neekvivalentní formální formy jsou nahrazeny neekvivalentními homogenními formami*
- *α_i jsou nahrazeny konkrétními prvky $\mathbb{F}^*$.*

Příklad 56. *Instance od formálního tvaru $\mathfrak{S}_1$*
$\mathfrak{I}_1 = (X + Y)X + (X^2 + XY + Y^2) + X^2$
$\mathfrak{I}_2 = (X + Y)Y + (X^2 + XY + Y^2) + XY$

Definice 57 (Viditelně ireducibilní tvar (VIS))**.** *Viditelně ireducibilní tvar (VIS) stupně d nad $\mathbb{F}_q$ je formální tvar homogenního součtu stupně d, který navíc splňuje podmínku:*
(VIS-1) Pro všechny n, n $1 \leq n \leq \lfloor d/2 \rfloor$ obsahuje VIS právě $|\mathcal{I}(q,n)|$ neekvivalentních homogenních forem stupně n. Každá z nich se objevuje v každém až na právě jednom sčítanci. Pouze jediná formální forma L_Y, která reprezentuje konkrétní lineární formu Y, nemusí tuto podmínku splňovat.

Z definice přímo vyplývá, že každá forma, jež je HVID, je zároveň instancí VIS. Naopak každá homogenní forma, jež je instancí VIS, splňuje podmínku HVID-1. Není však zaručeno, že splňuje také podmínku HVID-2. Bohužel splnění podmínky HVID-2 obecně zaručit neumíme a budeme ji muset ověřovat ručně.

6.1 $\mathcal{I}(q,d)$ obsahující jedinou Γ-orbitu

V této sekci detailněji rozebereme $\mathcal{I}(q,d)$, které mají pouze jednu Γ-orbitu. Jde o nejlehčí případ, protože jak nám ukáže následující lemma stačí najít jediný VIS a jeho instance nám vytvoří všechny formy $\mathcal{I}(q,d)$.

Lemma 58. *Nechť VIS $\mathfrak{S}$ je tvar, kde forma L_Y splňuje podmínku HVID-1. Pokud jedna instance tvaru VIS $\mathfrak{S}$ náleží Γ-orbitě $\mathfrak{o}$, potom všechny formy náležející $\mathfrak{o}$ jsou instancemi $\mathfrak{S}$.*

Důkaz. Nechť forma $F = \sum_{i=1}^{r} \prod_{j=1} F_j^k$ je právě tou instancí tvaru $\mathfrak{S}$, která leží v orbitě $\mathfrak{o}$. Potom pro všechny $\overline{F} \in \mathfrak{o}$, platí, že existuje $g \in \Gamma$, tž. $\overline{F} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} F = \sum_{i=1}^{r} \prod_{j=1} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} F_j^k$. Nyní dokážeme, že poslední výraz je opět instancí $\mathfrak{S}$. K tomu si stačí uvědomit, že $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} F_j$ je také konkrétní forma stupně stejného jako F_j (může a nemusí být ekvivalentní). Může nastat, že $F_j = Y$, což nevadí, protože předpokládáme, že $\mathfrak{S}$ je tvar, kde forma L_Y splňuje také podmínku HVID-1. □

Poznámka. Pro VIS, kde forma L_Y podmínku nesplňuje HVID-1, lemma platit nemusí.

Uveďme příklad takového tvaru. VIS $\mathfrak{S} = L_1^2 + L_2^2$. Potom $\mathfrak{S}$ má jednu instanci: $(X+Y)^2 + X^2$ a vidíme, že ireducibilní formu $Y(X+Y) + X^2$ tímto tvarem získat nemůžeme.

Abychom dokázali sestavit tvary VIS pro všechny dvojice (q,d), musíme najít všechny formy $P(X,Y)$ (stačí monické) stupně nejvýše $\lfloor d/2 \rfloor$.

(q,d)	$\lvert\mathcal{I}(q,d)\rvert$	$P(X,Y)$
(2,1)	3	$X,\ Y,\ X+Y$
(2,2)	1	X^2+XY+Y^2
(2,3)	2	$X^3+X^2Y+Y^3,\ X^3+XY^2+Y^3$
(3,1)	4	$X,\ Y,\ X+Y,\ X+2Y$
(3,2)	3	$X^2+XY+2Y^2,\ X^2+2XY+2Y^2,\ X^2+Y^2$
(4,1)	5	$X,\ Y,\ X+Y,\ X+\alpha Y,\ X+\alpha Y+Y$
(5,1)	6	$X,\ Y,\ X+Y,\ X+2Y,\ X+3Y,\ X+4Y$

Nyní už dokážeme snadno sestavit všechny možné tvary VIS. Definice tvaru VIS nám přímo udává jak postupovat.

Případ (2,2)
V tomto případě VIS obsahuje tři lineární formy L_1, L_2, L_Y. Protože počítáme nad $\mathbb{F}_2$, žádné c zde vystupovat nebude. VIS budeme sestavovat postupně pro rostoucí $r \geq 2$.
$r = 2$
Formy L_1, L_2 se musí objevovat v každém až na právě jednom sčítanci. Nejdříve předpokládejme, že se objevují ve dvou různých. BÚNO L_1 se objevuje v prvním a L_2 ve druhém. Nyní potřebujme zajistit, aby každý sčítanec byl stupně 2. Můžeme buď přidat formu L_3, nebo zvýšit stupeň forem L_1, L_2. Dostáváme následující VIS:

$$L_1{}^2 + L_2{}^2$$
$$L_1{}^2 + L_2 L_Y$$
$$L_1 L_Y + L_2{}^2 L_Y$$

Hned vidíme ze poslední případ je dělitelný L_Y, tedy každá jeho instance je určitě dělitelná formou Y.

Nyní uvažujme, že obě formy L_1, L_2 se nacházejí ve stejném, například prvním sčítanci. Potom máme dostáváme jediný VIS:

$$L_1 L_2 + L_Y{}^2$$

$r = 3$

BÚNO L_1 umístíme pouze do prvního a druhého členu a L_2 umístíme do prvního a třetího členu. Opět do každého sčítance přidáme L_Y nebo zvýšíme stupeň u L_1 a L_2.Dostáváme následující VIS:

$$L_1 L_2 + L_1{}^2 + L_2{}^2$$
$$L_1 L_2 + L_1 L_Y + L_2{}^2$$
$$L_1 L_2 + L_1 L_Y + L_2 L_Y$$

$r \geq 4$

BÚNO L_1 umístíme do prvního, druhého a třetího členu. Dále potřebujeme umístit do třech členů také L_2. Potom ale budou minimálně dva členy stejné a to $L_1 L_2$. Nad tělesem $\mathbb{F}_2$ se tyto členy odečtou a tím pádem nemá cenu je do součtu zahrnovat. Dostáváme tak opět jen součty, kde $r \leq 3$.

Případ (4,2)

V tomto případě VIS obsahuje pět lineárních forem L_1, L_2, L_3, L_4, L_Y. Počítáme nad $\mathbb{F}_4 = \{0,1, \alpha, \alpha + 1\}$. VIS budeme opět sestavovat postupně pro rostoucí $r \geq 2$.

$r = 2$

Potřebujeme umístit každou z forem L_1, L_2, L_3, L_4, do jednoho sčítance. BÚNO L_1, L_2 leží v prvním a L_3, L_4 leží ve druhém. BÚNO c se bude vyskytovat u druhého sčítance. Dostáváme jeden VIS:

$$L_1 L_2 + c L_3 L_4$$

Vidíme, že formu L_Y už umístit nelze.

$r \geq 3$

V tomto případě, ať už umístíme formy do prvních dvou sčítanců jakkoliv, ve třetím se musí objevit všechny čtyři lineární formy, což nelze, protože $d = 2$.

Pro případ (4,2) jsme nalezli tedy jediný VIS.

V následující tabulce, jsou uvedeny tvary VIS pro všechny dvojice (q,d), které mají podle předchozí kapitoly jednu Γ-orbitu.

(q,d)	příklady VIS	$\lvert\mathcal{I}(q,d)\rvert$
(2,2)	$L_1L_2 + L_2L_3 + L_3L_1$	2
	$L_1^2 + L_2^2$	
(2,3)	$L_1^2L_2 + L_2^2L_3 + L_3^2L_1$	2
	$L_1^3 + L_2L_3^2$	
(2,4)	$L_1L_2Q + L_3^4$	3
	$L_1^2L_2^2 + Q^2$	
(2,5)	$L_1^2L_2^3 + QL_3^3$	6
	$L_1^5 + L_2^3Q$	
(3,2)	$L_1L_2 + cL_3L_Y$	3
	$L_1L_2 + L_3^2$	
(3,3)	$L_1^2L_2 + cL_3^2L_4$	8
	$L_1^2L_2 + c_2L_2^2L_3 + c_1L_3^2L_1$	
(4,2)	$L_1L_2 + cL_3L_4$	6
(4,3)	$L_1^2L_2 + cL_3L_4L_5$	20
	$L_1L_2L_3 + c_1L_2L_3L_4 + c_2L_1^2L_4$	
(5,3)	$L_1L_2L_3 + cL_4L_5L_6$	40
	$L_1L_2L_3 + cL_4L_5^2$	

Rozepíšeme více už zmíněný případ (4,2). Nalezneme všechny instance jediného tvaru $L_1L_2 + cL_3L_4$. Můžeme libovolně dosazovat čtyři lineární formy a tři prvky $c \in \mathbb{F}_4^*$. Celkem takto dostaneme 72 instancí, z nichž spoustu se na první pohled rovnají, protože $L_1L_2 + cL_3L_4$ je symetrický vzhledem k dosazení L_1, L_2 a L_3, L_4. Instancí tedy můžeme uvažovat mnohem méně.

- $c = 1$
  $X(X+Y) + (X+\alpha Y)(X+\alpha Y+Y) = Y^2$
  $X(X+Y) + X(X+\alpha Y+Y) = (\alpha+1)Y^2$
  $X(X+\alpha Y+Y) + X(X+Y) = \alpha Y^2$

- $c = \alpha + 1$
  $X(X+Y) + (\alpha+1)(X+\alpha Y)(X+\alpha Y+Y) = \alpha X^2 + \alpha XY + \alpha Y$
  $X(X+\alpha Y) + (\alpha+1)(X+Y)(X+\alpha Y+Y) = X^2\alpha XY + \alpha Y^2$
  $X(X+\alpha Y+Y) + (\alpha+1)(X+Y)(X+\alpha Y) = \alpha X^2 + XY + Y^2$
  $(\alpha+1)X(X+Y) + (X+\alpha Y)(X+\alpha Y+Y) = \alpha X^2 + \alpha XY + Y^2$
  $(\alpha+1)X(X+\alpha Y) + (X+Y)(X+\alpha Y+Y) = \alpha X^2 + (\alpha+1)XY + (\alpha+1)Y^2$
  $(\alpha+1)X(X+\alpha Y+\alpha Y) + (X+Y)(X+\alpha Y) = \alpha X^2 + XY + \alpha Y^2$

- $c = \alpha$
  Protože $\alpha, \alpha+1$ jsou v $\mathbb{F}_4^*$ inverzní prvky, nemusíme už další instance uvažovat. Např. $(\alpha+1)(X(X+Y) + \alpha(X+Y)(X+\alpha Y+Y)) = (\alpha+1)X(X+Y) + (X+Y)(X+\alpha Y+Y)$

Vidíme, že některé instance nesplňují požadovaný stupeň, ostatní vynásobíme konstantou, aby formy náležely $\mathcal{I}(4,2)$. Tím dostaneme všech šest neekvivalentních forem $\mathcal{I}(4,2)$.
$X^2 + XY + Y^2$
$X^2 + \alpha XY + (\alpha+1)Y^2$
$X^2 + (\alpha+1)XY + (\alpha+1)Y^2$
$X^2 + XY + (\alpha+1)Y^2$

$X^2 + \alpha XY + \alpha Y^2$
$X^2 + (\alpha + 1)XY + Y^2$
.

6.2 Formy stupně 6 nad $\mathbb{F}_2$

V této podkapitole detailněji rozebereme případ $\mathcal{I}(2,6)$. Z důsledku 50 plyne, že $\mathcal{I}(2,6)$ obsahuje více, jak jednu Γ- orbitu.

Z tvrzení 5.2 spočítáme, že $|\mathcal{I}(2,6)| = 1/6(2^6 - 2^3 - 2^2 + 2) = 9$.

Nyní zjistíme, že ve skutečnosti $\mathcal{I}(2,6)$ obsahuje právě dvě Γ- orbity. První z nich nazveme speciální a obsahuje tři formy , $X^6 + X^5Y + X^3Y^3 + X^2Y^4 + Y^6$, $X^6 + X^4Y^2 + X^3Y^3 + XY^5 + Y^6$, $X^6 + X^3Y^3 + Y^6$. Druhou orbitu nazveme obecnou a obsahuje zbývajících šest forem $X^6 + X^4Y^2 + X^2Y^4 + XY^5 + Y^6$, $X^6 + X^5Y + X^2Y^4 + XY^5 + Y^6$, $X^6 + X^5Y + X^4Y^2 + XY^5 + Y^6$, $X^6 + XY^5 + Y^6$, $X^6 + X^5Y + X^4Y^2 + X^2Y^4 + Y^6$, $X^6 + X^5Y + X^3Y^3 + XY^5 + Y^6$. K těmto výsledkům jsme bohužel přišli vypsáním všech možností.

Nyní potřebujeme najít ke každé orbitě VIS, splňující podmínku z lemmatu 58 který reprezentuje aspoň jeden její prvek. Jak už jsme ukázali v předchozí sekci, potom tento VIS reprezentuje všechny její prvky. Instance nalezených tvarů VIS nám tedy pokryjí všechny formy $\mathcal{I}(2,6)$.

Nejdříve nalezneme všechny tvaru VIS nad $\mathbb{F}_2$ stupně 6. Z tabulky 6.1 víme, že VIS musí obsahovat tři formální lineární formy L_1,L_2,L_3, z nichž jedna je speciální forma L_Y. Dále obsahuje jednu kvadratickou formu Q a dvě kubické formy C_1,C_2.

Tvary VIS rozdělíme na dva případy.

1. Lineární forma L_Y také musí splňovat podmínku HVID-1. Poté se podíváme na tvary VIS podle toho, kde se nacházejí jejich kubické členy.

Pokud C_1, C_2 leží ve stejném členu (BÚNO v prvním).
První člen už má stupeň 6, ve druhém členu musí ležet L_1, L_2,L_3, Q. Dostáváme tedy následující tvary VIS:

$$F_L = C_1C_2 + Q{L_1}^2L_1L_3$$

Instance tohoto tvaru se budou měnit, jen pokud budeme permutovat konkrétní dosazení lineárních forem za L_1,L_2,L_3. Tento VIS má tedy 3 instance, a proto nemůže reprezentovat všechny prvky v obecné orbitě. Podle lemmatu 58 nemůže reprezentovat žádný prvek z obecné orbity. Musí tedy reprezentovat prvky ze speciální a podle lemmatu 58 je reprezentuje všechny.

Pokud C_1, C_2 leží v různých členech
Dosaďme například do druhého členu kvadratickou formu Q a zjistíme, že VIS už musí nutně vypadat následovně:

$$F_A = C_1{L_1}^2L_2 + C_2QL_3$$

Tento VIS má 12 instancí, protože jednotlivé instance se budou lišit, pokud budeme v dosazovaní prohazovat jak lineární, tak i kubické formy. Vidíme, že in-

stancí je více než spočtená velikost $\mathcal{I}(2,6)$, to znamená, že některé instance nám dají stejné homogenní formy.

VIS nemůže obsahovat více jak dva sčítance, protože ve třetím sčítanci by se muselo nacházet všech šest formálních forem, což by neodpovídalo požadovanému stupni VIS.

2. Nyní uvažujme případ, kdy forma L_Y nemusí splňovat podmínku HVID-1.

Pokud C_1,C_2 leží ve stejném sčítanci. Potom dostáváme dva tvary:
$C_1C_2 + QL_1{}^3L_2$, $C_1C_2 + QL_1{}^2L_2{}^2$
Vidíme, že oba dva tvary VIS mají 2 instance.

Pokud C_1,C_2 leží v různých sčítancích, máme jediný tvar $C_1QL_1 + C_2L_2{}^3$. Tento VIS má 4 instance.

Vidíme, že jediný VIS, jehož instance můžou pokrýt všechny formy $\mathcal{I}(2,6)$ je $F_A = C_1L_1{}^2L_2 + C_2QL_3$. Pokusíme se dokázat, že tomu tak skutečně je.

Věta 59. *Všechny formy náležející* $\mathcal{I}(2,6)$ *jsou instancemi tvaru* $F_A = C_1L_1{}^2L_2 + C_2QL_3$.

Důkaz. Víme, že VIS $F_L = C_1C_2 + QL_1{}^2L_2L_3$ reprezentuje všechny prvky ve speciální orbitě. Potřebujeme tedy zjistit kolik instancí $F_A = C_1L_1{}^2L_2 + C_2QL_3$ se shoduje s instancemi $F_L = C_1C_2 + QL_1{}^2L_1L_3$. (pozn. tvary VIS jsou pouze přepsány z předchozích odstavců, ve skutečnosti L_1 z tvaru F_A se nemusí rovnat L_1 z tvaru F_L).

Uvažujme tedy tvar $F_A = C_1L_1{}^2L_2 + C_2QL_3$ a všechny tři variace tvaru F_L, které nám dávají různé instance, přičemž nyní si L_1,L_2,L_3, C_1,C_2,Q už odpovídají.

Označme $F_{L_1} = C_1C_2 + QL_1{}^2L_2L_3$, $F_{L_2} = C_1C_2 + QL_2{}^2L_1L_3$, $F_{L_3} = C_1C_2 + QL_3{}^2L_1L_2$. Podíváme se, kdy tvary VIS dávají stejné instance.

Předpokládejme, že $F_{L_1} = F_A$. Tedy $C_1C_2 + QL_1{}^2L_2L_3 = C_1L_1{}^2L_2 + C_2QL_3$. Vytknutím některých členů a převedením na stejnou stranu dostáváme, že $L_1{}^2L_2(L_3Q + C_1) = C_2(C_1 + L_3Q)$, tedy $L_1{}^2L_2 = C_2$, což nemůže nastat, protože C_2 je ireducibilní.

Předpokládejme, že $F_{L_2} = F_A$. Tedy $C_1C_2 + QL_2{}^2L_1L_3 = C_1L_1{}^2L_2 + C_2QL_3$. Opět vytčením dostaneme, že $C_1(L_1{}^2L_2 + C_2) = L_3Q(C_2 + L_1{}^2L_2)$. Tedy $L_3Q = C_1$, což je opět spor s tím, že C_1 je ireducibilní.

Předpokládejme poslední možnost, že $F_{L_3} = F_A$. Tedy $C_1C_2 + QL_3{}^2L_1L_2 = C_1L_1{}^2L_2 + C_2QL_3$. Po vytčení dostaneme, že $L_3Q(C_2 + L_1L_2L_3) = C_1(L_1{}^2L_2 + C_2)$. Protože $C_2 + L_1L_2L_3 \neq L_1{}^2L_2 + C_2$ musí platit, že
a) $C_2 + L_1L_2L_3 = C_1$
b) $L_3Q = L_1{}^2L_2 + C_2$

Nyní si všimneme, že bod a) platí vždy. Protože C_1, C_2 reprezentují jediné dvě ireducibilní formy, tedy z předchozí kapitoly víme, že mají svůj HVID. Pokud C_1 lze naspat ve tvaru HVID, potom si všimněme, že $L_1L_2L_3 + C_1$ je stále HVID.

Protože $L_1L_2L_3 + C_1 \neq C_1$, musí platit, že $L_1L_2L_3 + C_1 = C_2$. Odtud plyne, že pro jakékoliv konkrétní dosazení do formálních forem bod a) platí.

Zbývá rozebrat bod b). Chceme zjistit, kdy $C_2 = L_3Q + {L_1}^2L_2$. Výraz na pravé straně má 6 instancí. Zároveň si všimněme, že $L_3Q + {L_1}^2L_2$ je HVID, ale nemusí se už nutně rovnat C_2, protože se může rovnat i C_1.

Podíváme se, co po dosazení konkrétně dostaneme.
$(X+Y)(X^2+XY+Y^2) + X^2Y = X^3 + X^2Y + Y^3$
$Y(X^2+XY+Y^2) + X^2(X+Y) = X^3 + XY^2 + Y^3$
$(X+Y)(X^2+XY+Y^2) + Y^2X = X^3 + XY^2 + Y^3$
$X(X^2+XY+Y^2) + Y^2(X+Y) = X^3 + X^2Y + Y^3$
$Y(X^2+XY+Y^2) + (X+Y)^2X = X^3 + X^2Y + Y^3$
$X(X^2+XY+Y^2) + (X+Y)^2Y = X^3 + XY^2 + Y^3$

Vidíme, že v polovině případů $L_3Q + {L_1}^2L_2$ se rovná C_1 a ve druhé polovině C_2.

Shrňme si naše pozorování a výsledky. Pro všechny instance tvaru $F_A = C_1{L_1}^2L_2 + C_2QL_3$ platí, že se nerovnají $F_{L_1} = C_1C_2 + Q{L_1}^2L_1L_3$, ani $F_{L_2} = C_1C_2 + Q{L_2}^2L_1L_3$. Pro polovinu instancí platí, že se rovnají F_{L_3}, pro druhou polovinu platí, že se F_{L_3} nerovnají. Tedy 6 instancí leží ve speciální orbitě a 6 instancí musí ležet v obecné. Podle lemmatu 58 tímto dostaneme všechny instance obecné orbity.

□

6.3 Formy stupně 7 nad $\mathbb{F}_2$

Podobného postupu jako v případě $\mathcal{I}(2,6)$ lze využít i v případě zjišťování VIS pro $\mathcal{I}(2,7)$. Podrobněji je rozepsán ve článku [1], tady jen zmíníme, že $|\mathcal{I}(2,7)| = 18$, nacházejí se zde 3 orbity, každá velikosti 6. Tvrzení, které potom je potřeba dokázat zní, že každá ireducibilní forma nad $\mathbb{F}_2$ je instancí $L_1^i{L_2}^{4-i}C_1 + L_3^2QC_2$.

6.4 Formy stupně 5 nad $\mathbb{F}_3$

.

Zbývá dokázat poslední část věty 5, tedy dokázat, že pro polovinu forem stupně 5 nad $\mathbb{F}_3$ existuje VID.

Nejdříve dosazením do vzorečku (5.2) spočítáme velikost $\mathcal{I}(3,5)$.
$|\mathcal{I}(3,5)| = \frac{1}{5}(3^5 - 3) = 48$.
Pro připomenutí rovnost (5.1) říká, že $|\Gamma| = q(q-1)(q+1)$. Tedy v našem případě $|\Gamma| = 3 \cdot 2 \cdot 4 = 24$.

Dále připomeňme lemma 17, díky kterému víme, že stabilizátor každé formy je cyklická grupa řádu dělícího d. Využijeme nerovnost (5.5) za tímto lemmatem,

že pro každé $f \in \mathcal{I}(3{,}5)$ platí:

$$|[f]| = \frac{|\Gamma|}{|\Gamma_f|} \geq \frac{|\Gamma|}{NSD(|\Gamma|,5)}$$
$$|[f]| = \frac{24}{\Gamma_f} \geq \frac{24}{1}$$

Z nerovnosti vidíme, že $\Gamma_f \leq 1$. Jelikož ve stabilizátoru leží určitě identita, dostáváme, že $\Gamma_f = 1$. Tedy velikost každé orbity $|[f]| = 24$.

Celkem je v $\mathcal{I}(3{,}5)$ 48 prvků, proto $\mathcal{I}(3{,}5)$ musí obsahovat 2 orbity, každou o velikosti 24.

Sestavme nyní všechny tvary VIS. Podle definice tvaru VIS musí obsahovat všechny lineární a kvadratické ireducibilní formy. Z tabulky 6.1 vidíme, že to jsou právě čtyři lineární formy L_1, L_2, L_3, L_4, z nichž jedna je speciální forma L_Y, a tři kvadratické Q_1, Q_2, Q_3.

Jako obvykle r značí počet sčítanců v HVID. Můžeme využít lemma 19, které nám dává na r omezení.

$$dr \geq (r-1)\left|\bigcup_{n=1}^{\lfloor d/2 \rfloor} \mathbb{F}_{q^n}\right|$$
$$5r \geq (r-1)(9-3)$$
$$r \leq 6$$

Podrobným rozebráním však zjistíme, že r nemůže být ve skutečnosti větší než 2.

Problém rozdělíme na dva případy, podle toho kde se nacházejí kvadratické formy Q_1, Q_2, Q_3.

Nejdříve uvažujme, že jedna z kvadratických forem BÚNO Q_1 se nachází v prvním i druhém sčítanci. Potom kvůli stupni součtu $d = 5$ se zbývající Q_2, Q_3 musí nacházet v různých sčítancích. Celkový stupeň v obou sčítancích je nyní 4, tedy každý může obsahovat ještě jednu lineární formu. Tvar součtu bude vypadat například takto: $Q_1Q_2L_1 + c_1Q_1Q_2L_2 + c_2F_3 + \cdots + c_{r-1}F_r$, kde c_i jsou konstanty v $\mathbb{F}_3$. Vidíme, že ani v jednom z prvních dvou sčítanců se už nemůže nacházet forma L_3. Tedy L_3 nesplňuje podmínku HVID-1 a tento součet není VIS.

Ve druhém případě uvažujme, že se každá z forem Q_1, Q_2, Q_3 nachází v prvních dvou sčítancích jen jednou. Potom aby byla splněna podmínka HVID-1, musí se ve zbývajících sčítancích nacházet všechny formy Q_1, Q_2, Q_3 zároveň. Tím byl ale překročen stupeň součtu, proto ani tento součet není VIS.

Nyní už víme, že $r = 2$.

Pokud L_Y také splňuje podmínku HVID-1, pak pro VIS máme až na permutaci indexů u forem L_i a forem Q_i jedinou možnost:

$$F_1 = L_1Q_2Q_3 + cL_2L_3L_4Q_1$$

Různé instance můžeme dostat, pokud za $L_1,\ Q_1$ dosazujeme různé formy a za c různé konstanty. Pro L_1 máme čtyři možnosti, pro Q_1 tři a pro c dvě možnosti. Celkem tedy dostaneme nejvýše 24 různých instancí.

Zároveň dokážeme, že VIS F_1 má nejméně 24 různých instancí. Zřejmě F_1 reprezentuje aspoň jednu z forem z $\mathcal{I}(3{,}5)$. Protože také forma L_Y splňuje podmínku HVID-1, pro VIS F_1 platí lemma 12. Neboli pokud F_1 reprezentuje jednu z forem Γ-orbity, pak už reprezentuje všechny formy této orbity. Odtud vyplývá, že F_1 má právě 24 instancí .

Odtud také plyne, že VIS F_1 reprezentuje všechny formy v jedné orbitě, ale už nemůže reprezentovat formy ve druhé orbitě. Obě orbity jsou stejně velké, tedy reprezentuje právě polovinu forem.

Forma L_Y ovšem podmínku HVID-1 splňovat nemusí. Pro $r = 2$ to znamená, že L_Y se ve tvaru VIS vůbec neobjevuje.

Opět až na permutaci indexů u forem L_i a forem Q_i máme pro VIS jedinou možnost.

$$F_2 = L_1Q_2Q_3 + cL_2^2L_3L_4Q_1$$

Díky podobné úvaze jako výše vidíme, že pro L_2 máme tři možnosti, pro Q_1 také tři a pro c dvě možnosti.

Tedy celkem můžeme dostat 18 instancí. Nyní je potřeba ověřit, že každá z těchto instancí buď nesplňuje podmínku HVID-2, nebo dostaneme stejnou instanci jako už reprezentuje F_1. Konkrétní instance zde uvádět nebudeme, ale po vypsání všech možností zjistíme, že žádné další instance už nedostaneme.

Závěr

Obecnější definicí tvaru VID jsme dosáhli tvarů VID, které definice ze článku [1] nepřipouštěla. Zejména v hlavní větě 18 přibyla nová dvojice $(q,d) = (4,2)$.

Na druhou stranu jsme také ztratili některé z pěkných vlastností působení Γ na $\mathcal{I}(q,d)$. V lemmatu 41, které říká, že Γ zachovává tvary HVID-S jsme museli pracovat z definicí ze článku [1] a v lemmatu 58, které určuje, že instance tvaru VIS pokrývají všechny prvky Γ-orbity, jsme taky museli přidat podmínku, která koresponduje s definicí HVID-S.

Tímto se nám ztížilo hledání rozkladů HVID, protože jsme u tvarů VIS, které neodpovídají definici HVID-S museli podmínku HVID-2 ověřovat mechanicky konkrétním výpisem všech instancí.

Seznam použité literatury

[1] Evan M. O'Dorney. Visibly irreducible polynomials over finite fields. page 11, 2018, arXiv:1808.10440 [math.NT].

[2] Tůma J. Barto, L. Konečná tělesa. http://www.karlin.mff.cuni.cz/ barto/ student/SkriptaKonTel.pdf.

[3] D. Stanovský. *Základy algebry*. MatfyzPress, Praha, 2010.