UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika - uporabna smer (UNI)

Maruša Stanek

NORMALNE BAZE NIZKE KOMPLEKSNOSTI

Diplomsko delo

Ljubljana, 2005

Kazalo

PROGRAM DIPLOMSKEGA DELA

Delo naj predstavi matematične osnove, potrebne za razumevanje normalnih baz končnih obsegov, ki jih uporabljamo za implementacije kod za odpravljanje napak in kriptografskih šifer. Poudarek naj bo na konstrukcijah baz nizke kompleksnosti. Glavna cilja sta

(a) Sidel'nikova konstrukcija družine normalnih baz s pomočjo linearne ulomljene funkcije $\varphi(x) = (ax + b)/(cx + d)$ in karakterizacija takšnih baz,

(b) učinkovit prehod med normalnimi in polinomskimi bazami.

Literatura:

I.F. Blake, S. Gao in R.C. Mullin, *Normal and self-dual normal bases from factorization of* $cx^{q+1} + dx^q - ax - b$, SIAM J. Discr. Math. **7** (1994), 499–512.

S. Gao, *Normal bases over finite fields*, Ph.D. Thesis, University of Waterloo, 1993.

A. J. Menezes, I. F. Blake, S. Gao, R. C. Mullin, S. A. Vanstone in T. Yaghoobian, *Applications of Finite Fields*, Kluwer Academic Publishers, 1992.

D. Hankerson, A. J. Menezes in S. Vanstone, *Guide to Elliptic Elliptic Curve Cryptography*, Springer-Verlag, 2004.

Povzetek

V tem delu preučujemo normalne baze končnih obsegov. Z razvojem teorije kodiranja in kriptografije se je pojavila potreba po učinkoviti implementaciji aritmetike v končnih obsegih. Elemente iz končnega obsega lahko predstavimo v različnih bazah. S predstavitvijo elementov v določeni bazi lahko dosežemo učinkovite izboljšave algoritmov. V kriptografiji se je uveljavilo več vrst baz, med njimi tudi normalne baze, ki so zanimive tako s stališča matematične teorije, kot tudi zaradi njihove praktične uporabe. Prednost uporabe normalnih baz za predstavitev elementov končnega obsega s q^n elementi je učinkovito potenciranje na q-to potenco. Posebna vrsta normalnih baz so optimalne normalne baze, v katerih se poenostavi množenje. Ker pa optimalne normalne baze ne obstajajo v vseh končnih obsegih, poskušamo najti normalne baze čim nižje kompleksnosti. Predstavili bomo konstrukcijo normalnih baz nizke kompleksnosti ter sebidualnih normalnih baz.

Ključne besede: Končni obsegi, normalne baze, optimalne normalne baze, normalne baze nizke kompleksnosti, sebidualne normalne baze, prehod med bazami.

Abstract

In this thesis we study normal bases of finite fields. With the development of coding theory and cryptography the implementation of finite field arithmetics is required. We can represent elements from finite fields in various bases and get efficient improvement of arithmetics algorithms. There are several sorts of bases used in cryptography. One of them are normal bases. An interest in normal bases over finite fields stems both from mathematical theory and practical applications. The advantage of using normal bases to represent elements of finite field with q^n elements is in efficient exponentiation with the exponent q. Optimal normal bases, which simplify multiplication, are a special kind of normal bases. Since an optimal normal basis does not exist in every finite field we search for normal basis with as low complexity as possible. We present some constructions of normal bases with low complexity and some constructions of self-dual normal bases.

Key words: Finite Fields, Normal Bases, Optimal Normal Bases, Normal Bases of Low Complexity, Self-dual Normal Bases, Basis Conversion.

Math. subj. class (2005): 11G05, 11T71, 11Y16, 14H52.

Poglavje 1

UVOD

Ob vse večji ogroženosti zasebnosti je varovanje informacij izrednega pomena in je torej nujna uporaba kriptografije. V sodobnem elektronskem svetu se kriptografija uporablja tudi za ostale varnostne storitve, ne le za zagotovljanje tajnosti podatkov. Uporablja se na primer pri digitalnem podpisu, pri plačevanju z digitalnim denarjem in na mnogih drugih področjih. Z razvojem teorije kodiranja in kriptografije ter nastankom številnih kriptosistemov, se je pojavila potreba po učinkoviti implementaciji aritmetičnih operacij v končnih obsegih. Mnogi kriptosistemi temeljijo na končnih obsegih, ki predstavljajo za javno kriptografijo pomembno algebraično strukturo. Elemente končnega obsega lahko predstavimo v različnih bazah. S predstavitvijo elementov v določeni bazi lahko izboljšamo algoritme. V kriptografiji se je uveljavilo več vrst baz, med njimi tudi normalne baze, ki so zanimive tako s stališča matematične teorije, kot tudi zaradi njihove praktične uporabe. Normalne baze so praktične za implementacijo aritmetike končnih obsegov tako v strojni kot tudi v programski opremi. Prednost uporabe normalnih baz za predstavitev elementov končnega obsega $\mathbb{F}_{q^n}$ je učinkovito potenciranje na q-to potenco. Posebna vrsta normalnih baz so optimalne normalne baze, v katerih je učinkovito tudi množenje. Optimalne normalne baze so osnova za varno in učinkovito implementacijo številnih kriptosistemov. Žal pa optimalne normalne baze ne obstajajo v vseh končnih obsegih. Poskušamo najti take baze, ki sicer niso optimalne, vendar pa je v njih množenje še vedno zadosti učinkovito. To so normalne baze nizke kompleksnosti in z njimi se ukvarja pričujoče diplomsko delo.

Obstajata dva različna koncepta kriptografije. V zgodovini se je najprej pojavil koncept *simetrične kriptografije*, pri katerem je ključ za šifriranje enak kot ključ za odšifriranje. Pri tem nastane težava z dogovorom o ključih. Težava je v tem, kako vsakemu, ki bi želel zašifrirano sporočilo prebrati, ta ključ varno dostaviti. Zato sta leta 1976 Whitfield Diffie in

Martin Hellman predlagala nov koncept *asimetrične kriptografije*. Pri javni oziroma asimetrični kriptografiji ima vsak uporabnik svoj par ključev, javnega in zasebnega. Če sporočilo zašifriramo z javnim ključem prejemnika, ga lahko samo ta uporabnik odšifrira s svojim zasebnim ključem. Ravno obratno velja pri digitalnem podpisu, ko pošiljatelj podpiše sporočilo s svojim zasebnim ključem, prejemnik pa na podlagi njegovega javnega ključa preveri, če je to sporočilo res podpisala prava oseba. Če uporabnik za digitalni podpis uporablja overjeno potrdilo, je tak digitalni podpis lahko enakovreden lastnoročnemu podpisu in uporabnik ne more več preklicati vsebine dokumenta. Varnost asimetričnih kriptosistemov temelji na težkih matematičnih problemih, kot sta na primer faktorizacija velikih števil ali računanje diskretnega logaritma. Problem diskretnega logaritma predstavlja računanje logaritma v končni grupi, kot sta na primer multiplikativna grupa praštevilskega obsega ali grupa na eliptični krivulji nad končnim obsegom. V slednji grupi je problem diskretnega logaritma najtežji, zato je dolžina ključa lahko pri enaki varnosti nekajkrat krajša kot če se uporablja faktorizacija števil ali problem diskretnega logaritma v multiplikativni grupi praštevilskega obsega. Eliptične krivulje so vsebovane v standardih, kjer so podrobno opisane. Med drugim so podane priporočene eliptične krivulje in končni obsegi, nad katerimi so definirane. Tako pri implementaciji dobimo visoko varnost sistema, seveda le v primeru, če popolnoma zaupamo tistim, ki so standard napisali. Osnutke za standarde kriptosistemov z eliptičnimi krivuljami pripravljajo različne komisije, omenimo le standard IEEE P1363 (Institute of Electrical and Electronics Engineers). Standard IEEE vključuje kriptosisteme z eliptičnimi krivuljami, ki se uporabljajo za podpise in protokole za dogovor o ključu. Vendar pa standard temelji na polinomskih bazah, saj je bilo potrebno izbrati en tip baz. Zato moramo znati tudi učinkovito prehajati med bazami, na primer pretvoriti elemente iz izbrane polinomske v določeno normalno bazo in obratno. Iz tega razloga je v tem delu vključeno tudi poglavje o prehodu med bazami.

Če želimo računati z elementi končnega obsega, moramo te elemente na nek način predstaviti. V kriptografski praksi najpogosteje delamo z obsegi oblike $\mathbb{F}_{2^n}$, kjer je n veliko naravno število, ali pa obsegi oblike $\mathbb{F}_{p^n}$, kjer je p veliko praštevilo in je n lahko tudi kakšno majhno število. Elemente iz končnega obsega lahko predstavimo v različnih bazah. Izbor baze je v veliki meri odvisen od tega, kaj bomo z elementi obsega počeli. Pomembno je, katere operacije bomo izvajali in kako pogosto. Na podlagi izbora posamezne baze dobimo eksplicitna pravila, kako sešteti ali zmnožiti dva elementa. S predstavitvijo elementov v določeni bazi lahko dosežemo učinkovite izboljšave algoritmov aritmetičnih

operacij. Prednost normalnih baz je učinkovito potenciranje, kajti v normalni bazi nad obsegom karakteristike 2 je kvadriranje kar ciklični zamik. Vendar pa množenje elementov v normalni bazi ostane težko. Mullin, Onyszchuk, Vanstone in Wilson so leta 1988 definirali posebno obliko normalnih baz, tako imenovane optimalne normalne baze, s katerimi lahko bolj učinkovito implementiramo množenje.

Razdelitev po poglavjih je opisana v sledečem odstavku. Za razumevanje baz končnih obsegov potrebujemo nekaj algebraičnega predznanja, zato je naslednje poglavje posvečeno osnovam končnih obsegov, na katerih temelji celotno diplomsko delo. V tretjem poglavju so opisane normalne baze in njihove lastnosti, podana sta tudi dva načina konstrukcije normalnih elementov. Temu sledi poglavje o optimalnih normalnih bazah, katere so najbolj zaželjene v implementaciji končnih obsegov. Peto poglavje je najpomembnejše, v njem se posvetimo normalnim bazam nizke kompleksnosti. Najprej si ogledamo nekaj lastnosti linearnih ulomljenih funkcij in faktorizacijo polinoma, kar nam nato pomaga pri konstrukciji normalnih baz nizke kompleksnosti. V šestem poglavju predstavimo še sebidualne normalne baze in njihovo konstrukcijo. V sedmem poglavju se posvetimo prehodu med različnimi bazami istega končnega obsega. Najprej si ogledamo prehod z matriko, nato pa še izboljšani algoritem prehoda linearne prostorske zahtevnosti. Za zaključek predstavimo še nekaj odprtih problemov, povezanih z normalnimi bazami.

Poglavje 2

KONČNI OBSEGI

V abstraktni algebri končen oziroma Galoisov obseg predstavlja tak obseg, ki vsebuje le končno število elementov. Končni obsegi so pomembna struktura v teoriji števil, algebraični geometriji, Galoisovi teoriji, kriptografiji in teoriji kodiranja. Pojem obsega je vpeljal *Evariste Galois* (1811 - 1832), znani francoski matematik, ki je še kot najstnik določil potreben in zadosten pogoj, da je polinom rešljiv z radikali. Položil je temelje Galoisove teorije, ene glavnih vej abstraktne algebre. Čeprav je bil prvi, ki je dejansko uporabil besedo grupa (le-ta je predstavljala permutacijsko grupo), so matematiki že dolgo pred tem pripravljali teren in preučevali pravila algebraičnih struktur. Grupe so se implicitno uporabljale v kontekstu geometrijske simetrije že od antike. V osemnajstem stoletju so začeli eksplicitno raziskovati specifične grupe, večinoma v obliki permutacij korenov polinomov. Že *Joseph Louis Lagrange* (1736 - 1813), italijanski matematik, je preučeval teorijo grup. Naslednji je bil *Augustin Louis Cauchy* (1789 - 1857), francoski matematik, ki se je med drugim ukvarjal tudi s permutacijskimi grupami. Med tem je *Niels Henrik Abel* (1802 - 1829), norveški matematik, s pomočjo teorije grup pokazal, da enačba 5. stopnje ni rešljiva z radikali. Po njemu so dobile ime tudi abelove grupe in nekateri drugi matematični objekti. Splošne grupe je definiral *Arthur Cayley* (1821 – 1895), angleški matematik, ki je pokazal, da se grupo lahko definira ne glede na naravo njenih elementov. Cayley je prvi definiral koncept grupe v moderni obliki, kot množico z binarno operacijo, ki zadošča ustreznim pogojem.

V tem poglavju bomo obravnavali končne obsege. Najprej bomo podali nekaj temeljnih definicij in lastnosti, nato si bomo ogledali osnovne aritmetične operacije v končnih obsegih, v zadnjem razdelku pa bomo obravnavali reševanje kvadratnih enačb. Glavna referenca za to poglavje je Vidav [24].

2.1 Osnove

Začnimo z definicijami nekaterih osnovnih algebraičnih struktur. Neprazna množica G z neko binarno operacijo $\circ$ je **grupa**, če velja:

- množica G je *zaprta* za operacijo $\circ$, kar pomeni, da je za vsaka dva elementa $x, y \in G$ tudi njun kompozitum $x \circ y \in G$,
- operacija $\circ$ je *asociativna*, torej za vse $x, y, z \in G$ velja $(x \circ y) \circ z = x \circ (y \circ z)$,
- v množici G obstaja *enota* e za operacijo $\circ$, tako da za vsak element $x \in G$ velja $x \circ e = e \circ x = x$ in
- za vsak element x iz množice G obstaja njegov *inverz* glede na operacijo $\circ$, torej tak element $y \in G$, za katerega velja $x \circ y = y \circ x = e$.

Če za operacijo $\circ$ velja še *komutativnost*, torej

$$x \circ y = y \circ x \quad \text{za vse } x, y \in G,$$

potem pravimo, da je grupa G **Abelova**. V aditivno pisanih grupah enoto za seštevanje včasih označimo z 0 in ji rečemo *ničla*. To pomeni, da je

$$a + 0 = 0 + a = a \quad \text{za vsak } a \in G.$$

V multiplikativno pisanih grupah pa enoto za množenje včasih označimo z 1 in ji rečemo *enica*, kar pomeni, da velja

$$a \cdot 1 = 1 \cdot a = a \quad \text{za vsak } a \in G.$$

Neprazna množica K, na kateri imamo definirani dve binarni operaciji, seštevanje in množenje, je **kolobar**, če velja:

- množica K je za seštevanje Abelova grupa,
- množica K je za množenje zaprta in asociativna ter
- operaciji sta *distributivni*, kar pomeni, da za vse elemente $x, y, z \in K$ velja

$$(x + y) \cdot z = x \cdot z + y \cdot z,$$

$$z \cdot (x + y) = z \cdot x + z \cdot y.$$

Naj bo sedaj K kolobar z enico, v katerem ima vsak od nič različen element inverz. Potem K imenujemo **obseg**. Vselej privzamemo, da je obseg netrivialen kolobar, to pomeni, da ima vsaj en neničeln element. Množica $\{0, 1\}$ je torej najmanjši obseg. Podmnožico obsega, ki je za isti operaciji tudi obseg, pa imenujemo **podobseg**. Najmanjše tako število $p \in \mathbb{N} \cup 0$, da velja $px = 0$ za vsak element $x \in K$, imenujemo **karakteristika obsega** K. Oglejmo si naslednje zaporedje v obsegu K. Naj bo $a_0 = 0$, za $i \in \mathbb{N}$ pa velja $a_i = a_{i-1} + 1$. Elementi zaporedja so torej 0,1,2,3,... Če so vsi ti elementi različni, pravimo, da ima obseg *ničelno karakteristiko*. Lahko pa obstajata dva elementa, ki sta si enaka. Potem označimo prvi element, ki se ponovi z a_{k+c}, torej velja $a_{k+c} = a_k$. Če bi bil $k \neq 0$, bi moral biti tudi $a_{k-1+c} = a_{k-1}$. Tako dobimo $k = 0$ in $a_0 = a_c = c \cdot 1 = 0$. Potem je število c karakteristika obsega. Od nič različna karakteristika obsega je vselej praštevilo. Predpostavimo nasprotno, naj bo $c = c_1c_2$ za $c_1, c_2 \in \mathbb{N}$ in $1 < c_1, c_2 < c$. Za zgoraj definirano zaporedje velja $a_{ij} = a_i a_j$ za vsak par naravnih števil i in j, torej tudi $a_c = a_{c_1c_2} = a_{c_1}a_{c_2}$. Vemo, da je $a_c = 0$, a_{c_1} in a_{c_2} pa sta zaradi minimalnosti karakteristike različna od nič. Ker v obsegu ni deliteljev niča, smo dobili protislovje. Neničelna karakteristika obsega je torej vedno praštevilo in v tem primeru obseg K vsebuje množico ostankov pri deljenju s p, ki jo označimo z $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, kot podobseg. V obsegu $\mathbb{Z}_p$ velja $p \cdot 1 = p \equiv 0 \mod p$, torej ima karakteristiko p. Obseg $\mathbb{Z}_p$ imenujemo **praobseg**.

Naj bo L končen obseg, ki vsebuje podobseg K. Pravimo, da je L **razširitev** obsega K. Razširitev L nad obsegom K označimo s L/K. Množico vseh polinomov spremenljivke x s koeficienti iz obsega K označimo s $K[x]$. Množica polinomov $K[x]$ tvori kolobar. Naj bo $f(x)$ poljuben polinom iz $K[x]$ in $a \in L$. Potem je $f(a) \in L$ in elementi $f(a)$, ki jih dobimo za vse polinome $f(x) \in K[x]$, prav tako tvorijo kolobar. Označimo ga s $K[a]$. Kolobar $K[a]$ je podkolobar obsega L. Ker je L obseg, za vsak od nič različen element $f(a) \in L$ obstaja inverz $(f(a))^{-1}$. Potem definiramo kvocient $h(a)/f(a)$ kot produkt poljubnega elementa $h(a) \in K[a]$ z inverzom $(f(a))^{-1}$. Vsi taki kvocienti sestavljajo obseg, ki ga označimo s $K(a)$. To je najmanjši podobseg obsega L, ki vsebuje obseg K in element a. Pravimo, da razširitev $K(a)$ dobimo z **adjunkcijo** elementa a. Če je $a \in K$, je seveda $K(a) = K$.

Analogno lahko posplošimo na razširitev z n elementi $a_1, \ldots, a_n \in L$. V tem primeru vrednosti $f(a_1, \ldots, a_n)$ vseh polinomov $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ tvorijo kolobar, ki ga označimo s $K[a_1, \ldots, a_n]$. Podobno kot prej za $f(a_1, \ldots, a_n) \neq 0$ obstaja inverz in lahko definiramo kvociente. Množica vseh kvocientov z neničelnim imenovalcem tvori obseg, in sicer najmanjši obseg, ki vsebuje K in elemente $a_1, \ldots, a_n \in L$. Tak obseg označimo s

$K(a_1, \ldots, a_n)$.

Obseg L je **enostavna razširitev** obsega K, če lahko pridemo do obsega L iz obsega K z adjunkcijo enega samega elementa a, če je torej $L = K(a)$. Element a imenujemo v tem primeru **primitivni element razširitve**.

Naj bo obseg L razširitev obsega K in $f(x) \in K[x]$. Koreni $a_1, \ldots, a_n$ enačbe $f(x) = 0$ naj bodo elementi obsega L. Obseg $K(a_1, \ldots, a_n)$ je najmanjša razširitev obsega K, ki vsebuje vse korene polinoma $f(x) \in K[x]$. Imenujemo ga **razpadni obseg** polinoma $f(x)$ nad K. V razpadnem obsegu razpade polinom na same linearne faktorje. Ničle nerazcepnega polinoma $f(x) \in K[x]$ v razpadnem obsegu za $f(x)$ nad K imenujemo **konjugiranke**. Če vsak polinom $f(x) \in K[x]$, ki ima v obsegu L vsaj eno ničlo, razpade v obsegu L na same linearne faktorje, pravimo razširitvi L obsega K **normalna razširitev**. Naslednja izreka, katerih dokaza se nahajata v Vidav [24, poglavje 9], govorita o razpadnem obsegu polinomov.

Izrek 2.1.1. *Razpadni obsegi danega polinoma $f(x) \in K[x]$ so med seboj izomorfni.* □

Izrek 2.1.2. *Razpadni obseg polinoma $f(x) \in K[x]$ je normalna razširitev obsega, v katerem ležijo koeficienti tega polinoma.* □

Na končen obseg K lahko za neko naravno število n in praštevilo p gledamo kot na razširitev praobsega $\mathbb{Z}_p$ stopnje n. Tak obseg bomo označili z $\mathbb{F}_{p^n}$. Pogosto govorimo o končnem obsegu $\mathbb{F}_{p^n}$ nad $\mathbb{F}_p$, pri tem pa vedno mislimo na vektorski prostor $\mathbb{F}_{p^n}$ nad $\mathbb{F}_p$. Če so elementi $\alpha_0, \ldots, \alpha_{n-1}$ baza prostora $\mathbb{F}_{p^n}$ nad praobsegom $\mathbb{Z}_p$, lahko vsak element $A \in \mathbb{F}_{p^n}$ zapišemo v obliki $A = a_0\alpha_0 + \ldots + a_{n-1}\alpha_{n-1}$, pri čemer so koeficienti $a_0, \ldots, a_{n-1}$ iz $\mathbb{Z}_p$. Za vsakega od teh koeficientov si lahko izberemo katerikoli element iz $\mathbb{Z}_p$. Ker je p elementov v $\mathbb{Z}_p$, ima obseg $\mathbb{F}_{p^n}$ natanko p^n elementov. Torej je število elementov končnega obsega potenca njegove karakteristike.

Množica od nič različnih elementov obsega $\mathbb{F}_{p^n}$ je za množenje grupa. Njena moč je enaka $p^n - 1$. Če potenciramo element končne grupe na moč grupe, dobimo enoto. Torej vsak element $x \in \mathbb{F}_{p^n}^*$ ustreza enačbi

$$x^{p^n-1} - 1 = 0. \tag{2.1}$$

Če enačbo (2.1) pomnožimo z x, dobimo

$$x^q - x = 0, \text{ kjer je } q = p^n. \tag{2.2}$$

Tej enačbi zadošča tudi element $x = 0$, torej so njeni koreni ravno vsi elementi obsega $\mathbb{F}_{p^n}$. Od tod sledi, da razpade polinom na levi na linearne faktorje

$$x^q - x = (x - a_1)(x - a_2)\dots(x - a_q),$$

pri čemer so $a_1, a_2, \dots, a_q$ vsi elementi obsega $\mathbb{F}_q$. Koeficienti enačbe (2.2) so v obsegu $\mathbb{Z}_p$. Zato je po izreku 2.1.2 obseg $\mathbb{F}_{p^n}$ normalna razširitev praobsega $\mathbb{Z}_p$. Dobimo jo z adjunkcijo korenov enačbe (2.2).

Rešitve enačbe (2.1) so $(q-1)$-vi koreni enote v obsegu $\mathbb{F}_{p^n}$. Ker ima ta enačba $q-1$ rešitev, torej toliko, kolikor je njena stopnja, obstaja primitivni koren. Primitivni koren θ je tak, da so vsi drugi koreni enačbe (2.1) potence tega korena. Grupa je **ciklična**, če so vsi elementi grupe potence enega izmed njih, katerega imenujemo **generator** grupe. Multiplikativna grupa obsega $\mathbb{F}_{p^n}$ je torej ciklična. Generator grupe $\mathbb{F}_{p^n}^*$ imenujemo **primitivni element** obsega $\mathbb{F}_{p^n}$. Obseg $\mathbb{F}_{p^n}$ vsebuje poleg teh elementov samo še element 0. Torej so njegovi elementi

$$\mathbb{F}_{p^n} = \{0, \theta, \theta^2, \dots, \theta^{q-1} = 1\}.$$

Če adjungiramo praobsegu $\mathbb{Z}_p$ primitivni koren θ, dobimo ves obseg $\mathbb{F}_{p^n}$, tako da je $\mathbb{F}_{p^n} = \mathbb{Z}_p(\theta)$. Koren θ je potemtakem tudi primitivni element za razširitev $\mathbb{F}_{p^n}/\mathbb{Z}_p$. Vsak končen obseg je zato enostavna razširitev svojega praobsega. Prav tako je končen obseg $\mathbb{F}_{p^n}$ enostavna razširitev vsakega svojega podobsega. Iz teorije grup vemo, da je vsaka ciklična grupa komutativna. Ker je multiplikativna grupa $\mathbb{F}_{p^n}^*$ ciklična, je vsak končen obseg $\mathbb{F}_{p^n}$ komutativen.

Vzemimo poljubna elementa $x, y \in \mathbb{F}_{p^n}$. Po binomski formuli je

$$(x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}.$$

Binomski simbol

$$\binom{p}{i} = \frac{p \cdot (p-1)\dots(p-i+1)}{1 \cdot 2 \dots i}$$

je celo število. Ker je p praštevilo, se faktor p v števcu ne more krajšati z nobenim faktorjem v imenovalcu, če je $1 < i < p$. Zato je za tako število i binomski koeficient $\binom{p}{i}$ deljiv s p, ustrezni člen, pomnožen z njim, pa je torej enak 0, ker je p karakteristika obsega $\mathbb{F}_{p^n}$. Torej v vsakem obsegu s karakteristiko p velja formula

$$(x + y)^p = x^p + y^p$$

za poljubna elementa obsega x, y. Enakost se da razširiti tudi na več sumandov, dobimo formulo

$$(x_1 + x_2 + \ldots + x_n)^p = x_1^p + x_2^p + \ldots + x_n^p.$$

Galoisov obseg $\mathbb{F}_{p^n}$ obstaja za vsako praštevilsko karakteristiko p in vsako naravno število n. Dobimo ga, če obsegu $\mathbb{Z}_p$ adjungiramo korene enačbe (2.2). Pravzaprav sestavljajo že koreni te enačbe obseg $\mathbb{F}_{p^n}$. Ker je $(x^q - x)' = -1 \neq 0$, so vsi koreni enostavni in jih je $q = p^n$, kolikor je stopnja enačbe. Naj bosta x in y korena te enačbe. Potencirajmo enakost

$$(x \pm y)^p = x^p \pm y^p$$

$(n-1)$-krat na p in pri vsakem koraku uporabimo na desni strani to enakost. Dobimo

$$(x \pm y)^q = x^q \pm y^q, \text{ kjer je } \ q = p^n.$$

Ker ustrezata x in y enačbi (2.2), torej $x^q = x$ in $y^q = y$, velja $(x \pm y)^q = x \pm y$. Od tod sklepamo, da sta vsota $x+y$ in razlika $x-y$ korena enačbe (2.2). Nadalje je $(xy)^q = x^q y^q = xy$ in $(x^{-1})^q = (x^q)^{-1} = x^{-1}$. Torej sta produkt xy in inverzni element x^{-1}, če je $x \neq 0$, prav tako korena te enačbe. Zato je množica korenov enačbe (2.2) obseg, ki ima $q = p^n$ elementov. S tem smo dokazali eksistenco obsega $\mathbb{F}_{p^n}$ pri poljubnem naravnem številu n.

Oglejmo si še sled. To je preslikava, ki ima v teoriji končnih obsegov pomembno vlogo. Naj bo p praštevilo in n neko naravno število. Naj bo element $\alpha \in \mathbb{F}_{p^n}$. **Sled** elementa α nad $\mathbb{F}_p$ je preslikava iz $\mathbb{F}_{p^n}$ v $\mathbb{Z}_p$, definirana s predpisom

$$\mathrm{Tr}_{p^n \,|\, p}(\alpha) = \sum_{i=0}^{n-1} \alpha^{p^i}.$$

Sled elementa nad praobsegom včasih imenujemo tudi *absolutna sled*. Naslednjo trditev bomo potrebovali v razdelku o rešljivosti kvadratnih enačb v končnih obsegih.

Trditev 2.1.3. *Sled je neničeln linearen funkcional. Moč njegovega jedra je enaka* p^{n-1}.

Dokaz. Linearnost preslikave Tr je lahko preveriti. Pokažimo, da ta preslikava res slika v $\mathbb{F}_p$. Vzemimo $x \in \mathbb{F}_{p^n}$. Potem je

$$(\mathrm{Tr}(x))^p = \left(\sum_{i=0}^{n-1} x^{p^i} \right)^p = \sum_{i=0}^{n-1} x^{p^{i+1}} = \mathrm{Tr}(x).$$

Pri zadnjem enačaju smo upoštevali, da v obsegu $\mathbb{F}_{p^n}$ za vsak element x velja $x^{p^n} = x$. Ker enačbi $x^p = x$ v obsegu $\mathbb{F}_{p^n}$ zadoščajo natanko elementi obsega $\mathbb{Z}_p$, sled res slika v obseg $\mathbb{Z}_p$ in je torej funkcional.

Jedro sledi je enako množici ničel polinoma $\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{p^i}$, ki je stopnje $p^{n-1} < p^n$. Torej je moč jedra kvečjemu p^{n-1} in zato je sled neničeln funkcional. Vsak neničeln funkcional je surjektiven, zato je zaloga vrednosti sledi enaka $\mathbb{F}_p$ in je torej njena dimenzija enaka 1. Potem iz dimenzijske enačbe, ki pravi, da je vsota dimenzije jedra in dimenzije slike dane linearne preslikave enaka dimenziji domene te preslikave, sledi, da je dimenzija jedra enaka $n-1$. Torej je jedro sledi izomorfno direktni vsoti $n-1$ sumandov praobsegov $\mathbb{Z}_p$. Zato je moč jedra sledi enaka p^{n-1}. □

Potrebovali bomo bolj splošno definicijo sledi. Naj bo p praštevilo in $q = p^m$, kjer je $m \in \mathbb{N}$. Naj bo $\alpha \in \mathbb{F}_{q^n}$, kjer je $n \in \mathbb{N}$. Sled elementa α nad $\mathbb{F}_q$ je preslikava iz $\mathbb{F}_{q^n}$ v $\mathbb{F}_q$, definirana s predpisom

$$\mathrm{Tr}_{q^n \mid q}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i}.$$

To definicijo lahko še posplošimo. Gledali bomo na primer elemente vektorskega prostora $\mathbb{F}_{q^{vt}}$ nad $\mathbb{F}_{q^t}$, kjer sta v in t tuji si naravni števili. Za element α iz takega prostora $\mathbb{F}_{q^{vt}}$ definiramo sled kot preslikavo iz $\mathbb{F}_{q^{vt}}$ v $\mathbb{F}_{q^t}$ s predpisom

$$\mathrm{Tr}_{q^{vt} \mid q^t}(\alpha) = \sum_{i=0}^{v-1} (\alpha^{q^t})^i = \sum_{i=0}^{v-1} \alpha^{q^{ti}}.$$

Kadar je iz konteksta razvidno, v katerem obsegu se nahajamo, lahko sled preprosto označimo kot $\mathrm{Tr}(\alpha)$. Oglejmo si še nekaj lastnosti sledi, ki jih bomo potrebovali v nadaljevanju.

Trditev 2.1.4. *Naj bosta α, β elementa vektorskega prostora $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ in naj bo $c \in \mathbb{F}_q$. Za $\mathrm{Tr} = \mathrm{Tr}_{q^n \mid q}$ veljajo naslednje lastnosti:*

- $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$,
- $\mathrm{Tr}(c\alpha) = c\mathrm{Tr}(\alpha)$ *in*
- $\mathrm{Tr}(c) = nc$.

Dokaz. Dokažimo najprej prvo trditev. Računamo:

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

S tem smo dokazali, da velja $\mathrm{Tr}(\alpha+\beta)=\mathrm{Tr}(\alpha)+\mathrm{Tr}(\beta)$ za vse elemente $\alpha,\beta\in\mathbb{F}_{q^n}$.

Za $c\in F_q$ velja $c^{q^j}=c$ za vse $j\geq 0$. Zato za vsak $\alpha\in F_{q^n}$ dobimo

$$\begin{aligned}\mathrm{Tr}(c\alpha) &= c\alpha+c^q\alpha^q+\cdots+c^{q^{n-1}}\alpha^{q^{n-1}}\\ &= c\alpha+c\alpha^q+\cdots+c\alpha^{q^{n-1}}\\ &= c\mathrm{Tr}(\alpha).\end{aligned}$$

Za $c\in F_q$ velja

$$\mathrm{Tr}(c)=c+c^q+\cdots+c^{q^{n-1}}=c+c+\cdots+c=nc.$$

Dokazali smo trditev. □

Za zaključek razdelka si oglejmo še en pojem, ki ga bomo srečali v nadaljevanju, to je nerazcepen polinom. Pravimo, da je polinom $f\in\mathbb{F}_q[x]$ stopnje $n\in\mathbb{N}$ **nerazcepen** nad $\mathbb{F}_q$, če ga ne moremo razcepiti v $\mathbb{F}_q$ na produkt polinomov, ki so stopnje manj kot n. Obstaja mnogo različnih algoritmov za testiranje nerazcepnosti polinomov, glej na primer [9]. Poznamo tudi več postopkov za konstrukcijo nerazcepnih polinomov višje stopnje iz nerazcepnih polinomov nižje stopnje, med drugim so opisani v Menezes et al. [18, poglavje 3]. Ne poznamo pa nobenega deterministčnega algoritma polinomske časovne zahtevnosti za konstrukcijo nerazcepnega polinoma stopnje n v $\mathbb{F}_q[x]$ za dan končen obseg $\mathbb{F}_q$ in dano naravno število n. Nerazcepen polinom stopnje n nad $\mathbb{F}_2$ za $n\leq 1000$ lahko preberemo iz tabele v standardu [26, A.8.1].

2.2 Aritmetika v končnih obsegih

Naj bo p praštevilo in $q=p^m$, kjer je m neko naravno število. Obseg $\mathbb{F}_{q^n}$ je n razsežna razširitev obsega $\mathbb{F}_q$. Pogosto govorimo o bazi končnega obsega $\mathbb{F}_{q^n}$, pri tem pa imamo

vedno v mislih bazo za vektorski prostor $\mathbb{F}_{q^n}$ nad obsegom $\mathbb{F}_q$. Vektorski prostor $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ je končno razsežen, torej obstaja množica linearno neodvisnih elementov nad $\mathbb{F}_q$, to je množica $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$, $\alpha_i \in \mathbb{F}_{q^n}$ za vsako število $i \in \{0, 1, \ldots, n-1\}$. Tako množico imenujemo **baza** vektorskega prostora $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$. Potem lahko vsak element A iz obsega $\mathbb{F}_{q^n}$ zapišemo kot

$$A = \sum_{i=0}^{n-1} a_i \alpha_i,$$

kjer je $a_i \in \mathbb{F}_q$ za vsako število $i \in \{0, 1, \ldots, n-1\}$. Tako identificiramo obseg $\mathbb{F}_{q^n}$ z obsegom $(\mathbb{F}_q)^n$ in poljuben element A lahko predstavimo kot vektor $(a_0, a_1, \ldots, a_{n-1})$ v pripadajoči bazi.

Oglejmo si seštevanje v obsegu $\mathbb{F}_{q^n}$. Naj bosta $A = (a_0, a_1, \ldots, a_{n-1})$ in $B = (b_0, b_1, \ldots, b_{n-1}) \in \mathbb{F}_{q^n}$. Seštevanje v $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ je kar seštevanje po komponentah, torej

$$A + B = (a_0 + b_0, a_1 + b_1, \ldots, a_{n-1} + b_{n-1}).$$

Odštevanje gre podobno. Velja

$$A - B = A + (-B).$$

Ker je obseg po definiciji Abelova grupa za seštevanje, ima vsak element svoj nasprotni element, torej za vsak element $B \in \mathbb{F}_{q^n}$ obstaja element $-B \in \mathbb{F}_{q^n}$, tako da velja $B + (-B) = 0$. Torej je tudi odštevanje kar odštevanje po komponentah. Poglejmo še množenje in deljenje. Naj bo $A \cdot B = C = (c_0, c_1, \ldots, c_{n-1})$. Za linearno neodvisne elemente $\alpha_i \in \mathbb{F}_{q^n}$ velja:

$$\alpha_i \alpha_j = \sum_{k=0}^{n-1} t_{ij}^{(k)} \alpha_k \quad \text{za vsaka} \quad i, j \in \{0, 1, \ldots, n-1\},$$

kjer je $t_{ij}^{(k)} \in \mathbb{F}_q$. Potem je

$$c_k = \sum_{i,j=0}^{n-1} a_i b_j t_{ij}^{(k)} \text{ za vsak } \; k \in \{0, 1, \ldots, n-1\}.$$

Deljenje pa je pravzaprav množenje z inverzom. V multiplikativni grupi ima vsak element inverz. Za vsak $A \in \mathbb{F}_{q^n}^*$ velja $A^{q^n} = A$ in zato

$$A^{q^n - 2} = A^{-1}.$$

Tako smo dobili eksplicitno formulo za računanje inverza v obsegu $\mathbb{F}_{q^n}$. V končnem obsegu $\mathbb{F}_{q^n}$ lahko vsak element B delimo s poljubnim neničelnim elementom A takole

$$B/A = BA^{-1} = BA^{q^n-2}.$$

V kriptografiji najpogosteje uporabljamo razširitve obsega $\mathbb{F}_2$. Zato želimo učinkovit algoritem za izračun inverza elementa $A \in \mathbb{F}_{2^n}^*$. Vemo, da za elemente obsega $\mathbb{F}_{2^n}$ velja $A^{2^n} = A$ in od tod sledi

$$A^{-1} = A^{2^n-2},$$

kar lahko zapišemo kot

$$A^{2^n-2} = A^2 \cdot A^{2^2} \cdot \ldots \cdot A^{2^{n-1}}.$$

Na prvi pogled na ta način potrebujemo $n-2$ množenj in $n-1$ kvadriranj, vendar lahko število množenj še bistveno zmanjšamo. Če uporabimo normalne baze za predstavitev elementov obsega $\mathbb{F}_{2^n}$, je kvadriranje le ciklični zamik, kar je zanemarljivo v primerjavi z množenjem. Algoritem invertiranja v normalni bazi obsega $\mathbb{F}_{2^n}$ bomo predstavili v razdelku 3.1.

Inverz neničelnega elementa lahko izračunamo tudi z razširjenim Evklidovim algoritmom. Za izvajanje Evklidovega algoritma moramo zmanjševati stopnjo polinoma. Torej ta metoda deluje le v primeru, ko so elementi obsega predstavljeni v polinomski bazi, v normalnih bazah pa je ne moremo uporabiti.

2.3 Kvadratna enačba

V tem razdelku bomo obravnavali rešljivost kvadratnih enačb v končnih obsegih. Ločili bomo dva primera, reševanje kvadratnih enačb v obsegih karakteristike 2 in obsegih karakteristike več od 2. Reševanje kvadratnih enačb bomo potrebovali v poglavju o normalnih bazah nizke kompleksnosti, kjer bomo privzeli, da znamo rešiti kvadratno enačbo v končnem obsegu. Referenci za ta razdelek sta [3] in [24].

Obsegi karakteristike $p > 2$

Naj bo p liho praštevilo in m, n naravni števili ter $q = p^m$. Element $x \in \mathbb{F}_{q^n}$ je **kvadrat**, če obstaja tak $y \in \mathbb{F}_{q^n}$, da je $x = y^2$. Elemente, ki niso kvadrati, pa imenujemo **nekvadrati**. Ogledali si bomo reševanje kvadratne enačbe

$$ax^2 + bx + c = 0,\ a \neq 0,\ a, b, c \in \mathbb{F}_{q^n}. \tag{2.3}$$

Trditev 2.3.1. *Kvadratna enačba (2.3) ima v obsegu $\mathbb{F}_{q^n}$, $p > 2$, rešitev natanko tedaj, ko je diskriminanta $b^2 - 4ac$ kvadrat.*

Dokaz. Tisti del enačbe (2.3), v katerem nastopa x, dopolnimo do popolnega kvadrata:

$$(x + b/2a)^2 + c/a - b^2/4a^2 = 0.$$

Zadnja enačba ima rešitev natanko tedaj, ko je element $b^2/4a^2 - c/a$ kvadrat. Element obsega pa je kvadrat natanko takrat, kadar je njegov produkt s poljubnim kvadratom tudi kvadrat. □

Če je diskriminanta kvadrat, lahko dobimo eno ali dve različni rešitvi. Ker je karakteristika različna od 2, ima enačba (2.3) dve različni rešitvi natanko tedaj, ko je diskriminanta neničeln kvadrat. Obseg karakteristike več od 2 ima liho število elementov. Izmed neničelnih elementov je natanko polovica kvadratov, druga polovica pa so nekvadrati (za dokaz glej Vidav [24, poglavje 6]). Pri iskanju kvadratov si lahko pomagamo z naslednjo karakterizacijo.

Trditev 2.3.2. *Neničeln element $x \in \mathbb{F}_{q^n}$ je kvadrat natanko tedaj, ko je $x^{(q^n-1)/2} = 1$.*

Dokaz. Ker je število q^n liho, lahko faktoriziramo

$$x^{q^n} - x = x(x^{q^n-1} - 1) = x(x^{(q^n-1)/2} - 1)(x^{(q^n-1)/2} + 1).$$

Ničle polinoma na levi strani so natanko vsi elementi obsega $\mathbb{F}_{q^n}$. Zato je vsak element obsega $\mathbb{F}_{q^n}$ ničla natanko enega od faktorjev na desni strani enakosti. Faktor x ustreza elementu 0. Torej za natanko polovico neničelnih elementov x obsega $\mathbb{F}_{q^n}$ velja $x^{(q^n-1)/2} = 1$. Združimo jih v množico

$$A := \{x \in \mathbb{F}_{q^n} \mid x^{(q^n-1)/2} = 1, x \neq 0\}.$$

Za drugo polovico elementov pa velja $x^{(q^n-1)/2} = -1 \neq 1$. Naj ti elementi tvorijo množico

$$B := \{x \in \mathbb{F}_{q^n} \mid x^{(q^n-1)/2} = -1, x \neq 0\}.$$

Pokažimo, da množica A sovpada z neničelnimi kvadrati, množica B pa z nekvadrati. Naj bo neničeln element $x \in \mathbb{F}_{q^n}$ kvadrat. Torej je $x = y^2$ za nek neničeln $y \in \mathbb{F}_{q^n}$. Red poljubnega elementa multiplikativne grupe deli moč te grupe in od tod sledi

$$x^{(q^n-1)/2} = y^{q^n-1} = 1.$$

Torej so vsi elementi iz množice A neničelni kvadrati. Ker pa je neničelnih kvadratov enako število kot nekvadratov, so v množici B natanko vsi nekvadrati. □

Recimo, da smo za nek neničeln $d \in \mathbb{F}_{q^n}$ ugotovili, da je kvadrat in želimo najti njegov kvadratni koren. V primeru, ko je q^n kongruentno 3 po modulu 4, korena ni težko določiti. Potem je namreč $(q^n+1)/4$ naravno število in velja

$$(d^{(q^n+1)/4})^2 = d^{(q^n+1)/2} = d \cdot d^{(q^n-1)/2} = d.$$

Torej je

$$\sqrt{d} = d^{(q^n+1)/4}.$$

Ko najdemo en koren $x \in \mathbb{F}_{q^n}$, po Viétovih pravilih za rešitvi x_1, x_2 kvadratne enačbe (2.3)

$$x_1 + x_2 = -\frac{b}{a} \text{ in } x_1 \cdot x_2 = \frac{c}{a}$$

sledi, da je drugi koren enak $-x$.

Ker je število q^n liho, ostane le še primer, ko je $q^n \equiv 1 \bmod 4$. V tem primeru pa je iskanje kvadratnih korenov precej zahtevnejše, zato bomo na tem mestu podali le referenco, kjer se nahaja algoritem za iskanje kvadratnih korenov, to je Cohen [5].

Obsegi karakteristike $p = 2$

V obsegu s karakteristiko 2 običajni pristop za reševanje kvadratne enačbe odpove. V takem končnem obsegu nekvadratov sploh ni in je enačba $x^2 = d$ rešljiva za vsak $d \in \mathbb{F}_{2^n}$. Velja $-d = d$, zato ima pri vsakem $d \in \mathbb{F}_{2^n}$ enačba $x^2 = d$ natanko eno dvojno rešitev. Od tod sledi

$$x^2 - d = (x - \sqrt{d})(x + \sqrt{d}) = (x + \sqrt{d})(x + \sqrt{d}).$$

Tudi korena elementa d ni težko poiskati, ker velja

$$(d^{2^{n-1}})^2 = d^{2^n} = d \text{ in } \sqrt{d} = d^{2^{n-1}}.$$

To pa še ne pomeni, da je vsaka kvadratna enačba v obsegu $\mathbb{F}_{2^n}$ rešljiva. Oglejmo si kvadratno enačbo oblike

$$ax^2 + bx + c = 0, \text{ kjer je } a \neq 0 \text{ in so } a, b, c \in \mathbb{F}_{2^n}. \tag{2.4}$$

Če enačbo (2.4) pomnožimo z a^{-1}, dobimo

$$x^2 + ux + v = 0 \text{ za neka } u, v \in \mathbb{F}_{2^n}. \tag{2.5}$$

Primer, ko je $u = 0$, smo že obravnavali, zato naj bo v nadaljevanju $u \neq 0$. Enačbo (2.5) pomnožimo z u^{-2} in uvedemo novo neznanko $y = u^{-1}x$ ter dobimo

$$y^2 + y = w, \text{ kjer je } w = vu^{-2} \in \mathbb{F}_{2^n}. \tag{2.6}$$

Obstaja preprost kriterij za rešljivost zadnje enačbe, podan v naslednji trditvi, za dokaz glej [3, poglavje 1].

Trditev 2.3.3. *Enačba (2.6) ima rešitev v obsegu $\mathbb{F}_{2^n}$ natanko tedaj, ko je sled elementa $w \in \mathbb{F}_{2^n}$ enaka 0.* □

Ker v primeru obsega karakteristike 2 sled slika v praobseg $\mathbb{F}_2$, je vrednost sledi nekega elementa lahko le 0 ali 1. Sled je neničeln funkcional, zato obstajajo elementi w z neničelno sledjo in iz trditve 2.1.3 sledi, da je takih w v $\mathbb{F}_{2^n}$ natanko $2^n - 2^{n-1}$. Torej v vsakem obsegu $\mathbb{F}_{2^n}$ obstajajo nerešljive kvadratne enačbe.

Posledica 2.3.4. *V obsegu $\mathbb{F}_{q^n}$ obstajajo kvadratne enačbe s koeficienti iz tega obsega, ki v $\mathbb{F}_{q^n}$ nimajo rešitve.*

Dokaz. Če karakteristika ni enaka 2, so to kar enačbe oblike $x^2 - d = 0$, kjer je d nekvadrat. Če pa je karakteristika enaka 2, poiščemo element w s sledjo enako 1 in rezultat sledi po trditvi 2.3.3. □

Poglavje 3

NORMALNE BAZE

Zanimanje za normalne baze izvira tako iz matematične teorije kot tudi iz praktičnih aplikacij. Normalne baze so se pojavile v osemnajstem stoletju. Eden od možnih razlogov za preučevanje normalnih baz bi lahko bilo dejstvo, da je že *Johann Carl Friedrich Gauss* (1777 – 1855), nemški matematik, uporabil normalne elemente, ki jih je imenoval periode. To so elementi, ki generirajo normalne baze. S pomočjo period je rešil problem, kako narisati regularen poligon le s šestilom in ravnilom. Prednosti uporabe normalnih baz je opazil tudi pruski matematik *Kurt Hensel* (1861 – 1941), še preden so se končni obsegi začeli praktično uporabljati v raznih aplikacijah. Hensel je leta 1888 prvi dokazal izrek o obstoju normalnih baz za vse končne razširitve obsegov. Domnevo o tem je postavil že leta 1850 nemški matematik *Ferdinand Eisenstein* (1823-1852), Gaussov najljubši učenec, vendar pa je ni znal dokazati. Kasneje se je s tem ukvarjalo mnogo znanih matematikov, ki so podali različne dokaze izreka o normalnih bazah, med drugimi tudi *Emmy Amalie Noether* (1882 – 1935).

Gledano s praktičnega stališča pa se je z razvojem teorije kodiranja in nastankom večih kriptosistemov, ki temeljijo na končnih obsegih, pojavila potreba po učinkoviti implementaciji aritmetike v končnih obsegih. Na tem področju je bilo narejenih mnogo implementacij, tako v programski kot tudi v strojni opremi, med drugim tudi enkripcijski procesor za končen obseg $\mathbb{F}_{2^{593}}$ za javno kriptografijo.

Naj bo p praštevilo in $q = p^m$, kjer je $m \in \mathbb{N}$. Obseg $\mathbb{F}_q$ ima q elementov in $\mathbb{F}_{q^n}$ je njegova n razsežna razširitev. Še enkrat poudarimo, da bomo pogosto uporabljali izraz baza obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ (ali kar baza obsega $\mathbb{F}_{q^n}$, če bo iz konteksta razvidno, nad katerim podobsegom se nahajamo), vedno pa bomo pri tem imeli v mislih bazo vektorskega prostora $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$. Normalne baze končnega obsega $\mathbb{F}_{q^n}$ so posebna družina baz za vektorski prostor $\mathbb{F}_{q^n}$

nad $\mathbb{F}_q$. Podmnožica N vektorskega prostora $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ je **normalna baza**, če ustreza naslednjima pogojema:

- N je baza za vektorski prostor $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ in
- $N = \{\alpha^{q^0}, \alpha^{q^1}, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ za nek element $\alpha \in \mathbb{F}_{q^n}$.

Pravimo, da element α generira normalno bazo N oziroma je **normalni element** obsega $\mathbb{F}_{q^n}$. V obsegu je lahko več normalnih elementov, vendar pa elementa α in α^{q^i} za vsako število $i \in \{0, \ldots, n-1\}$ generirata enako normalno bazo, saj v obsegu $\mathbb{F}_{q^n}$ velja $\alpha^{q^n} = \alpha$. V nadaljevanju bomo pogosto označevali $\alpha_i = \alpha^{q^i}$. Za vsako število $i \in \{0, 1, \ldots, n-1\}$ je produkt $\alpha\alpha_i$ linearna kombinacija elementov $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ s koeficienti iz obsega $\mathbb{F}_q$. Zato velja

$$\alpha\alpha_i = \sum_{j=0}^{n-1} m_{ij}\alpha_j, \quad \text{kjer so} \quad m_{ij} \in \mathbb{F}_q \quad \text{za vse} \quad i, j \in \{0, 1, \ldots, n-1\}$$

in

$$\alpha_0 \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} = M \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{pmatrix},$$

kjer je matrika $M = (m_{ij})_{i,j=0}^{n-1}$ razsežnosti $n \times n$. Matrika M se imenuje **multiplikacijska matrika** normalne baze N ali multiplikacijska matrika normalnega elementa α. Število neničelnih elementov v matriki M imenujemo **kompleksnost** normalne baze N in označimo s c_N. Obstaja mnogo baz vektorskega prostora $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$. Za nekatere baze so ustrezne multiplikacijske matrike M preprostejše kot za druge, v smislu, da imajo manj neničelnih elementov. Tako si lahko z izborom normalne baze nizke kompleksnosti poenostavimo množenje elementov obsega.

V tem poglavju se bomo posvetili normalnim bazam, glavna referenca je Gao [6]. Najprej si bomo ogledali aritmetiko v normalnih bazah, potem pa še nekaj lastnosti normalnih baz. Temu sledi razdelek o porazdelitvi normalnih elementov. Poglavje bomo zaključili s konstruiranjem normalnega elementa, opisali bomo tako verjetnostni kot tudi deterministični algoritem konstrukcije normalnega elementa.

3.1 Aritmetika normalnih baz

Naj bo $N = \{\alpha^{q^0}, \alpha^{q^1}, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ normalna baza obsega $\mathbb{F}_{q^n}$. Vsak element A iz $\mathbb{F}_{q^n}$ lahko zapišemo kot

$$A = \sum_{i=0}^{n-1} a_i \alpha^{q^i},$$

kjer je $a_i \in \mathbb{F}_q$ za vsako število $i \in \{0, \ldots, n-1\}$. Element A iz $\mathbb{F}_{q^n}$ lahko torej pišemo kot n terico $(a_0, a_1, \ldots, a_{n-1})$. Seštevanje je kar seštevanje po komponentah. Nadaljujmo s potenciranjem. Normalne baze obsega $\mathbb{F}_{q^n}$ imajo lepo lastnost, da je v njih potenciranje na q zelo enostavno. Oglejmo si q-to potenco elementa A:

$$A^q = \sum_{i=0}^{n-1} a_i^q \alpha^{q^{i+1}} = \sum_{i=0}^{n-1} a_i \alpha^{q^{i+1}} = a_{n-1}\alpha + \sum_{i=1}^{n-1} a_{i-1}\alpha^{q^i}.$$

Potemtakem je element A^q kar enak n terici $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$. Koordinate vektorja A^q so torej le ciklično zamaknjene v desno koordinate vektorja A in zato je potenciranje učinkovito. To je zelo pomembno pri mnogih implementacijah, kot je na primer Diffie-Hellmanov dogovor o ključu, kjer je potrebno računati visoke potence elementov v končnih obsegih. Tudi q-korenjenje v normalnih bazah je enostavno, kajti q-ti koren elementa A je tisti element, ki ga dobimo s cikličnim premikom koordinat elementa A v levo.

Množenje je nekoliko bolj zapleteno. Naj bo $B = (b_0, b_1, \ldots, b_{n-1}) \in \mathbb{F}_{q^n}$ in produkt $A \cdot B = C = (c_0, c_1, \ldots, c_{n-1})$. Za elemente normalne baze $\alpha_i = \alpha^{q^i} \in \mathbb{F}_{q^n}$ za vse $i, j \in \{0, 1, \ldots, n-1\}$ velja

$$\alpha_i \alpha_j = \alpha^{q^i}\alpha^{q^j} = \alpha^{q^i+q^j} = \alpha^{q^i(1+q^{j-i})} = (\alpha\alpha_{j-i})^{q^i} = \left(\sum_{k=0}^{n-1} m_{j-i,k}\alpha_k\right)^{q^i} = \sum_{k=0}^{n-1} m_{j-i,k-i}\alpha_k,$$

kjer je $M = (m_{ij})_{i,j=0}^{n-1}$ multiplikacijska matrika normalne baze N in indekse računamo po modulu števila n. Potem koeficiente produkta izračunamo po formuli

$$c_k = \sum_{i,j=0}^{n-1} a_i b_j m_{j-i,k-i} \quad \text{za vsak} \quad k \in \{0, 1, \ldots, n-1\}.$$

Normalna baza je določena z normalnim elementom. Naj bo $p_0(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}_q[x]$ polinom, ki ima za ničlo normalni element α, torej $p_0(\alpha) = 0$. Če potenciramo polinom p_0 na q-to potenco in upoštevamo, da so koeficienti a_i iz obsega $\mathbb{F}_q$, dobimo

$$p_0(\alpha)^q = \sum_{i=0}^{n} a_i^q \alpha^{iq} = \sum_{i=0}^{n} a_i(\alpha^q)^i = p_0(\alpha^q) = 0.$$

Od tod sledi, da je v primeru, ko je element α ničla polinoma $p_0(x)$, tudi α^q ničla polinoma $p_0(x)$. Tako dobimo, da so vsi elementi $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ ničle polinoma $p_0(x)$.

Sedaj bomo opisali algoritem za invertiranje neničelnih elementov v končnem obsegu $\mathbb{F}_{2^n}$, ki najprej privzame posebno obliko eksponenta n, nato pa njegovo posplošitev na poljubno naravno število. Ta algoritem je povzet po [10]. Naj bo najprej eksponent oblike $n = 2^r + 1$ za neko naravno število r. V tem primeru velja $2^n - 2 = (2^{n-1} - 1) \cdot 2$ in multiplikativni inverz elementa $A \in \mathbb{F}_{2^n}^*$ je enak $A^{-1} = (A^{2^{2^r}-1})^2$. Zato lahko zapišemo število $2^{2^r} - 1$ kot

$$2^{2^r} - 1 = (2^{2^{r-1}} - 1)2^{2^{r-1}} + (2^{2^{r-1}} - 1).$$

Zdaj lahko opišemo algoritem.

ALGORITEM 1 Algoritem za izračun inverza.

Input: $A \in \mathbb{F}_{q^n}^*$, $n = 2^r + 1$.
Output: Inverzni element A^{-1}.
1. $C = A$.
2. For i from 0 to $r-1$ do
   $D = C^{2^{2^i}}$,
   $C = C \cdot D$.
3. Return(C^2).

V algoritmu se izvede r iteracij. V vsaki iteraciji je eno množenje in i cikličnih zamikov za $i \in \{0, 1, \ldots, r-1\}$. Skupaj dobimo torej $r = \log_2(n-1)$ množenj in $n-1$ cikličnih zamikov.

Algoritem posplošimo na poljubno vrednost eksponenta n. Število $n-1$ zapišemo kot vsoto t različnih potenc števila 2

$$n - 1 = \sum_{i=1}^{t} 2^{k_i},$$

kjer velja $k_1 > k_2 > \ldots > k_t$, $k_i \in \mathbb{N} \cup 0$ in $t \in \mathbb{N}$. V obsegu $\mathbb{F}_{2^n}$ za vsak element A velja $A^{2^n} = A$. Če privzamemo, da je $A \neq 0$ in pomnožimo zadnjo enakost z A^{-2}, dobimo

$$A^{-1} = A^{2^n-2} = A^{2\cdot(2^{n-1}-1)} = (A^{2^{n-1}-1})^2.$$

Zato lahko inverz elementa A zapišemo kot

$$A^{-1} = (A^{2^{n-1}-1})^2 = \left[(A^{2^{2^{k_t}}-1}) \left((A^{2^{2^{k_{t-1}}}-1}) \dots \left[(A^{2^{2^{k_2}}-1})(A^{2^{2^{k_1}}-1})^{2^{2^{k_2}}} \right]^{2^{2^{k_3}}} \dots \right)^{2^{2^{k_t}}} \right]^2. \tag{3.1}$$

Za izračun $A^{2^{2^{k_1}}-1}$ potrebujemo tudi vse ostale vrednosti $A^{2^{2^{k_i}}-1}$ za $k_i < k_1$. Naj bo **teža** eksponenta n število enic v binarni predstavitvi števila n. Označimo jo z $W(n)$. V zgornjem računu je potrebno izvesti $\lfloor \log_2(n-1) \rfloor + W(n-1) - 1$ množenj v $\mathbb{F}_{2^n}$ in $n-1$ cikličnih zamikov.

Primer: Poiskali bomo inverz elementa v normalni bazi obsega $\mathbb{F}_{2^{173}}$. Uporabili bomo zgoraj predstavljeno metodo. Naš eksponent n je torej 173 in $n-1$ lahko zapišemo kot vsoto $172 = 128+32+8+4 = 2^7+2^5+2^3+2^2$, od koder dobimo $k_1 = 7$, $k_2 = 5$, $k_3 = 3$ in $k_4 = 2$. Izračunajmo inverzni element $A^{-1} = A^{2^{173}-2} = (A^{2^{172}-1})^2$ elementa $A \in \mathbb{F}_{2^{173}}$. Najprej moramo izračunati naslednje potence elementa A, pri čemer potrebujemo 7 množenj:

$$A^{2^2-1} = A^2 \cdot A$$

$$A^{2^4-1} = (A^{2^2-1})^{2^2} \cdot A^{2^2-1}$$

$$A^{2^8-1} = (A^{2^4-1})^{2^4} \cdot A^{2^4-1}$$

$$A^{2^{16}-1} = (A^{2^8-1})^{2^8} \cdot A^{2^8-1}$$

$$A^{2^{32}-1} = (A^{2^{16}-1})^{2^{16}} \cdot A^{2^{16}-1}$$

$$A^{2^{64}-1} = (A^{2^{32}-1})^{2^{32}} \cdot A^{2^{32}-1}$$

$$A^{2^{128}-1} = (A^{2^{64}-1})^{2^{64}} \cdot A^{2^{64}-1}.$$

Inverz elementa $A \in \mathbb{F}_2^{173}$ izračunamo po formuli (3.1). Potrebovali bomo še 3 množenja za izračun inverznega elementa:

$$A^{-1} = \left[(A^{2^4-1}) \cdot \left((A^{2^8-1}) \cdot \left[(A^{2^{32}-1}) \cdot (A^{2^{128}-1})^{2^{32}} \right]^{2^8} \right)^{2^4} \right]^2.$$

Za izračun inverza tako porabimo deset množenj.

Če bi računali inverz v polinomski bazi predstavljenega elementa, bi z razširjenim Evklidovim algoritmom porabili le približno štiri množenja, glej na primer [19, poglavje 3]. $\diamond$

3.2 Lastnosti normalnih baz

Pogledali bomo, kako za dani normalni bazi nekih končnih obsegov, recimo $\mathbb{F}_{q^t}$ in $\mathbb{F}_{q^v}$ nad $\mathbb{F}_q$, skonstruiramo normalno bazo večjega obsega, recimo $\mathbb{F}_{q^{vt}}$ nad $\mathbb{F}_q$. Začnimo v nasprotni smeri, torej kako za dano normalno bazo obsega $\mathbb{F}_{q^{vt}}$ nad $\mathbb{F}_q$ skonstruiramo normalno bazo obsega $\mathbb{F}_{q^v}$ (ali $\mathbb{F}_{q^t}$) nad $\mathbb{F}_q$.

Izrek 3.2.1. *Naj bosta t in v naravni števili ter α normalen element obsega $\mathbb{F}_{q^{vt}}$ nad $\mathbb{F}_q$. Potem je $\gamma = \mathrm{Tr}_{q^{vt}|q^t}(\alpha)$ normalni element obsega $\mathbb{F}_{q^t}$ nad $\mathbb{F}_q$.*

Dokaz. Zložimo konjugiranke elementa α v obsegu $\mathbb{F}_{q^{vt}}$ nad $\mathbb{F}_q$ po stolpcih v naslednjo $(t \times v)$ razsežno matriko:

$$\begin{pmatrix} \alpha & \alpha^{q^t} & \dots & \alpha^{q^{t(v-1)}} \\ \alpha^q & \alpha^{q^{t+1}} & \dots & \alpha^{q^{t(v-1)+1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{q^{t-1}} & \alpha^{q^{t+t-1}} & \dots & \alpha^{q^{t(v-1)+t-1}} \end{pmatrix}.$$

Omenimo, da je $t(v-1)+t-1 = vt-1$. Vsi elementi matrike so linearno neodvisni nad $\mathbb{F}_q$, ker je α normalen element obsega $\mathbb{F}_{q^{vt}}$ nad $\mathbb{F}_q$. Konjugiranke elementa $\gamma = \sum_{i=0}^{v-1} \alpha^{q^{ti}}$ so vrstične vsote zgornje matrike in zato morajo biti linearno neodvisne nad $\mathbb{F}_q$. □

Lema 3.2.2. *Naj bosta t in v taki naravni števili, da velja $\gcd(v,t) = 1$. Naj bo $A = \{\alpha_0, \alpha_1, \dots, \alpha_{v-1}\}$ baza vektorskega prostora $\mathbb{F}_{q^v}$ nad $\mathbb{F}_q$. Potem je A tudi baza vektorskega prostora $\mathbb{F}_{q^{vt}}$ nad $\mathbb{F}_{q^t}$.*

Dokaz. Najprej omenimo, da lahko kot množici identificiramo $\mathbb{F}_{q^v}/\mathbb{F}_q$ in $\mathbb{F}_{q^{vt}}/\mathbb{F}_{q^t}$. Dokazati moramo, da so elementi $\alpha_0, \alpha_1, \dots, \alpha_{v-1}$ linearno neodvisni nad $\mathbb{F}_{q^t}$. Predpostavimo, da obstajajo elementi $a_i \in \mathbb{F}_{q^t}$ za $i \in \{0, 1, \dots, v-1\}$, tako da velja

$$\sum_{i=0}^{v-1} a_i \alpha_i = 0. \tag{3.2}$$

Za vsak $j \in \mathbb{N}$ velja

$$\left(\sum_{i=0}^{v-1} a_i \alpha_i \right)^{q^{tj}} = \sum_{i=0}^{v-1} a_i^{q^{tj}} \alpha_i^{q^{tj}} = \sum_{i=0}^{v-1} a_i \alpha_i^{q^{tj}}.$$

Ker sta v in t tuji si števili, velja, da ko j preteče vrednosti $0, 1, \dots, v-1$, tudi tj po modulu v preteče vse vrednosti $0, 1, \dots, v-1$. Spomnimo se še, da za element $\alpha_i \in \mathbb{F}_{q^v}$

velja $\alpha_i^{q^v} = \alpha_i$ in potem $\alpha_i^{q^u} = \alpha_i^{q^k}$, kadar je $u \equiv k \pmod{v}$. Potem nam enakost (3.2) implicira

$$\sum_{i=0}^{v-1} a_i \alpha_i^{q^j} = 0 \ \text{ za vsak } \ j \in \{0, 1, \ldots, v-1\},$$

kar lahko zapišemo v matrični obliki kot

$$\begin{pmatrix} \alpha_0 & \alpha_1 & \ldots & \alpha_{v-1} \\ \alpha_0^q & \alpha_1^q & \ldots & \alpha_{v-1}^q \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{q^{v-1}} & \alpha_1^{q^{v-1}} & \ldots & \alpha_{v-1}^{q^{v-1}} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{v-1} \end{pmatrix} = 0.$$

Ker so elementi $\alpha_0, \alpha_1, \ldots, \alpha_{v-1}$ linearno neodvisni nad $\mathbb{F}_q$, je zgornja matrika koeficientov nesingularna. Potem mora biti vektor $(a_0, a_1, \ldots, a_{v-1})^T$ enak nič, torej morajo biti vsi koeficienti $a_0, a_1, \ldots, a_{v-1}$ enaki nič, kar nam dokazuje, da so $\alpha_0, \alpha_1, \ldots, \alpha_{v-1}$ linearno neodvisni nad obsegom $\mathbb{F}_{q^t}$. □

Sledi izrek, s katerim si pomagamo pri rekurzivni konstrukciji normalnih baz.

Izrek 3.2.3. *Naj bo $n = vt$, kjer sta v in t tuji si naravni števili. Potem je za $\alpha \in \mathbb{F}_{q^v}$ in $\beta \in \mathbb{F}_{q^t}$ element $\gamma = \alpha\beta \in \mathbb{F}_{q^n}$ normalen element obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ natanko tedaj, ko sta α in β zaporedoma normalna elementa obsegov $\mathbb{F}_{q^v}$ in $\mathbb{F}_{q^t}$ nad $\mathbb{F}_q$.*

Dokaz. ($\Rightarrow$) Predpostavimo najprej, da je γ normalen element obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$. Ker je $\beta \in \mathbb{F}_{q^t}$ in je sled linearna preslikava, velja

$$\mathrm{Tr}_{q^n|q^t}(\gamma) = \mathrm{Tr}_{q^n|q^t}(\alpha\beta) = \beta \mathrm{Tr}_{q^n|q^t}(\alpha).$$

Potem je po izreku 3.2.1

$$\mathrm{Tr}_{q^n|q^t}(\gamma) = \beta \mathrm{Tr}_{q^v|q}(\alpha)$$

normalen element obsega $\mathbb{F}_{q^t}$ nad $\mathbb{F}_q$. Sled $\mathrm{Tr}_{q^v|q}(\alpha)$ ni enaka nič in je element obsega $\mathbb{F}_q$. Torej je β normalen element obsega $\mathbb{F}_{q^t}$ nad $\mathbb{F}_q$. Analogno izpeljemo, da je α normalni element obsega $\mathbb{F}_{q^v}$ nad $\mathbb{F}_q$. ($\Leftarrow$) Zdaj pa predpostavimo, da sta α in β zaporedoma normalna elementa obsegov $\mathbb{F}_{q^v}$ in $\mathbb{F}_{q^t}$ nad $\mathbb{F}_q$. Dokazali bomo, da je γ normalen element obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$. Ker je $\gcd(v, t) = 1$, po kitajskem izreku o ostankih sledi, da za vsak $i \in \{0, 1, \ldots, v-1\}$ in vsak $j \in \{0, 1, \ldots, t-1\}$ obstaja enolično določeno število k, tako da velja

$$k \equiv i \pmod{v} \ \text{ in } \ k \equiv j \pmod{t}.$$

Sledi

$$\gamma^{q^k} = \alpha^{q^i}\beta^{q^j}.$$

Torej so konjugiranke elementa γ natanko vsi elementi

$$\alpha^{q^i}\beta^{q^j}, \text{ kjer je } i \in \{0, 1, \ldots, v-1\} \text{ in } j \in \{0, 1, \ldots, t-1\}. \tag{3.3}$$

Dokazati moramo še, da so elementi iz (3.3) linearno neodvisni nad obsegom $\mathbb{F}_q$. Naj bodo koeficienti $a_{ij} \in \mathbb{F}_q$ taki, da velja

$$\sum_{i=0}^{v-1}\sum_{j=0}^{t-1} a_{ij}\alpha^{q^i}\beta^{q^j} = 0. \tag{3.4}$$

Naj bo $b_j = \sum_{i=0}^{v-1} a_{ij}\alpha^{q^i}$ za $j \in \{0, 1, \ldots, t-1\}$. Potem je $b_j \in \mathbb{F}_{q^v}$, ker je izražen kot linearna kombinacija baznih elementov $\mathbb{F}_{q^v}$ in (3.4) implicira

$$\sum_{j=0}^{t-1} b_j\beta^{q^j} = 0. \tag{3.5}$$

Elementi $\beta, \beta^q, \ldots, \beta^{q^{t-1}}$ so linearno neodvisni nad $\mathbb{F}_{q^v}$ po lemi 3.2.2. Od tod sledi $b_j = 0$ za vsak $j \in \{0, 1, \ldots, t-1\}$. Ker so tudi elementi $\alpha, \alpha^q, \ldots, \alpha^{q^{v-1}}$ linearno neodvisni nad $\mathbb{F}_q$, nam $b_j = 0$ za vse $j \in \{0, 1, \ldots, t-1\}$ implicira $a_{ij} = 0$ za vse $i \in \{0, 1, \ldots, v-1\}$ in vse $j \in \{0, 1, \ldots, t-1\}$. Sledi, da elementi iz (3.3) tvorijo bazo vektorskega prostora $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$. S tem je izrek dokazan. □

3.3 Porazdelitev normalnih elementov

V tem razdelku si bomo ogledali, kako so porazdeljeni normalni elementi. Posledično bomo lahko prešteli vse normalne elemente in normalne baze vektorskega prostora $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$. Potrebujemo nekaj konceptov linearne algebre, ki so povzeti po Gao [6].

Naj bo T linearna transformacija na končno razsežnem vektorskem prostoru V nad obsegom F. Polinom $f(x) = \sum_{i=0}^{m} a_i x^i \in F[x]$ **anihilira** T, če velja

$$a_m T^m + \cdots + a_1 T + a_0 I = 0,$$

kjer je I **identična preslikava** in 0 **ničelna preslikava** na V. Enolično določen monični polinom najmanjše stopnje s to lastnostjo se imenuje **minimalni polinom** za T in deli

vsak drug polinom v $F[x]$, ki anihilira T. V izbrani bazi vektorskega prostora V pripada transformaciji T matrika, ki jo tudi označimo s T. Vemo, da je determinanta te matrike neodvisna od baze. Vsaka lastna vrednost λ transformacije T ustreza enačbi

$$\det(\lambda I - T) = 0.$$

Leva stran enačbe je za λ polinom z vodilnim koeficientom 1. Imenujemo ga **karakteristični polinom transformacije** T. Po Cayley-Hamiltonovem izreku minimalni polinom transformacije T deli tudi karakteristični polinom transformacije T.

Podprostor $W \subseteq V$ je **T-invarianten**, če je $Tu \in W$ za vsak $u \in W$. Za vsak vektor $u \in V$ je podprostor, napet na $u, Tu, T^2u, \ldots$ T-invarianten podprostor prostora V in se imenuje **T-cikličen podprostor**, generiran z u. Označimo ga z $Z(u,T)$. Če je $Z(u,T) = V$, potem u imenujemo **ciklični vektor** prostora V za T.

Naj bo u poljuben element vektorskega prostora V. **T-red elementa** u oziroma **minimalni polinom elementa** u je tisti moničen polinom $g(x) \in F[x]$ najnižje stopnje, za katerega velja $g(T)u = 0$. Označimo ga z $\mathrm{Ord}_{u,T}(x)$ ali $\mathrm{Ord}_u(x)$, če je transformacija T razvidna iz konteksta. Ta polinom deli vsak polinom $h(x)$, ki anihilira element u, torej tak h, da je $h(T)u = 0$, tudi minimalni in karakteristični polinom za T. Strnimo rezultate iz linearne algebre v naslednjo lemo, glej Menezes et al. [18, poglavje 4].

Lema 3.3.1. *Naj bo T linearna transformacija na končno razsežnem vektorskem prostoru V nad obsegom F. Predpostavimo, da sta minimalni in karakteristični polinom za T enaka, recimo $f(x)$.*

(i) Naj bo polinom $g(x) \in F[x]$ in W jedro polinoma $g(x)$. Naj bo polinom

$$d(x) := \gcd(f(x), g(x))$$

in polinom $e(x) = f(x)/d(x)$. Potem je razsežnost prostora W enaka stopnji polinoma $d(x)$ in

$$W = \{u \in V \mid d(T)u = 0\} = \{e(T)u \mid u \in V\}.$$

(ii) Naj ima polinom $f(x)$ naslednjo faktorizacijo

$$f(x) = \prod_{i=1}^{r} f_i^{d_i}(x),$$

kjer so $f_i(x) \in F[x]$ različni nerazcepni faktorji polinoma $f(x)$ in $d_i \in \mathbb{N}$. Naj bo V_i jedro polinoma $f_i^{d_i}(x)$. Potem velja

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r.$$

Naj velja $\Psi_i(x) = f(x)/f_i^{d_i}(x)$. *Potem za vsak* $u_j \in V_j$ *velja* $\Psi_i(T)u_j = 0$ *za* $i \neq j$ *ter* $\Psi_i(T)u_j \neq 0$ *za* $i = j$ *in* $u_j \neq 0$.

□

V našem primeru gledamo obseg $\mathbb{F}_{q^n}$ kot n razsežen vektorski prostor nad $\mathbb{F}_q$. **Frobeniusova preslikava**, definirana s predpisom $\sigma : \eta \to \eta^q$, $\eta \in \mathbb{F}_{q^n}$, pa je linearna transformacija vektorskega prostora $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$.

Trditev 3.3.2. *Minimalni in karakteristični polinom preslikave* σ *sta enaka polinomu* $x^n - 1$.

Dokaz. Vemo, da je $\sigma^n\eta = \eta^{q^n} = \eta$ za vsak element $\eta \in \mathbb{F}_{q^n}$. Torej je $\sigma^n - I = 0$ oziroma polinom $x^n - 1$ anihilira preslikavo σ. Dokažimo, da je $x^n - 1$ minimalni polinom preslikave σ. Predpostavimo, da je $f(x) = \sum_{i=0}^{n-1} f_i x^i \in \mathbb{F}_q[x]$ polinom stopnje manjše od n, ki anihilira σ; torej tak, da velja $\sum_{i=0}^{n-1} f_i\sigma^i = 0$. Potem za vsak element $\eta \in \mathbb{F}_{q^n}$ velja

$$\left(\sum_{i=0}^{n-1} f_i\sigma^i\right)\eta = \sum_{i=0}^{n-1} f_i\eta^{q^i} = 0,$$

torej je η koren polinoma $F(x) = \sum_{i=0}^{n-1} f_i x^{q^i}$. To pa je nemogoče, saj je stopnja polinoma $F(x)$ največ q^{n-1} in zato ne more imeti $q^n > q^{n-1}$ korenov v $\mathbb{F}_{q^n}$. Torej je $x^n - 1$ minimalni polinom preslikave σ.

Ker je karakteristični polinom preslikave σ moničen stopnje n in je deljiv z minimalnim polinomom preslikave σ, morata biti enaka, oba $x^n - 1$. □

Naj bo element $\alpha \in \mathbb{F}_{q^n}$ normalen. Potem so vektorji $\alpha, \sigma\alpha, \sigma^2\alpha, \ldots, \sigma^{n-1}\alpha$ linearno neodvisni nad $\mathbb{F}_q$ in zato ne obstaja polinom stopnje manj kot n, ki anihilira α. Sledi, da mora biti σ-red elementa α enak $x^n - 1$ in da je α ciklični vektor prostora $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ za σ. Sklenimo ugotovitve v naslednjo trditev.

Trditev 3.3.3. *Element* $\alpha \in \mathbb{F}_{q^n}$ *je normalen v vektorskem prostoru* $\mathbb{F}_{q^n}$ *nad* $\mathbb{F}_q$ *natanko tedaj, ko je* $Ord_{\alpha,\sigma}(x) = x^n - 1$.

Dokaz. ($\Rightarrow$) Naj bo element $\alpha \in \mathbb{F}_{q^n}$ normalen, polinom $g(x) = x^n - 1$ in σ Frobeniusiova preslikava. Potem je $g(\sigma) = \sigma^n - I$. Računajmo

$$g(\sigma)\alpha = \sigma^n(\alpha) - \alpha = \alpha^{q^n} - \alpha = 0.$$

Torej polinom g anihilira element α. Ker je α normalen, je množica $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ linearno neodvisna. Zato je $\alpha \neq \alpha^{q^i}$ za $i \in \{1, 2, \ldots, n-1\}$. Torej mora biti najmanjši polinom, ki anihilira element α, stopnje n. Ker je polinom $\mathrm{Ord}_{\alpha,\sigma}(x)$ moničen in deli minimalni polinom, je $\mathrm{Ord}_{\alpha,\sigma}(x) = x^n - 1$.

($\Leftarrow$) Naj bo sedaj $\mathrm{Ord}_{\alpha,\sigma}(x) = x^n - 1$. To pomeni, da je polinom $x^n - 1$ polinom najmanjše stopnje, ki anihilira element $\alpha \in \mathbb{F}_{q^n}$. Ker ni polinoma nižje stopnje, ki bi anihiliral element α, morajo biti elementi α^{q^i} linearno neodvisni nad obsegom $\mathbb{F}_q$. Torej je α normalen element. □

Naj bosta $n_1, p \in \mathbb{N}$ in $n = n_1 p^e$, kjer sta p in n_1 tuji si števili ter $e \in \mathbb{N} \cup 0$. Označimo $p^e = t$. Predpostavimo, da ima polinom $x^n - 1$ v $\mathbb{F}_q[x]$ naslednjo faktorizacijo

$$x^n - 1 = (\varphi_1(x)\varphi_2(x) \ldots \varphi_r(x))^t, \tag{3.6}$$

kjer so $\varphi_i(x) \in \mathbb{F}_q[x]$ različni nerazcepni faktorji polinoma $x^n - 1$. Naj bo d_i stopnja faktorjev φ_i za $i = 1, 2, \ldots, r$ in naj bo

$$\Phi_i(x) = (x^n - 1)/\varphi_i(x)$$

ter

$$\Psi_i(x) = (x^n - 1)/\varphi_i^t(x) \text{ za vsak } i \in \{1, 2, \ldots, r\}.$$

Izrek 3.3.4. *Element $\alpha \in \mathbb{F}_{q^n}$ je normalen natanko tedaj, ko velja*

$$\Phi_i(\sigma)\alpha \neq 0 \quad za\ i = 1, 2, \ldots, r. \tag{3.7}$$

Dokaz. Po definiciji je α normalen element nad $\mathbb{F}_q$ natanko tedaj, ko so $\alpha_i = \alpha^{q^i} = \sigma^i(\alpha)$, $i \in \{0, 1, \ldots, n-1\}$ linearno neodvisni nad $\mathbb{F}_q$, torej takrat, ko je σ-red elementa α enak $x^n - 1$. To pa drži takrat, ko noben pravi faktor polinoma $x^n - 1$ ne anihilira α, torej natanko tedaj, ko velja (3.7). □

V posebnem primeru, ko je $n = p^e$, se pogoj iz zgornjega izreka poenostavi.

Posledica 3.3.5. *Naj bo $n = p^e$. Potem je element $\alpha \in \mathbb{F}_{q^n}$ normalen nad $\mathbb{F}_q$, če in samo če velja*

$$\mathrm{Tr}_{q^n|q}(\alpha) \neq 0.$$

Dokaz. Iz $n = p^e$ sledi $(x-1)^n = x^n - 1$. Torej je v faktorizaciji (3.6) število r enako 1, $\varphi_1(x) = x - 1$ in $\Phi_1(x) = x^{n-1} + \ldots + x + 1$. Po izreku (3.3.4) je element $\alpha \in \mathbb{F}_{q^n}$ normalen nad $\mathbb{F}_q$, če in samo če velja $\Phi_1(\sigma)\alpha = \sum_{i=0}^{n-1} \alpha^{q^i} = \mathrm{Tr}_{q^n|q}(\alpha) \neq 0$. □

Naslednji izrek razstavi vektorski prostor $\mathbb{F}_{q^n}$ nad obsegom $\mathbb{F}_q$ na direktno vsoto podprostorov, od katerih je polovica σ-invariantnih podprostorov. S pomočjo tega izreka vidimo, kje ležijo normalni elementi obsega $\mathbb{F}_{q^n}$.

Izrek 3.3.6. *Naj bodo faktorji φ_i in število t taki, kot so v faktorizaciji (3.6). Naj bo W_i jedro preslikave $\varphi_i^t(x)$ in $\widetilde{W_i}$ jedro preslikave $\varphi_i^{t-1}(x)$. Naj bo $\overline{W_i}$ tak podprostor prostora W_i, da velja $W_i = \overline{W_i} \oplus \widetilde{W_i}$. Potem je*

$$\mathbb{F}_{q^n} = \sum_{i=1}^{r} \overline{W_i} \oplus \widetilde{W_i}$$

direktna vsota, kjer je $\overline{W_i}$ d_i razsežen podprostor, $\widetilde{W_i}$ pa $(t-1)d_i$ razsežen podprostor. Element $\alpha \in \mathbb{F}_{q^n}$ lahko zapišemo v obliki

$$\alpha = \sum_{i=1}^{r} (\overline{\alpha_i} + \widetilde{\alpha_i}), \quad \textit{kjer je} \quad \overline{\alpha_i} \in \overline{W_i} \quad \textit{in} \quad \widetilde{\alpha_i} \in \widetilde{W_i}.$$

Element α je normalen nad $\mathbb{F}_q$, če in samo če velja $\overline{\alpha_i} \neq 0$ za vsako število $i \in \{1, 2, \ldots, r\}$.

Dokaz. Prva trditev izreka je direktna posledica leme 3.3.1. Dokazati moramo le drugo trditev. Opazimo, da če velja $i \neq j$, potem $\varphi_j^t(x) \mid \Phi_i(x)$. Torej za vsak element $\alpha_j \in W_j$ velja $\Phi_i(\sigma)\alpha_j = 0$. Sledi

$$\Phi_i(\sigma)\alpha = \Phi_i(\sigma)(\overline{\alpha_i} + \widetilde{\alpha_i}) = \Phi_i(\sigma)\overline{\alpha_i} + \Phi_i(\sigma)\widetilde{\alpha_i} = \Phi_i(\sigma)\overline{\alpha_i},$$

kajti polinom $\Phi_i(x) = \Psi_i(x)\varphi_i^{t-1}(x)$ je deljiv s $\varphi_i^{t-1}(x)$. Po izreku 3.3.4 sledi, da je element α normalen nad $\mathbb{F}_q$, če in samo če je $\Phi_i(\sigma)\overline{\alpha_i} \neq 0$ za vsak $i \in \{1, 2, \ldots, r\}$.

Zdaj pa bomo dokazali, da je $\Phi_i(\sigma)\overline{\alpha_i} \neq 0$ natanko tedaj, ko je $\overline{\alpha_i} \neq 0$. Očitno velja: če $\Phi_i(\sigma)\overline{\alpha_i} \neq 0$, potem je tudi $\overline{\alpha_i} \neq 0$. Naj bo zdaj $\overline{\alpha_i} \neq 0$. Potem je $\overline{\alpha_i} \in W_i \backslash \widetilde{W_i}$, kadar je $\varphi_i^t(\sigma)\overline{\alpha_i} = 0$ in $\varphi_i^{t-1}(\sigma)\overline{\alpha_i} \neq 0$. Ker sta si polinoma $\Psi_i(x)$ in $\varphi_i(x)$ tuja, obstajata taka polinoma $a(x)$ in $b(x)$ v $\mathbb{F}_q[x]$, da velja

$$a(x)\varphi_i(x) + b(x)\Psi_i(x) = 1.$$

Torej je

$$\overline{\alpha_i} = a(\sigma)\varphi_i(\sigma)\overline{\alpha_i} + b(\sigma)\Psi_i(\sigma)\overline{\alpha_i}.$$

Od tod sledi

$$\varphi_i^{t-1}(\sigma)\overline{\alpha_i} = a(\sigma)\varphi_i^t(\sigma)\overline{\alpha_i} + b(\sigma)\varphi_i^{t-1}(\sigma)\Psi_i(\sigma)\overline{\alpha_i} =$$
$$= b(\sigma)\Phi_i(\sigma)\overline{\alpha_i} = b(\sigma)(\Phi_i(\sigma)\overline{\alpha_i}).$$

Ker je $\varphi_i^{t-1}(\sigma)\overline{\alpha_i} \neq 0$, mora biti tudi $\Phi_i(\sigma)\overline{\alpha_i} \neq 0$. S tem je izrek dokazan. □

Dimenzija podprostora $\overline{W_i}$ je $d_i \geq 1$, zato v vsakem končnem obsegu obstaja normalen element, kar sledi direktno iz izreka 3.3.6.

Posledica 3.3.7 (Izrek o normalnih bazah). *V vsakem končnem obsegu $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ obstaja normalna baza.* □

V drugi posledici izreka 3.3.6 bomo prešteli, koliko je normalnih elementov in normalnih baz v končnem obsegu. Upoštevamo še dejstvo, da vsak element normalne baze generira isto bazo.

Posledica 3.3.8. *Število normalnih elementov v obsegu $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ je*

$$v(n,q) = \prod_{i=1}^{r} q^{d_i(t-1)}(q^{d_i} - 1),$$

število vseh normalnih baz končnega obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ pa je $v(n,q)/n$. □

3.4 Konstrukcija normalnega elementa

Najpreprostejši algoritem za konstrukcijo normalne baze je kar zaporedno naključno izbiranje elementa $\alpha \in \mathbb{F}_{q^n}$, dokler ne dobimo linearno neodvisne množice $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$. To je polinomski algoritem, kajti verjetnost, da je α normalni element, je večja ali enaka $1/34$, če je $n \leq q^4$, in večja od $(16 \log_q n)^{-1}$, če je $n \geq q^4$, kot sta dokazala Gathen in Giesbrecht v [8].

Poglejmo še deterministične algoritme za konstruiranje normalne baze. Predpostavili bomo, da imamo dan nerazcepen polinom $f(x)$ stopnje n nad $\mathbb{F}_q$ in njegov koren α. Potem je množica $\{1, \alpha, \ldots, \alpha^{n-1}\}$ baza in lahko izračunamo matrično reprezentacijo Frobeniusove preslikave $\sigma : x \to x^q, x \in \mathbb{F}_{q^n}$.

Izrek 3.3.6 nam poda deterministični algoritem za konstruiranje normalne baze. Najprej faktoriziramo $x^n - 1$ nad $\mathbb{F}_q$, da dobimo $x^n - 1 = (\varphi_1(x), \varphi_2(x), \ldots, \varphi_r(x))^t$. Nato izračunamo bazo vsakega podprostora v dekompoziciji prostora $\mathbb{F}_{q^n}$. Tako dobimo bazo

prostora $\mathbb{F}_{q^n}$, normalni elementi pa so tisti, katerih ustrezne koordinate iz podprostora $\overline{W_i}$ so neničelne. Prednost tega algoritma je, da nam vrne vse normalne elemente. Vendar pa je ta algoritem neučinkovit, saj ne poznamo polinomskega deterministočnega algoritma za faktorizacijo polinoma $x^n - 1$. V nadaljevanju si bomo ogledali boljši verjetnostni algoritem in nato še en deterministični algoritem.

Verjetnostni algoritem

Naslednji verjetnostni algoritem temelji na Artinovem izreku, glej [1].

Izrek 3.4.1. *Naj bo $f(x)$ narazcepen polinom stopnje n nad $\mathbb{F}_q$ in α koren polinoma $f(x)$. Naj bo funkcija*

$$g(x) = \frac{f(x)}{(x-\alpha)f'(\alpha)}.$$

Potem obstaja vsaj $q - n(n-1)$ takih elementov u v $\mathbb{F}_q$, da je $g(u)$ normalen element obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$.

Dokaz. Naj bo σ_i avtomorfizem, podan s predpisom $\theta \to \theta^{q^i}$, $\theta \in \mathbb{F}_{q^n}$, za $i \in \{1, \ldots, n\}$. Potem je element $\alpha_i = \sigma_i(\alpha)$ prav tako koren polinoma $f(x)$ za $i \in \{1, \ldots, n\}$. Naj bo

$$g_i(x) = \sigma_i(g(x)) = \frac{f(x)}{(x-\alpha_i)f'(\alpha_i)}.$$

Opomnimo, da velja $\sigma_i\sigma_j(g(x)) = \sigma_{i+j}(g(x))$. Potem je $g_i(x)$ polinom v $\mathbb{F}_{q^n}[x]$, katerega koren je α_k za $k \neq i$ in velja $g_i(\alpha_i) = 1$. Zato je

$$g_i(x)g_k(x) \equiv 0 \mod f(x) \text{ za } i \neq k. \tag{3.8}$$

Opazimo, da je

$$g_1(x) + g_2(x) + \ldots + g_n(x) - 1 = 0, \tag{3.9}$$

kajti leva stran je polinom stopnje največ $n-1$ in ima korene $\alpha_1, \alpha_2, \ldots, \alpha_n$. Če pomnožimo levo in desno stran enakosti (3.9) z $g_i(x)$ in uporabimo kongruenco (3.8), dobimo

$$(g_i(x))^2 \equiv g_i(x) \mod f(x). \tag{3.10}$$

Zdaj si bomo ogledali determinanto $D(x)$ matrike

$$D = [\sigma_i\sigma_j(g(x))]_{i,j=1}^n.$$

Iz (3.8), (3.9) in (3.10) sledi, da so vsi koeficienti matrike $D^T D$ po modulu polinoma $f(x)$ enaki 0, razen diagonalnih elementov, ki so vsi enaki 1. Zato

$$(D(x))^2 = \det(D^T D) \equiv 1 \mod f(x).$$

To dokazuje, da je $D(x)$ neničeln polinom stopnje največ $n(n-1)$. Torej ima $D(x)$ največ $n(n-1)$ korenov v $\mathbb{F}_q$. Za $u \in \mathbb{F}_q$ je $g(u)$ normalen element obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ natanko tedaj, ko je $D(u) \neq 0$. □

Zdaj je algoritem preprost. Izberemo naključni element $u \in \mathbb{F}_q$ in naj bo $\theta = g(u)$. Potem preverimo, če je θ normalen element obsega $\mathbb{F}_{q^n}$. Izrek 3.4.1 nam pove, da je θ normalen element z verjetnostjo vsaj $1/2$, če je $q > 2n(n-1)$. Celotno računanje zahteva $\mathcal{O}((n + \log q)(n \log q)^2)$ operacij po bitih.

ALGORITEM 2 Algoritem za testiranje normalnosti elementa.

1. Vzamemo poljuben element $u \in \mathbb{F}_q$.
2. Izračunamo $\theta = g(u)$, kjer je $g(x) = f(x)/((x-\alpha)f'(\alpha))$.
3. Preverimo, če je element θ normalen v $\mathbb{F}_{q^n}$:
   če je $det[(\sigma_i\sigma_j(\theta))_{i,j=1}^n] \neq 0$, potem je element θ normalen;
   sicer element θ ni normalen v obsegu $\mathbb{F}_{q^n}$.
4. Vrnemo ustrezno sporočilo: element θ "je normalen" ali "ni normalen".

Deterministični algoritem

Ogledali si bomo Lenstrov algoritem. Najprej moramo poiskati σ-red $\mathrm{Ord}_\theta(x)$ poljubnega elementa $\theta \in \mathbb{F}_{q^n}$. Stopnja polinoma $\mathrm{Ord}_\theta(x)$ je tako naravno število k, da element $\sigma^k\theta$ pripada linearni ogrinjači $\{\sigma^i\theta \mid 0 \leq i < k\}$. Če je $\sigma^k\theta = \sum_{i=0}^{k-1} c_i\sigma^i\theta$ za to število k, potem je

$$\mathrm{Ord}_\theta(x) = x^k - \sum_{i=0}^{k-1} c_i x^i.$$

Torej lahko polinom $\mathrm{Ord}_\theta(x)$ izračunamo v polinomskem času. Lenstrov algoritem je algebraično obarvan in za njegov opis bomo potrebovali naslednji lemi.

Lema 3.4.2. *Naj bo element $\theta \in \mathbb{F}_{q^n}$, $\mathrm{Ord}_\theta(x) \neq x^n - 1$ in $g(x) = (x^n-1)/\mathrm{Ord}_\theta(x)$. Potem obstaja tak element $\beta \in \mathbb{F}_{q^n}$, da je*

$$g(\sigma)\beta = \theta. \tag{3.11}$$

Dokaz. Naj bo element γ obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ normalen. Potem obstaja tak polinom $f(x) \in \mathbb{F}_q[x]$, da je $f(\sigma)\gamma = \theta$. Ker je $\mathrm{Ord}_\theta(\sigma)\theta = 0$, velja

$$(\mathrm{Ord}_\theta(\sigma)f(\sigma))\gamma = 0.$$

Torej je polinom $\mathrm{Ord}_\theta(x)f(x)$ deljiv z $x^n - 1$ in zato je polinom $f(x)$ deljiv s polinomom $g(x)$. Naj bo $f(x) = g(x)h(x)$. Potem velja

$$g(\sigma)(h(\sigma)\gamma) = \theta,$$

kar pove, da element $\beta = h(\sigma)\gamma$ ustreza enakosti (3.11). □

Lema 3.4.3. *Naj bo element $\theta \in \mathbb{F}_{q^n}$, $\mathrm{Ord}_\theta(x) \neq x^n - 1$ in $g(x) = (x^n - 1)/\mathrm{Ord}_\theta(x)$. Predpostavimo, da obstaja rešitev β enačbe (3.11), tako da je stopnja polinoma $\mathrm{Ord}_\beta(x)$ manjša ali kvečjemu enaka stopnji polinoma $\mathrm{Ord}_\theta(x)$. Potem obstaja tak neničeln element $\eta \in \mathbb{F}_{q^n}$, da je*

$$g(\sigma)\eta = 0. \tag{3.12}$$

Za element η velja

$$\deg(\mathrm{Ord}_{\theta+\eta}(x)) > \deg(\mathrm{Ord}_\theta(x)). \tag{3.13}$$

Dokaz. Naj bo γ normalni element obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$. Potem je

$$\eta = \mathrm{Ord}_\theta(\sigma)\gamma \neq 0$$

rešitev enačbe (3.12). Dokazali bomo, da drži neenakost (3.13) za vsako neničelno rešitev η enačbe (3.12). Iz enakosti (3.11) sledi, da polinom $\mathrm{Ord}_\theta(x)$ deli polinom $\mathrm{Ord}_\beta(x)$, torej nam hipoteza

$$\deg(\mathrm{Ord}_\beta(x)) \leq \deg(\mathrm{Ord}_\theta(x))$$

implicira, da je $\mathrm{Ord}_\beta(x) = \mathrm{Ord}_\theta(x)$. Zato morata biti polinoma $g(x)$ in $\mathrm{Ord}_\theta(x)$ tuja. Ker polinom $\mathrm{Ord}_\eta(x)$ deli polinom $g(x)$, sta si $\mathrm{Ord}_\theta(x)$ in $\mathrm{Ord}_\eta(x)$ tuja. Od tod sledi

$$\mathrm{Ord}_{\theta+\eta}(x) = \mathrm{Ord}_\theta(x)\mathrm{Ord}_\eta(x).$$

Potem neenakost (3.13) sledi iz $\eta \neq 0$. □

Zdaj lahko opišemo Lenstrov algoritem, ki vrne normalni element obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$.

ALGORITEM 3 Lenstrov algoritem.

1. Vzamemo poljuben element $\theta \in \mathbb{F}_{q^n}$ in določimo polinom $\mathrm{Ord}_\theta(x)$.
2. Če je $\mathrm{Ord}_\theta(x) = x^n - 1$, se algoritem konča.
3. Izračunamo $g(x) = (x^n - 1)/\mathrm{Ord}_\theta(x)$ in rešimo sistem enačb $g(\sigma)\beta = \theta$ za β.
4. Določimo polinom $\mathrm{Ord}_\beta(x)$.
5. Če je stopnja polinoma $\mathrm{Ord}_\beta(x)$ večja od stopnje polinoma $\mathrm{Ord}_\theta(x)$, potem zamenjamo element θ z elementom β in se vrnemo na korak 2. V nasprotnem primeru poiščemo tak neničeln element η, da velja $g(\sigma)\eta = 0$, zamenjamo element θ s $\theta + \eta$, določimo red novega θ ter se vrnemo na korak 2.

Poglavje 4

OPTIMALNE NORMALNE BAZE

Optimalne normalne baze so temelj učinkovite implementacije mnogih kriptosistemov. Omenili smo že, da z optimalnimi normalnimi bazami pospešimo množenje elementov končnega obsega. Njihova poglavitna lastnost je ta, da imajo v multiplikacijski matriki najmanjše možno število neničelnih elementov in je zato tudi množenje hitrejše kot v ostalih normalnih bazah. Obstajata dva različna tipa optimalnih normalnih baz, to so optimalne normalne baze tipa I in optimalne normalne baze tipa II. Ta koncept so leta 1988 zasnovali *R. C. Mullin*, *I. M. Onyszchuk*, *S. A. Vanstone* in *R. M. Wilson*.

V tem poglavju najprej definiramo optimalne normalne baze, nato se posvetimo njihovi konstrukciji in povezavi s polinomskimi bazami, na koncu pa navedemo izrek, ki nam pove, kdaj obstajajo optimalne normalne baze. Glavna referenca za to poglavje je Menezes et al. [18, poglavje 5].

4.1 Konstrukcija optimalnih normalnih baz

Ko smo obravnavali množenje v končnih obsegih, smo definirali multiplikacijsko matriko M normalne baze $N = \{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$. To je tista $n \times n$ razsežna matrika, katere elementi so koeficienti v produktu

$$\alpha\alpha_i = \sum_{j=0}^{n-1} m_{ij}\alpha_j \quad \text{za} \quad i \in \{0, \ldots, n-1\} \quad \text{in} \quad m_{ij} \in \mathbb{F}_q. \tag{4.1}$$

Kot smo že povedali, število neničelnih elementov v matriki M imenujemo kompleksnost normalne baze N in označimo s c_N.

Izrek 4.1.1. *Spodnja meja kompleksnosti za vsako normalno bazo obsega* $\mathbb{F}_{q^n}$ *je* $2n - 1$.

Dokaz. Naj bo $N = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ normalna baza obsega $\mathbb{F}_{q^n}$. Potem je $b = \sum_{i=0}^{n-1} \alpha_i = \mathrm{Tr}(\alpha) \in \mathbb{F}_q$. Če seštejemo enačbe (4.1) in primerjamo koeficente pri α_k, dobimo

$$\sum_{i=0}^{n-1} m_{ij} = \begin{cases} b, & j = 0 \\ 0, & 1 \leq j \leq n-1. \end{cases}$$

Ker je $\alpha \neq 0$ in je $\{\alpha\alpha_i \mid 0 \leq i \leq n-1\}$ tudi baza, je multiplikacijska matrika M obrnljiva. Torej je za vsak j vsaj en neničeln m_{ij}. Za vsak $j \neq 0$ morata biti vsaj dva neničelna koeficienta m_{ij}, da se stolpec matrike M sešteje v 0. Torej obstaja vsaj $2n-1$ neničelnih elementov v matriki M. Enakost je dosežena natanko tedaj, ko ima α neničeln koeficient v natanko enem členu produkta $\alpha\alpha_i$ (s koeficientom b) in se vsi ostali elementi N pojavijo v natanko dveh takih produktih. Njihovi koeficienti so si aditivni inverzi. □

Normalna baza N je **optimalna**, če je njena kompleksnost $c_N = 2n-1$. Pogledali bomo izrek, na katerem temelji konstrukcija normalnih baz in v posebnem primeru tudi konstrukcija optimalnih normalnih baz. Najprej pa bomo dokazali lemo, ki jo bomo potrebovali kasneje v dokazu omenjenega izreka.

Lema 4.1.2. *Naj bosta k, n taki naravni števili, da je $nk+1$ praštevilo in naj bo red elementa q po modulu $nk+1$ enak e. Predpostavimo, da velja $\gcd(nk/e, n) = 1$. Naj bo τ primitivni k-ti koren enote v $\mathbb{Z}_{nk+1}$. Potem lahko vsak neničeln element r v $\mathbb{Z}_{nk+1}$ zapišemo enolično v obliki*

$$r = \tau^i q^j \quad za \quad i \in \{0, 1, \ldots, k-1\} \quad in \quad j \in \{0, 1, \ldots, n-1\}.$$

Dokaz. Naj bo $e_1 = nk/e$. Potem obstaja primitivni element g v $\mathbb{Z}^*_{nk+1}$, tako da je $q = g^{e_1}$. Ker je red elementa g enak nk in red elementa τ enak k, obstaja tako število a, da velja

$$\tau = g^{na}, \quad \text{kjer je} \quad \gcd(a, k) = 1.$$

Zdaj pa predpostavimo, da obstajajo taka naravna števila $i, s \in \{0, 1, \ldots, k-1\}$ in $j, t \in \{0, 1, \ldots, n-1\}$, da velja

$$\tau^i q^j \equiv \tau^s q^t \pmod{nk+1},$$

kar pomeni, da velja

$$\tau^{i-s} = q^{t-j} \pmod{nk+1} \text{ in } g^{na(i-s)} \equiv g^{e_1(t-j)}.$$

Potem sledi

$$na(i-s) \equiv e_1(t-j) \pmod{nk}. \tag{4.2}$$

Ker smo predpostavili, da je $\gcd(n, e_1) = 1$, nam enačba (4.2) implicira, da $n \mid (t-j)$. Zato mora veljati $t = j$. Tako iz kongruence (4.2) sledi

$$a(i-s) \equiv 0 \pmod{k}.$$

Vemo pa, da je $\gcd(a, k) = 1$, zato velja tudi $k \mid (i-s)$. Sledi $i = s$. To nam dokazuje, da so

$$\tau^i q^j \pmod{nk+1} \text{ za } i \in \{0, 1, \ldots, k-1\} \text{ in } j \in \{0, 1, \ldots, n-1\}$$

vsi različni. Ker je produkt $\tau^i q^j$ različen od 0 po modulu $nk+1$, lahko vsak neničeln element iz $\mathbb{Z}_{nk+1}$ enolično izrazimo v željeni obliki. □

Izrek 4.1.3. *Naj bo q praštevilo ali njegova potenca in n, k taki naravni števili, da je $nk+1$ praštevilo, ki ne deli q. Naj bo β primitivni $(nk+1)$-vi koren enote v $\mathbb{F}_{q^{nk}}$ in $\gcd(nk/e, n) = 1$, kjer je e red q po modulu $nk+1$. Potem za vsak primitivni k-ti koren enote $\tau \in \mathbb{Z}_{nk+1}$ element*

$$\alpha = \sum_{i=0}^{k-1} \beta^{\tau^i}$$

generira normalno bazo obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ s kompleksnostjo največ $(k+1)n-k$ ali $kn-1$, kjer je $k \equiv 0 \bmod p$ in p karakteristika obsega $\mathbb{F}_q$.

Dokaz. Najprej bomo dokazali, da je element $\alpha \in \mathbb{F}_{q^n}$. Ker je

$$q^{nk} \equiv 1 \pmod{nk+1},$$

je q^n k-ti koren enote v $\mathbb{Z}_{nk+1}$. Potem obstaja tako naravno število l, da je $q^n = \tau^\ell$. Sledi

$$\alpha^{q^n} = \sum_{i=0}^{k-1} \beta^{\tau^i q^n} = \sum_{i=0}^{k-1} \beta^{\tau^{i+\ell}} = \sum_{i=0}^{k-1} \beta^{\tau^i} = \alpha.$$

Torej je α element obsega $\mathbb{F}_{q^n}$.

Zdaj bomo dokazali, da so elementi $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ linearno neodvisni nad obsegom $\mathbb{F}_q$. Predpostavimo, da velja

$$\sum_{i=0}^{n-1} \lambda_i \alpha^{q^i} = \sum_{i=0}^{n-1} \lambda_i \sum_{j=0}^{k-1} \beta^{\tau^j q^i} = 0, \quad \text{kjer so } \lambda_i \in \mathbb{F}_q.$$

Obstajajo enolično določeni $u_i \in \mathbb{F}_q$ za $i \in \{1, 2, \ldots, kn\}$, tako da za vse $(kn+1)$-vi korene enote γ velja

$$\sum_{i=0}^{n-1} \sum_{j=0}^{k-1} \lambda_i \gamma^{\tau^j q^i} = \sum_{j=1}^{nk} u_j \gamma^j = \gamma \sum_{j=0}^{nk-1} u_{j+1} \gamma^j.$$

Po prejšnji lemi namreč $\tau^j q^i$ po modulu $nk+1$ preteče $\mathbb{Z}^*_{nk+1}$ za $j \in \{0,1,\ldots,k-1\}$ in $i \in \{0,1,\ldots,n-1\}$. Naj bo

$$f(x) = \sum_{j=0}^{nk-1} u_{j+1} x^j.$$

Za vsak $r \in \{1,\ldots,nk\}$ obstajata taki števili u in v, da velja $r = \tau^u q^v$. Ker je β^r prav tako $nk+1$-vi koren enote, velja

$$\beta^r f(\beta^r) = \sum_{i=0}^{n-1} \lambda_i \sum_{j=0}^{k-1} (\beta^r)^{\tau^j q^i} = \sum_{i=0}^{n-1} \lambda_i \left(\sum_{j=0}^{k-1} \beta^{\tau^{u+j} q^i} \right)^{q^v} =$$

$$= \left(\sum_{i=0}^{n-1} \lambda_i \sum_{j=0}^{k-1} \beta^{\tau^j q^i} \right)^{q^v} = 0.$$

Torej je β^r koren polinoma $f(x)$ za $r \in \{1,\ldots,nk\}$ in potemtakem produkt

$$\prod_{r=1}^{nk} (x - \beta^r) = \frac{x^{nk+1} - 1}{x - 1} = x^{nk} + \cdots + x + 1$$

deli $f(x)$. Ker pa je $f(x)$ stopnje največ $nk-1$, dobimo protislovje. Torej morajo biti $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ linearno neodvisni nad $\mathbb{F}_q$ in zato tvorijo normalno bazo obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$.

Zdaj bomo izračunali multiplikacijsko matriko te baze. Za vse $i \in \{0,1,\ldots,n-1\}$ velja

$$\alpha \alpha^{q^i} = \sum_{u=0}^{k-1} \sum_{v=0}^{k-1} \beta^{\tau^u + \tau^v q^i} = \sum_{u=0}^{k-1} \sum_{v=0}^{k-1} \beta^{\tau^u (1 + \tau^{v-u} q^i)} =$$

$$\sum_{v=0}^{k-1} \left(\sum_{u=0}^{k-1} \beta^{\tau^u (1+\tau^v q^i)} \right). \tag{4.3}$$

Obstaja enolično določen par (v_0, i_0) za $v_0 \in \{0,1,\ldots,k-1\}$ in $i_0 \in \{0,1,\ldots,n-1\}$, tako da velja

$$1 + \tau^{v_0} q^{i_0} \equiv 0 \mod nk+1.$$

Če je $(v,i) \neq (v_0, i_0)$, potem je

$$1 + \tau^v q^i \equiv \tau^w q^j \mod nk+1$$

za neki števili $w \in \{0,1,\ldots,k-1\}$ in $j \in \{0,1,\ldots,n-1\}$ in velja

$$\sum_{u=0}^{k-1} \beta^{\tau^u (1+\tau^v q^i)} = \sum_{u=0}^{k-1} \beta^{\tau^{u+w} q^j} = \left(\sum_{u=0}^{k-1} \beta^{\tau^u} \right)^{q^j} = \alpha^{q^j}.$$

Če je $(v, i) = (v_0, i_0)$, potem velja

$$\sum_{u=0}^{k-1} \beta^{\tau^u(1+\tau^v q^i)} = k,$$

kar je enako 0, če je $k \equiv 0 \pmod{p}$. Torej je za vse $i \neq i_0$ produkt (4.3) vsota največ k baznih elementov. Potem je kompleksnost te baze največ $(n-1)k + n = (k+1)n - k$. Če je $k \equiv 0 \pmod{p}$ in je $i = i_0$, potem je (4.3) vsota največ $k-1$ baznih elementov. Če je torej $k \equiv 0 \pmod{p}$, potem je kompleksnost baze največ $(n-1)k + k - 1 = kn - 1$. S tem je izrek dokazan. □

Element α iz izreka 4.1.3 imenujemo **Gaussova perioda**. Gaussove periode se uporabljajo tudi na primer za faktorizacijo števil ali konstrukcijo nerazcepnih polinomov. Kot posebna primera izreka 4.1.3 sledita konstrukciji optimalnih normalnih baz tipa I in tipa II. Kadar je q lih in je $k = 2$, element α iz izreka 4.1.3 generira normalne baze kompleksnosti $3n-2$. Točno kompleksnost normalne baze je v splošnem težko določiti. Brez dokaza bomo navedli izrek, ki govori o kompleksnosti normalnih baz, glej [2].

Izrek 4.1.4. *Naj bo $q = 2$. Normalna baza, ki je generirana z elementom α iz izreka 4.1.3, ima kompleksnost*

- $4n - 7$, *če je* $k = 3, 4$ *in* $n > 1$;
- $6n - 21$, *če je* $k = 5$ *in* $n > 2$ *ali* $k = 6$ *in* $n > 12$;
- $8n - 43$, *če je* $k = 7$ *in* $n > 6$.

□

Za $k = 1$ iz izreka 4.1.3 dobimo optimalne normalne baze tipa I.

Posledica 4.1.5. *Naj bo $n + 1$ praštevilo in q primitiven v $\mathbb{Z}_{n+1}$, kjer je q praštevilo ali njegova potenca. Potem je n od enote različnih $(n+1)$-ih primitivnih korenov enote linearno neodvisnih in tvorijo optimalno normalno bazo obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$.* □

Oglejmo si multiplikacijsko matriko te baze. Naj bo element α $(n+1)$-i primitivni koren enote. Potem je α koren polinoma $x^n + \cdots + x + 1$. Ker pa je $n + 1$ praštevilo, $n + 1$ deli $q^n - 1$ in vsi $(n+1)$-i koreni enote so v $\mathbb{F}_{q^n}$. Ker je q primitiven v $\mathbb{Z}_{n+1}$, obstaja n različnih konjugirank elementa α, ki so vse od enote različni $(n+1)$-i koreni enote. Torej je

$$N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\} = \{\alpha, \alpha^2, \ldots, \alpha^n\}$$

normalna baza obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$. Velja

$$\alpha\alpha^i = \alpha^{i+1} \in N, \text{ za vsak } i \in \{1, \ldots, n-1\}$$

in

$$\alpha\alpha^n = 1 = -\mathrm{Tr}(\alpha) = -\sum_{i=1}^{n} \alpha^i.$$

V vseh teh produktih je natanko $2n-1$ neničelnih členov in zato je N optimalna. Matrika M, ki ustreza tej bazi, ima naslednje lastnosti: v vsaki vrstici je natanko ena 1, razen ene vrstice, v kateri so vsi elementi enaki -1. Vsi ostali elementi matrike M so seveda enaki 0. Optimalno normalno bazo, dobljeno s to konstrukcijo, imenujemo **optimalna normalna baza tipa I**.

Iz izreka 4.1.3 za $k = 2$ in $q = 2$ dobimo konstrukcijo optimalne normalne baze tipa II.

Izrek 4.1.6. *Naj bo $2n+1$ praštevilo in naj velja*

(i) *2 je primitiven element v $\mathbb{Z}_{2n+1}$, ali*

(ii) *$2n+1 \equiv 3 \bmod 4$ in 2 generira kvadrate v $\mathbb{Z}_{2n+1}$.*

Potem $\alpha = \gamma + \gamma^{-1}$ generira optimalno normalno bazo obsega $\mathbb{F}_{2^n}$ nad $\mathbb{F}_2$, kjer je γ primitivni $(2n+1)$-i koren enote. □

Za tak $\alpha \in \mathbb{F}_{2^n}$ so elementi $\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}$ linearno neodvisni nad $\mathbb{F}_2$. Torej je $N = \{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$ normalna baza obsega $\mathbb{F}_{2^n}$. Ker je γ primitivni $(2n+1)$-i koren enote, je $\gamma^{n+1} = \gamma^{-n}$. Zato velja

$$\gamma^{n+1} + \gamma^{-(n+1)} = \gamma^n + \gamma^{-n}. \tag{4.4}$$

Potem je

$$N = \{\gamma + \gamma^{-1}, \gamma^2 + \gamma^{-2}, \ldots, \gamma^n + \gamma^{-n}\}.$$

Produkti baznih elementov so

$$(\gamma + \gamma^{-1})(\gamma^i + \gamma^{-i}) = (\gamma^{(1+i)} + \gamma^{-(1+i)}) + (\gamma^{(1-i)} + \gamma^{-(1-i)}),$$

kar je vsota dveh različnih elementov iz N, razen za $i = 1$. Če je $i = 1$, je ta vsota enaka α^2, kar je v N. Če torej označimo $\alpha_i = \alpha^{2^i}$ za $i \in \{1, \ldots, n-1\}$, dobimo

$$\alpha\alpha_i = \alpha_{i+1} + \alpha_{i-1}.$$

N je optimalna normalna baza obsega $\mathbb{F}_{2^n}$. Matrika M, ki ustreza tej bazi, ima v vsaki vrstici natanko dve 1, razen v prvi vrstici, kjer je natanko ena 1, vsi ostali elementi so seveda enaki 0. Optimalno normalno bazo, dobljeno s to konstrukcijo, imenujemo **optimalna normalna baza tipa II**.

Za praktične aplikacije potrebujemo optimalne normalne baze nad $\mathbb{F}_2$. Obstajajo preprosta pravila za preverjanje hipotez iz posledic 4.1.5 in 4.1.6. Strnimo jih v naslednji rezultat, glej Leveque [13, stran 68].

Trditev 4.1.7. *Naj bosta r in s praštevili. Potem veljajo naslednje lastnosti:*

- 2 *je primitiven v* $\mathbb{Z}_r$, *če je* $r = 4s + 1$, *kjer je* s *liho.*
- 2 *je primitiven v* $\mathbb{Z}_r$, *če je* $r = 2s + 1$, *kjer je* $s \equiv 1 \bmod 4$.
- 2 *generira kvadrate v* $\mathbb{Z}_r$, *če je* $r = 2s + 1$, *kjer je* $s \equiv 3 \bmod 4$. □

4.2 Povezava s polinomskimi bazami

Polinomske baze so za kriptografske namene tradicionalno najpogosteje uporabljene baze. Na voljo so v vsaki karakteristiki p in za vsak obseg $\mathbb{F}_{q^n}$.

Trditev 4.2.1. *Naj bo α ničla nekega nerazcepnega polinoma f stopnje n iz $\mathbb{F}_q[x]$. Množica $P = \{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ je baza vektorskega prostora $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$, f pa je minimalni polinom elementa α.*

Dokaz. Preveriti moramo, da so elementi množice P linearno neodvisni. Minimalni polinom elementa α mora deliti nerazcepni polinom f, to pa velja le, če je f enak minimalnemu polinomu. Torej α ni ničla nobenega polinoma iz $\mathbb{F}_q[x]$, ki ima stopnjo manjšo od n. Zato so vsi elementi P linearno neodvisni. Ker je moč množice P enaka n, je P res baza. □

Množica P se imenuje **polinomska baza** vektorskega prostora $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$. Za nerazcepni polinom f iz definicije polinomske baze je faktorski kolobar $\mathbb{F}_q[x]/f(x)$ obseg. Moč tega obsega je $q^{\deg(f)} = q^n$, torej je ta obseg izomorfen obsegu $\mathbb{F}_{q^n}$. Povzemimo zgornje ugotovitve v naslednjo trditev, za dokaz glej Vidav [24, poglavje 9].

Trditev 4.2.2. *Naj bo $\mathbb{F}_q$ končen obseg in $\mathbb{F}_{q^n}$ njegova razširitev stopnje n. Potem v $\mathbb{F}_q[x]$ obstaja nerazcepen polinom $f(x)$ stopnje n in je $\mathbb{F}_{q^n} \cong \mathbb{F}_q[x]/f(x)$ obseg, kjer je $\mathbb{F}_q[x]/f(x)$ obseg polinomov nad obsegom $\mathbb{F}_q$, reduciranih po modulu polinoma $f(x)$.* □

Optimalne normalne baze tipa I

Ogledali si bomo minimalne polinome generatorjev optimalnih normalnih baz. Minimalni polinom generatorja optimalne normalne baze tipa I je kar polinom $f(x) = x^n + \ldots + x + 1$, njegovo nerazcepnost pa nam zagotovi naslednji izrek, glej Vidav [24, poglavje 9].

Izrek 4.2.3. *Polinom $x^n + \ldots + x + 1$ je nerazcepen nad $\mathbb{F}_q$ natanko tedaj, ko je $n+1$ praštevilo in q primitiven v $\mathbb{Z}_{n+1}$.* □

Optimalne normalne baze tipa II

Minimalni polinom generatorja optimalne normalne baze tipa II je težje poiskati. Naj bo $2n+1$ praštevilo, γ $(2n+1)$-i primitivni koren enote in polinom $f_n(x) = \prod_{j=1}^{n}(x-\gamma^j-\gamma^{-j}) = \sum_{i=0}^{n} m_i x^i$, $m_i \in \mathbb{F}_2$. Če veljajo pogoji izreka 4.1.6, je polinom $f(x)$ minimalni polinom elementa $\alpha = \gamma + \gamma^{-1}$. Poiskali bomo eksplicitno formulo polinoma $f_n(x)$ brez γ. Za vsak $j \in \{1, \ldots, n\}$ je γ^j prav tako $(2n+1)$-i koren enote, ker je $\gcd(j, 2n+1) = 1$, kajti $2n+1$ je praštevilo po predpostavki. Iz enakosti (4.4) sledi, da velja

$$(\gamma^j)^n + (\gamma^j)^{-n} = (\gamma^j)^{n+1} + (\gamma^j)^{-(n+1)},\ j \in \{0, 1, \ldots, n\}. \tag{4.5}$$

Uporabili bomo Waringovo formulo (glej [15, poglavje 1.3]):

$$A^n + B^n = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-1)^i (A+B)^{n-2i}(AB)^i,\ A, B \in \mathbb{F}_{2^n}. \tag{4.6}$$

Iz formule (4.6) sledi, da za vsako naravno število k velja

$$(\gamma^j)^k + (\gamma^{-j})^k = (\gamma^j)^k + (\gamma^j)^{-k} = \sum_{i=0}^{\lfloor k/2 \rfloor} \frac{k}{k-i}\binom{k-i}{i}(-1)^i (\gamma^j + \gamma^{-j})^{k-2i}. \tag{4.7}$$

Vsota na desni strani strani enačbe je zelo podobna Dicksonovemu polinomu. Dicksonovi polinomi so posebna vrsta permutacijskih polinomov nad končnimi obsegi, definirani z naslednjo vsoto

$$D_k(x) = \sum_{i=0}^{\lfloor k/2 \rfloor} \frac{k}{k-i}\binom{k-i}{i}(-1)^i x^{k-2i}. \tag{4.8}$$

Izkazalo se je, da so Dicksonovi polinomi pomembni tako v teoretični kot tudi v uporabni matematiki. Več o Dicksonovih polinomih se nahaja v [14]. Iz (4.7) in (4.8) sledi

$$D_k(\gamma^j + \gamma^{-j}) = (\gamma^j)^k + (\gamma^j)^{-k}. \tag{4.9}$$

Oglejmo si zdaj polinom $D_{n+1}(x) - D_n(x)$. Ta je po (4.9) enak

$$D_{n+1}(x) - D_n(x) = (\gamma^j)^{n+1} + (\gamma^j)^{-(n+1)} - (\gamma^j)^n - (\gamma^j)^{-n}.$$

Potem iz enakosti (4.5) sledi, da je $\gamma^j + \gamma^{-j}$ za vsak $j \in \{0, 1, \ldots, n\}$ koren polinoma $D_{n+1}(x) - D_n(x)$. Po definiciji mora biti polinom $D_{n+1}(x) - D_n(x)$ stopnje $n+1$ in zato ima $n+1$ ničel. Ker so vsi $\gamma^j + \gamma^{-j}$ različni za različne $j \in \{0, 1, \ldots, n\}$, so to natanko vsi koreni polinoma $D_{n+1}(x) - D_n(x)$. Hkrati pa vemo, da so vsi $\gamma^j + \gamma^{-j}$ za $j \in \{1, \ldots, n\}$ koreni minimalnega polinoma elementa α. Zato velja

$$D_{n+1}(x) - D_n(x) = \prod_{j=0}^{n}(x - \gamma^j - \gamma^{-j}) = (x-2)f_n(x).$$

Tako dobimo minimalni polinom elementa $\alpha = \gamma + \gamma^{-1}$

$$f_n(x) = \sum_{j=0}^{[(n-1)/2]} (-1)^j \binom{n-1-j}{j} x^{n-(2j+1)} + \sum_{j=0}^{[n/2]} (-1)^j \binom{n-j}{j} x^{n-2j}.$$

Ponavadi pa je lažje rekurzivno določiti $f_n(x)$. Pri tem nam pomaga naslednja trditev.

Trditev 4.2.4. *Za zaporedje polinomov $f_n(x)$ velja rekurzivna zveza:*

$$f_0(x) = 1,\ f_1(x) = x + 1,\ f_n(x) = xf_{n-1}(x) - f_{n-2}(x) \text{ za } n \geq 2.$$

Dokaz. Najprej izračunajmo prvih nekaj polinomov $f_n(x)$.

$$f_0(x) = 1$$

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

$$f_2(x) = x + x^2 - 1 = x(x+1) - 1 = xf_1(x) - f_0(x)$$

$$f_3(x) = x^3 + x^2 - 2x - 1 = x(x(x+1) - 1) - (1+x) = xf_2(x) - f_1(x)$$

Zdaj pa predpostavimo, da trditev velja za neko naravno število n in dokažimo, da velja tudi za $n+1$.

$$f_{n+1}(x) = \sum_{j=0}^{[n/2]} (-1)^j \binom{n-j}{j} x^{n-2j} + \sum_{j=0}^{[(n+1)/2]} (-1)^j \binom{n+1-j}{j} x^{n+1-2j} =$$

$$= x\left(\sum_{j=0}^{[n/2]}(-1)^j\left[\binom{n-1-j}{j}+\binom{n-1-j}{j-1}\right]x^{n-(2j+1)}+\right.$$

$$\left.+\sum_{j=0}^{[(n+1)/2]}(-1)^j\left[\binom{n-j}{j}+\binom{n-j}{j-1}\right]x^{n-2j}\right)=$$

$$= xf_n(x)+\sum_{j=0}^{[n/2]}(-1)^j\binom{n-1-j}{j-1}x^{n-2j}+\sum_{j=0}^{[(n+1)/2]}(-1)^j\binom{n-j}{j-1}x^{n-2j+1}=$$

$$= xf_n(x)+\sum_{k=1}^{[n/2]}(-1)^{k+1}\binom{n-k-2}{k}x^{n-2k-2}+\sum_{k=1}^{[(n+1)/2]}(-1)^{k+1}\binom{n-k-1}{k}x^{n-2k-1}=$$

$$= xf_n(x)-f_{n-1}$$

Ker ta rekurzivna zveza velja za $n+1$, velja za vsako naravno število. Z indukcijo smo dokazali trditev. □

Opomnimo še, da je polinom $f_n(x)$ nerazcepen nad $\mathbb{F}_q$ natanko tedaj, ko je multiplikativna grupa $\mathbb{Z}^*_{2n+1}$ generirana z elementoma q in -1 ter je $f_n(x)$ nerazcepen nad obsegom racionalnih števil, ko je $2n+1$ praštevilo.

Elemente optimalne normalne baze tipa II lahko takole izrazimo v polinomski bazi:

$$x^{2^i} \bmod f_n = \sum_{j=0}^{n-1} s_{ij}x^j, \text{ za } i \in \{0,1,\ldots,n-1\}.$$

Potem lahko vsak element $A \in \mathbb{F}_{2^n}$ izrazimo v polinomski bazi s pomočjo matrike $S = (s_{ij})$

$$A = \sum_{i=0}^{n-1} a_i x^{2^i} = S\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}.$$

4.3 Določitev vseh optimalnih normalnih baz

V prejšnjem razdelku smo videli dve konstrukciji optimalnih normalnih baz. Ob tem se poraja naravno vprašanje, če obstajajo še kakšne druge optimalne normalne baze.

Naj bo N optimalna normalna baza obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ in $a \in \mathbb{F}_q$. Potem je tudi $aN = \{a\alpha : \alpha \in N\}$ optimalna normalna baza obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$. Pravimo, da sta si bazi N in aN **ekvivalentni**. Gao je dokazal, da mora biti vsaka optimalna normalna baza končnega obsega ekvivalentna optimalni normalni bazi tipa I ali tipa II. Torej so vse optimalne normalne baze v končnih obsegih popolnoma določene z izrekoma 4.1.5 in 4.1.6. Leta 1992 sta Gao in Lenstra dokazala naslednji izrek, ki nam pove, kdaj obstajajo optimalne normalne baze. Za dokaz izreka glej Gao [6, poglavje 4.2], za obširen dokaz splošnejše verzije izreka pa Gao in Lenstra [7].

Izrek 4.3.1. *Naj bo* $N = \{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ *optimalna normalna baza obsega* $\mathbb{F}_{q^n}$ *nad* $\mathbb{F}_q$. *Naj bo* $b = \mathrm{Tr}_{q^n|q}(\alpha)$ *sled elementa* α *v* $\mathbb{F}_q$. *Potem velja eden izmed naslednjih pogojev:*

(i) število $n+1$ *je praštevilo, število* q *je primitivno v* $\mathbb{Z}_{n+1}$ *in* $-\alpha/b$ *je primitiven* $(n+1)$*-i koren enote ali*

(ii) število $q = 2^v$ *za nek* $v \in \mathbb{N}$, *kjer je* $\gcd(n, v) = 1$, *število* $2n + 1$ *je praštevilo, števili* 2 *in* -1 *generirata multiplikativno grupo* $\mathbb{Z}^*_{2n+1}$ *in* $\alpha/b = \gamma + \gamma^{-1}$, *kjer je element* γ *nek primitiven* $(2n + 1)$*-i koren enote.*

□

Poglavje 5

NORMALNE BAZE NIZKE KOMPLEKSNOSTI

Spomnimo se, da število neničelnih elementov multiplikacijske matrike imenujemo kompleksnost normalne baze N in označimo s c_N. Pokazali smo, da so vse normalne baze kompleksnosti vsaj $2n-1$, tiste z najnižjo kompleksnostjo pa imenujemo optimalne. Vendar optimalne normalne baze ne obstajajo v vseh končnih obsegih. Za praktično uporabo želimo normalne baze čim nižje kompleksnosti, saj se nam tako poenostavi množenje elementov. V tem poglavju bomo predstavili družino normalnih baz, ki jih je vpeljal Sidel'nikov [22]. Vse elemente baze lahko dobimo iz enega elementa s ponavljajočo uporabo linearne ulomljene funkcije $\varphi(x) = (ax+b)/(cx+d)$, kjer so $a, b, c, d \in \mathbb{F}_q$. Sidel'nikov je dokazal, da so produkti elementov take normalne baze oblike $\alpha_i\alpha_j = e_{i-j}\alpha_i + e_{j-i}\alpha_j + \gamma$ za $i \neq j$, kjer so $e_i, \gamma \in \mathbb{F}_q$. Pokazali bomo, da lahko vse take baze dobimo iz korenov nerazcepnega faktorja polinoma $F(x) = cx^{q+1} + dx^q - ax - b$. Skonstruirali bomo normalne baze obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ s kompleksnostjo $3n-2$ za vsako število n, ki deli $q-1$ in za $n = p$, kjer je p karakteristika obsega $\mathbb{F}_q$.

V prvem razdelku si bomo ogledali lastnosti linearnih ulomljenih funkcij. Nato bomo preučevali popolno faktorizacijo polinoma $F(x) = cx^{q+1} + dx^q - ax - b$. V zadnjem razdelku pa se nahaja konstrukcija normalnih baz kompleksnosti $3n-2$. Referenci za to poglavje sta Blake, Gao in Mullin [4] ter Gao [6].

5.1 Linearne ulomljene funkcije

Ogledali si bomo nekaj lastnosti linearne ulomljene funkcije $\varphi(x) = (ax+b)/(cx+d)$, kjer so $a, b, c, d \in \mathbb{F}_q$ in je $ad-bc \neq 0$. Kompozitum poljubnih dveh linearnih ulomljenih funkcij je prav tako linearna ulomljena funkcija. Funkcija $\varphi(x)$ inducira permutacijo na $\mathbb{F}_{q^n} \cup \infty$ za vsako naravno število n. Privzeli bomo

$$\frac{a\infty + b}{c\infty + d} := \frac{a}{c} \text{ za } c \neq 0,$$

$$\frac{a\infty + b}{c\infty + d} := \infty \text{ za } ad \neq 0, c = 0 \text{ in}$$

$$\frac{a}{0} := \infty \text{ za } a \neq 0.$$

Inverz linearne ulomljene funkcije φ je podan s funkcijo

$$\varphi^{-1}(x) = (-dx + b)/(cx - a).$$

Red preslikave φ pa je najmanjše število t, za katerega velja $\varphi^t(x) = x$.

Potrebovali bomo take funkcije φ, ki imajo koeficient c različen od 0. Fiksna točka funkcije $\varphi(x)$ zadošča kvadratni enačbi

$$cx^2 - (a-d)x - b = 0. \tag{5.1}$$

Naslednjih dveh lem ni težko preveriti, potrebovali pa ju bomo v nadaljevanju.

Lema 5.1.1. *Naj bo $\varphi(x) = (ax+b)$ linearna preslikava, kjer sta $a, b \neq 0, 1$. Potem velja*

$$\varphi = h^{-1}\Psi h,$$

kjer je $\Psi(x) = ax$ in $h(x) = x + b/(a-1)$.

Dokaz. Iz definicije preslikave h sledi, da je njen inverz enak $h^{-1}(x) = x - b/(a-1)$. Preverimo:

$$h^{-1}(\Psi(h(x))) = h^{-1}(\Psi(x + b/(a-1))) = h^{-1}(ax + ab/(a-1))) = ax + b = \varphi(x).$$

□

Lema 5.1.2. *Naj bo funkcija*

$$\varphi(x) = (ax + b)/(cx + d),$$

kjer so $a, b, c, d \in \mathbb{F}_q$, $c \neq 0$ *in* $ad - bc \neq 0$ *in naj bo* $\Delta = (a - d)^2 + 4bc$. *Potem velja*

$$\varphi = h^{-1}\psi h,$$

kjer sta funkciji $h(x)$ *in* $\psi(x)$ *definirani v naslednjih dveh točkah.*

(i) Če je $\Delta = 0$, *je* x_0 *edina rešitev enačbe (5.1) v* $\mathbb{F}_q$, x_0 *torej zadošča pogojema* $cx_0^2 = -b$ *in* $2cx_0 = a - d$. *Potem je*

$$h(x) = (a/c - x_0)/(x - x_0) \quad in \quad \Psi(x) = x + 1.$$

(ii) Če je $\Delta \neq 0$, *obstajata dve rešitvi* x_0, x_1 *enačbe (5.1) v* $\mathbb{F}_{q^2}$ *in označimo* $\xi = (a - cx_0)/(a - cx_1)$. *Potem je*

$$h(x) = \frac{x - x_0}{x - x_1} \quad in \quad \psi(x) = x\xi.$$

Dokaz. Iz definicije funkcije h sledi, da je njen inverz enak $h^{-1}(x) = (a/c - x_0)/x + x_0$. Računamo:

$$h^{-1}(\psi(h(x))) = h^{-1}(\psi((a/c-x_0)/(x-x_0)) = h^{-1}((a/c-x_0)/(x-x_0)+1) = \frac{ax - cx_0^2}{a - 2cx_0 + x}.$$

Vstavimo ustrezne izraze namesto x_0 in prvi del leme je dokazan. Drugi del gre podobno, le z nekoliko več računanja. □

Zdaj lahko določimo red funkcije φ, ki je kar enak redu funkcije ψ. Če je ψ oblike $x+1$, potem je red ψ enak aditivnemu redu p enice v $\mathbb{F}_q$, kjer je p karakteristika obsega $\mathbb{F}_q$. Če je ψ oblike $x\xi$, pa je red funkcije ψ enak multiplikativnemu redu ξ. V primeru (ii) leme 5.1.2, če je Δ kvadrat v $\mathbb{F}_q$, so $x_0, x_1, \xi \in \mathbb{F}_q$. Tako dobimo $\xi^{q-1} = 1$ in red ξ je delitelj števila $q - 1$. Če je Δ nekvadrat v $\mathbb{F}_q$, pa sta $x_0, x_1 \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ in velja $x_0^q = x_1$ in $x_1^q = x_0$. Sledi

$$\xi^q = ((a - cx_0)/(a - cx_1))^q = (a - cx_0^q)/(a - cx_1^q) = (a - cx_1)/(a - cx_0) = 1/\xi.$$

Torej je $\xi^{q+1} = 1$ in red ξ deli $q + 1$. Potemtakem je red funkcije φ vedno delitelj enega od naslednjih števil: p, $q - 1$ ali $q + 1$.

Lema 5.1.3. *Naj bodo $a, b, c, d \in \mathbb{F}_q$, $c \neq 0$ in $ad - bc \neq 0$. Naj bo funkcija*

$$\varphi(x) = (ax + b)/(cx + d)$$

reda t. Potem za vsak $i \in \{1, \ldots, t-1\}$ velja

$$\varphi^i(x) = \frac{e_i x + b/c}{x - e_{t-i}} \quad in \quad e_i + e_{t-i} = \frac{a-d}{c}, \tag{5.2}$$

kjer je $e_1 = a/c$ in $e_{i+1} = \varphi(e_i)$ za vsak $i \in \{1, \ldots, t-2\}$.

Dokaz. Z indukcijo po i dokažemo, da obstajajo taki $e_i, f_i \in \mathbb{F}_q$, $e_1 = a/c$, $f_1 = d/c$, da velja

$$\varphi^i(x) = \frac{e_i x + b/c}{x + f_i}$$

in

$$e_i - f_i = \frac{a-d}{c}, \; e_i = \varphi(e_{i-1})$$

za $i \in \{1, \ldots, t-1\}$, kjer je $e_0 = \infty$. Velja

$$\frac{e_{t-i}x + b/c}{x + f_{t-i}} = \varphi^{t-i}(x) = \varphi^{-i}(x) = (\varphi^i)^{-1}(x) = \frac{-f_i x + b/c}{x - e_i}.$$

Vidimo, da je $f_i = -e_{t-i}$. S tem je lema dokazana. □

Lema 5.1.4. *Pri enakih oznakah kot v lemi 5.1.3 velja*

$$\sum_{j=1}^{t-1} e_j = \begin{cases} (t-1)(a-d)/(2c), & \text{če } p \neq 2, \\ a/c = d/c, & \text{če } p = 2 \text{ in } t = 2, \\ (a-d)/c, & \text{če } p = 2 \text{ in } t \equiv 3 \mod 4, \\ 0, & \text{če } p = 2 \text{ in } t \equiv 1 \mod 4. \end{cases}$$

kjer je p karakteristika obsega $\mathbb{F}_q$.

Dokaz. Ločimo dva primera glede na tip funkcije $\varphi(x)$. Naj bo najprej

$$\Delta = (a-d)^2 + 4bc = 0.$$

Potem je $t = p$ in po lemi 5.1.2 je $\varphi(x) = h^{-1}\psi h(x)$, kjer velja

$$\psi(x) = x + 1, \; h(x) = \frac{a/c - x_0}{x - x_0} \text{ in } h^{-1}(x) = x_0 + \frac{a/c - x_0}{x},$$

in x_0 zadošča pogojema $2cx_0 = a - d$ in $cx_0^2 = -b$. Opomnimo, da je $\psi^i(x) = x + i$. Velja

$$\begin{aligned}\varphi^i(x) &= h^{-1}\psi^i h(x)\\ &= h^{-1}\left(\frac{a/c - x_0}{x - x_0} + i\right)\\ &= \frac{(a/c - x_0 - ix_0)x - ix_0^2}{ix + (a/c - x_0 - ix_0)}.\end{aligned}$$

Tako dobimo

$$e_i = \frac{a/c - x_0}{i} + x_0 \ \text{ za } \ i \in \{1, 2, \ldots, t-1\}.$$

Potem velja

$$\begin{aligned}\sum_{i=1}^{p-1} e_i &= (p-1)x_0 + (a/c - x_0)\sum_{i=1}^{p-1} i^{-1}\\ &= (p-1)x_0 + (a/c - x_0)\sum_{i=1}^{p-1} i\\ &= \begin{cases}(p-1)x_0 = (t-1)(a-d)/(2c), & \text{če } \ p \neq 2,\\ a/c = d/c, & \text{če } \ p = 2.\end{cases}\end{aligned}$$

V drugem primeru je

$$\Delta = (a-d)^2 + 4bc \neq 0.$$

Potem je red t funkcije $\varphi(x)$ faktor enega od števil $q-1$ ali $q+1$. Torej je $t \in \mathbb{F}_q^*$. Po lemi 5.1.2 je funkcija $\varphi(x) = h^{-1}\psi h(x)$, kjer velja

$$h(x) = \frac{x - x_0}{x - x_1},\ \psi(x) = \xi x,\ \xi = \frac{a/c - x_0}{a/c - x_1}$$

in $x_0 + x_1 = (a-d)/c$ ter $x_0x_1 = -b/c$. Opomnimo, da je

$$h^{-1}(x) = (x_1x - x_0)/(x-1) \ \text{ in } \ \psi^i(x) = \xi^i x.$$

Velja

$$\begin{aligned}\varphi^i(x) &= h^{-1}\psi^i h(x)\\ &= h^{-1}\left(\xi^i\frac{x - x_0}{x - x_1}\right)\\ &= \frac{(x_1\xi^i - x_0)x - x_0x_1(\xi^i - 1)}{(\xi^i - 1)x + x_1 - x_0\xi^i}.\end{aligned}$$

Torej je

$$e_i = \frac{x_1\xi^i - x_0}{\xi^i - 1} = x_1 + \frac{x_1 - x_0}{\xi^i - 1} \ \text{ za } \ i \in \{1, 2, \ldots, t-1\}$$

in

$$\sum_{i=1}^{t-1} e_i = (t-1)x_1 + (x_0 - x_1)\sum_{i=1}^{t-1} \frac{1}{1-\xi^i}.$$

Ker je ξ t-ti primitivni koren enote, velja

$$\prod_{i=1}^{t-1}(x-\xi^i) = (x^t-1)/(x-1) = x^{t-1} + x^{t-2} + \ldots + x + 1. \tag{5.3}$$

Naj bo v enačbi (5.3) $x = 1$. Dobimo

$$\prod_{i=1}^{t-1}(1-\xi^i) = t. \tag{5.4}$$

Če odvajamo enakost (5.3) glede na x na obeh straneh, dobimo

$$\prod_{i=1}^{t-1}(x-\xi^i)\left(\sum_{i=1}^{t-1}\frac{1}{x-\xi^i}\right) = (t-1)x^{t-2} + (t-2)x^{t-3} + \ldots + 2x + 1. \tag{5.5}$$

Naj bo v enačbi (5.5) $x = 1$. Dobimo

$$\sum_{i=1}^{t-1}\frac{1}{1-\xi^i} = \left(\sum_{i=1}^{t-1} i\right)/t = \begin{cases} (t-1)/2, & \text{če } p \neq 2, \\ 1, & \text{če } p = 2 \text{ in } t \equiv 3 \bmod 4, \\ 0, & \text{če } p = 2 \text{ in } t \equiv 1 \bmod 4. \end{cases}$$

Opomnimo, da je t lih, če je $p = 2$. Zato velja

$$\sum_{i=1}^{t-1} e_i = \begin{cases} ((t-1)/2)(x_0+x_1) = (t-1)(a-d)/(2c), & \text{če } p \neq 2, \\ x_0 - x_1 = (a-d)/c, & \text{če } p = 2 \text{ in } t \equiv 3 \bmod 4, \\ 0, & \text{če } p = 2 \text{ in } t \equiv 1 \bmod 4. \end{cases}$$

S tem je lema dokazana. □

Naslednji izrek je dokazal Sidel'nikov [22, Izrek 2].

Izrek 5.1.5. *Naj bodo $a, b, c, d \in \mathbb{F}_q$, $c \neq 0$ in $ad - bc \neq 0$. Naj bo θ koren polinoma*

$$F(x) = cx^{q+1} + dx^q - ax - b$$

v neki razširitvi obsega $\mathbb{F}_q$. Koren θ naj ne bo fiksna točka funkcije $\varphi(x) = (ax+b)/(cx+d)$, katere red naj bo t. Potem so

$$\theta, \varphi(\theta), \ldots, \varphi^{t-1}(\theta)$$

linearno neodvisni nad $\mathbb{F}_q$, če je $\sum_{i=0}^{t-1}\varphi^i(\theta) \neq 0$. □

Ta izrek pove: če znamo faktorizirati polinom $F(x)$, dobimo normalno bazo nad $\mathbb{F}_q$. Faktorizacijo polinoma $F(x)$ bomo obravnavali v naslednjem razdelku.

5.2 Faktorizacija polinoma $F(x) = cx^{q+1} + dx^q - ax - b$

Naj bo $\varphi(x) = (ax + b)/(cx + d)$ linearna ulomljena funkcija. Predpostavili bomo, da je $ad - bc \neq 0$, da izključimo trivialne primere. Prav tako bomo v tem razdelku predpostavili, da je red funkcije φ enak t.

Naj bo θ koren polinoma $F(x) = (cx + d)x^q - (ax + b)$. Potem je

$$\theta^q = \frac{a\theta + b}{c\theta + d} = \varphi(\theta).$$

Od tod sledi

$$\theta^{q^2} = (\varphi(\theta))^q = \varphi(\theta^q) = \varphi(\varphi(\theta)) = \varphi^2(\theta).$$

Z indukcijo dobimo $\theta^{q^i} = \varphi^i(\theta)$ za $i \geq 0$. Potem so

$$\theta, \varphi(\theta), \ldots, \varphi^{t-1}(\theta) \tag{5.6}$$

konjugiranke elementa θ nad $\mathbb{F}_q$. Če je θ fiksna točka linearne ulomljene funkcije $\varphi(x)$, potem je $\theta \in \mathbb{F}_q$ in je $x - \theta$ faktor polinoma $F(x)$. Če pa θ ni fiksna točka funkcije $\varphi(x)$, potem so po izreku 5.1.5 elementi v (5.6) različni in je θ stopnje t nad $\mathbb{F}_q$. V tem primeru je minimalni polinom elementa θ nad $\mathbb{F}_q$ nerazcepen faktor polinoma $F(x)$ stopnje t. Torej je nerazcepen faktor polinoma $F(x)$ linearen ali pa stopnje t. Najprej bomo obravnavali dva posebna primera.

Izrek 5.2.1. *Naj bo $\xi \in \mathbb{F}_q \backslash \{0\}$ multiplikativnega reda t. Potem je naslednja faktorizacija nad $\mathbb{F}_q$ popolna:*

$$x^{q-1} - \xi = \prod_{j=1}^{(q-1)/t} (x^t - \beta_j),$$

kjer so β_j vsi različni koreni polinoma $x^{(q-1)/t} - \xi$ v $\mathbb{F}_q$.

Dokaz. Naj bo θ koren polinoma $x^{q-1} - \xi$ v neki razširitvi obsega $\mathbb{F}_q$. Potem je

$$\theta^{q^i} = \theta\xi^i \quad \text{za} \quad i \geq 1.$$

Vse različne konjugiranke elementa θ nad $\mathbb{F}_q$ so

$$\theta, \theta\xi, \ldots, \theta\xi^{t-1}.$$

Minimalni polinom elementa θ nad $\mathbb{F}_q$ je

$$\prod_{i=0}^{t-1}(x-\theta\xi^i) = x^t - \theta^t$$

in deli $x^{q-1}-\xi$. To pomeni, da je vsak nerazcepen faktor polinoma $x^{q-1}-\xi$ oblike $x^t-\beta$, kjer je $\beta \in \mathbb{F}_q$. Dokaz zaključimo s tem, da $x^t-\beta$ deli $x^{q-1}-\xi$ natanko tedaj, ko je β koren $x^{(q-1)/t}-\xi$. □

Izrek 5.2.2. *Za $x^q-(x+b)$, $b \in \mathbb{F}_q^*$ je naslednja faktorizacija nad $\mathbb{F}_q$ popolna:*

$$x^q-(x+b) = \prod_{j=1}^{q/p}(x^p - b^{p-1}x - b^p\beta_j), \tag{5.7}$$

kjer so β_j različni elementi obsega $\mathbb{F}_q$, za katere je

$$\mathrm{Tr}_{q|p}(\beta_j) = 1$$

in je praštevilo p karakteristika končnega obsega $\mathbb{F}_q$.

Dokaz. Naj bo θ koren polinoma $F(x) = x^q-(x+b)$. Potem je

$$\theta^{q^i} = \theta + ib$$

za $i \geq 1$. Torej so konjugiranke elementa θ nad obsegom $\mathbb{F}_q$ enake

$$\theta, \theta+b, \ldots, \theta+(p-1)b.$$

Minimalni polinom elementa θ nad $\mathbb{F}_q$ je

$$\begin{aligned}\prod_{i=0}^{p-1}\big[x-(\theta+ib)\big] &= b^p\prod_{i=0}^{p-1}\Big(\frac{x-\theta}{b}-i\Big)\\ &= b^p\left[\left(\frac{x-\theta}{b}\right)^p - \frac{x-\theta}{b}\right]\\ &= x^p - b^{p-1}x + \theta(b^{p-1}-\theta^{p-1}).\end{aligned}$$

Zato je nerazcepen faktor polinoma $x^q-(x+b)$ oblike

$$x^p - b^{p-1}x - \beta, \quad \text{kjer je} \quad \beta \in \mathbb{F}_q. \tag{5.8}$$

Naj bo γ koren polinoma (5.8) v neki razširitvi obsega $\mathbb{F}_q$. Potem velja

$$\left(\frac{\gamma}{b}\right)^{p^i} - \left(\frac{\gamma}{b}\right)^{p^{i-1}} = \left(\frac{\beta}{b^p}\right)^{p^{i-1}} \text{ za } i \in \{1, \ldots, m\}, \tag{5.9}$$

kjer je $q = p^m$. Če seštejemo po i vse izraze v enakosti (5.9), dobimo

$$\gamma^{p^m} - \gamma = b\mathrm{Tr}_{q|p}(\beta/b^p).$$

Sledi, da polinom (5.8) deli polinom $F(x) = x^{p^m} - x - b$ natanko tedaj, ko je $\mathrm{Tr}_{q|p}(\beta/b^p) = 1$. V obsegu $\mathbb{F}_q$ pa je ravno $q/p = p^{m-1}$ elementov β s sledjo enako 1. □

V splošnem lahko faktorizacijo polinoma $F(x)$ zreduciramo na faktorizacijo enega od polinomov

$$x^q - x - 1, \; x^{q-1} - \xi \;\text{ ali }\; x^{q+1} - \xi.$$

Naj bo funkcija

$$\varphi = h^{-1}\psi h$$

kot v lemah 5.1.1 in 5.1.2. Za vsak koren θ polinoma $F(x)$, ki ni fiksna točka funkcije φ, velja

$$h(\theta^q) = \psi(h(\theta)). \tag{5.10}$$

Če je Δ kvadrat v $\mathbb{F}_q$, potem je

$$h(\theta^q) = (h(\theta))^q.$$

Torej je $\eta = h(\theta)$ koren polinoma $x^q - x - 1$ ali $x^q - \xi x = x(x^{q-1} - \xi)$, glede na $\psi(x)$, ki je ali $x + 1$ ali pa ξx, $\xi \in \mathbb{F}_q$. Tako lahko s faktorizacijo polinoma

$$x^q - x - 1 \;\text{ ali }\; x^{q-1} - \xi$$

kot v izrekih 5.2.1 in 5.2.2 dobimo faktorizacijo polinoma $F(x)$. Kako, nam povedo naslednji izreki, glej Gao [6, poglavje 5].

Izrek 5.2.3. *Za $a, b \in \mathbb{F}_q$, kjer je $a \neq 0, 1$ je naslednja faktorizacija nad $\mathbb{F}_q$ popolna:*

$$x^q - (ax + b) = \left(x - \frac{b}{a-1}\right) \prod_{j=1}^{(q-1)/t} \left[\left(x - \frac{b}{a-1}\right)^t - \beta_j\right],$$

kjer je t multiplikativni red a in so elementi β_j vsi različni koreni polinoma

$$x^{(q-1)/t} - a.$$

□

Izrek 5.2.4. *Za $a, b, c, d \in \mathbb{F}_q$, kjer je $c \neq 0$, $ad - bc \neq 0$ in $\Delta = (a-d)^2 + 4bc = 0$, je naslednja faktorizacija nad $\mathbb{F}_q$ popolna:*

$$(cx+d)x^q - (ax+b) = (x-x_0)\prod_{j=1}^{q/p}[(x-x_0)^p + \frac{1}{\beta_j}(a/c - x_0)(x-x_0)^{p-1} - \frac{1}{\beta_j}(a/c-x_0)^p],$$

kjer je $x_0 \in \mathbb{F}_q$ rešitev enačbe (5.1) in so β_j vsi različni elementi obsega $\mathbb{F}_q$ s sledjo

$$\mathrm{Tr}_{q|p}(\beta_j) = 1.$$

□

Izrek 5.2.5. *Za $a, b, c, d \in \mathbb{F}_q$, kjer je $c \neq 0$, $ad - bc \neq 0$ in $\Delta = (a-d)^2 + 4bc \neq 0$ kvadrat v $\mathbb{F}_q$, je naslednja faktorizacija nad $\mathbb{F}_q$ popolna:*

$$(cx+d)x^q - (ax+b) = (x-x_0)(x-x_1)\prod_{j=1}^{(q-1)/t}\frac{1}{1-\beta_j}\Big[(x-x_0)^t - \beta_j(x-x_1)^t\Big],$$

kjer sta $x_0, x_1 \in \mathbb{F}_q$ dva različna korena enačbe (5.1), t je multiplikativni red elementa

$$\xi = (a - cx_0)/(a - cx_1)$$

in so elementi β_j vsi različni koreni polinoma

$$x^{(q-1)/t} - \xi$$

v $\mathbb{F}_q$. □

Če $\Delta = (a-d)^2 + 4bc$ ni kvadrat v $\mathbb{F}_q$, je situacija malo bolj kompliciran, tako kot v primeru, ko $x_0, x_1, \xi \notin \mathbb{F}_q$. Iz $x_0^q = x_1$ in $x_1^q = x_0$ sledi

$$h(\theta^q) = (1/h(\theta))^q.$$

Potem enačba (5.10) implicira, da je $\eta = 1/h(\theta)$ koren polinoma $x^{q+1} - \xi$. Tako lahko s faktorizacijo polinoma $x^{q+1} - \xi$ nad $\mathbb{F}_{q^2}$ dobimo faktorizacijo polinoma $F(x)$ nad $\mathbb{F}_{q^2}$. Kako pridemo do faktorizacije $F(x)$ nad $\mathbb{F}_q$, nam pove naslednji izrek.

Izrek 5.2.6. *Za $a, b, c, d \in \mathbb{F}_q$, kjer je $c \neq 0$, $ad - bc \neq 0$ in $\Delta = (a-d)^2 + 4bc \neq 0$ nekvadrat v $\mathbb{F}_q$, je naslednja faktorizacija nad $\mathbb{F}_q$ popolna:*

$$(cx+d)x^q - (ax+b) = \prod_{j=1}^{(q+1)/t}\frac{1}{1-\beta_j}[(x-x_0)^t - \beta_j(x-x_1)^t], \tag{5.11}$$

kjer sta $x_0, x_1 \in \mathbb{F}_{q^2}$ *dva različna korena enačbe (5.1),* t *je multiplikativni red elementa*

$$\xi = (a - cx_1)/(a - cx_0)$$

in so β_j *vsi različni koreni polinoma*

$$x^{(q+1)/t} - \xi$$

v $\mathbb{F}_{q^2}$. □

Naj bo $f(x)$ katerikoli nelinearen nerazcepen faktor polinoma $F(x)$ stopnje t in naj bo α koren $f(x)$. Potem so $\varphi^i(\alpha)$ za vse $i \in \{0, 1, \ldots, t-1\}$ koreni $f(x)$ in so po izreku 5.1.5 linearno neodvisni nad $\mathbb{F}_q$, če je $\mathrm{Tr}(\alpha) \neq 0$. Ampak $\mathrm{Tr}(\alpha)$ je le nasprotni element koeficienta pri x^{t-1} v $f(x)$.

Izrek 5.2.7. *Naj bo*

$$F(x) = (cx + d)x^q - (ax + b)$$

polinom, kjer so $a, b, c, d \in \mathbb{F}_q$, $c \neq 0$ *in* $ad - bc \neq 0$. *Potem ima moničen nelinearen nerazcepen faktor* $f(x)$ *stopnje* t *v* $F(x)$ *linearno neodvisne korene nad* $\mathbb{F}_q$, *če in samo če je koeficient pri* x^{t-1} *v* $f(x)$ *enak 0. To se zgodi le v primeru, ko je* $\Delta = (a-d)^2 + 4bc \neq 0$ *in je* $f(x)$ *oblike*

$$\frac{1}{x_1 - x_0}[x_1(x - x_0)^t - x_0(x - x_1)^t],$$

kjer sta x_0 *in* x_1 *rešitvi enačbe (5.1).*

□

Od tod vidimo, da ima vsak nelinearen nerazcepen faktor polinoma $F(x)$ linearno neodvisne korene, razen morda enega.

5.3 Konstrukcija

Izrek 5.2.7 nam pokaže, da v primeru, ko je $c \neq 0$, koreni nerazcepnega nelinearnega faktorja polinoma $F(x)$ tvorijo normalno bazo nad $\mathbb{F}_q$ (razen morda enega). V tem razdelku si bomo ogledali lastnosti teh baz. Pokazali bomo, kako konstruirati normalno bazo obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$, ki ima kompleksnost največ $3n - 2$, za $n = p$ in za vsak n, ki deli $q - 1$. Najprej bomo izračunali multiplikacijsko matriko za normalne baze, sestavljene iz korenov nerazcepnega faktorja polinoma $F(x)$.

Brez izgube splošnosti lahko predpostavimo, da je polinom

$$F(x) = x^{q+1} + dx^q - ax - b,$$

kjer so $a, b, d \in \mathbb{F}_q$ in je $b \neq ad$. Naj bo funkcija

$$\varphi(x) = (ax + b)/(x + d)$$

reda n in potem po lemi 5.1.3 velja

$$\varphi^i(x) = (e_i x + b)/(x - e_{n-i}),$$

kjer je $e_i = \varphi^{i-1}(a)$ za vsak $i \in \{1, \ldots, n-1\}$. Naj bo $f(x)$ katerikoli nelinearen nerazcepen faktor polinoma $F(x)$ in α koren $f(x)$. Potem je $f(x)$ stopnje n in njegovi koreni

$$\alpha_i = \alpha^{q^i} = \varphi^i(\alpha) \text{ za } i \in \{0, 1, \ldots, n-1\}$$

tvorijo normalno bazo obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$, če je koeficient pri x^{n-1} v $f(x)$ različen od 0 (ali $\mathrm{Tr}(\alpha) \neq 0$), po izreku 5.2.7.

Izrek 5.3.1. *Naj bo polinom*

$$F(x) = x^{q+1} + dx^q - ax - b,$$

kjer so $a, b, d \in \mathbb{F}_q$ in je $b \neq ad$. Naj bo $f(x)$ nerazcepen faktor polinoma $F(x)$ stopnje $n > 1$ in naj bo α njegov koren. Potem so

$$\alpha_i = \alpha^{q^i} = \varphi^i(\alpha) \quad za \quad i \in \{0, 1, \ldots, n-1\} \tag{5.12}$$

vsi koreni faktorja $f(x)$, kjer je φ linearna ulomljena funkcija

$$\varphi(x) = (ax + b)/(x + d).$$

Če je $\tau = \sum_{i=0}^{n-1} \alpha_i$, negativ koeficienta pri x^{n-1} v $f(x)$, različen od 0, potem elementi (5.12) tvorijo tako normalno bazo obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$, da velja

$$\alpha_0 \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} = \begin{pmatrix} \tau^* & -e_{n-1} & -e_{n-2} & \ldots & -e_1 \\ e_1 & e_{n-1} & & & \\ e_2 & & e_{n-2} & & \\ \vdots & & & \ddots & \\ e_{n-1} & & & & e_1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} + \begin{pmatrix} b^* \\ b \\ b \\ \vdots \\ b \end{pmatrix}, \tag{5.13}$$

kjer je $e_1 = a$, $e_{i+1} = \varphi(e_i)$ *za* $i \geq 1$, $b^* = -b(n-1)$ *in* $\tau^* = \tau - \varepsilon$ *za*

$$\varepsilon = \sum_{i=1}^{n-1} e_i = \begin{cases} (n-1)(a-d)/2, & \text{če je } p \neq 2, \\ a = d, & \text{če je } p = n = 2, \\ a - d, & \text{če je } p = 2 \text{ in } n \equiv 3 \mod 4, \\ 0, & \text{če je } p = 2 \text{ in } n \equiv 1 \mod 4. \end{cases}$$

Dokaz. Dokazati moramo le (5.13). Po lemi 5.1.3 za $i \geq 1$ velja

$$\alpha_i = \varphi^i(\alpha) = \frac{e_i\alpha_0 + b}{\alpha_0 - e_{n-i}}.$$

Torej je

$$\alpha_0\alpha_i = e_i\alpha_0 + e_{n-i}\alpha_i + b.$$

Za $i = 0$ velja

$$\alpha_0\alpha_0 = \alpha_0\left(\tau - \sum_{j=1}^{n-1}\alpha_j\right) = \left(\tau - \sum_{j=1}^{n-1} e_j\right)\alpha_0 - \sum_{j=1}^{n-1} e_{n-j}\alpha_j - b(n-1).$$

Izrek sledi po lemi 5.1.4. □

Naslednji izrek nam poda karakterizacijo normalnih baz takšnega tipa.

Izrek 5.3.2. *Naj bo* $n > 2$. *Predpostavimo, da je množica* $\{\alpha, \alpha^q, \ldots, \alpha_{n-1}\}$ *normalna baza obsega* $\mathbb{F}_{q^n}$ *nad* $\mathbb{F}_q$, *ki za* $i \neq j$ *zadošča pogoju*

$$\alpha_i\alpha_j = a_{ij}\alpha_i + b_{ij}\alpha_j + \gamma_{ij} \quad \text{za vse} \quad i, j \in \{0, 1, \ldots, n-1\}, \tag{5.14}$$

kjer so $a_{ij}, b_{ij}, \gamma_{ij} \in \mathbb{F}_q$. *Potem obstajajo take konstante* $\gamma, e_1, \ldots, e_{n-1} \in \mathbb{F}_q$, *da velja*

(i) $e_i = \varphi(e_{i-1})$ *za vsak* $i \in \{2, \ldots, n-1\}$ *in*

$$a_{ij} = e_{j-i},\ b_{ij} = e_{i-j},\ \gamma_{ij} = \gamma \quad \text{za } i \neq j,$$

kjer je φ *linearna ulomljena funkcija*

$$\varphi(x) = (e_1x + \gamma)/(x - e_{n-1})$$

in se indeksi pri koeficientih e_i *računajo po modulu* n;

(ii) minimalni polinom elementa α *je faktor polinoma*

$$F(x) = x^{q+1} - e_{n-1}x^q - (e_1x + \gamma)$$

in n *mora biti potemtakem faktor enega od števil* p, $q-1$ *ali* $q+1$.

Dokaz. Naj bo $e_k = a_{0k}$ in $\gamma_k = \gamma_{0k}$ za vsak $k \in \{1, 2, \ldots, n-1\}$. Potem je

$$\alpha_0\alpha_k = e_k\alpha_0 + b_{0k}\alpha_k + \gamma_k. \tag{5.15}$$

Sedaj enačbo (5.15) dvignemo na q^{n-k}-to potenco na obeh straneh in dobimo

$$\alpha_0\alpha_{n-k} = b_{0k}\alpha_0 + e_k\alpha_{n-k} + \gamma_k. \tag{5.16}$$

Če odštejemo enačbo (5.16) od enačbe (5.15), kjer v (5.15) k zamenjamo z $n-k$, dobimo

$$(e_{n-k} - b_{0k})\alpha_0 + (b_{0n-k} - e_k)\alpha_{n-k} + \gamma_{n-k} - \gamma_k = 0. \tag{5.17}$$

Ker je $n > 2$ in so elementi α_i linearno neodvisni nad obsegom $\mathbb{F}_q$, enačba (5.17) implicira, da velja

$$b_{0k} = e_{n-k} \text{ in } \gamma_k = \gamma_{n-k} \text{ za vsak } k \in \{1, \ldots, n-1\}.$$

Od tod sledi

$$\alpha_0\alpha_k = e_k\alpha_0 + e_{n-k}\alpha_k + \gamma_k \text{ za vsak } k \in \{1, \ldots, n-1\}. \tag{5.18}$$

Zdaj pa za vsak $i \neq j$ enačbo (5.18) dvignemo na q^i-to potenco, pišemo $k = j - i$ in dobimo

$$\alpha_i\alpha_j = e_{j-i}\alpha_i + e_{i-j}\alpha_j + \gamma_{j-i}. \tag{5.19}$$

Primerjava izrazov (5.14) in (5.19) nam da naslednje enakosti

$$a_{ij} = e_{j-i}, \quad b_{ij} = e_{i-j} \text{ in } \gamma_{ij} = \gamma_{j-i}, \tag{5.20}$$

s čimer smo dokazali prvi del točke (i) izreka 5.3.2.

Zapišimo poseben primer enačbe (5.19):

$$\alpha_i\alpha_{i+1} = e_{n-1}\alpha_{i+1} + e_1\alpha_i + \gamma_1 \text{ za vsak } i \in \{0, 1, \ldots, n-2\}$$

ali

$$\alpha_{i+1} = \frac{e_1\alpha_i + \gamma_1}{\alpha_i - e_{n-1}} = \varphi(\alpha_i) \text{ za vsak } i \in \{0, 1, \ldots, n-2\}, \tag{5.21}$$

kjer je funkcija

$$\varphi(x) = (e_1x + \gamma)/(x - e_{n-1})$$

in $\gamma = \gamma_1$. Z indukcijo po številu i dobimo

$$\alpha_i = \varphi^i(\alpha_0) = \varphi^i(\alpha) \text{ za vsak } i \in \{0, \ldots, n-1\}.$$

Po lemi 5.1.3 vemo, da je

$$\varphi^i(x) = (a_i x + \gamma)/(x - a_{n-i}) \text{ za vsak } i \in \{0, \ldots, n-1\},$$

kjer je $a_i = \varphi(a_{i-1})$ za $i \geq 1$ in $a_1 = e_1$. Potem enakost (5.21) implicira, da je

$$\alpha_i = \frac{a_i \alpha_0 + \gamma}{\alpha_0 - a_{n-i}},$$

torej je

$$\alpha_0 \alpha_i = a_i \alpha_0 + a_{n-i} \alpha_i + \gamma. \tag{5.22}$$

S primerjavo enačb (5.22) in (5.18) dobimo

$$e_i = a_i, \ e_{n-i} = a_{n-i} \text{ in } \gamma_i = \gamma.$$

Dokazali smo točko (i) izreka. Za točko (ii) upoštevamo, da je element $\alpha_1 = \alpha^q$ in da izraz (5.18) za $k = 1$ pomeni, da je element α koren polinoma

$$F(x) = x^{q+1} - e_{n-1} x^q - e_1 x - \gamma.$$

Torej minimalni polinom elementa α deli polinom $F(x)$. S tem je izrek dokazan. □

Izrek 5.3.3. *Za vsak $\alpha, \beta \in \mathbb{F}_q^*$ s sledjo $\mathrm{Tr}_{q|p}(\beta) = 1$, je polinom*

$$x^p - \frac{1}{\beta} a x^{p-1} - \frac{1}{\beta} a^p \tag{5.23}$$

nerazcepen nad $\mathbb{F}_q$ in njegovi koreni tvorijo normalno bazo obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ s kompleksnostjo največ $3p - 2$. Multiplikacijska matrika je oblike

$$\begin{pmatrix} \tau^* & -e_{p-1} & -e_{p-2} & \ldots & -e_1 \\ e_1 & e_{p-1} & & & \\ e_2 & & e_{p-2} & & \\ \vdots & & & \ddots & \\ e_{p-1} & & & & e_1 \end{pmatrix}, \tag{5.24}$$

kjer je $e_1 = a$, $e_{i+1} = \varphi(e_i)$ za $i \geq 1$, funkcija $\varphi(x) = ax/(x + a)$ in $\tau^* = \alpha/\beta$, če je praštevilo $p \neq 2$ oziroma $\alpha/\beta - a$, če je $p = 2$.

Dokaz. Naj bo $F(x) = (x + a)x^q - ax$ polinom in $\varphi(x) = ax/(x + a)$. Potem polinom $F(x)$ zadovolji pogoje izreka 5.2.4 z naslednjimi vrednostmi: $b = 0$, $c = 1$, $d = a$, $\Delta = 0$

in $x_0 = 0$. Torej je polinom (5.23) nerazcepen faktor polinoma $F(x)$. Ker je koeficient pri x^{p-1} v polinomu (5.23) enak $-\alpha/\beta \neq 0$, po izreku 5.3.1 koreni polinoma (5.23) tvorijo normalno bazo in njena multiplikacijska matrika je enaka matriki (5.24). Njena kompleksnost je očitno največ $3p - 2$. □

Izrek 5.3.4. *Naj bo n faktor števila $q-1$. Naj bo $\beta \in \mathbb{F}_q$ multiplikativnega reda t, tako da velja $\gcd(n, (q-1)/t) = 1$ in naj bo $a = \beta^{(q-1)/n}$. Potem je polinom*

$$x^n - \beta(x - a + 1)^n \tag{5.25}$$

nerazcepen nad obsegom $\mathbb{F}_q$ in njegovi koreni tvorijo normalno bazo obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ s kompleksnostjo največ $3n - 2$. Multiplikacijska matrika je enaka

$$\begin{pmatrix} \tau^* & -e_{n-1} & -e_{n-2} & \dots & -e_1 \\ e_1 & e_{n-1} & & & \\ e_2 & & e_{n-2} & & \\ \vdots & & & \ddots & \\ e_{n-1} & & & & e_1 \end{pmatrix}, \tag{5.26}$$

kjer je $e_1 = a$, $e_{i+1} = \varphi(e_i)$ za $i \geq 1$, funkcija $\varphi(x) = ax/(x + a)$ in

$$\tau^* = -n(a-1)\beta/(1-\beta) - \varepsilon,$$

kjer je ε enak kot v izreku 5.3.1 (za d=1).

Dokaz. Ni težko videti, da je a multiplikativnega reda n. Potem ima linearna ulomljena funkcija $\varphi(x) = ax/(x + a)$ fiksni točki $x_0 = 0$ in $x_1 = a - 1$, funkcija

$$\xi(x) = (a - x_0)/(a - x_1) = a$$

pa je reda n. Tudi funkcija $\varphi(x)$ je reda n. Element β je koren polinoma

$$x^{(q-1)/n} - a.$$

Po izreku 5.2.5 je polinom (5.25) nerazcepen faktor polinoma

$$F(x) = x^{q+1} + x^q - ax.$$

Koeficient pri x^{n-1} v polinomu (5.25) je $n(a-1) \neq 0$. Po izreku 5.3.1 (za $b = 0$ in $d = 1$) koreni polinoma (5.25) tvorijo normalno bazo obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ z multiplikacijsko matriko

(5.26), katere kompleksnost je očitno največ $3n - 2$. □

Naslednja tabela je rezultat računalniškega iskanja minimalne kompleksnosti normalne baze, glej Gao [6, poglavje 5]. Izkaže se, da je v primeru, ko število n deli $q-1$, minimalna kompleksnost pogosto enaka $3n - 3$ ali $3n - 2$. Normalne baze, ki jih skonstruiramo s pomočjo zadnjih dveh izrekov, imajo pogosto kompleksnost blizu minimalne kompleksnosti. V naslednji tabeli z znakom ♯ označimo, da je pripadajoča minimalna kompleksnost $3n-2$, znak ♮ pa nam označuje optimalno kompleksnost, torej $2n - 1$. Ostale vrednosti so oblike $3n - 3$.

q	5	7	7	11	11	13	13	17	19
n	4	3	6	5	10	3	4	4	3
min	9	6	16♯	12	28♯	6	7♮	7♮	6

Tabela 5.1: Minimalna kompleksnost normalne baze obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$.

Poglavje 6

SEBIDUALNE NORMALNE BAZE

Pomembna poddružina normalnih baz so sebidualne normalne baze. V tem poglavju si bomo najprej ogledali, kaj so dualne in sebidualne baze ter podali nekaj osnovnih trditev o njihovem obstoju in obliki. V drugem razdelku pa bomo skonstruirali sebidualne normalne baze končnega obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ v primerih, ko je

- n enak karakteristiki obsega $\mathbb{F}_q$,
- n lih faktor števila $q-1$ ali
- n lih faktor števila $q+1$.

Glavna referenca za to poglavje je Gao [6].

6.1 Osnove

Za začetek poglejmo, kaj sploh predstavlja pojem dualna baza. Predpostavimo, da imamo dve bazi končnega obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$, $\overline{\alpha} = \{\alpha_0, \ldots, \alpha_{n-1}\}$ in $\overline{\beta} = \{\beta_0, \ldots, \beta_{n-1}\}$. Potem je $\overline{\beta}$ **dualna baza** baze $\overline{\alpha}$, če velja

$$\mathrm{Tr}(\alpha_i \beta_j) = \delta_{ij} \quad \text{za vse} \quad i, j \in \{0, \ldots, n-1\},$$

kjer δ_{ij} označuje *Kroneckerjevo delta funkcijo*, torej $\delta_{ij} = 0$ za $i \neq j$ in $\delta_{ij} = 1$ za $i = j$. Naslednji izrek zagotovi obstoj in enoličnost dualne baze.

Izrek 6.1.1. *Za vsako bazo obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ obstaja enolično definirana dualna baza.*

Dokaz. Naj bosta $\overline{\alpha} = \{\alpha_0, \ldots, \alpha_{n-1}\}$ in $\overline{\beta} = \{\beta_0, \ldots, \beta_{n-1}\}$ bazi obsega $\mathbb{F}_{q^n}$. Za element $\theta \in \mathbb{F}_{q^n}$ naj bo

$$\theta = \sum_{i=0}^{n-1} c_i(\theta)\alpha_i$$

enolična reprezentacija glede na bazo $\overline{\alpha}$. Preslikava c_i je linearen funkcional iz $\mathbb{F}_{q^n}$ v $\mathbb{F}_q$, zato obstajajo elementi $\beta_i \in \mathbb{F}_{q^n}$, tako da velja

$$c_i(\theta) = \mathrm{Tr}(\beta_i\theta) \text{ za vsak } i \in \{0, \ldots, n-1\}.$$

Torej je

$$\theta = \sum_{i=0}^{n-1} \mathrm{Tr}(\beta_i\theta)\alpha_i$$

za vsak $\theta \in \mathbb{F}_{q^n}$. V primeru, ko je element $\theta = \alpha_j$, velja

$$\alpha_j = \sum_{i=0}^{n-1} \mathrm{Tr}(\beta_i\alpha_j)\alpha_i,$$

od koder sledi

$$\mathrm{Tr}(\beta_i\alpha_j) = \delta_{ij}.$$

Če je

$$\sum_{i=0}^{n-1} d_i\beta_i = 0$$

za $d_i \in \mathbb{F}_q$, potem je

$$(\sum_{i=0}^{n-1} d_i\beta_i)\alpha_j = 0 \text{ in } \mathrm{Tr}(\sum_{i=0}^{n-1} d_i\beta_i\alpha_j) = 0.$$

Torej iz

$$\sum_{i=0}^{n-1} d_i\mathrm{Tr}(\beta_i\alpha_j) = 0$$

sledi $d_j = 0$ za vsak $j \in \{0, \ldots, n-1\}$. Potem je $\overline{\beta} = \{\beta_0, \ldots, \beta_{n-1}\}$ dualna baza baze $\overline{\alpha} = \{\alpha_0, \ldots, \alpha_{n-1}\}$ in je enolično definirana. □

Naslednja trditev je pomembna, da lahko sploh definiramo sebidualne normalne baze, kajti pove nam, da je dualna baza normalne baze prav tako normalna.

Trditev 6.1.2. *Dualna baza normalne baze je normalna baza.*

Dokaz. Naj bo $\overline{\alpha} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ normalna baza obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ in $\overline{\beta} = \{\beta_0, \ldots, \beta_{n-1}\}$ njena dualna baza. Potem velja

$$AB = \begin{pmatrix} \alpha & \alpha^q & \cdots & \alpha^{q^{n-1}} \\ \alpha^q & \alpha^{q^2} & \cdots & \alpha \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{q^{n-1}} & \alpha & \cdots & \alpha^{q^{n-2}} \end{pmatrix} \begin{pmatrix} \beta_0 & \beta_1 & \cdots & \beta_{n-1} \\ \beta_0^q & \beta_1^q & \cdots & \beta_{n-1}^q \\ \vdots & \vdots & \ddots & \vdots \\ \beta_0^{q^{n-1}} & \beta_1^{q^{n-1}} & \cdots & \beta_{n-1}^{q^{n-1}} \end{pmatrix} = I_n$$

in tudi $BA = I_n$. Sledi

$$(AB)^T = B^T A^T = B^T A = I_n,$$

ker je A simetrična matrika. Ker velja

$$BA = I_n = B^T A,$$

lahko zaključimo, da je tudi B simetrična matrika, torej $B = B^T$. Sledi, da je $\beta_i = \beta_0^{q^{i-1}}$ in je torej tudi $\overline{\beta}$ normalna baza. □

Naslednji izrek poda metodo, s katero dobimo dualno bazo normalne baze, ki je po trditvi 6.1.2 prav tako normalna.

Izrek 6.1.3. *Naj bo $N = \{\alpha_0, \ldots, \alpha_{n-1}\}$ normalna baza obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$. Naj bosta $t_i = \mathrm{Tr}_{q^n \mid q}(\alpha_0 \alpha_i)$ in $N(x) = \sum_{i=0}^{n-1} t_i x^i$. Nadalje naj bo polinom*

$$D(x) = \sum_{i=0}^{n-1} d_i x^i, \quad \textit{kjer so} \quad d_i \in \mathbb{F}_q,$$

enolično določen, in sicer tak, da velja

$$N(x)D(x) \equiv 1 \bmod x^n - 1.$$

Potem je dualna baza baze N generirana z elementom

$$\beta = \sum_{i=0}^{n-1} d_i \alpha_i.$$

Dokaz. Oglejmo si produkt

$$N(x)D(x) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} t_i d_j x^{i+j} = \sum_{i=0}^{n-1} \sum_{k=0}^{n-1} d_k t_{i-k} x^i \bmod x^n - 1.$$

Iz $N(x)D(x) \equiv 1 \bmod x^n - 1$ sledi

$$\sum_{k=0}^{n-1} d_k t_{i-k} = \begin{cases} 1, & \text{če } i = 0, \\ 0, & \text{sicer.} \end{cases}$$

Potemtakem je

$$\begin{aligned} \mathrm{Tr}(\alpha_i \beta^{q^j}) &= \mathrm{Tr}\left(\alpha_i \sum_{k=0}^{n-1} d_k \alpha_{j+k}\right) = \sum_{k=0}^{n-1} d_k \mathrm{Tr}(\alpha_i \alpha_{j+k}) \\ &= \sum_{k=0}^{n-1} d_k \mathrm{Tr}(\alpha_0 \alpha_{i-j-k}) = \sum_{k=0}^{n-1} d_k t_{i-j-k} \\ &= \begin{cases} 1, & \text{če } i = j, \\ 0, & \text{sicer.} \end{cases} \end{aligned}$$

To pomeni, da je množica $\{\beta, \beta^q, \ldots, \beta^{q^{n-1}}\}$ dualna baza baze N. □

Izrek 6.1.4. *Naj bosta N in $D(x)$ taka, kot v izreku 6.1.3. Naj bo*

$$\gamma = \sum_{i=0}^{n-1} a_i \alpha_i,$$

kjer so $a_i \in \mathbb{F}_q$ za vse $i \in \{0, 1, \ldots, n-1\}$, normalen element obsega $\mathbb{F}_{q^n}$ in naj bo

$$\delta(x) = \sum_{i=0}^{n-1} b_i x^i$$

enolično določen polinom, tako da velja

$$\gamma(x)\delta(x) \equiv 1 \mod x^n - 1,$$

kjer je $\gamma(x) = \sum_{i=0}^{n-1} a_i x^i$. Koeficienti c_i so definirani z naslednjo vsoto

$$c_i = \sum_{k=0}^{n-1} b_k d_{i+k} \quad za \quad i \in \{0, 1, \ldots, n-1\}.$$

Potem element

$$\delta = \sum_{i=0}^{n-1} c_i \alpha_i$$

generira dualno bazo normalne baze, generirane z elementom γ.

Dokaz. Naj bo množica $\{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$ dualna baza baze N. Potem podobno kot v dokazu izreka 6.1.3 vidimo, da element

$$\delta = \sum_{i=0}^{n-1} b_{-i}\beta_i \tag{6.1}$$

generira dualno bazo normalne baze, generirane z elementom γ. Po izreku 6.1.3 je

$$\beta = \sum_{i=0}^{n-1} d_i\alpha_i,$$

kar vstavimo v enakost (6.1) in izrek sledi. □

Poseben primer dualnih baz so sebidualne baze. Najprej definiramo koncept, povezan s sebidualnostjo, potem pa še sebidualne baze. Baza $\overline{\alpha} = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ je **ortogonalna glede na sled**, če velja $\mathrm{Tr}(\alpha_i\alpha_j) = 0$ za vsak $i \neq j$. Če velja še $\mathrm{Tr}(\alpha_i^2) = 1$ za $i \in \{0, 1, \ldots, n-1\}$, je baza $\overline{\alpha}$ **sebidualna**. Sebidualna baza je torej baza, ki je enaka svoji dualni bazi. Nas bodo zanimale le sebidualne normalne baze, torej take normalne baze, ki so enake svoji dualni bazi. Vemo, da za vsak končen obseg obstaja normalna baza. Sebidualne normalne baze pa ne obstajajo kar v vseh končnih obsegih. Lempel in Weinberger [12] sta pokazala, kakšni morata biti naravni števili n in q, da obstaja sebidualna normalna baza obsega $\mathbb{F}_{q^n}$.

Izrek 6.1.5. *V obsegu $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ obstaja sebidualna normalna baza, če je n liho število ali če je q sodo število in je $n \equiv 2 \bmod 4$.* □

6.2 Konstrukcija

V tem razdelku bomo konstruirali sebidualne normalne baze končnega obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ v primerih, ko je naravno število n enako karakteristiki obsega $\mathbb{F}_q$ ali pa je n lih faktor enega od števil $q-1$ ali $q+1$. Za začetek pa poglejmo dualno bazo normalne baze, definirane v prejšnjem poglavju.

Izrek 6.2.1. *Naj bo $N = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$, kjer je $\alpha_i = \alpha^{q^i}$, normalna baza obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$, ki zadošča pogoju*

$$\alpha_i\alpha_j = e_{j-i}\alpha_i + e_{i-j}\alpha_j + \gamma \quad za \quad i \neq j,$$

kjer so $e_1, e_2, \ldots, e_{n-1}, \gamma \in \mathbb{F}_q$. *Naj bo* $\tau = \mathrm{Tr}_{q^n|q}(\alpha)$ *in* $\lambda = -(e_1 + e_{n-1}) - n\gamma/\tau$. *Potem je*

$$\left\{ \frac{1}{\tau(\tau + n\lambda)}(\alpha_i + \lambda) \mid i \in \{0, 1, \ldots, n-1\} \right\}$$

dualna baza baze N.

Dokaz. Za $i \neq j$ velja

$$\begin{aligned} \mathrm{Tr}_{q^n|q}(\alpha_i(\alpha_j + \lambda)) &= \mathrm{Tr}_{q^n|q}(\lambda\alpha_i + e_{j-i}\alpha_i + e_{i-j}\alpha_j + \gamma) \\ &= \lambda\tau + e_{j-i}\tau + e_{i-j}\tau + n\gamma \\ &= \tau(\lambda + e_1 + e_{n-1}) + n\gamma \\ &= 0 \end{aligned}$$

in

$$\begin{aligned} \mathrm{Tr}_{q^n|q}(\alpha_i(\alpha_i + \lambda)) &= \mathrm{Tr}_{q^n|q}(\alpha_i(\tau + \lambda - \sum_{j \neq i} \alpha_j)) \\ &= \mathrm{Tr}_{q^n|q}(\alpha_i(\tau + n\lambda - \sum_{j \neq i} (\alpha_j + \lambda))) \\ &= \mathrm{Tr}_{q^n|q}(\alpha_i)(\tau + n\lambda) - \sum_{j \neq i} \mathrm{Tr}_{q^n|q}(\alpha_i(\alpha_j + \lambda)) \\ &= \tau(\tau + n\lambda). \end{aligned}$$

S tem je izrek dokazan. □

Zdaj pa poglejmo, kdaj koreni nerazcepnega faktorja polinoma

$$F(x) = x^{q+1} + dx^q - ax - b$$

tvorijo sebidualno normalno bazo. Naj bo $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ normalna baza, generirana s korenom α polinoma $F(x)$, kjer je $\alpha_i = \alpha^{q^i}$ in naj bo $\tau = \mathrm{Tr}_{q^n|q}(\alpha)$. Po izreku 5.3.1 in lemi 5.1.3 sledi, da za $i \neq 0$ velja

$$\begin{aligned} \mathrm{Tr}_{q^n|q}(\alpha_0\alpha_i) &= e_i \mathrm{Tr}(\alpha_0) + e_{n-i}\mathrm{Tr}(\alpha_i) + nb \\ &= \tau(e_i + e_{n-i}) + nb \\ &= \tau(a - d) + nb \end{aligned} \tag{6.2}$$

in

$$\begin{aligned} \mathrm{Tr}_{q^n|q}(\alpha_0\alpha_0) &= \tau(\tau - \varepsilon) - \tau\varepsilon - nb(n-1) \\ &= \begin{cases} \tau^2, & \text{če } p = 2 \\ \tau^2 - (n-1)(\tau(a-d) + nb), & \text{če } p \neq 2. \end{cases} \end{aligned} \tag{6.3}$$

Torej α generira sebidualno normalno bazo, če je $\tau = \mathrm{Tr}(\alpha) = 1$ in $(a-d)+nb = 0$. S preučevanjem nerazcepnih faktorjev v izrekih 5.2.4, 5.2.5 in 5.2.6 ugotovimo, da lahko zadostimo tema dvema pogojema. Rezultat sledi v naslednjih treh izrekih.

Izrek 6.2.2. *Za vsak $\beta \in \mathbb{F}_q^*$, za katerega velja $\mathrm{Tr}_{q|p}(\beta) = 1$, je polinom*

$$x^p - x^{p-1} - \beta^{p-1} \tag{6.4}$$

nerazcepen nad obsegom $\mathbb{F}_q$ in njegovi koreni tvorijo sebidualno normalno bazo obsega $\mathbb{F}_{q^p}$ nad $\mathbb{F}_q$ s kompleksnostjo največ $3p-2$. Multiplikacijska matrika je enaka matriki (5.24), torej je oblike

$$\begin{pmatrix} \tau^* & -e_{p-1} & -e_{p-2} & \dots & -e_1 \\ e_1 & e_{p-1} & & & \\ e_2 & & e_{p-2} & & \\ \vdots & & & \ddots & \\ e_{p-1} & & & & e_1 \end{pmatrix},$$

kjer je $e_1 = \beta$, $e_{i+1} = \varphi(e_i)$ za $i \geq 1$, funkcija

$$\varphi(x) = \beta x/(x+\beta)$$

in $\tau^* = 1$, če je praštevilo $p \neq 2$ in $\tau^* = 1-\beta$, če je $p = 2$.

Dokaz. Naj bo polinom $F(x) = (x+\beta)x^q - \beta x$. Potem je po izreku 5.2.4 polinom (6.4) nerazcepen faktor polinoma $F(x)$, kjer je $b = 0, c = 1, d = a = \beta, x_0 = 0$ in $\beta_j = \beta$. Ker je $a - d = b = 0$ in je $\tau = 1$ v izrazih (6.2) in (6.3), koreni polinoma (6.4) tvorijo sebidualno normalno bazo. Njena multiplikacijska matrika je po izreku 5.3.1 kar enaka (5.24). □

Izrek 6.2.3. *Naj bo n lih faktor števila $q-1$ in $\xi \in \mathbb{F}_q$ multiplikativnega reda n. Potem obstaja element $u \in \mathbb{F}_q$, tako da je $(u^2)^{(q-1)/n} = \xi$. Naj bo*

$$x_0 = (1+u)/n \quad in \quad x_1 = (1+u)/(nu).$$

Potem je moničen polinom

$$\frac{1}{1-u^2}\big((x-x_0)^n - u^2(x-x_1)^n\big) \tag{6.5}$$

nerazcepen nad $\mathbb{F}_q$ in njegovi koreni tvorijo sebidualno normalno bazo obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$. Multiplikacijska matrika je kar enaka (5.13), kjer je $a = (x_0 - \xi x_1)/(1-\xi)$, $b = -x_0x_1$, $d = a - (x_0 + x_1)$ in $\tau = 1$.

Dokaz. Najprej bomo dokazali, da obstaja vsaj en koren $x^{(q-1)/n} - \xi$, ki je kvadrat v $\mathbb{F}_q$. Naj bo ζ primitivni element v $\mathbb{F}_q$. Naj bo t tak lih faktor števila $q-1$, da $n \,|\, t$ in $\gcd(n, (q-1)/t) = 1$. Potem je

$$\zeta_0 = \zeta^{(q-1)/t}$$

t-ti primitivni koren enote. Ker je t lih, je tudi ζ_0^2 t-ti primitivni koren enote. Naj bo $d = t/n$. Potem obstaja tako število i, da velja $(\zeta_0^2)^{id} = \xi$, torej

$$(\zeta^{(q-1)/t})^{2id} = (\zeta^{2i})^{(q-1)/n} = \xi.$$

Torej je ζ^{2i} koren polinoma

$$x^{(q-1)/n} - \xi$$

in kvadrat v $\mathbb{F}_q$. Potem lahko vzamemo $u = \zeta^i$.

Po izreku 5.2.5 vidimo, da je (6.5) nerazcepen faktor polinoma $F(x) = (x+d)x^q - (ax+b)$. Negativ koeficienta pri x^{n-1} v (6.5) je

$$\tau = \frac{n(x_0 - u^2 x_1)}{1-u^2} = 1.$$

Po izreku 5.3.1 koreni (6.5) tvorijo normalno bazo obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$. Vidimo, da velja

$$a - d = x_0 + x_1 = \frac{(u+1)}{n} + \frac{u+1}{nu} = \frac{(u+1)^2}{nu} = nx_0x_1 = -nb,$$

torej $\tau(a-d) + nb = 0$. Iz enakosti(6.2) in (6.3) sledi, da koreni polinoma (6.5) tvorijo sebidualno normalno bazo. □

Izrek 6.2.4. *Naj bo n lih faktor števila $q+1$ in naj bo $\xi \in \mathbb{F}_{q^2}$ koren $x^{q+1} - 1$ multiplikativnega reda n. Potem obstaja koren u polinoma $x^{q+1} - 1$, tako da je*

$$(u^2)^{(q+1)/n} = \xi.$$

Naj bo

$$x_0 = (1+u)/n \quad in \quad x_1 = (1+u)/(nu).$$

Potem je polinom

$$\frac{1}{1-u^2}[(x-x_0)^n - u^2(x-x_1)^n] \in \mathbb{F}_q[x] \tag{6.6}$$

nerazcepen nad $\mathbb{F}_q$ in njegovi koreni tvorijo sebidualno normalno bazo obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$, katere multiplikacijska matrika je kar (5.13) z $a = (x_1 - \xi x_0)/(1-\xi)$, $b = -x_0x_1$, $d = a - (x_0 + x_1)$ in $\tau = 1$.

Dokaz. Dokaz obstoja u je podoben kot v dokazu prejšnjega izreka, s tem, da za ζ vzamemo primitivni $(q+1)$-vi koren enote v $\mathbb{F}_{q^2}$. Elementi ξ, u in u^2 so vsi $(q+1)$-vi koreni enote in imamo $\xi^q = 1/\xi$, $u^q = 1/u$ in $(u^2)^q = 1/u^2$. Torej je $x_0^q = x_1$ in $x_1^q = x_0$ in tako $a^q = a$, $b^q = b$ in $d^q = d$, kar pomeni, da so $a, b, d \in \mathbb{F}_q$. Označimo polinom (6.6) s $\phi(x)$ in računajmo

$$\begin{aligned}(\phi(x))^q &= \frac{1}{1-(u^2)^q}[(x^q - x_0^q)^n - (u^2)^q(x^q - x_1^q)^n] \\ &= \frac{1}{1-1/u^2}[(x^q - x_1)^n - 1/u^2(x^q - x_0)^n] \\ &= (\phi(x)^q). \end{aligned} \tag{6.7}$$

Tako vidimo, da so koeficienti $\phi(x)$ iz $\mathbb{F}_q$.

S pomočjo izreka 5.2.6 dokažemo, da je polinom (6.6) nerazcepen nad $\mathbb{F}_q$. Ni težko preveriti, da sta pri ustreznih koeficientih a, b, d elementa x_0 in x_1 dve različni rešitvi enačbe (5.1), kjer je $c = 1$ in $\xi = (a - x_1)/(a - x_0)$ reda n. Ker je u^2 rešitev $x^{(q+1)/q} - \xi$, iz izreka 5.2.6 sledi, da je polinom (6.6) nerazcepen faktor polinoma $F(x) = (x+d)x^q - (ax+b)$.

Ker je koeficient pri x^{n-1} v (6.6) enak

$$(-nx_0 + nu^2x_1)/(1-u^2) = -1,$$

je sled kateregakoli korena (6.6) enaka $\tau = 1$. Prav tako ni težko preveriti, da je

$$\tau(a-d) + nb = 0.$$

Iz (6.2) in (6.3) sledi, da koreni (6.6) tvorijo sebidualno normalno bazo, katere multiplikacijska matrika je (5.13), kot sledi iz izreka 5.3.1. □

Poglavje 7

PREHOD MED BAZAMI

Idealno bi bilo, če bi lahko vsako operacijo naredili v tisti bazi, v kateri jo znamo najbolj učinkovito izvajati. V standardu so podrobno opisane polinomske baze, zato moramo znati prehajati med bazami, pretvoriti elemente iz izbrane polinomske v določeno normalno bazo in obratno. Včasih želimo priti tudi iz normalne baze z enim generatorjem v normalno bazo z drugim generatorjem. Prehodu med bazami je namenjeno sledeče poglavje. Vsako bazo končnega obsega $\mathbb{F}_{q^n}$ sestavlja n elementov obsega, torej n nizov dolžine n. Ker je tak prostor vektorski prostor, je osnovni način za pretvorbo med dvema bazama kar množenje z matriko. Množenje vektorja dolžine n z matriko velikosti $n \times n$ v splošnem zahteva $\mathcal{O}(n^2)$ množenj znotraj obsega. Seveda je v določenih primerih prehodna matrika lepe oblike, ima malo neničelnih elementov. Tedaj je prehod hitrejši.

Najprej bomo pogledali, kako poiščemo ničlo nerazcepnega polinoma nad binarnim obsegom, nato prehod med bazama z matriko – kot izomorfizem med dvema končnima vektorskima prostoroma. Potem pa bomo opisali še učinkovitejši algoritem, ki bistveno zmanjša prostorsko zahtevnost prehoda med bazama.

7.1 Prehod z matriko

Baze končnega obsega lahko generiramo s polinomi, in sicer polinomsko bazo z nerazcepnim polinomom stopnje n nad $\mathbb{F}_q$, normalno bazo pa z normalnim polinomom stopnje n nad $\mathbb{F}_q$, torej takim nerazcepnim polinomom, ki ima za ničlo normalni element. V vsakem primeru moramo poiskati ničlo nerazcepnega polinoma. Kadar se nahajamo v binarnem obsegu, si pri tem lahko pomagamo z naslednjim algoritmom, glej [26, str. 103,104].

ALGORITEM 4 Iskanje ničle nerazcepnega polinoma nad binarnim obsegom.

Input: Nerazcepen polinom $f(t)$ stopnje d, in obseg $\mathbb{F}_{2^m}$, kjer d deli m.
Output: Ničla polinoma $f(t)$ v $\mathbb{F}_{2^m}$.
1. $g(t) \leftarrow f(t)$.
2. While $\deg(g) > 1$
   2.1 Izberi $u \in \mathbb{F}_{2^m}$.
   2.2 $c(t) \leftarrow ut$.
   2.3 For i from 1 to $m-1$ do
   $c(t) \leftarrow c(t)^2 + ut \mod g(t)$.
   2.4 $h(t) \leftarrow \gcd(c(t), g(t))$.
   2.5 If $h(t) = \text{const}$ or $\deg(g) = \deg(h)$ then go to 2.1.
   2.6 If $2\deg(h) > \deg(g)$ then $g(t) \leftarrow g(t)/h(t)$.
   Else $g(t) = h(t)$.
3. Return $g(0)$.

Denimo, da imamo element $\varepsilon \in \mathbb{F}_{q^n}$, predstavljen v bazi $\Omega = \{\omega_0, \ldots, \omega_{n-1}\}$ kot $b = (b_0, \ldots, b_{n-1})$, radi pa bi imeli zapis tega elementa v bazi $\Psi = \{\psi_0, \ldots, \psi_{n-1}\}$, torej tak $a = (a_0, \ldots, a_{n-1})$, da velja

$$\varepsilon = \sum_{i=0}^{n-1} a_i \psi_i = \sum_{i=0}^{n-1} b_i \omega_i.$$

Iščemo torej prehodno matriko $S : \Omega \to \Psi$, $S = (s_{ij})_{i,j=0}^{n-1}$, tako da velja $a = Sb$. Potem je

$$a_i = \sum_{j=0}^{n-1} s_{ij} b_j.$$

Sledi

$$\sum_{i=0}^{n-1} a_i \psi_i = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} b_j s_{ij} \psi_i = \sum_{j=0}^{n-1} b_j \sum_{i=0}^{n-1} s_{ij} \psi_i.$$

Od tod vidimo, da je

$$\omega_j = \sum_{i=0}^{n-1} s_{ij} \psi_i.$$

Torej je j-ta vrstica prehodne matrike razvoj elementa ω_j glede na bazo Ψ. Zdaj pa si bomo ogledali algoritem za določanje elementov prehodne matrike med bazami končnega obsega.

ALGORITEM 5 Izračun elementov prehodne matrike.

Input: Polinoma $p_0(u)$ in $p_1(t)$, ki generirata bazi Ω in Ψ obsega $\mathbb{F}_{q^n}$.
Output: Prehodna matrika S med bazama Ω in Ψ.

1. Izračunamo u, ničlo polinoma $p_0(u)$ glede na bazo Ψ.
2. Izračunamo elemente s_{ij} matrike S za $0 \leq i, j \leq n-1$.
   2.1 Če sta Ω in Ψ polinomski bazi, za $i \in \{0, 1, \ldots, n-1\}$:
   $u^i = \sum_{j=0}^{n-1} s_{n-1-i,j} t^{n-1-j}$.
   2.2 Če je Ω polinomska in Ψ normalna baza, za $i \in \{0, 1, \ldots, n-1\}$:
   $u^i = \sum_{j=0}^{n-1} s_{n-1-i,j} t^{q^j}$.
   2.3 Če je Ω normalna in Ψ polinomska baza, za $i \in \{0, 1, \ldots, n-1\}$:
   $u^{q^i} = \sum_{j=0}^{n-1} s_{i,j} t^{n-1-j}$.
   2.4 Če sta Ω in Ψ normalni bazi:
   $u = \sum_{j=0}^{n-1} s_{0,j} t^{q^j}$,
   vsako naslednjo vrstico matrike S pa dobimo s pomikom prejšnje v desno.
3. Return(S).

Algoritem vrne prehodno matriko velikosti $n \times n$, s katero prehajamo med bazama Ω in Ψ po formuli $a = Sb$. Za prehod v obratni smeri pa rabimo inverzno matriko S^{-1} in računamo po formuli $b = S^{-1}a$. Inverzno matriko bi lahko izračunali tudi iz matrike S, kar pa bi bila potrata časa. Slabost prehoda med bazama z matriko je velika prostorska zahtevnost, kajti matrika ima n^2 koeficientov obsega $\mathbb{F}_q$. Želimo izboljšati prehod med bazama in izkoristiti učinkovitost operacij določene baze.

Primer: Recimo, da imamo polinomsko bazo, definirano z nerazcepnim polinomom

$$p_0(u) = u^5 + u^2 + 1$$

in optimalno normalno bazo tipa II za $\mathbb{F}(2^5)$. Potem je koren polinoma $p_0(u)$ dan z

$$u = t^2 + t^4 + t^8 + t^{16}.$$

Računamo:

$$\begin{aligned} 1 &= t + t^2 + t^4 + t^8 + t^{16} \\ u &= t^2 + t^4 + t^8 + t^{16} \\ u^2 &= t + t^4 + t^8 + t^{16} \\ u^3 &= t + t^4 + t^{16} \\ u^4 &= t + t^2 + t^8 + t^{16}. \end{aligned}$$

Dobimo naslednjo prehodno matriko.

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

$\diamond$

7.2 Prehod linearne prostorske zahtevnosti

Prehod med bazama z matriko zahteva hranjenje n^2 koeficientov prehodne matrike. Tehnika prehoda, ki temelji na [11], porabi veliko manj prostora, zahteva pa nekaj več operacij pri vsakem prehodu. Opisali bomo algoritme prehoda med bazami končnega obsega s pomočjo uvoza in izvoza. Operaciji prehoda iz zunanje v notranjo bazo bomo rekli **uvoz**, operaciji v obratni smeri pa **izvoz**. Za **notranjo bazo** vzamemo tisto, katere aritmetiko poznamo, predvsem znamo učinkovito množiti elemente obsega. Drugo bazo bomo imenovali **zunanja baza**, ta je lahko polinomska ali normalna. To pomeni, da je element $\varepsilon \in \mathbb{F}_{q^n}$ razvit po zunanji bazi oblike

$$\varepsilon = \sum_{i=0}^{n-1} b_i \gamma^i \quad \text{ali} \quad \varepsilon = \sum_{i=0}^{n-1} b_i \gamma^{q^i}, \tag{7.1}$$

kjer so koeficienti $b_0, \ldots, b_{n-1} \in \mathbb{F}_q$ komponente b v zunanji bazi in γ generator zunanje baze. Algoritmi za prehod bodo neodvisni od izbire notranje baze, ki je lahko polinomska, normalna ali pa tudi kakšnega drugega tipa. Splošnejši problem prehoda med dvema zunanjima bazama Ω in Ω' bomo rešili tako, da bomo element iz Ω najprej uvozili v notranjo bazo Ψ, nato pa izvozili v zunanjo bazo Ω'.

Algoritem za uvoz iz zunanje baze lahko skonstruiramo na podlagi direktnega računanja enačbe (7.1). Poznamo namreč notranjo reprezentacijo u generatorja γ, zato lahko pretvorimo vsak element zunanje baze v notranjo bazo zgolj z operacijami v notranji bazi. Pri izvozu v zunanjo bazo pa moramo uporabiti drug pristop, kajti po predpostavki poznamo aritmetiko notranje baze, zunanje pa ne.

Uvoz iz polinomske baze

Potrebujmo generator zunanje baze, predstavljen v notranji bazi, ki ga označimo z u. Izračunamo ga iz informacij o zunanji in notranji bazi, in sicer tako, da najprej vzamemo tisti nerazcepni polinom $p_0(t)$, ki generira zunanjo polinomsko bazo. Potem poiščemo ničlo u polinoma $p_0(t)$ glede na notranjo bazo. Te algoritme sta podrobneje opisala Kaliski in Yin v [11]. Lahko obstaja več sprejemljivih predstavitev generatorja (in posledično več ekvivalentnih predstavitev danega elementa obsega v notranji bazi) in zato moramo pri prehodu enolično določiti generator naše baze. V primeru, ko imamo normalno notranjo bazo in polinomsko zunanjo bazo, je najbolje izbrati polinomsko bazo s takim polinomom $p_0(t)$, ki je hkrati tudi normalni polinom notranje baze. Potem ni potrebno računati ničle u, kajti le ta je kar element, ki je v notranji bazi predstavljen z vektorjem $(1, 0, \ldots, 0)$.

Priprava (le enkrat za izbrano bazo)

1. Izračunamo koren polinoma zunanje baze $p_0(t)$, predstavljen v notranji bazi, in ga označimo z u.

Sledeči algoritem pretvori elemente obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ iz polinomske baze v notranjo bazo z uporabo operacij notranje baze. Enoto za množenje v notranji bazi obsega $\mathbb{F}_{q^n}$ označimo z e.

ALGORITEM 6 Uvoz iz polinomske baze.

Input: $b = (b_0, \ldots, b_{n-1}) \in \mathbb{F}_{q^n}$ v polinomski bazi in konstanta u.
Output: $a \in \mathbb{F}_{q^n}$, isti element v notranji bazi.
1. $a \leftarrow b_{n-1}e$.
2. For i from $n-2$ down to 0 do
   $a \leftarrow au$,
   $a \leftarrow a + b_i e$.
3. Return(a).

V zgornjem algoritmu imamo $n-1$ množenj med elementi obsega ter n množenj s skalarjem. Potrebujemo pa tudi prostor za konstanto u, torej niz n elementov iz obsega $\mathbb{F}_q$. Algoritem nam vrne element

$$a = \sum_{i=0}^{n-1} b_i u^i.$$

To lahko hitro preverimo, kajti a lahko zapišemo tudi kot

$$a = b_0 e + u(b_1 e + u(b_2 e + \ldots + u(b_{n-1}e)\ldots)).$$

Uvoz iz normalne baze

Potrebujemo generator zunanje baze, predstavljen v notranji bazi, ki ga označimo z u. Izračunamo ga iz informacij o zunanji in notranji bazi, in sicer tako, da najprej vzamemo normalen polinom $p_0(t)$ zunanje baze in poiščemo njegovo ničlo.

Priprava (le enkrat za izbrano bazo)

1. Izračunamo koren normalnega polinoma zunanje baze $p_0(t)$, predstavljen v notranji bazi, in ga označimo z u.

Sledeči algoritem pretvori elemente obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ iz normalne baze v notranjo bazo z uporabo operacij notranje baze.

ALGORITEM 7 Uvoz iz normalne baze.

Input: $b = (b_0, \ldots, b_{n-1}) \in \mathbb{F}_{q^n}$ v normalni bazi in konstanta u.
Output: $a \in \mathbb{F}_{q^n}$, isti element v notranji bazi.
1. $a \leftarrow b_{n-1}u$.
2. For i from $n-2$ down to 0 do
   $a \leftarrow a^q$,
   $a \leftarrow a + b_i u$.
3. Return(a).

V tem algoritmu je $n-1$ potenciranj na potenco q in n množenj s skalarjem. Potrebujemo pa tudi prostor za konstanto u (generator zunanje baze, predstavljen v notranji bazi) ter dodatno še za vmesni rezultat potenciranja. Upoštevali smo, da je $(a+b_iu)^q = a^q + b_i u^q$. Algoritem vrne

$$a = b_0 u + (b_1 u + \ldots + (b_{n-2}u + (b_{n-1}u)^q)^q \ldots)^q = \sum_{i=0}^{n-1} b_i u^{q^i}.$$

Izvoz v polinomsko bazo

Pri algoritmu za izvoz v polinomsko bazo si pomagamo s preprosto lemo, ki nam pove, da je v primeru polinomske zunanje baze, ko je $b_0 = 0$, množenje z γ^{-1} kar pomik koeficientov v levo. Najprej izračunamo b_0 in ga odštejemo, nato pa množimo z u^{-1}. To ponavljamo, dokler ne dobimo vseh koeficientov b_i.

Lema 7.2.1. *Naj bo zunanja baza polinomska z generatorjem γ, $b = (b_0, \ldots, b_{n-1})$ predstavitev elementa $\varepsilon \in \mathbb{F}_{q^n}$ v zunanji bazi in $C = (c_0, \ldots, c_{n-1})$ predstavitev elementa $\varepsilon\gamma^{-1}$ v zunanji bazi. Če je $b_0 = 0$, potem za vsak $i \in \{0, 1, \ldots, n-2\}$ velja $c_i = b_{i+1}$.*

Dokaz. Ker je $b_0 = 0$, veljata naslednji enakosti:

$$\varepsilon = \sum_{i=0}^{n-1} b_i\gamma^i = \sum_{i=1}^{n-1} b_i\gamma^i$$

in

$$\varepsilon\gamma^{-1} = \sum_{i=1}^{n-1} b_i\gamma^{i-1} = \sum_{i=0}^{n-2} b_{i+1}\gamma^i.$$

Po drugi strani pa je

$$\varepsilon\gamma^{-1} = \sum_{i=0}^{n-1} c_i\gamma^i.$$

Sledi $c_i = b_{i+1}$ za vsak $i \in \{0, 1, \ldots, n-2\}$. □

Priprava (le enkrat za izbrano bazo)

1. Izračunamo u – v notranji bazi predstavljen koren polinoma zunanje baze $p_0(t)$.
2. Izračunamo prehodno matriko S.
3. Izračunamo $w := u^{-1}$.
4. Izračunamo $\Delta := S^{-1}$ in označimo prvi stolpec matrike Δ kot $\delta := (\delta_{0,0}, \delta_{1,0}, \ldots, \delta_{n-1,0})$.
5. Izračunamo multiplikacijsko matriko M notranje baze.
6. Označimo $z := \delta M^{-1}$.

Naslednji algoritem pretvori elemente končnega obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ iz notranje baze v zunanjo polinomsko bazo z uporabo operacij notranje baze.

ALGORITEM 8 Izvoz v polinomsko bazo.

Input: $a = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_{q^n}$ v notranji bazi in konstanti w, z.
Output: $b = (b_0, \ldots, b_{n-1}) \in \mathbb{F}_{q^n}$, isti element v polinomski bazi.

1. $a \leftarrow az$.
2. For i from 0 to $n-2$ do
   $b_i \leftarrow a_0$,
   $a \leftarrow a - b_i z$,
   $a \leftarrow aw$.
3. $b_{n-1} \leftarrow a_0$.
4. Return(b).

V vsakem koraku iteracije se izračuna en koeficient. V tem algoritmu je n množenj med elementi obsega in $n-1$ množenj s skalarjem. Potrebujemo pa tudi prostor za dve konstanti.

Izvoz v normalno bazo

V primeru, ko je zunanja baza normalna, izkoristimo lepo lastnost normalnih baz, da je q-ta potenca ciklični pomik koeficientov v desno. Naslednjo lemo uporabimo pri algoritmu za izvoz v normalno bazo, kjer najprej izračunamo koeficient b_{n-1}, nato q-to potenco in to ponavljamo, dokler ne izračunamo vseh koeficientov.

Priprava (le enkrat za izbrano bazo)

1. Izračunamo prehodno matriko S.

2. Izračunamo matriko $\Delta := S^{-1}$ in označimo z $\delta := (\delta_{0,n-1}, \delta_{1,n-1}, \ldots, \delta_{n-1,n-1})$ zadnji stolpec matrike Δ.

3. Izračunamo multiplikacijsko matriko M notranje baze.

4. Označimo $z := \delta M^{-1}$.

Sledeči algoritem pretvori elemente končnega obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ iz notranje baze v zunanjo normalno bazo z uporabo operacij notranje baze.

ALGORITEM 9 Izvoz v normalno bazo.

Input: $a = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_{q^n}$ v notranji bazi in konstanta z.
Output: $b = (b_0, \ldots, b_{n-1}) \in \mathbb{F}_{q^n}$, isti element v normalni bazi.
1. For i from $n-1$ down to 1 do
   $v \leftarrow az$,
   $b_i \leftarrow v_0$,
   $a \leftarrow a^q$.
2. $v \leftarrow az$, $b_0 \leftarrow v_0$.
3. Return(b).

V zadnjem algoritmu imamo $n-1$ potenciranj na potenco q in n množenj med elementi obsega $\mathbb{F}_{q^n}$. Potrebujemo pa tudi prostor za konstanto ter dodatno še za vmesni rezultat potenciranja.

Analiza algoritma

Izvedemo lahko štiri vrste prehodov med bazami in vsakega opravimo v dveh korakih; najprej uvoz, nato izvoz. Če želimo na primer iz polinomske baze v normalno, moramo najprej narediti uvoz iz polinomske baze in nato še izvoz v normalno bazo. Sledeča tabela prikazuje analizo prehoda med dvema bazama z opisanimi algoritmi, kjer opazujemo tako število operacij kot tudi prostorsko zahtevnost. Zanemarili smo seštevanje med elementi obsega in množenje s skalarjem iz $\mathbb{F}_q$, kajti ti dve operaciji sta hitri. Število množenj v tabeli pomeni število množenj med elementi obsega. S kratico PB smo označili polinomsko bazo, z NB pa normalno bazo.

vrsta prehoda	število množenj med elementi $\mathbb{F}_{q^n}$	število potenciranj na potenco q	vhodne konstante
PB $\rightarrow$ PB	$2n-1$	-	u, u^{-1}, z
PB $\rightarrow$ NB	$2n-1$	$n-1$	u, z
NB $\rightarrow$ NB	n	$2n-2$	u, z
NB $\rightarrow$ PB	n	$n-1$	u, u^{-1}, z

Tabela 7.1: Zahtevnosti prehodov med bazami.

Število vhodnih konstant (vektorjev dolžine n s koeficienti iz $\mathbb{F}_q$) nam določa prostorsko zahtevnost prehoda, ki je pri tem pristopu enaka $\mathcal{O}(n)$, medtem ko smo pri prehodu z matriko potrebovali n^2 koeficientov iz $\mathbb{F}_q$ za prehodno matriko. Zgoraj opisani algoritmi so torej boljše prostorske zahtevnosti.

Poglavje 8

ODPRTI PROBLEMI

V prejšnjih poglavjih smo si ogledali normalne baze, optimalne normalne baze, normalne baze nizke kompleksnosti in sebidualne normalne baze ter podali njihove konstrukcije. Za zaključek bomo izpostavili nekaj problemov, ki si zaslužijo nadaljne raziskave. Problemi so povzeti po Gao [6, poglavje 6] in Menezes et al. [18].

Za dan nerazcepen polinom stopnje n nad $\mathbb{F}_q$ znamo deterministično skonstruirati normalno bazo obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ v polinomskem času. Tako problem konstrukcije normalne baze zreduciramo na naslednji problem, ki je pomemben v teoriji končnih obsegov in računalniški algebri.

Problem 1. *Poiskati deterministični algoritem polinomske časovne zahtevnosti (v n in $\log n$) za konstrukcijo nerazcepnega polinoma stopnje n v $\mathbb{F}_q[x]$, za dan končen obseg $\mathbb{F}_q$ in dano naravno število n.*

V kriptografiji je pomembno poznati primitiven element ali pa element visokega multiplikativnega reda v $\mathbb{F}_{2^n}$. V splošnem imajo generatorji optimalnih normalnih baz tipa II visok multiplikativni red in so dokaj pogosto primitivni. Ta fenomen je opazil Rybowicz [21].

Problem 2. *Naj bo n pozitivno število in γ $(2n+1)$-i primitivni koren enote v neki razširitvi obsega $\mathbb{F}_2$. Določi multiplikativni red elementa $\alpha = \gamma + \gamma^{-1}$.*

Zanima nas primer, ko je $2n+1$ praštevilo in je $\mathbb{Z}^*_{2n+1}$ generiran z elementoma 2 in -1, torej ko α generira optimalno normalno bazo obsega $\mathbb{F}_{2^n}$. Želeli bi določiti red elementa α, ne da bi poznali popolno faktorizacijo $2^n - 1$ za velike n. Naslednji problem je na nek način nasprotje zgornjega.

Problem 3. *Naj bo α element v neki razširitvi obsega $\mathbb{F}_2$. Za dan multiplikativni red α določi multiplikativni red elementa γ, kjer je $\gamma + \gamma^{-1} = \alpha$.*

Kompleksnost normalne baze, definirane v tem delu, ne predstavlja nujno realne kompleksnosti množenja v končnem obsegu v dani bazi. Skonstruirali smo normalne baze obsega $\mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ s produkti oblike

$$\alpha_i \alpha_j = e_{i-j}\alpha_i + e_{j-i}\alpha_j + \gamma$$

za $i \neq j$, kjer sta $e_k, \gamma \in \mathbb{F}_q$. Če je $\gamma \neq 0$, je kompleksnost normalne baze blizu n^2. Ker pa je le $3n-1$ konstant v vseh n produktih $\alpha_0\alpha_i$ za $i \in \{0, 1, \ldots, n-1\}$, lahko zmnožimo dva elementa v $\mathbb{F}_{q^n}$, predstavljena v tej bazi, s približno $3n-1$ množenji elementov v $\mathbb{F}_q$. Odtod vidimo, da je prava kompleksnost množenja v obsegu $\mathbb{F}_{q^n}$ v normalni bazi takega tipa manjša od definirane kompleksnosti baze.

Literatura

[1] E. Artin, *Galois Theory*, University of Notre Dame Press, South Bend, 1966.

[2] D. Ash, I. Blake in S. Vanstone, *Low Complexity Normal Bases*, Discrete Applied Math **25** (1989), 191–210.

[3] J. Barbič, *Schoofov algoritem*, diplomsko delo, Fakulteta za matematiko in fiziko, Univerza v Ljubljani, 2000.

[4] I. F. Blake, S. Gao in R. C. Mullin, *Normal and Self-dual Normal Bases from Factorization of* $cx^{q+1} + dx^q - ax - b$, SIAM J. Discr. Math. **7** (1992), 499–512.

[5] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, Springer-Verlag, 1995.

[6] S. Gao, *Normal Bases over Finite Fields*, Ph.D. Thesis, University of Waterloo, 1993.

[7] S. Gao in H. V. Lenstra, *Optimal Normal Bases*, Designs, Codes and Cryptography **2** (1992), 315–323.

[8] J. von zur Gathen in M. Giesbrecht, *Constructing Normal Bases in Finite Fields*, J. Symbolic Computation **10** (1990), 547–570.

[9] D. Hankerson, A. Menezes in S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer-Verlag, 2004.

[10] T. Itoh in S. Tsujii, *A fast algorithm for computing multiplicative inverses in GF(2m) using normal bases*, Information and Computation **78** (1988), 171–177.

[11] B. S. Kaliski in Y. L. Yin, *Storage Efficient Finite Field Basis Conversion*, Proceedings of the Selected Areas in Cryptography, Lecture Notes In Computer Science **1556** (1998), 81–93.

[12] A. Lempel in M. J. Weinberger, *Self-complementary Normal Bases in Finite Fields*, SIAM J. Disc. Math. **1** (1988), 193–198.

[13] W. J. Leveque, *Topics in Number Theory 1*, Addison–Wesley, Reading, Mass., 1956.

[14] R. Lidl, G. Mullen in G. Turnwald, *Dickson Polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics **65**, Longman Scientific and Technical, 1993.

[15] R. Lidl in H. Niederreiter, *Encyclopedia of Mathematics and Its Applications: Finite fields*, Cambridge University Press, 1987.

[16] A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, 1993.

[17] A. J. Menezes, P. van Oorschot in S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[18] A. Menezes, I. A. Blake, X. Gao, R. C. Mullin, S. A. Vanstone in T. Yaghoobian, *Applications of Finite Fields*, Kluwer Academic Publishers, 1992.

[19] V. Nastran, *Baze binarnih končnih obsegov*, diplomsko delo, Fakulteta za matematiko in fiziko, Univerza v Ljubljani, 2003.

[20] M. Rosing, *Implementing Elliptic Curve Cryptography*, Manning Publications, 1998.

[21] M. Rybowicz, *Search of primitive polynomials over finite fields*, J. of Pure and Applied Algebra **65** (1990), 139–151.

[22] V. M. Sidel'nikov, *On normal bases of a finite field*, Math. USSR Sbornik **61** (1988), 485–494.

[23] D. R. Stinson, *Cryptography:Theory and Practice*, CRC Press, 2002.

[24] I. Vidav, *Algebra*, Mladinska knjiga, Ljubljana, 1989.

[25] E. W. Weisstein, *CRC concise encyclopedia of mathematics*, CRC, 1999.

[26] IEEE P1363, *Standard Specifications for Public Key Cryptography, Draft version 13, Annex A*, 1999.
`http://grouper.ieee.org/groups/1363/passwdPK/draft.html`