UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

Zaključna naloga

# Kvadratne forme nad končnimi obsegi

(Quadratic Forms over Finite Fields)

Ime in priimek: Borut Umer
Študijski program: Matematika
Mentor: doc. dr. Marko Orel

**Koper, avgust 2014**

# Ključna dokumentacijska informacija

Ime in PRIIMEK: Borut UMER

Naslov zaključne naloge: Kvadratne forme nad končnimi obsegi

Kraj: Koper

Leto: 2014

Število listov: 31

Število referenc: 10

Mentor: doc. dr. Marko Orel

Ključne besede: Končni obseg, polje, sled elementa, kvadratna forma

Math. Subj. Class. (2010): 15A63, 12E20, 15B33

**Izvleček:**
Zaključna projektna naloga preučuje kvadratne forme nad končnim obsegom $\mathbb{F}_q$. V nalogi smo poiskali število $n$-teric $(x_1, x_2, \ldots, x_n)$, ki rešijo enačbo $f(x_1, x_2, \ldots, x_n) = b$, kjer je $f(x_1, x_2, \ldots, x_n)$ kvadratna forma nad končnim obsegom $\mathbb{F}_q$ in $b$ nek fiksen element iz obsega $\mathbb{F}_q$. Izkazalo se je, da se je potrebno posvetiti posebej končnim obsegom lihe in posebej končnim obsegom sode karakteristike. Do ekvivalentnosti natančno so klasificirane vse nedegenerirane kvadratne forme. S pomočjo kanoničnih form za simetrične matrike klasificiramo tudi vse degenerirane kvadratne forme nad končnim obsegom lihe karakteristike.

# Key words documentation

Name and SURNAME: Borut UMER

Title of final project paper: Quadratic Forms over Finite Fields

Place: Koper

Year: 2014

Number of pages: 31

Number of references: 10

Mentor: Assist. Prof. Marko Orel, PhD

Keywords: Finite Field, Trace of an Element, Quadratic Forms

Math. Subj. Class. (2010): 15A63, 12E20, 15B33

**Abstract:**
In the final project paper we study quadratic forms over finite fields $\mathbb{F}_q$. We get the number of $n$-tuples $(x_1, x_2, \ldots, x_n)$, such that $f(x_1, x_2, \ldots, x_n) = b$, where $f(x_1, x_2, \ldots, x_n)$ is a quadratic form over a finite field $\mathbb{F}_q$ and $b$ is a fixed number in $\mathbb{F}_q$. We address the problem where the characteristic of the finite field $\mathbb{F}_q$ is odd and even. Nondegenerate quadratic forms are classified up to equivalence. With canonical forms for symmetric matrices we classify also degenerate quadratic forms over finite fields of odd characteristic.

# Zahvala

Hvaležen sem Fakulteti za matematiko, naravoslovje in informacijske tehnologije Univerze na Primorskem, ki je zadnja tri leta omogočala moj študij na omenjeni fakulteti.

Želel bi se zahvaliti vsem profesorjem Fakultete za matematiko, naravoslovje in informacijske tehnologije v Kopru, ki so me kadar koli učili in me pripeljali do te točke v življenju, kjer sem sedaj.

Posebna zahvala gre mentorju dr. Marku Orlu, ki mi je predlagal uporabno literaturo in je bil na voljo vedno, ko sem potreboval nasvete in popravke.

Hvala staršem in prijateljem, ki so me vzpodbujali in podpirali v času nastajanja te zaključne naloge.

Najlepša hvala tudi Kseniji Terglav Jakopin, ki si je vzela čas in pregledala mojo zaključno nalogo.

Na koncu bi želel omeniti mojo najdražjo, ki mi je ves čas nastajanja zaključne naloge potrpežljivo stala ob strani, me vzpodbujala pri delu in si je vedno rada vzela čas in mi pomagala pri izdelavi te naloge.

# Kazalo vsebine

**1 Uvod** **1**

**2 Končni obsegi** **2**

2.1 Nekaj osnovnih lastnosti . . . . . 2

2.2 Sled elementa . . . . . 5

**3 Kvadratne forme nad končnimi obsegi** **8**

3.1 Kvadratne forme nad končnimi obsegi lihe karakteristike . . . . . 9

3.2 Kvadratne forme nad končnimi obsegi sode karakteristike . . . . . 15

**4 Kanonične forme simetričnih matrik nad končnimi obsegi lihe karakteristike** **19**

**5 Zaključek** **24**

**6 Literatura** **25**

# Seznam kratic

*tj.* to je
*npr.* na primer

# 1 Uvod

Kvadratna forma v $n$ spremenljivkah nad končnim obsegom $\mathbb{F}_q$ je polinom oblike

$$f(x_1, x_2, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j,$$

kjer so $a_{ij}$ fiksni elementi obsega $\mathbb{F}_q$. V nalogi bomo izpeljali formulo za število $n$-teric $(x_1, x_2, \ldots, x_n)$, ki rešijo enačbo $f(x_1, x_2, \ldots, x_n) = b$, kjer je $b$ fiksen element iz $\mathbb{F}_q$.

Uporabnost tovrstnega rezultata sega do Lagrangea [3]. Slednji je pri dokazu izreka, ki pravi, da lahko vsako naravno število zapišmo kot vsoto štirih kvadratov, uporabil dejstvo, da je enačba $x^2 + by^2 = c$ v praševilskem končnem obsegu vedno rešljiva, če sta $b$ in $c$ neničelna. V sodobni matematiki zasledimo kvadratne forme nad končnimi obsegi na številnih področjih. Sorodne so simetričnim matrikam [9, 10], v končni geometriji predstavljajo ogrodje ortogonalnih polarnih prostorov [8], uporabne so v teoriji kodiranja [7], zasledimo pa jih tudi na področju ohranjevalcev [5]. Za osrednje izreke iz naloge je v tej splošnosti najbolj odgovoren Dickson [1, 2].

V nalogi si bomo najprej ogledali osnovne lastnosti končnih obsegov, ki jih je potrebno ponoviti. Omenili bomo pomembne definicije, izreke in trditve, ki jih bomo uporabljali v nadaljevanju naloge. Ogledali si bomo tudi nekaj primerov končnih obsegov neprašteviske moči in njihovo konstrukcijo.

Glavni del naloge bo potekal v dveh razdelkih poglavja 3, kjer bomo ločili primer, ko je karakteristika končnega obsega liha oziroma soda. V obeh primerih bomo izpeljali formulo, ki nam natančno pove, koliko rešitev ima enačba $f(x_1, x_2, \ldots, x_n) = b$ v obsegu $\mathbb{F}_q$. Izpeljava temelji na klasifikaciji nedegeneriranih kvadratnih form. Poglavje 3 se bo v največji meri opiralo na knjigo [4].

V poglavju 4 si bomo ogledali kanonične forme simetričnih matrik nad končnimi obsegi lihe karakteristike. S pomočjo le teh bomo klasificirali tudi degenerirane kvadratne forme nad končnimi obsegi lihe karakteristike. Snov iz tega poglavja je povzeta iz knjige [9].

# 2 Končni obsegi

V tem razdelku bomo navedli nekaj lastnosti o končnih obsegih, ki jih bomo potrebovali v nadaljevanju.

**Definicija 2.1.** Naj bo $F$ poljubna neprazna množica z notranjima binarnima operacijama $+$ in $\cdot$. Trojici $(F, +, \cdot)$ pravimo obseg, če velja:

1. $(F, +)$ je abelova grupa za seštevanje z enoto 0;
2. $(F\backslash\{0\}, \cdot)$ je grupa z enoto 1;
3. operaciji $+$ in $\cdot$ sta povezani z distributivnostjo (za vse $a, b, c \in F$ velja $a(b + c) = ab + ac$, $(b + c)a = ba + ca$).

*Opomba* 2.2. Kot običajno bomo privzeli, da velja $1 \neq 0$.

V primeru, ko je moč množice $F$ enaka $q$, kjer je $q < \infty$, govorimo o končnih obsegih.

Spodnja trditev je dobro znana in se nahaja npr. v izreku 0.3.4 iz knjige [6].

**Trditev 2.3.** *Naj bo $K$ komutativen kolobar praštevilske karakteristike $p$. Potem velja:*

$$(a + b)^{p^n} = a^{p^n} + b^{p^n} \quad in \quad (a - b)^{p^n} = a^{p^n} - b^{p^n}$$

*za vse $a, b \in K$ in $n \in \mathbb{N}$.*

Končni obseg $(F, +, \cdot)$ s $q$ elementi bomo označili s $\mathbb{F}_q$. Množico $\mathbb{F}_q\backslash\{0\}$ bomo označili s $\mathbb{F}_q^*$. Množico polinomov v nedoločenki $x$ s koeficienti iz obsega $\mathbb{F}_q$ bomo označevali s $\mathbb{F}_q[x]$.

## 2.1 Nekaj osnovnih lastnosti

Dokaz izreka 2.4 najdemo npr. v izreku 10.4.1 v knjigi [6].

**Izrek 2.4** (Wedderburnov izrek)**.** *Vsak končni obseg je polje.*

Dokaz Izrekov 2.5, 2.6 ter trditev 2.7 in 2.9 najdemo v razdelkih 8.1 in 8.2 knjige [6].

**Izrek 2.5.** *Vsak končni obseg je moči $p^k$, kjer je $p$ praštevilo, $k$ pa naravno število.*

**Izrek 2.6.** *Za vsako praštevilo $p$ in naravno število $k$ obstaja do izomorfnosti natanko en obseg moči $p^k$.*

**Trditev 2.7.** *Množica $\mathbb{F}_q^*$ je ciklična grupa za množenje.*

Stopnjo polinoma $f$ bomo označili z $\deg(f)$.

**Definicija 2.8.** Polinom $f \in \mathbb{F}_q[x]$ je *nerazcepen* nad $\mathbb{F}_q$, če ne obstajata polinoma $g, h \in \mathbb{F}_q[x]$, za katera velja $\deg(g), \deg(h) < \deg(f)$ in $f = gh$.

**Trditev 2.9.** *Obseg $\mathbb{F}_{q^k}$ je vektorski prostor dimenzije $k$ nad obsegom $\mathbb{F}_q$.*

Oznaka $F[\alpha]$ predstavlja množico $\{f(\alpha); f \in F[x]\}$. Dokaz izrekov 2.10 in 2.11 najdemo v knjigi [9].

**Izrek 2.10.** *Naj bo $E$ polje, $F$ podpolje polja $e$ in $\alpha \in e$. Naj bo $f(x)$ nerazcepen polinom stopnje $n$ nad poljem $F$ in predpostavimo, da je $f(\alpha) = 0$. Potem je $F[\alpha]$ podpolje polja $E$ in velja*

$$F[\alpha] = \left\{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}; a_i \in F\right\}.$$

*Vsak element iz $F[\alpha]$ se da enolično zapisati v obliki $a_0+a_1\alpha+a_2\alpha^2+\cdots+a_{n-1}\alpha^{n-1}$, kjer so $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}$. Še več, $F[\alpha]$ je izomorfen kvocientnemu polju $F[x]/\langle f(x)\rangle$. V primeru, ko je $\mathbb{F}$ končno polje s $q$ elementi, je moč polja $F[\alpha]$ enaka $q^n$.*

**Izrek 2.11.** *Naj bo $F$ polje in $f(x)$ nerazcepen polinom stopnje $n$ nad $F$. Označimo razred ostanka polinoma $x \pmod{f(x)}$ z $\alpha$. Potem je*

$$F[x]/\langle f(x)\rangle \simeq F[\alpha].$$

*Če je $F$ končno polje s $q$ elementi, potem je moč množice $F[x]/\langle f(x)\rangle$ enaka $q^n$.*

**Primer 2.12.** Naj bo $p$ praštevilo. Množica $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ je končni obseg z operacijama $+$ in $\cdot$ definiranima na naslednji način: za poljubna $a, b \in \mathbb{F}_p$ velja $a + b = a + b \pmod p$ in $a \cdot b = a \cdot b \pmod p$.

V naslednjih primerih bomo računali po modulu $p$, kar pomeni, da nam bo izraz $a + b$ pomenil $a + b \pmod p$ in $ab$ bo pomenil $ab \pmod p$.

**Primer 2.13.** Ena od možnih konstrukcij polja $\mathbb{F}_4$ je sledeča. Začnemo s poljem $\mathbb{F}_2 = \{0, 1\}$. Poiščemo nerazcepen polinom $f$ stopnje 2 nad poljem $\mathbb{F}_2$. V našem primeru je to polinom $f(x) = x^2 + x + 1$, za katerega se je lahko prepričati, da je nerazcepen. Če bi bil razcepen, bi razpadel na dva linearna faktorja, kar pomeni, da nam je dovolj preveriti vrednosti $f(0)$ in $f(1)$. Velja $f(0) = 0 + 0 + 1 = 1 \neq 0$ in $f(1) = 1 + 1 + 1 = 1 \neq 0$. Po izreku 2.11 obstaja polje moči 4, ki vsebuje polje $\mathbb{F}_2$ in tak element $\alpha$ , da velja $\alpha^2 + \alpha + 1 = 0$. Po izreku 2.10 je to polje

$$\mathbb{F}_2[\alpha] = \{0, 1, \alpha, 1 + \alpha\} = \mathbb{F}_4.$$

**Primer 2.14.** Na podoben način skonstruiramo tudi polje $\mathbb{F}_9$. Poiščemo nerazcepen polinom $f$ nad poljem $\mathbb{F}_3 = \{0, 1, 2\}$. Po podobnem premisleku kot zgoraj nam je za nerazcepnost polinoma $f(x) = x^2 + 1$ dovolj preveriti vrednosti $f(0)$, $f(1)$ in $f(2)$. Velja $f(0) = 1 \neq 0$, $f(1) = 1 + 1 = 2 \neq 0$ in $f(2) = 1 + 1 \neq 0$. Polinom $f$ je torej nerazcepen. Vzemimo tak $\alpha$, za katerega velja $f(\alpha) = 0$. Po izreku 2.10 je iskano polje

$$\mathbb{F}_3[\alpha] = \{0, 1, 2, \alpha, 1 + \alpha, 2 + \alpha, 2\alpha, 1 + 2\alpha, 2 + 2\alpha\} = \mathbb{F}_9.$$

**Primer 2.15.** Konstrukcija polja $\mathbb{F}_{16}$ je že malo bolj zapletena, saj zanjo potrebujemo nerazcepen polinom stopnje 4. Začnimo s poljem $\mathbb{F}_2$ in preverimo, da je polinom $f(x) = x^4 + x + 1$ res nerazcepen nad tem poljem. Iz $f(0) = 0 + 0 + 1 = 1 \neq 0$ in $f(1) = 1+1+1 = 1 \neq 0$ vidimo, da polinom ne razpade na linearne faktorje. Potrebno je preveriti le, če polinom ne razpade na kvadratne faktorje. Hitro opazimo, da so le štirje kvadratni polinomi nad $\mathbb{F}_2$, natančneje, $x^2$, $x^2 + 1$, $x^2 + x$ in $x^2 + x + 1$. Z deljenjem polinoma $f$ s temi štirimi kvadratnimi polinomi se prepričamo, da je le ta res nerazcepen. Vzemimo tak $\alpha$, za katerega velja $f(\alpha) = 0$. Po izreku 2.10 je iskano polje

$$\begin{aligned}\mathbb{F}_2[\alpha] \;=\; & \{0, 1, \alpha, \alpha + 1,\\ & \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1,\\ & \alpha^3, \alpha^3 + 1, \alpha^3 + \alpha, \alpha^3 + \alpha^2,\\ & \alpha^3 + \alpha + 1, \alpha^3 + \alpha^2 + 1, \alpha^3 + \alpha^2 + \alpha\\ & \alpha^3 + \alpha^2 + \alpha + 1\} = \mathbb{F}_{16}.\end{aligned}$$

Naj bo $\mathbb{F}_q$ končni obseg s $q$ elementi. Množici $\{x^2; x \in \mathbb{F}_q\}$ in $\{x^2; x \in \mathbb{F}_q^*\}$ bomo označili s $\mathbb{F}_q^2$ in s $\mathbb{F}_q^{*2}$.

**Izrek 2.16.** *Naj bo $\mathbb{F}_q$ končni obseg s $q$ elementi, kjer je $q$ potenca praštevila.*

*(i) Če je $q = 2^n$ za nek $n \in \mathbb{N}$, je vsak element iz $\mathbb{F}_q$ kvadrat. Z drugimi besedami, velja $\mathbb{F}_q = \mathbb{F}_q^2$ in $\mathbb{F}_q^* = \mathbb{F}_q^{*2}$. Še več, vsak element iz $\mathbb{F}_q$ ima enolično določen kvadratni koren v $\mathbb{F}_q$.*

*(ii) Če je $q$ liho število, potem je $\mathbb{F}_q^{*2}$ podgrupa indeksa 2 v grupi $\mathbb{F}_q^*$. Za poljuben $z \in \mathbb{F}_q^* \backslash \mathbb{F}_q^{*2}$ je $\mathbb{F}_q^{*2} \cup z\mathbb{F}_q^{*2} = \mathbb{F}_q^*$ disjunktna unija. Poleg tega ima vsak element iz $\mathbb{F}_q^{*2}$ dva kvadratna korena v $\mathbb{F}_q^*$ in vsak element iz $z\mathbb{F}_q^{*2}$ nima nobenega kvadratnega korena v $\mathbb{F}_q^*$.*

*Dokaz.* $(i)$ Oglejmo si preslikavo $\sigma_2$ iz $\mathbb{F}_{2^n}$ v $\mathbb{F}_{2^n}$, ki je definirana s predpisom $\sigma_2(x) = x^2$. Predpostavimo, da je $\sigma_2(x) = \sigma_2(y)$. To pomeni, da je $x^2 = y^2$. Po trditvi 2.3

je $(x-y)^2 = x^2 - y^2$ in $x^2 - y^2 = 0$. Toda $\mathbb{F}_{2^n}$ nima deliteljev niča, torej sta $x$ in $y$ enaka. To dokazuje injektivnost preslikave $\sigma_2$. Ker je $\mathbb{F}_{2^n}$ končni obseg, je $\sigma_2$ bijektivna preslikava. Zato velja $\mathbb{F}_{2^n}^2 = \mathbb{F}_{2^n}$. Ker je $0^2 = 0$, velja tudi $\mathbb{F}_{2^n}^{*2} = \mathbb{F}_{2^n}^*$.

Za poljuben $x \in \mathbb{F}_{2^n}$ obstaja tak element $x_0 \in \mathbb{F}_{2^n}$, da je $x = x_0^2$. Predpostavimo, da je $x = x_0^2 = y_0^2$, kjer sta $x_0, y_0 \in \mathbb{F}_{2^n}$. Potem je $(x_0 - y_0)^2 = 0$ in zato $x_0 = y_0$. To pomeni, da ima vsak element v $\mathbb{F}_{2^n}$ enolično določen kvadratni koren v $\mathbb{F}_{2^n}$.

(*ii*) Po trditvi 2.7 je $\mathbb{F}_q^*$ ciklična grupa. Ker je $q$ liho število, je $|\mathbb{F}_q^*| = q-1$ sodo število. Naj bo $\xi$ primitiven element v $\mathbb{F}_q$, to pomeni, da je $\mathbb{F}_q^* = \langle \xi \rangle$ in $\xi$ je reda $q-1$. Očitno je tudi $\mathbb{F}_q^{*2} = \langle \xi^2 \rangle$, kjer je $\xi^2$ reda $\frac{q-1}{2}$ in je $\mathbb{F}_q^* = \mathbb{F}_q^{*2} \cup \xi\mathbb{F}_q^{*2}$ disjunktna unija. To pomeni, da je $\mathbb{F}_q^{*2}$ podgrupa indeksa 2 v $\mathbb{F}_q^*$. Za poljuben $z \in \mathbb{F}_q^* \backslash \mathbb{F}_q^{*2}$ je tudi $\mathbb{F}_q^{*2} \cup z\mathbb{F}_q^{*2} = \mathbb{F}_q^*$ disjunktna unija.

Opazimo, da za poljuben element $x \in \mathbb{F}_q^{*2}$ obstaja tak element $x_0 \in \mathbb{F}_q^*$, da je $x = x_0^2$. Imamo tudi element $-x_0 \neq x_0$, za katerega velja $(-x_0)^2 = x$. Predpostavimo, da je $x = x_0^2 = y_0^2$, kjer sta $x_0, y_0 \in \mathbb{F}_q^*$. Potem je $(x_0^{-1}y_0)^2 = 1$, kar nam da $x_0^{-1}y_0 = \pm 1$ in torej $y_0 = \pm x_0$. To pomeni, da ima vsak element iz $\mathbb{F}_q^{*2}$ dva kvadratna korena v $\mathbb{F}_q^*$. Za poljuben element $y \in z\mathbb{F}_q^{*2}$ velja $y = zu^2$ za nek $u \in \mathbb{F}_q^*$. Predpostavimo, da obstaja tak element $y_0 \in \mathbb{F}_q^{*2}$, za katerega velja $y = y_0^2$. Potem je $zu^2 = y_0^2$ oziroma $z = (y_0u^{-1})^2 \in \mathbb{F}_q^{*2}$, kar je v protislovju s predpostavko, da je $z \in \mathbb{F}_q^* \backslash \mathbb{F}_q^{*2}$. To pomeni, da noben od elementov iz $z\mathbb{F}_q^{*2}$ nima kvadratnega korena v $\mathbb{F}_q^*$. □

Za lih $q$ elementom iz množice $\mathbb{F}_q^{*2}$ rečemo *kvadrati elementov* $\mathbb{F}_q^*$ in elementom iz množice $\mathbb{F}_q^* \backslash \mathbb{F}_q^{*2}$ rečemo *nekvadrati elementov* $\mathbb{F}_q^*$.

## 2.2 Sled elementa

**Definicija 2.17.** Za $\alpha \in F = \mathbb{F}_{q^m}$ in $K = \mathbb{F}_q$ je *sled elementa* $\alpha$ nad $K$ definirana kot

$$\alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}}.$$

Vsoto bomo označili s $\mathrm{Tr}_{F/K}(\alpha)$. Če je $K = \mathbb{F}_p$, kjer je $p$ praštevilo, potem sledi $\mathrm{Tr}_{F/K}(\alpha)$ pravimo *absolutna sled* elementa $\alpha$ in jo označimo s $\mathrm{Tr}_F(\alpha)$.

Ker je $\mathrm{Tr}_{F/K}(\alpha)^q = \mathrm{Tr}_{F/K}(\alpha)$, sledi $\mathrm{Tr}_{F/K}(\alpha) \in K$ za vsak $\alpha \in F$.

**Trditev 2.18.** *Naj bosta $F = \mathbb{F}_{q^m}$ in $K = \mathbb{F}_q$ končna obsega, potem ima funkcija $\mathrm{Tr}_{F/K}$ naslednje lastnosti:*

*(i)* $\mathrm{Tr}_{F/K}(\alpha + \beta) = \mathrm{Tr}_{F/K}(\alpha) + \mathrm{Tr}_{F/K}(\beta)$ *za vse* $\alpha, \beta \in F$*;*

*(ii)* $\mathrm{Tr}_{F/K}(c\alpha) = c\mathrm{Tr}_{F/K}(\alpha)$ *za vse* $c \in K$ *in* $\alpha \in F$*;*

*(iii)* $\mathrm{Tr}_{F/K}$ *je surjektivna linearna transformacija iz* $F$ *v* $K$*, kjer tako na* $F$ *kot na* $K$ *gledamo kot na vektorska prostora nad prostorom* $K$*;*

*(iv)* $\mathrm{Tr}_{F/K}(a) = ma$ *za vse* $a \in K$*;*

*(v)* $\mathrm{Tr}_{F/K}(\alpha^q) = \mathrm{Tr}_{F/K}(\alpha)$ *za vse* $\alpha \in F$*.*

*Dokaz.* (i) Za $\alpha, \beta \in F$ in po izreku 2.3 dobimo

$$\begin{aligned}\mathrm{Tr}_{F/K}(\alpha+\beta) &= \alpha+\beta+(\alpha+\beta)^q+\cdots+(\alpha+\beta)^{q^{m-1}}\\ &= \alpha+\beta+\alpha^q+\beta^q+\cdots+\alpha^{q^{m-1}}+\beta^{q^{m-1}}\\ &= \mathrm{Tr}_{F/K}(\alpha)+\mathrm{Tr}_{F/K}(\beta).\end{aligned}$$

(ii) Za $c \in K$ velja $c^{q^j} = c$ za vse $j \geq 0$. Posledično za $\alpha \in F$ velja

$$\begin{aligned}\mathrm{Tr}_{F/K}(c\alpha) &= c\alpha+c^q\alpha^q+\cdots+c^{q^{m-1}}\alpha^{q^{m-1}}\\ &= c\alpha+c\alpha^q+\cdots+c\alpha^{q^{m-1}}\\ &= c\mathrm{Tr}_{F/K}(\alpha).\end{aligned}$$

(iii) Lastnosti (i) in (ii) skupaj z dejstvom, da je $\mathrm{Tr}_{F/K}(\alpha) \in K$ za vse $\alpha \in F$, nam pokažejo, da je $\mathrm{Tr}_{F/K}$ linearna transformacija iz $F$ v $K$. Potrebno je pokazati še surjektivnost. Dovolj nam je pokazati, da obstaja tak $\alpha \in F$, za katerega velja $\mathrm{Tr}_{F/K}(\alpha) \neq 0$. Lastnost $\mathrm{Tr}_{F/K}(\alpha) = 0$ velja, če in samo če je $\alpha$ ničla polinoma $x^{q^{m-1}} + x^{q^{m-2}} + \cdots + x \in K[x]$. Polinom $x^{q^{m-1}} + x^{q^{m-2}} + \cdots + x$ ima kvečjemu $q^{m-1}$ ničel, obseg $F$ pa ima $q^m$ elementov, kar pomeni, da obstaja nek $\beta \in F$, za katerega velja $\mathrm{Tr}_{F/K}(\beta) \neq 0$.

(iv) Za $a \in K$ velja $\mathrm{Tr}_{F/K}(a) = a + a^q + \cdots + a^{q^{m-1}} = a + a + \cdots + a = ma$.

(v) Za $\alpha \in F$ velja $\alpha^{q^m} = \alpha$, torej je $\mathrm{Tr}_{F/K}(\alpha^q) = \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^m} = \mathrm{Tr}_{F/K}(\alpha)$.

□

**Trditev 2.19.** *Naj bosta* $F = \mathbb{F}_{q^m}$ *in* $K = \mathbb{F}_q$ *končna obsega. Linearne preslikave iz* $F$ *v* $K$ *so ravno preslikave* $L_\beta$*, kjer je* $\beta \in F$ *in je* $L_\beta(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha)$ *za vse* $\alpha \in F$*. Poleg tega velja še* $L_\beta \neq L_\gamma$ *za poljubna različna elementa* $\beta$ *in* $\gamma$ *iz obsega* $F$*.*

*Dokaz.* Vsaka preslikava $L_\beta$ je linearna transformacija iz $F$ v $K$ po trditvi 2.18. Naj bosta $\beta, \gamma \in F$ različna. S pravilno izbranim $\alpha \in F$ dobimo

$$L_\beta(\alpha) - L_\gamma(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha) - \mathrm{Tr}_{F/K}(\gamma\alpha) = \mathrm{Tr}_{F/K}((\beta-\gamma)\alpha) \neq 0,$$

kar pomeni, da sta preslikavi $L_\beta$ in $L_\gamma$ res različni. Ker je $\beta \in F$, lahko z $L_\beta$ dobimo natanko $q^m$ različnih linearnih transformacij iz $F$ v $K$. Po drugi strani lahko vsako

linearno transformacijo iz $F$ v $K$ dobimo tako, da vsakemu izmed $m$-tih elementov iz baze $F$ nad $K$ priredimo en element iz množice $K$. To lahko naredimo ravno na $q^m$ načinov, kar je ravno število vseh možnih preslikav $L_\beta$. □

**Trditev 2.20.** *Naj bosta $F = \mathbb{F}_{q^m}$ in $K = \mathbb{F}_q$ končna obsega. Za poljuben $\alpha \in F$ velja $\mathrm{Tr}_{F/K}(\alpha) = 0$, če in samo če velja $\alpha = \beta^q - \beta$ za nek $\beta \in F$.*

*Dokaz.* Predpostavimo, da je $\alpha = \beta^q - \beta$ za nek $\beta \in F$. Če delujemo s $\mathrm{Tr}_{F/K}$ na obe strani enačbe, dobimo $\mathrm{Tr}_{F/K}(\alpha) = 0$ po trditvi 2.18.

Predpostavimo, da je $\alpha \in F$, za katerega velja $\mathrm{Tr}_{F/K}(\alpha) = 0$ in naj bo $\beta$ tak element neke razširitve obsega $F$, za katerega bo veljalo, da je ničla polinoma $x^q - x - \alpha$. Potem je $\beta^q - \beta = \alpha$. Poleg tega velja tudi

$$\begin{aligned} 0 &= \mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}} \\ &= (\beta^q - \beta) + (\beta^q - \beta)^q + \cdots + (\beta^q - \beta)^{q^{m-1}} \\ &= \beta^{q^m} - \beta, \end{aligned}$$

kar pomeni, da je $\beta \in F$. □

# 3 Kvadratne forme nad končnimi obsegi

**Definicija 3.1.** Kvadratna forma nad končnim obsegom $\mathbb{F}_q$ je polinom oblike

$$f(x_1, x_2, \ldots, x_n) \;=\; \sum_{1 \le i \le j \le n} b_{ij} x_i x_j,$$

kjer so $b_{ij}$ fiksni elementi obsega $\mathbb{F}_q$.

Cilj tega poglavja je poiskati število $N(f(x_1, \ldots, x_n) = b)$, ki označuje število $n$-teric $x_1, \ldots, x_n$ v prostoru $\mathbb{F}_q^n$, ki rešijo enačbo $f(x_1, \ldots, x_n) = b$.

Za izračun števila $N(f(x_1, \ldots, x_n) = b)$ moramo najprej $f$ preoblikovati s pomočjo linearne substitucije nedoločenk v bolj enostavno obliko. V splošnem lahko linearno substitucijo predstavimo z linearno enačbo $\mathbf{x} = C\mathbf{y}$, kjer je $C$ $n \times n$ matrika s koeficienti iz obsega $\mathbb{F}_q$ in $\mathbf{y}$ nov vektor nedoločenk $y_1, y_2, \ldots, y_n$. Če je $C$ nesingularna, govorimo o *nesingularni linearni substituciji.*

**Definicija 3.2.** Za poljuben končni obseg $\mathbb{F}_q$ pravimo, da sta dve kvadratni formi $f$ in $g$ nad $\mathbb{F}_q$ ekvivalentni, če lahko $f$ preoblikujemo v $g$ s pomočjo nesingularne linearne substitucije nedoločenk.

Ni težko opaziti, da nam ekvivalenca kvadratnih form porodi ekvivalenčno relacijo. Še več. Če sta $f$ in $g$ ekvivalentni, imata enačbi $f(x_1, x_2, \ldots, x_n) = b$ in $g(x_1, x_2, \ldots, x_n) = b$ enako število rešitev v $\mathbb{F}_q^n$ za poljuben $b \in \mathbb{F}_q$, saj lahko s pomočjo matrike $C$ vzpostavimo bijekcijo med vektorji rešitev.

Pri izračunu števila $N(f(x_1, \ldots, x_n) = b)$ je potrebno obravnavati dva primera. Najprej se bomo posvetili problemu, ko je karakteristika polja $\mathbb{F}_q$ liha, nato si bomo ogledali primer, ko je karakteristika polja $\mathbb{F}_q$ soda.

## 3.1 Kvadratne forme nad končnimi obsegi lihe karakteristike

Naj bo $\mathbb{F}_q$ končni obseg lihe karakteristike. Naredimo nove koeficiente $a_{ij}$ polinoma $f$, za katere velja:

$$\begin{aligned} a_{ij} = a_{ji} &= \frac{1}{2}b_{ij} \quad 1 \leq i < j \leq n, \\ a_{ii} &= b_{ii} \qquad 1 \leq i \leq n. \end{aligned}$$

Polinom $f$ lahko zapišemo v obliki

$$f(x_1, x_2, \ldots, x_n) = \sum_{1 \leq i,j \leq n} a_{ij} x_i x_j,$$

kjer velja

$$a_{ij} = a_{ji}, \quad 1 \leq i, j \leq n.$$

Polinomu $f$ lahko nato priredimo simetrično $n \times n$ matriko $A$, ki ima na $(i, j)$-tem mestu koeficiente $a_{ij}$. Matriki $A$ rečemo *matrika koeficientov*.

Če je $\mathbf{x}$ stolpični vektor nedoločenk $x_1, x_2, \ldots, x_n$, potem lahko $f(x_1, \ldots, x_n)$ zapišemo kot $\mathbf{x}^T A\mathbf{x}$.

**Primer 3.3.** Oglejmo si kvadratno formo $f(x_1, x_2) = 2x_1^2 + x_1x_2 + x_2^2$ v dveh nedoločenkah nad obsegom $\mathbb{F}_5$. Matrika koeficientov polinoma $f$ je enaka

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

Očitno velja tudi

$$\mathbf{x}^T A\mathbf{x} = \begin{bmatrix} x_1 & x_2 \end{bmatrix} \begin{bmatrix} 2 & 3 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = 2x_1^2 + x_1x_2 + x_2^2 = f(x_1, x_2).$$

Matriki $A$ in $B$ dveh ekvivalentnih kvadratnih form nad obsegom $\mathbb{F}_q$ sta povezani z zvezo $B = C^T AC$, saj velja $(C\mathbf{y})^T A(C\mathbf{y}) = \mathbf{y}^T(C^T AC)\mathbf{y}$.

Za lih $q$ bomo pokazali, da je vsaka kvadratna forma nad obsegom $\mathbb{F}_q$ ekvivalentna *diagonalni kvadratni formi* $a_1x_1^2 + \ldots + a_nx_n^2$ nad $\mathbb{F}_q$. Uporabili bomo naslednjo terminologijo: kvadratna forma $f$ nad $\mathbb{F}_q$ *predstavlja* $a \in \mathbb{F}_q$, če ima enačba $f(x_1, x_2, \ldots, x_n) = a$ kakšno rešitev v $\mathbb{F}_q^n$.

**Lema 3.4.** *V primeru, ko je $q$ liho število in kvadratna forma $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ predstavlja $a \in \mathbb{F}_q^*$, je $f$ ekvivalentna formi $ax_1^2 + g(x_2, \ldots, x_n)$, kjer je $g$ kvadratna forma nad $\mathbb{F}_q$ z $n-1$ nedoločenkami.*

*Dokaz.* Po predpostavki obstaja n-terica $(c_1, c_2, \ldots, c_n) \in \mathbb{F}_q^n$, za katero velja $f(c_1, c_2, \ldots, c_n) = a$. Ker je $a$ neničelen, je vektor $(c_1, \ldots, c_n)$ neničelen. Zato lahko poiščemo nesingularno $n \times n$ matriko $C$ nad $\mathbb{F}_q$, ki ima v prvem stolpcu koeficiente $c_1, \ldots c_n$. Nato na polinomu $f$ naredimo linearno substitucijo s pomočjo matrike $C$ in tako dobimo kvadratno formo z nedoločenkami $y_1, \ldots y_n$, pri kateri je koeficent pri členu $y_1^2$ ravno $f(c_1, c_2, \ldots, c_n) = a$. To pomeni, da je $f$ ekvivalenten kvadratni formi oblike

$$ay_1^2 + 2b_2y_1y_2 + \cdots + 2b_ny_1y_n + h(y_2, \ldots, y_n)$$
$$= a(y_1 + b_2a^{-1}y_2 + \cdots + b_na^{-1}y_n)^2 + g(y_2, \ldots, y_n)$$

za primerne $b_2, \ldots, b_n \in \mathbb{F}_q$ in kvadratni formi $h$, $g$ nad $\mathbb{F}_q$. Nesingularna linearna substitucija $x_1 = y_1 + b_2a^{-1}y_2 + \cdots + b_na^{-1}y_n$, $x_2 = y_2$, $\ldots$, $x_n = y_n$ nam da želeno obliko kvadratne forme. □

**Izrek 3.5.** *Naj bo q lih, potem je vsaka kvadratna forma nad $\mathbb{F}_q$ ekvivalentna diagonalni kvadratni formi.*

*Dokaz.* Trditev bomo dokazali z indukcijo po številu nedoločenk. V primeru, ko je $n = 1$, je $f(x_1) = a_{11}x_1^2$, kar je že diagonalna forma. Naj bo $n \geq 2$ in predpostavimo, da trditev velja za kvadratno formo z $n - 1$ nedoločenkami. Naj bo $f(x_1, \ldots, x_n)$ kvadratna forma v $n$ nedoločenkah. Če je $f$ ničelni polinom, trditev drži. V primeru, ko je $f$ neničelni polinom imamo dve možnosti. Prva možnost je, da obstaja nek $a_{ii}$, ki je različen od 0. V tem primeru $f$ predstavlja $a_{ii}$. Druga možnost je, da velja $a_{11} = a_{22} = \ldots = a_{nn} = 0$ in je $a_{ij} = a_{ji} \neq 0$ za nek $i \neq j$. V tem primeru $f$ predstavlja $2a_{ij}$, saj velja $f(c_1, \ldots c_n) = a_{ij}$, kjer je $c_i = c_j = 1$ in $c_k = 0$ za vsak $k \neq i, j$. V obeh primerih $f$ predstavlja nek element $a_i \in \mathbb{F}_q^*$, kar po lemi 3.4 pomeni, da je $f$ ekvivalenten formi $a_1x_1^2 + g(x_2, \ldots, x_n)$. Po indukcijski hipotezi je $g$ ekvivalenten diagonalni kvadratni formi $a_2x_2^2 + \cdots + a_nx_n^2$. Ker je ekvivalenca kvadratnih form ekvivalenčna relacija, kar pomeni, da je tranzitivna, je naša kvadratna forma $f$ ekvivalentna formi $a_1x_1^2 + \cdots + a_nx_n^2$. □

V nekaterih primerih se lahko zgodi, da je kvadratna forma $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ ekvivalentna diagonalni kvadratni formi $a_1x_1^2 + \cdots + a_nx_n^2$, ki ima nekatere člene $a_i$ enake 0. Množenje matrik z nesingularnimi matrikami ohranja rang. Ekvivalentne kvadratne forme imajo matrike istega ranga. Natančneje, število neničelnih $a_i$ v diagonalni kvadratni formi je enako rangu matrike koeficientov polinoma $f$. Naj bo $A$ matrika koeficientov kvadratne forme $f$ v $n$ nedoločenkah. Če je rang matrike $A$ enak $n$, pravimo, da je forma $f$ *nedegenerirana*. Podobno definiramo determinanto kvadratne forme $\det f$ kot determinanto matrike $A$. Za lihe $q$ lahko definiramo tudi *rang kvadratne forme* $f$ kot rang matrike koeficientov $A$.

Neničelni kvadratni formi $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ lahko brez škode za splošnost priredimo ekvivalentno diagonalno kvadratno formo oblike $a_1x_1^2+\cdots+a_kx_k^2$, kjer je $1 \leq k \leq n$ rang matrike koeficientov in so vsi $a_i$ neničelni. Ker je za poljuben $b \in \mathbb{F}_q$ število rešitev enačbe $a_1x_1^2 + \cdots + a_kx_k^2 = b$ v $\mathbb{F}_q^n$ enako $q^{n-k}$ krat število rešitev iste enačbe v $\mathbb{F}_q^k$, je dovolj obravnavati primer, ko je $k = n$, tj. ko obravnavamo nedegenerirano kvadratno formo.

**Definicija 3.6.** Za poljubnen končni obseg $\mathbb{F}_q$ definiramo funkcijo $v$: $\mathbb{F}_q \to \mathbb{Z}$ na nasledji način: $v(b) = -1$ za vse $b \in \mathbb{F}_q^*$ in $v(0) = q - 1$.

**Lema 3.7.** *za poljuben končen obseg $\mathbb{F}_q$ velja*

$$\sum_{c\in\mathbb{F}_q} v(c) = 0 \tag{3.1}$$

*in*

$$\sum_{c_1+\cdots+c_m=b} v(c_1)\cdots v(c_k) = \begin{cases} 0, & \text{če } 1 \leq k < m, \\ v(b)q^{m-1}, & \text{če } k = m, \end{cases} \tag{3.2}$$

*za poljuben $b \in \mathbb{F}_q$.*

*Dokaz.* Dokaz identitete (3.1) je trivialen. Za $1 \leq k < m$ iz enačbe (3.1) sledi

$$\begin{aligned} & \sum_{c_1+\cdots+c_m=b} v(c_1)\cdots v(c_k) \\ = & \sum_{c_1,\ldots,c_k\in\mathbb{F}_q} v(c_1)\cdots v(c_k) \sum_{c_{k+1}+\cdots c_m=b-c_1-\cdots-c_k} 1 \\ = & \; q^{m-k-1} \sum_{c_1,\ldots,c_k\in\mathbb{F}_q} v(c_1)\cdots v(c_k) \\ = & \; q^{m-k-1}(\sum_{c_1\in\mathbb{F}_q} v(c_1))\cdots(\sum_{c_k\in\mathbb{F}_q} v(c_k)) = 0. \end{aligned}$$

V primeru, ko je v enačbi (3.2) $k = m$, naredimo indukcijo po $m$. Primer, ko je $m = 1$, je trivialen. Predpostavimo, da formula drži za nek $m \geq 1$. Tedaj velja

$$\begin{aligned} & \sum_{c_1+\cdots+c_m+c_{m+1}=b} v(c_1)\cdots v(c_m)v(c_{m+1}) \\ = & \sum_{c_1+\cdots+c_m+c_{m+1}=b} v(c_1)\cdots v(c_m)\,[v(c_{m+1}) + 1] \\ = & \sum_{c_1,\ldots,c_m\in\mathbb{F}_q} v(c_1)\cdots v(c_m)\,[v(b - c_1 - \cdots - c_m) + 1] \\ = & \; q \sum_{c_1+\cdots+c_m=b} v(c_1)\cdots v(c_m) \\ = & \; qv(b)q^{m-1} \\ = & \; v(b)q^m. \end{aligned}$$

V zadnjem koraku je vrednost izraza v oglatih oklepajih 0, razen v primeru, ko je $c_1+c_2+\cdots+c_m = b$, takrat je vrednost $q$. Ostalo sledi iz indukcijske predpostavke. □

**Definicija 3.8.** Naj bo preslikava $\eta : \mathbb{F}_q \to \mathbb{Z}$ podana s predpisom

$$\eta(a) = \begin{cases} 0, & \text{če je } a = 0, \\ 1, & \text{če je } a \text{ neničelni kvadrat}, \\ -1, & \text{če je } a \text{ nekvadrat}. \end{cases}$$

Velja $\eta(a^{-1}) = \eta(a)$ za $a \neq 0$ in $\eta(ab) = \eta(a)\eta(b)$, za vse $a, b \in \mathbb{F}_q$.

**Lema 3.9.** *Naj bo $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$, kjer je $q$ liho število in je $a_2$ neničelen. Naj bo $d = a_1^2 - 4a_0a_2$. Potem velja:*

$$\sum_{c\in\mathbb{F}_q} \eta(f(c)) \;=\; \begin{cases} -\eta(a_2), & \text{če } d \neq 0, \\ (q-1)\eta(a_2) & \text{če } d = 0. \end{cases}$$

*Dokaz.* Vsoto $\sum_{c\in\mathbb{F}_q} \eta(f(c))$ pomnožimo z $\eta(4a_2^2) = 1$ in dobimo

$$\sum_{c\in\mathbb{F}_q} \eta(f(c)) \;=\; \eta(a_2) \sum_{c\in\mathbb{F}_q} \eta(4a_2^2c^2 + 4a_1a_2c + 4a_0a_2) \tag{3.3}$$

$$\;=\; \eta(a_2) \sum_{c\in\mathbb{F}_q} \eta((2a_2c + a_1)^2 - d) = \eta(a_2) \sum_{b\in\mathbb{F}_q} \eta(b^2 - d). \tag{3.4}$$

Če je $d$ enak 0, je vsota $\sum_{b\in\mathbb{F}_q} \eta(b^2) = q-1$. Tako dobimo iskani rezultat. Za neničelne $d$ uporabimo enakost

$$\sum_{b\in\mathbb{F}_q} \eta(b^2 - d) = -q + \sum_{b\in\mathbb{F}_q} (1 + \eta(b^2 - d)).$$

Število takih $c \in \mathbb{F}_q$, za katere velja $c^2 = b^2 - d$, je enako $1 + \eta(b^2 - d)$. Zato velja

$$\sum_{b\in\mathbb{F}_q} \eta(b^2 - d) \;=\; -q + S(d), \tag{3.5}$$

kjer je $S(d)$ število urejenih parov $(b, c)$, za katere velja $b^2 - c^2 = d$ in $b, c \in \mathbb{F}_q$. Za rešitev tega problema postavimo $b + c = u$ in $b - c = v$. Ker je $q$ liho število, opazimo, da obstaja bijektivna preslikava med urejenimi pari $(b, c)$ in $(u, v)$. To pomeni, da je $S(d)$ enako številu urejenih parov $(u, v)$, za katere velja $uv = d$, $u, v \in \mathbb{F}_q$. Torej je $S(d) = q - 1$. S pomočjo enačb (3.4) in (3.5) za neničelne $d$ dobimo

$$\sum_{c\in\mathbb{F}_q} \eta(f(c)) = -\eta(a_2).$$

□

**Lema 3.10.** *Naj bo $q$ liho število. Naj bo $b \in \mathbb{F}_q$ in $a_1, a_2 \in \mathbb{F}_q^*$. Potem je*

$$N(a_1x_1^2 + a_2x_2^2 = b) = q + v(b)\eta(-a_1a_2).$$

*Dokaz.* S pomočjo leme 3.9 dobimo

$$\begin{aligned} N(a_1x_1^2 + a_2x_2^2 = b) &= \sum_{c_1+c_2=b} N(a_1x_1^2 = c_1)N(a_2x_2^2 = c_2) \\ &= \sum_{c_1+c_2=b} \left[1 + \eta(c_1a_1^{-1})\right]\left[1 + \eta(c_2a_2^{-1})\right] \\ &= q + \eta(a_1)\sum_{c_1\in\mathbb{F}_q}\eta(c_1) + \eta(a_2)\sum_{c_2\in\mathbb{F}_q}\eta(c_2) \\ &\quad +\eta(a_1a_2)\sum_{c_1+c_2=b}\eta(c_1c_2) \\ &= q + \eta(a_1a_2)\sum_{c\in\mathbb{F}_q}\eta(bc - c^2) \\ &= q + \eta(a_1a_2)v(b)\eta(-1) \\ &= q + \eta(-a_1a_2)v(b). \end{aligned}$$

□

Lema 3.10 nam v posebnem pove, da ima kvadratna forma $a_1x_1^2 + a_2x_2^2 = b$ vedno rešitev v $\mathbb{F}_q^2$ za neničelna $a_1$ in $a_2$. Sedaj se lahko lotimo enega pomembnejših izrekov te naloge.

**Izrek 3.11.** *Naj bo $q$ lih. Naj bo $f$ nedegenerirana kvadratna forma nad $\mathbb{F}_q$ v sodem številu $n$ nedoločenk. Za $b \in \mathbb{F}_q$ je število rešitev enačbe $f(x_1, \ldots, x_n) = b$ v $\mathbb{F}_q^n$ enaka*

$$q^{n-1} + v(b)q^{\frac{n-2}{2}}\eta((-1)^{\frac{n}{2}}\det f).$$

*Dokaz.* Naj bo $a_1x_1^2 + \cdots + a_nx_n^2$ diagonalna kvadratna forma, ki je ekvivalentna formi $f$. Ker ekvivalenca ohranja tako število rešitev kot vrednost $\eta(\det f)$, je dovolj poiskati število rešitev enačbe $a_1x_1^2 + \cdots + a_nx_n^2 = b$, kjer so vsi $a_i$ neničelni. Naj bo $m = \frac{n}{2}$. S pomočjo leme 3.10 in leme 3.7 dobimo

$$
\begin{aligned}
&N(a_1x_1^2+\cdots+a_nx_n^2=b)\\
&\quad= \sum_{c_1+\cdots+c_m=b} N(a_1x_1^2+a_2x_2^2=c_1)\cdots N(a_{n-1}x_{n-1}^2+a_nx_n^2=c_m)\\
&\quad= \sum_{c_1+\cdots+c_m=b} [q+v(c_1)\eta(-a_1a_2)]\cdots[q+v(c_m)\eta(-a_{n-1}a_n)]\\
&\quad= q^{m-1}q^m+\eta((-1)^m a_1\cdots a_n)\sum_{c_1+\cdots+c_m=b} v(c_1)\cdots v(c_m)\\
&\quad= q^{n-1}+v(b)q^{\frac{n-2}{2}}\eta((-1)^{\frac{n}{2}}a_1\cdots a_n).
\end{aligned}
$$

□

**Izrek 3.12.** *Naj bo $q$ lih. Naj bo $f$ nedegenerirana kvadratna forma nad $\mathbb{F}_q$ v lihem številu $n$ nedoločenk. Za $b\in\mathbb{F}_q$ je število rešitev enačbe $f(x_1,\ldots,x_n)=b$ v $\mathbb{F}_q^n$ enako*

$$q^{n-1}+q^{\frac{n-1}{2}}\eta((-1)^{\frac{n-1}{2}}b\det f).$$

*Dokaz.* Kot v prejšnjem izreku nam je dovolj poiskati število rešitev diagonalne kvadratne enačbe $a_1x_1^2+\cdots+a_nx_n^2=b$, kjer so vsi $a_i$ neničelni. Iz izreka 3.11 in leme 3.7 sledi

$$
\begin{aligned}
N(a_1x_1^2+\cdots+a_nx_n^2=b) &= \sum_{c_1+c_2=b} N(a_2x_1^2=c_1)N(a_2x_2^2+\cdots+a_nx_n^2=c_2)\\
&= \sum_{c_1+c_2=b}[1+\eta(c_1a_1)]\\
&\quad\cdot\left[q^{n-2}+v(c_2)q^{\frac{n-3}{2}}\eta((-1)^{\frac{n-1}{2}}a_2\cdots a_n)\right]\\
&= q^{n-1}+q^{n-2}\eta(a_1)\sum_{c_1\in\mathbb{F}_q}\eta(c_1)\\
&\quad+q^{\frac{n-3}{2}}\eta((-1)^{\frac{n-1}{2}}a_2\cdots a_n)\sum_{c_2\in\mathbb{F}_q}v(c_2)\\
&\quad+q^{\frac{n-3}{2}}\eta((-1)^{\frac{n-1}{2}}a_1\cdots a_n)\sum_{c_1+c_2=b}\eta(c_1)v(c_2)\\
&= q^{n-1}+q^{\frac{n-3}{2}}\eta((-1)^{\frac{n-1}{2}}a_1\cdots a_n)\sum_{c\in\mathbb{F}_q}\eta(c)v(b-c)\\
&= q^{n-1}+q^{\frac{n-3}{2}}\eta((-1)^{\frac{n-1}{2}}a_1\cdots a_n)\sum_{c\in\mathbb{F}_q}\eta(c)\left[v(b-c)+1\right]\\
&= q^{n-1}+q^{\frac{n-3}{2}}\eta((-1)^{\frac{n-1}{2}}a_1\cdots a_n)q\eta(b)\\
&= q^{n-1}+q^{\frac{n-1}{2}}\eta((-1)^{\frac{n-1}{2}}b\det f).
\end{aligned}
$$

□

## 3.2 Kvadratne forme nad končnimi obsegi sode karakteristike

Posvetimo se še primeru, ko je karakteristika polja $\mathbb{F}_q$ enaka 2. Tudi tu se bomo posvetili le kvadratnim formam, ki so nedegenerirane.

**Lema 3.13.** *Naj bo $q$ sod in $n \geq 3$. Nedegenerirana kvadratna forma $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ je ekvivalentna formi $x_1x_2 + g(x_3, \ldots, x_n)$, kjer je $g$ nedegenerirana kvadratna forma nad $\mathbb{F}_q$ v $n-2$ nedoločenkah.*

*Dokaz.* Najprej bomo pokazali, da je $f$ ekvivalenten kvadratni formi, pri kateri je koeficient pred členom $x_1^2$ enak 0. Ker je $f$ kvadratna forma nad obsegom $\mathbb{F}_q$, jo lahko zapišemo v obliki

$$f(x_1, \ldots x_n) = \sum_{1 \leq i \leq j \leq n} a_{ij}x_ix_j. \tag{3.6}$$

Če je kakšen od koeficientov $a_{ii}$ enak 0, potem lahko s preimenovanjem dobimo, da je $a_{11} = 0$. Torej smemo predpostaviti, da so vsi $a_{ii}$ različni od 0. Če bi se pojavil primer, da je $a_{ij} = 0$ za vsak $i < j$, potem bi veljalo

$$f(x_1, \ldots, x_n) = a_{11}x_1^2 + \cdots + a_{nn}x_n^2 = (a_{11}^{\frac{q}{2}}x_1 + \cdots + a_{nn}^{\frac{q}{2}}x_n)^2.$$

To je ekvivalentno kvadratni formi z eno nedoločenko in v protislovju z začetno predpostavko. Torej lahko z ustreznim preimenovanjem nedoločenk dosežemo, da je $a_{23}$ neničelen. Če razstavimo člene polinoma $f$, ki vsebujejo $x_2$, dobimo

$$f(x_1, \ldots, x_n) = a_{22}x_2^2 + x_2(a_{12}x_1 + a_{23}x_3 + \cdots + a_{2n}x_n) + g_1(x_1, x_3, \ldots, x_n).$$

Nesingularna linearna substitucija

$$\begin{aligned} x_3 &= a_{23}^{-1}(a_{12}y_1 + y_3 + a_{24}y_4 + \cdots + a_{2n}y_n), \\ x_i &= y_i \text{ za } i \neq 3, \end{aligned}$$

nam da ekvivalentno formo

$$a_{22}y_2^2 + y_2y_3 + g_2(y_1, y_3, \ldots, y_n).$$

Ponovno naredimo nesingularno linearno substitucijo

$$\begin{aligned} y_2 &= (a_{22}^{-1}b_{11})^{\frac{q}{2}}z_1 + z_2, \\ y_i &= z_i \text{ za } i \neq 2, \end{aligned}$$

kjer je $b_{11}$ koeficient pred $y_1^2$ v polinomu $g_2$. Koeficient pred $z_1^2$ v novo dobljeni kvadratni formi je enak 0.

Naj bo $f$ oblike (3.6), kjer je $a_{11} = 0$. Ker je $f$ nedegenerirana, obstaja vsaj en člen $a_{1j}$, ki je različen od 0. Brez škode za splošnost lahko predpostavimo, da je $a_{12}$ neničelen. Nesingularna linearna substitucija

$$\begin{aligned} x_2 &= a_{12}^{-1}(y_2 + a_{13}y_3 + \cdots + a_{1n}y_n), \\ x_i &= y_i \text{ za } i \neq 2 \end{aligned}$$

spremeni $f$ v kvadratno formo oblike

$$y_1y_2 + \sum_{2 \leq i \leq j \leq n} c_{ij}y_iy_j.$$

Nesingularna linearna substitucija

$$\begin{aligned} y_1 &= z_1 + c_{22}z_2 + \cdots + c_{2n}z_n, \\ y_i &= z_i \text{ za } i \neq 1 \end{aligned}$$

nam da ekvivalentno kvadratno formo, ki je oblike $z_1z_2 + g(z_3, \ldots, z_n)$, kjer mora biti forma $g$ očitno nedegenerirana. □

**Izrek 3.14.** *Naj bo $q$ sod. Naj bo $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ nedegenerirana kvadratna forma. Če je $n$ liho število, potem je $f$ ekvivalentna kvadratni formi*

$$x_1x_2 + x_3x_4 + \cdots + x_{n-2}x_{n-1} + x_n^2.$$

*V primeru, ko je $n$ sod, je $f$ bodisi ekvivalentna kvadratni formi oblike*

$$x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n$$

*bodisi kvadratni formi oblike*

$$x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n + x_{n-1}^2 + ax_n^2,$$

*kjer je $a \in \mathbb{F}_q$, tak da zadošča pogoju $\mathrm{Tr}_{\mathbb{F}_q}(a) = 1$.*

*Dokaz.* Če je $n$ liho število, naredimo indukcijo po $n$ in z lemo 3.13 pokažemo, da je $f$ ekvivalentna kvadratni formi oblike $x_1x_2 + x_3x_4 + \cdots x_{n-2}x_{n-1} + ax_n^2$, kjer je $a \in \mathbb{F}_q^*$. Če zamenjamo $x_n$ z $a^{\frac{-q}{2}}x_n$, dobimo želeno kvadratno formo.

Če je $n$ sodo število, naredimo indukcijo po $n$ in z lemo 3.13 pokažemo, da je $f$ ekvivalentna kvadratni formi oblike

$$x_1x_2 + x_3x_4 + \cdots + x_{n-3}x_{n-2} + bx_{n-1}^2 + cx_{n-1}x_n + dx_n^2,$$

kjer so $b, c, d \in \mathbb{F}_q$. Ker je $f$ nedegenerirana mora veljati $c \neq 0$. Če to ne bi veljalo, bi nam identiteta

$$bx_{n-1}^2 + dx_n^2 = (b^{\frac{q}{2}}x_{n-1} + d^{\frac{q}{2}}x_n)^2$$

pomagala pridobiti ekvivalentno kvadrtatno formo v manj kot $n$ nedoločenkah. Če je $b = 0$, potem je

$$cx_{n-1}x_n + dx_n^2 = (cx_{n-1} + dx_n)x_n,$$

kar je ekvivalentno $x_{n-1}x_n$ in smo s tem zaključili. V primeru, ko velja $b \neq 0$, potem z zamenjavo $x_{n-1}$ z $b^{\frac{-q}{2}}x_{n-1}$ in $x_n$ z $b^{\frac{q}{2}}c^{-1}x_n$ opazimo, da je $bx_{n-1}^2 + cx_{n-1}x_n + dx_n^2$ ekvivalentna polinomu $x_{n-1}^2 + x_{n-1}x_n + ax_n^2$ za nek $a \in \mathbb{F}_q$. V primeru, ko je polinom $x^2 + x + a$ razcepen nad $\mathbb{F}_q[x]$, zanj velja

$$x^2 + x + a = (x + c_1)(x + c_2)$$

za neka dva $c_1, c_2 \in \mathbb{F}_q$. Iz tega sledi

$$x_{n-1}^2 + x_{n-1}x_n + ax_n^2 = (x_{n-1} + c_1x_n)(x_{n-1} + c_2x_n),$$

kar je ekvivalentno $x_{n-1}x_n$. Če je $x^2 + x + a$ nerazcepen nad $\mathbb{F}_q[x]$, po trditvi 2.20 zanj velja $\mathrm{Tr}_{\mathbb{F}_q}(a) = 1$. □

Ker je število rešitev enačbe $f(x_1, \dots x_n) = b$ enako številu rešitev $f$ ekvivalentne kvadratne forme, lahko po izreku 3.14 preučimo le ekvivalentne forme.

**Lema 3.15.** *Naj bo $a \in \mathbb{F}_q$, za katerega velja $\mathrm{Tr}_{\mathbb{F}_q}(a) = 1$ in $b \in \mathbb{F}_q$. Potem je*

$$N(x_1^2 + x_1x_2 + ax_2^2 = b) = q - v(b).$$

*Dokaz.* Ker je $x^2 + x + a$ nerazcepen nad $\mathbb{F}_q[x]$, dobimo

$$x^2 + x + a = (x + \alpha)(x + \alpha^q),$$

kjer je $\alpha \in \mathbb{F}_{q^2}$ in $\alpha \notin \mathbb{F}_q$, torej

$$f(x_1, x_2) = x_1^2 + x_1x_2 + ax_2^2 = (x_1 + \alpha x_2)(x_1 + \alpha^q x_2).$$

Za $(c_1, c_2) \in \mathbb{F}_q^2$ dobimo

$$f(c_1, c_2) = (c_1 + \alpha c_2)(c_1 + \alpha^q c_2) = (c_1 + \alpha c_2)(c_1 + \alpha c_2)^q = (c_1 + \alpha c_2)^{q+1}.$$

Ker je $\{1, \alpha\}$ baza za $\mathbb{F}_{q^2}$ nad $\mathbb{F}_q$, obstaja bijektivna preslikava, ki nam urejen par $(c_1, c_2)$ preslika v element $\gamma = c_1 + \alpha c_2 \in \mathbb{F}_{q^2}$. Iz tega sledi, da je $N(f(x_1, x_2) = b)$ ekvivalentno številu $\gamma \in \mathbb{F}_{q^2}$, za katerega velja $\gamma^{q+1} = b$. Torej je

$$N(f(x_1, x_2) = 0) = 1 = q - v(0).$$

Če je $b \neq 0$ in ker je $\mathbb{F}_{q^2}^*$ multiplikativna ciklična grupa po trditvi 2.7 in $b^{\frac{q^2-1}{q+1}} = b^{q-1} = 1$, obstaja natanko $q + 1$ elementov $\gamma \in \mathbb{F}_{q^2}$, za katere velja $\gamma^{q+1} = b$. Torej je $N(f(x_1, x_2) = b) = q + 1 = q - v(b)$. □

Sedaj lahko dokažemo izrek, ki nam odgovori na začetno vprašanje tega razdelka.

**Izrek 3.16.** *Naj bo $\mathbb{F}_q$ končni obseg sode karakteristike in naj bo $b \in \mathbb{F}_q$. Za lihe $n$ je število rešitev enačbe*

$$x_1x_2 + x_3x_4 + \cdots x_{n-2}x_{n-1} + x_n^2 = b$$

*v $\mathbb{F}_q^n$ enako $q^{n-1}$. Za sode $n$, je število rešitev enačbe*

$$x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n = b$$

*v $\mathbb{F}_q^n$ enako $q^{n-1} + v(b)q^{\frac{n-2}{2}}$. Za sode $n$ in $a \in \mathbb{F}_q$, za katerega velja $\mathrm{Tr}_{\mathbb{F}_q}(a) = 1$, je število rešitev enačbe*

$$x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n + x_{n-1}^2 + ax_n^2 = b \tag{3.7}$$

*v $\mathbb{F}_q^n$ enako $q^{n-1} - v(b)q^{\frac{n-2}{2}}$.*

*Dokaz.* Ker ima enačba $x^2 = c$ samo eno rešitev v $\mathbb{F}_q$ za poljuben $c \in \mathbb{F}_q$, dobimo

$$N(x_1x_2 + x_3x_4 + \cdots x_{n-2}x_{n-1} + x_n^2 = b) = q^{n-1}.$$

Za lihe $n$ lahko poljubno dodelimo vrednosti nedoločenkam $x_1, \ldots, x_{n-1}$ in je nato vrednost $x_n$ enolično določena.

Naj bo $n$ sod. Opazimo, da je $N(x_1x_2 = b) = q-1$, če je $b \neq 0$ in $N(x_1x_2 = b) = 2q-1$, če je $b = 0$. Torej je $N(x_1x_2 = b) = q + v(b)$ v obeh primerih. Naj bo $n = 2m$ in $c_1, \ldots, c_n \in \mathbb{F}_q$. Tedaj iz leme 3.7 sledi

$$\begin{aligned}
N(x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n = b) &= \sum_{c_1+\cdots+c_m=b} N(x_1x_2 = c_1)\cdots N(x_{n-1}x_n = c_m) \\
&= \sum_{c_1+\cdots+c_m=b} [q + v(c_1)]\cdots[q + v(c_m)] \\
&= q^{m-1}q^m + \sum_{c_1+\cdots+c_m=b} v(c_1)\cdots v(c_m) \\
&= q^{n-1} + v(b)q^{\frac{n-1}{2}}.
\end{aligned}$$

Pri formi (3.7) opazimo, da je formula veljavna za $n = 2$ po lemi 3.15. Za $n \geq 4$ uporabimo rezultat prejšnjega primera, lemo 3.7 in lemo 3.15 z $c_1, c_2 \in \mathbb{F}_q$.

$$\begin{aligned}
&N(x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n + x_{n-1}^2 + ax_n^2 = b) \\
&\quad= \sum_{c_1+c_2=b} N(x_1x_2 + \cdots + x_{n-3}x_{n-2} = c_1)N(x_{n-1}x_n + x_{n-1}^2 + ax_n^2 = c_2) \\
&\quad= \sum_{c_1+c_2=b} \left[q^{n-3} + v(c_1)q^{\frac{n-4}{2}}\right][q - v(c_2)] \\
&\quad= q^{n-1} + q^{\frac{n-2}{2}} \sum_{c_1\in\mathbb{F}_q} v(c_1) - q^{n-3} \sum_{c_2\in\mathbb{F}_q} v(c_2) - q^{\frac{n-4}{2}} \sum_{c_1+c_2=b} v(c_1)v(c_2) \\
&\quad= q^{n-1} - v(b)q^{\frac{n-2}{2}}.
\end{aligned}$$

□

# 4 Kanonične forme simetričnih matrik nad končnimi obsegi lihe karakteristike

**Definicija 4.1.** Kvadratni $n \times n$ matriki $A$ in $B$ sta kongruentni, če obstaja taka obrnljiva matrika $P$, da velja $P^T AP = B$.

Lema 4.2 se večkrat uporablja v linearni algebri.

**Lema 4.2.** *Kongruentne transformacije ohranjajo rang simetričnih matrik.*

**Lema 4.3.** *Naj bo $S$ simetrična $n \times n$ matrika ranga $r$ $(1 \leq r \leq n)$ nad obsegom $\mathbb{F}_q$, kjer je $q$ liho število. Predpostavimo, da je $S$ kongruentna matriki*

$$\begin{array}{c} \left[\begin{array}{cc} S_1 & 0 \\ 0 & 0 \end{array}\right] \begin{array}{c} r \\ n-r \end{array} \\ \begin{array}{cc} r & n-r \end{array} \end{array} .$$

*Potem velja, da je* $\det S_1$ *neničelna in matrika $S$ enolično določa levi odsek* $(\det S_1)\mathbb{F}_q^{*2}$.

*Dokaz.* Predpostavimo, da je $S$ kongruentna tako matriki

$$\begin{array}{c} \left[\begin{array}{cc} S_1 & 0 \\ 0 & 0 \end{array}\right] \begin{array}{c} r \\ n-r \end{array} \\ \begin{array}{cc} r & n-r \end{array} \end{array}$$

kot matriki

$$\begin{array}{c} \left[\begin{array}{cc} S_2 & 0 \\ 0 & 0 \end{array}\right] \begin{array}{c} r \\ n-r \end{array} \\ \begin{array}{cc} r & n-r \end{array} \end{array} .$$

Po lemi 4.2 sta $\det S_1$ in $\det S_2$ neničelni. Obstaja taka $n \times n$ obrnljiva matrika

$$\begin{array}{c} \left[\begin{array}{cc} A & B \\ C & D \end{array}\right] \begin{array}{c} r \\ n-r \end{array} \\ \begin{array}{cc} r & n-r \end{array} \end{array} ,$$

da velja

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix}^T \begin{bmatrix} S_1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} A & B \\ C & D \end{bmatrix} = \begin{bmatrix} S_2 & 0 \\ 0 & 0 \end{bmatrix}.$$

Iz tega sledi $A^T S_1 A = S_2$. Izračunamo determinanto izraza in dobimo $\det S_1 (\det A)^2 = \det S_2$, kar pomeni, da je $\det A$ neničelna. Torej velja $\det S_1 \mathbb{F}_q^{*2} = \det S_2 \mathbb{F}_q^{*2}$. □

**Lema 4.4.** *Vsaka $n \times n$ simetrična matrika $S$ ranga $r$ $(0 \leq r \leq n)$ nad obsegom $\mathbb{F}_q$, kjer je $q$ liho število, je kongruentna diagonalni matriki*

$$\begin{bmatrix} a_1 & & & & & & \\ & a_2 & & & & & \\ & & \ddots & & & & \\ & & & a_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix},$$

*kjer so $a_1, a_2, \ldots, a_r$ neničelni elementi obsega $\mathbb{F}_q$.*

*Dokaz.* Sledi neposredno iz izreka 3.5. □

**Lema 4.5.** *Naj bo $q$ liho število. Naj bo $z$ fiksen nekvadraten element iz množice $\mathbb{F}_q^*$. Naslednji $2 \times 2$ kvadratni matriki*

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad in \quad \begin{bmatrix} z & 0 \\ 0 & z \end{bmatrix}$$

*sta kongruentni.*

*Dokaz.* Naj bo $z$ fiksen nekvadraten element iz množice $\mathbb{F}_q^*$. Posebej moramo obravnavati primer, ko je $-1 \notin \mathbb{F}_q^{*2}$ in primer, ko $-1 \in \mathbb{F}_q^{*2}$. Najprej si oglejmo prvi primer. Ko $a$ preteče skozi množico $\mathbb{F}_q$, $1 + a^2$ preteče skozi $\frac{1}{2}(q+1)$ elementov iz $\mathbb{F}_q^*$. Torej obstaja tak $x \in \mathbb{F}_q$, da je $1 + x^2$ nekvadraten element iz $\mathbb{F}_q^*$. Po izreku 2.16 velja $\mathbb{F}_q^* = \mathbb{F}_q^{*2} \cup z\mathbb{F}_q^{*2}$. Torej $1 + x^2 \in z\mathbb{F}_q^{*2}$ in obstaja tak $y \in \mathbb{F}_q^*$, da velja $(1 + x^2)y^2 = z$. Potem velja

$$\begin{bmatrix} xy & -y \\ y & xy \end{bmatrix}^T \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} xy & -y \\ y & xy \end{bmatrix} = \begin{bmatrix} z & 0 \\ 0 & z \end{bmatrix}.$$

Oglejmo si še drugi primer, ko velja $-1 \in \mathbb{F}_q^{*2}$. Naj bo $-1 = w^2$, kjer je $w \in \mathbb{F}_q^*$. Potem velja

$$\begin{bmatrix} \frac{1}{2}(1+z) & \frac{w}{2}(1-z) \\ \frac{1}{2w}(1-z) & \frac{1}{2}(1+z) \end{bmatrix}^T \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{2}(1+z) & \frac{w}{2}(1-z) \\ \frac{1}{2w}(1-z) & \frac{1}{2}(1+z) \end{bmatrix} = \begin{bmatrix} z & 0 \\ 0 & z \end{bmatrix}.$$

□

**Izrek 4.6.** *Naj bo $q$ liho število. Poljubna $n \times n$ simetrična matrika ranga $r$ nad $\mathbb{F}_q$ je kongruentna eni od dveh matrik*

$$\begin{bmatrix} I^{(r)} & \\ & 0^{(n-r)} \end{bmatrix} \quad ali \quad \begin{bmatrix} I^{(r-1)} & & \\ & z & \\ & & 0^{(n-r)} \end{bmatrix},$$

*kjer je $z$ fiksen nekvadraten element iz $\mathbb{F}_q^*$ in je $I^{(r)}$ $r \times r$ identična matrika. Še več, matriki nista kongruentni.*

*Dokaz.* Naj bo $S$ neka $n \times n$ simetrična matrika ranga $r$ nad končnim obsegom $\mathbb{F}_q$. Po lemi 4.4 lahko matriko $S$ preoblikujemo v diagonalno matriko. S pravilno preureditvijo elementov $a_1, a_2, \ldots, a_r$ lahko dosežemo, da za nek $0 \leq t \leq r$ velja $a_1, a_2, \ldots, a_t \in \mathbb{F}_q^{*2}$ in $a_{t+1}, a_{t+2}, \ldots, a_r \notin \mathbb{F}_q^{*2}$. Po izreku 2.16 je $\mathbb{F}_q^{*2}$ podgrupa indeksa 2 v grupi $\mathbb{F}_q^*$. Naj bo $z$ fiksen nekvadraten element iz $\mathbb{F}_q^*$, potem velja $a_{t+1}, a_{t+2}, \ldots, a_r \in z\mathbb{F}_q^{*2}$. To pomeni, da velja $z^{-1}a_{t+1}, z^{-1}a_{t+2}, \ldots, z^{-1}a_r \in \mathbb{F}_q^{*2}$. Za poljuben element $b \in \mathbb{F}_q^{*2}$ obstaja vsaj en tak element $c \in \mathbb{F}_q^*$, za katerega velja $c^2 = b$. Zaradi lažje notacije bomo ta element $c$ označili z $b^{\frac{1}{2}}$. Naj bo

$$P = \begin{bmatrix} a_1^{-\frac{1}{2}} & & & & & & & \\ & \ddots & & & & & & \\ & & a_t^{-\frac{1}{2}} & & & & & \\ & & & (z^{-1}a_{t+1})^{-\frac{1}{2}} & & & & \\ & & & & \ddots & & & \\ & & & & & (z^{-1}a_r)^{-\frac{1}{2}} & & \\ & & & & & & I^{(n-r)} \end{bmatrix},$$

potem je

$$P^T \begin{bmatrix} a_1 & & & & \\ & a_2 & & & \\ & & \ddots & & \\ & & & a_r & \\ & & & & o^{(n-r)} \end{bmatrix} P = \begin{bmatrix} I^{(t)} & & \\ & zI^{(r-t)} & \\ & & 0^{(n-r)} \end{bmatrix}.$$

Prvi del izreka sledi iz leme 4.5, drugi del izreka pa neposredno iz leme 4.3. □

**Izrek 4.7.** *Naj bo $q$ liho število. Vsaka kvadratna forma ranga $r$ nad $\mathbb{F}_q$ je ekvivalentna eni izmed form*

$$\sum_{i=1}^{r} x_i^2 \qquad ali \qquad \sum_{i=1}^{r-1} x_i^2 + zx_r^2.$$

*Ti dve formi nista ekvivalentni.*

*Dokaz.* Simetrična matrika koeficientov kvadratne forme je po izreku 4.6 kongruentna eni od matrik

$$\begin{bmatrix} I^{(r)} & \\ & 0^{(n-r)} \end{bmatrix} \quad \text{ali} \quad \begin{bmatrix} I^{(r-1)} & & \\ & z & \\ & & 0^{(n-r)} \end{bmatrix},$$

iz česar sledi rezultat izreka. □

Obstaja še ena kanonična forma simetričnih matrik, ki se pogosto uporablja. Izrek 4.8 zasledimo že v knjigi [2] (glej tudi [9], [10]).

**Izrek 4.8.** *Naj bo $q$ lih in naj bo $S$ $n \times n$ simetrična matrika ranga $r$ nad $\mathbb{F}_q$. Če je $r$ liho število, pišemo $r = 2v + 1$ in je matrika $S$ kongruentna eni od matrik*

$$\begin{bmatrix} 0 & I^{(v)} & & \\ I^{(v)} & 0 & & \\ & & 1 & \\ & & & 0^{(n-r)} \end{bmatrix} \quad ali \quad \begin{bmatrix} 0 & I^{(v)} & & \\ I^{(v)} & 0 & & \\ & & z & \\ & & & 0^{(n-r)} \end{bmatrix}, \tag{4.1}$$

*kjer je $z$ fiksen nekvadraten element iz $\mathbb{F}_q^*$. Matriki (4.1) nista kongruentni. Če je $r$ sodo število, imamo $r = 2v$. Matrika $S$ je kongruentna eni od matrik*

$$\begin{bmatrix} 0 & I^{(v)} & \\ I^{(v)} & 0 & \\ & & 0^{(n-r)} \end{bmatrix} \quad ali \quad \begin{bmatrix} 0 & I^{(v-1)} & & & \\ I^{(v-1)} & 0 & & & \\ & & 1 & & \\ & & & -z & \\ & & & & 0^{(n-r)} \end{bmatrix},$$

*kjer je $z$ fiksen nekvadraten element iz $\mathbb{F}_q^*$ in matriki nista kongruentni.*

*Dokaz.* Sledi neposredno iz izreka 4.6 in leme 4.3. □

Matrikam iz izreka 4.8 pravimo *normalne forme* $n \times n$ simetričnih matrik glede na kongruenčnost. Če je $n \times n$ simetrična matrika kongruentna eni od prvih treh normalnih form, potem je njen *indeks* število $v$. V primeru, ko je kongruentna zadnji normalni formi, je njen *indeks* število $v - 1$.

S pomočjo izreka 4.8 je moč dokazati naslednjo trditev.

**Trditev 4.9.** *Indeks simetrične $n \times n$ matrike je invarianten za kongruenčne transformacije.*

*Indeks kvadratne forme* je definiran kot indeks njene matrike koefiecientov.

**Izrek 4.10.** *Naj bo $q$ lih, vsaka kvadratna forma indeksa $v$ nad $\mathbb{F}_q$ je kongruentna eni od naslednjih normalnih form:*

$$\sum_{i=1}^{v} 2x_i x_{v+i},$$
$$\sum_{i=1}^{v} 2x_i x_{v+i} + x_{2v+1}^2,$$
$$\sum_{i=1}^{v} 2x_i x_{v+i} + z x_{2v+1}^2,$$
$$\sum_{i=1}^{v} 2x_i x_{v+i} + x_{2v+1}^2 - z x_{2v+2}^2,$$

*kjer je $z$ fiksen nekvadraten element iz $\mathbb{F}_q^*$.*

*Dokaz.* Na kvadratni matriki koeficientov kvadratne forme uporabimo izrek 4.8. Tako dobimo iskane normalne forme. □

# 5 Zaključek

V zaključni projektni nalogi smo ugotovili, da je število $n$-teric $(x_1, x_2, \ldots, x_n)$, ki rešijo enačbo kvadratne forme $f(x_1, x_2, \ldots, x_n) = b$, kjer je $b$ nek fiksen element iz obsega $\mathbb{F}_q$, odvisno od tega ali je karakteristika obsega $\mathbb{F}_q$ liha ali soda. Pri tem je zadoščalo obravnavati zgolj nedegenerirane kvadratne forme. Za obsege lihe karakteristike je število rešitev podano v izrekih 3.11 in 3.12. Za obsege sode karakteristike je število rešitev podano v izreku 3.16 v kombinaciji z izrekom 3.14.

V zadnjem poglavju smo si ogledali še alternativni pristop pri iskanju števila rešitev enačbe $f(x_1, \ldots, x_n) = b$ za obsege lihe karakteristike. Slednji temelji na kanoničnih formah matrik. Prednost tega pristopa je v tem, da nam poda tudi klasifikacijo degeneriranih kvadratnih form. Žal se tovrstni pristop precej zakomplicira v karakteristiki 2. Zainteresirani bralec ga lahko preuči s pomočjo knjig [9] in [10].

# 6 Literatura

[1] L.E. Dickson, Determination of the Structure of All Linear Homogeneous Groups in a Galois Field Which are Defined by a Quadratic Invariant, *Amer. J. Math.* 21 (1899), 193–256. *(Citirano na strani 1.)*

[2] L.E. Dickson, *Linear groups with an exposition of the Galois field theory*, Teubner, Leipzig, 1901. *(Citirano na straneh 1 in 22.)*

[3] J.-L. Lagrange, *Démonstration d'un théorème d'arithmétique, Nouv. Mémoirs Acad. Roy.*, Berlin 1770. *(Citirano na strani 1.)*

[4] R. Lidl in H. Niederreiter, *Finite fields*, With a foreword by P. M. Cohn. Second edition. Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997. *(Citirano na strani 1.)*

[5] M. Orel, Adjacency preservers, symmetric matrices, and cores, *J. Algebraic Combin, no. 4* 35 (2012), 633–647. *(Citirano na strani 1.)*

[6] S. Roman, *Field theory*, Graduate Texts in Mathematics, 158. Springer-Verlag, New York, 1995. *(Citirano na strani 2.)*

[7] E. Snapper, Quadratic spaces over finite fields and codes, *J. Combin. Theory Ser. no. 3* A 27 no. 3 (1979), 263–268. *(Citirano na strani 1.)*

[8] J.-A. Thas, Projective geometry over a finite field, v: F. Buekenhout (ur.), *Handbook of incidence geometry. Buildings and foundations*, North-Holland, Amsterdam, 1995, 295–347. *(Citirano na strani 1.)*

[9] Z.-X. Wan, *Finite fields and Galois rings*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2012. *(Citirano na straneh 1, 3, 22 in 24.)*

[10] Z.-X. Wan, *Geometry of classical groups over finite fields*, Studentlitterature, Lund; Chartwell-Bratt Ltd., Bromley, 1993. *(Citirano na straneh 1, 22 in 24.)*