NORMALNE BAZE V KONČNIH OBSEGIH

Maruša Stanek

12. november 2004

Povzetek

Z razvojem teorije kodiranja in nastankom večih kriptosistemov, ki temeljijo na končnih obsegih, se je pojavila potreba po učinkoviti implementaciji aritmetičnih operacij v končnih obsegih, kar ima velik pomen v javni kriptografiji. Elemente iz končnega obsega lahko predstavimo v različnih bazah in s predstavitvijo elementov v določeni bazi 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 končnih obsegov je učinkovito potenciranje. Posebna vrsta normalnih baz so optimalne normalne baze, v katerih se poenostavi množenje. Optimalne normalne baze so osnova za varno in učinkovito implementacijo večih kriptosistemov.

Abstract

With the development of coding theory and the appearance of several cryptosystems using finite fields, the implementation of finite field arithmetic is required. It is important in public key cryptography. We can represent elements from finite fields in various bases and get efficient improvement of arithmetic algorithms with the representation in appointed base. There are several sorts of bases used in cryptography. One of them are normal bases. Interest in normal bases over finite fields stems both from mathematical theory and practical applications. The advantage of using normal bases to represent finite fields is in efficient exponentiation. Special kind of normal bases are optimal normal bases, which simplify multiplication. Optimal normal bases are basis in secure and efficient implementation of several cryptosystems.

Kazalo

1 UVOD

Če želimo v praksi računati z elementi končnega obsega, moramo te elemente v računalniku na nek način predstaviti. V kriptografski praksi najpogosteje delamo z obsegi oblike GF(2^n), kjer je n veliko naravno število, ali pa obsegi oblike GF(p^n), kjer je p veliko praštevilo. Ukvarjali se bomo s predstavitvijo obsega GF(p^n) s pomočjo elementov obsega GF(p). Elemente iz končnega obsega lahko predstavimo v različnih bazah, kot so polinomske ali normalne baze. Polinomske in normalne baze ter njihovo praktično realizacijo na računalnikih izčrpno opisuje ameriški standard IEEE P1363.

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 obsega GF(2^n) je kvadriranje ciklični zamik, množenje pa ostane težko. Normalne baze so praktične tako za hardwarsko kot tudi za softwarsko implementacijo aritmetičnih operacij v končnih obsegih. Mullin, Onyszchuk, Vanstone in Wilson so leta 1988 definirali posebno obliko normalnih baz, tako imenovane optimalne normalne baze, s katerimi lahko pospešimo množenje. Iz posebne oblike optimalnih normalnih baz lahko razvijemo novo vrsto baz, tako imenovane umbralne ali Chebysheve baze, ki pa jih tu ne bomo obravnavali. Z njimi se poenostavi računanje inverza.

1.1 Pregled sledečih poglavij

V naslednjem poglavju si bomo ogledali končne obsege in aritmetične operacije v njih. Poglavje bomo zaključili z razdelkom o kvadratnih enačbah.

V tretjem poglavju bomo obravnavali normalne baze. Začeli bomo z osnovnimi definicijami in si nato ogledali aritmetične operacije v normalnih bazah. Zadnji razdelek je namenjen porazdelitvi normalnih elementov.

V četrtem poglavju bomo obravnavali optimalne normalne baze. Ogledali si bomo njihovo konstrukcijo in nato povezavo s polinomskimi bazami. Na koncu bomo natanko določili vse optimalne normalne baze v končnih obsegih.

Zadnje poglavje je posvečeno nadaljnim raziskovalnim problemom. Za zaključek pa je podan še Lenstrov algoritem za konstrukcijo normalnih baz.

2 KONČNI OBSEGI

V tem poglavju bomo obravnavali končne obsege, torej obsege s končnim številom elementov. V zadnjem razdelku bomo obravnavali reševanje kvadratnih enačb.

Naj bo L končen obseg, ki vsebuje podobseg K. Potem je L razširitev obsega K. Vsak končen obseg ima najmanjši podobseg, ki ga imenujemo praobseg. Praobseg končnega obsega je izomorfen GF(p) za neko praštevilo p, ki se imenuje **karakteristika** obsega.

Izrek 2.1 *Vsak končen obseg s karakteristiko p ima p^n elementov za neko naravno število n.*

Dokaz : Naj bo L končen obseg in K praobseg obsega L. Vektorski prostor L nad K je končno razsežen, dimenzije n, torej obstaja baza $b_1, b_2, \ldots, b_n$ prostora L nad K. Vsak element a obsega L lahko enolično zapišemo kot linearno kombinacijo b_i nad K, $a = \sum_{i=1}^{n} \beta_i b_i$, $\beta_i \in K$, in ker ima K p elementov, mora imeti L p^n elementov. □

Definicija 2.1 *Naj bo $f(x) \in K[x]$. Potem najmanjši obseg, ki vsebuje K in vse ničle $f(x)$, imenujemo* **razpadni obseg** *polinoma $f(x)$ nad K.*

Po izreku, katerega dokaz se nahaja v Vidav [1, 9.8], so razpadni obsegi $f(x)$ med seboj izomorfni.

Izrek 2.2 *Razpadni obseg nerazcepnega polinoma $f(x) \in K[x]$ nad K obstaja in vsaka dva taka razpadna obsega sta izomorfna.* □

Definicija 2.2 *Ničle nerazcepnega polinoma $f(x) \in K[x]$ v razpadnem obsegu za $f(x)$ nad K imenujemo* **konjugiranke**.

Izrek 2.3 *Naj bo L obseg s karakteristiko p in praobsegom K. Potem je L razpadni obseg polinoma $f(x) = x^{p^n} - x$ nad K, če in samo če ima L p^n elementov.*

Dokaz : Naj bo L razpadni obseg polinoma $f(x) = x^{p^n} - x$ nad K. Koreni $f(x)$ so različni in zato ima L vsaj p^n elementov. Oglejmo si podmnožico $E = \{b \in L \mid b^{p^n} = b\}$, ki vsebuje p^n elementov, ker je sestavljena iz korenov polinoma $f(x)$. Naj bosta $a, b \in E$. Potem je $(ab)^{p^n} = (a)^{p^n}(b)^{p^n} = ab$ in je zato produkt ab v E. Torej je

$$(a+b)^{p^n} = \sum_{i=0}^{p^n} \binom{p^n}{i} a^i b^{p^n - i} = a^{p^n} + b^{p^n} = a + b$$

in zato je $a + b \in E$. Ker obstajata oba inverza, tako aditivni kot tudi multiplikativni, je E podobseg L in razpadni obseg za $f(x)$. Po prejšnjem izreku je $E = L$ in L vsebuje p^n elementov. Multiplikativna grupa obsega L, ki jo bomo označili z L^*, tvori grupo reda $p^n - 1$ in zato red vsakega elementa L^* deli $p^n - 1$. Torej je $a^{p^n} = a$ za vse $a \in L^*$, kar je trivialno izpolnjeno tudi za $a = 0$. Torej je L razpadni obseg polinoma $f(x) = x^{p^n} - x$.□

Sledi nekaj pomembnejših lem.

Lema 2.4 *Obstaja do izomorfizma natanko določen obseg reda p^n.*

Dokaz : Lema sledi iz dejstva, da $f(x)$ razpade nad vsakim obsegom s p^n elementi ter izreka (2.2), po katerem so razpadni obsegi do izomorfizma natanko določeni. □

Lema 2.5 $\mathrm{GF}(p^n)$ *je razpadni obseg za* $f(x) = x^{p^n} - x$ *nad* $\mathrm{GF}(p)$.

Dokaz : Lema sledi iz izreka (2.3) in leme (2.4). □

Lema 2.6 *Za vsako praštevilo p in naravno število n obstaja* $\mathrm{GF}(p^n)$.

Dokaz : Po izreku (2.2) razpadni obseg obstaja in po lemi (2.5) je enak $\mathrm{GF}(p^n)$. □

Izrek 2.7 *Za vsako praštevilo p in naravno število n je* $\mathrm{GF}(p^n)^*$ *ciklična grupa.*

Dokaz : Multiplikativna grupa $\mathrm{GF}(p^n)^*$ je po definiciji abelova in reda $p^n - 1$. Če je $p^n - 1 = p_1^{e_1} \dots p_k^{e_k}$, potem lahko $\mathrm{GF}(p^n)^*$ zapišemo kot direktni produkt njegovih podgrup Sylowa: $\mathrm{GF}(p^n)^* = S(p_1) \otimes \dots \otimes S(p_k)$, kjer je $S(p_i)$ podgrupa reda $p_i^{e_i}$ za $i \in \{1, \dots, k\}$. Red vsakega elementa grupe $S(p_i)$ je neka potenca p_i. Naj bo $a_i \in S(p_i)$ maksimalnega reda $p_i^{e'_i}$, kjer je $e'_i \leq e_i$ za $i \in \{1, \dots, k\}$. Ker je za $\gcd(p_i, p_j) = 1$ za i različen od j, ima element $a = a_1 \dots a_k$ maksimalni red $m = p_1^{e'_1} \dots p_k^{e'_k}$ v $\mathrm{GF}(p^n)^*$. Prav tako vsak element iz $\mathrm{GF}(p^n)^*$ zadosti polinomu $x^m - 1$ in zato je $m \geq p^n - 1$. Ker pa ima element $a \in \mathrm{GF}(p^n)^*$ red m, mora m deliti $p^n - 1$ in zato velja $m = p^n - 1$. Torej je element a generator in je $\mathrm{GF}(p^n)^*$ ciklična grupa. □

Definicija 2.3 *Generator grupe* $\mathrm{GF}(p^n)^*$ *imenujemo* **primitivni element** *obsega* $\mathrm{GF}(p^n)$.

Posledica 2.8 *Vsak končni obseg je komutativen.*

Dokaz : Sledi iz izreka (2.7), saj je vsaka ciklična grupa komutativna. □

Zdaj si bomo ogledali še sled. Ta funkcional ima v teoriji končnih obsegov pomembno vlogo.

Definicija 2.4 *Sled elementa α v obsegu $\mathrm{GF}(p^n)$ nad $\mathrm{GF}(p)$ je linearen funkcional*

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

Kadar je iz konteksta razvidno, v katerem obsegu se nahajamo, lahko sled preprosto označimo kot $\mathrm{Tr}(\alpha)$. Naslednja trditev bo pomembna v razdelku o rešljivosti kvadratnih enačb v končnih obsegih.

Trditev 2.9 *Sled je neničeln funkcional. Moč njegovega jedra je natanko p^{n-1}.*

Dokaz : 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 $\mathrm{GF}(p)$ in je torej njena dimenzija enaka 1. Jedro sledi označimo s ker Tr, zalogo vrednosti pa z im Tr. Potem iz dimenzijske enačbe $\dim(\mathrm{ker Tr}) + \dim(\mathrm{im\ Tr}) = \dim(\mathrm{GF}(p^n))$ sledi $\dim(\ker \mathrm{Tr}) = n - 1$. Torej je jedro sledi izomorfno direktni vsoti $n - 1$ faktorjev $\mathbb{Z}_p$. Zato je moč jedra sledi enaka p^{n-1}. □

2.1 Aritmetika v končnih obsegih

Naj bo p praštevilo in $q = p^m$, kjer je m naravno število. $\mathrm{GF}(q)$ je končen obseg s q elementi in karakteristiko p. $\mathrm{GF}(q^n)$ je n razsežna razširitev obsega $\mathrm{GF}(q)$. Pogosto govorimo o bazi končnega obsega $\mathrm{GF}(q^n)$, pri tem pa imamo vedno v mislih bazo za vektorski prostor $\mathrm{GF}(q^n)$ nad $\mathrm{GF}(q)$.

Oglejmo si seštevanje v $\mathrm{GF}(q^n)$. Vektorski prostor $\mathrm{GF}(q^n)$ nad $\mathrm{GF}(q)$ je končno razsežen, torej obstaja množica $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, $\alpha_i \in \mathrm{GF}(q^n)$, linearno neodvisnih elementov nad $\mathrm{GF}(q)$. Potem lahko vsak element A iz $\mathrm{GF}(q^n)$ zapišemo kot

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

kjer je $a_i \in \mathrm{GF}(q)$ za vsak $i \in \{1, \ldots, n\}$. Tako identificiramo $\mathrm{GF}(q^n)$ z $\mathrm{GF}(q)^n$ in poljuben element lahko zapišemo kot $A = (a_1, a_2, \ldots, a_n)$ v pripadajoči bazi. Naj bo $B = (b_1, b_2, \ldots, b_n) \in \mathrm{GF}(q^n)$. Seštevanje v $\mathrm{GF}(q^n)$ nad $\mathrm{GF}(q)$ je kar seštevanje po komponentah, torej

$$A + B = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n).$$

Poglejmo še množenje in deljenje. Naj bo $A \cdot B = C = (c_1, c_2, \ldots, c_n)$. Za linearno neodvisne elemente α_i velja:

$$\alpha_i \alpha_j = \sum_{k=1}^{n} t_{ij}^{(k)} \alpha_k, \ i \in \{1, \ldots, n\},$$

kjer je $t_{ij}^{(k)} \in \mathrm{GF}(q)$. Potem je

$$c_k = \sum_{i,j=1}^{n} a_i b_j t_{ij}^{(k)}, 1 \leq k \leq n.$$

O množenju v normalnih bazah bomo govorili v razdelku 3.2. Deljenje pa je pravzaprav množenje z inverzom. V multiplikativni grupi ima vsak element inverz in ker za vsak $A \in \mathrm{GF}(q^n)^*$ velja $A^{q^n} = A$, sledi $A^{q^n-2} = A^{-1}$. Tako smo dobili eksplicitno formulo za računanje inverza v obsegu $\mathrm{GF}(q^n)$. V končnem obsegu $\mathrm{GF}(q^n)$ lahko vsak element B delimo s poljubnim neničelnim elementom A: $B/A = BA^{-1} = BA^{q^n-2}$.

V kriptografiji najpogosteje uporabljamo razširitve obsega $\mathrm{GF}(2)$. Zato želimo imeti učinkovit algoritem za izračun inverza elementa $A \in \mathrm{GF}(2^n)^*$. Vemo, da velja $A^{-1} = A^{2^n-2}$, kar lahko zapišemo kot $A^{2^n-2} = A^2 \cdot A^{2^2} \ldots A^{2^{n-1}}$. Na prvi pogled potrebujemo $n-2$ množenj in $n-1$ kvadriranj. Število množenj lahko bistveno zmanjšamo. Če uporabimo normalne baze za predstavitev elementov obsega $\mathrm{GF}(2^n)$, je kvadriranje le ciklični zamik, kar je zanemarljivo v primerjavi z množenjem. Algoritem invertiranja v normalni bazi obsega $\mathrm{GF}(2^n)$ bomo predstavili v razdelku 3.2.

Inverz neničelnega elementa lahko izračunamo tudi z razširjenim Evklidovim algoritmom, ki je v večini primerov najbolj učinkovita metoda. Vendar pa ta metoda deluje le v primeru, ko so elementi obsega predstavljeni v polinomski bazi, v normalnih bazah pa je ne moremo uporabiti.

2.2 Kvadratna enačba

V tem delu bomo obravnavali rešljivost kvadratnih enačb v končnih obsegih.

Definicija 2.5 *Element $x \in \mathrm{GF}(q^n)$ je* **kvadrat**, *če obstaja tak $y \in \mathrm{GF}(q^n)$, da je $x = y^2$. Elemente, ki niso kvadrati, pa imenujemo* **nekvadrati**.

Ogledali si bomo reševanje kvadratne enačbe

$$aX^2 + bX + c = 0,\ a \neq 0,\ a, b, c \in \mathrm{GF}(q^n). \tag{1}$$

2.2.1 Obsegi karakteristike $p > 2$

Trditev 2.10 *Kvadratna enačba (1) ima v obsegu* $\mathrm{GF}(q^n)$, $p > 2$, *rešitev natanko tedaj, ko je diskriminanta* $b^2 - 4ac$ *kvadrat.*

Dokaz : Levo stran enačbe (1) dopolnimo do popolnega kvadrata:
$(X + \frac{b}{2a})^2 + \frac{c}{a} - \frac{b^2}{4a^2} = 0$. Zadnja enačba ima rešitev natanko tedaj, ko je element $\frac{b^2}{4a^2} - \frac{c}{a}$ kvadrat. Element obsega pa je kvadrat natanko takrat, kadar je njegov produkt s poljubnim kvadratom tudi kvadrat. □

V obsegu karakteristike več od 2 je natanko polovica neničelnih elementov kvadratov, druga polovica pa so nekvadrati. Pri iskanju kvadratov si lahko pomagamo z naslednjo karakterističnolastnostjo.

Trditev 2.11 *Neničeln element* $x \in \mathrm{GF}(q^n)$ *je kvadrat natanko tedaj, ko je* $x^{(q^n-1)/2} = 1$.

Dokaz : Ker je q^n lih, 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 $\mathrm{GF}(q^n)$ in vse ničle so enostavne. Zato je vsak element obsega $\mathrm{GF}(q^n)$ ničla natanko enega od faktorjev na desni strani enakosti, in sicer enostavna. Faktor x je rezerviran za element 0. Torej za natanko polovico neničelnih elementov x obseg $\mathrm{GF}(q^n)$ velja $x^{(q^n-1)/2} = 1$. Za drugo polovico pa velja $x^{(q^n-1)/2} = -1 \neq 1$. Pokažimo, da prva polovica sovpada z neničelnimi kvadrati, druga pa z nekvadrati. Naj bo neničeln element $x \in \mathrm{GF}(q^n)$ kvadrat. Torej je $x = y^2$ za nek neničeln $y \in \mathrm{GF}(q^n)$. Sledi $x^{(q^n-1)/2} = y^{q^n-1} = 1$. Torej so vsi neničelni kvadrati v prvi polovici elementov obsega $\mathrm{GF}(q^n)$. Ker pa je neničelnih kvadratov enako število kot nekvadratov, v drugi polovici ne bomo našli nobenega nekvadrata. □

Recimo, da smo za nek neničeln $d \in \mathrm{GF}(q^n)$ ugotovili, da je kvadrat in želimo najti njegov kvadratni koren. V primeru, ko je $q^n \equiv 3 \bmod 4$, 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 $x \in \mathrm{GF}(q^n)$, iz Viétove formule sledi, da je drugi koren enak $-x$. Ker je q^n liho število, nam ostane le še primer, ko je $q^n \equiv 1 \bmod 4$. V tem primeru je

$$\sqrt{d} = \begin{cases} d^{k+1} \bmod q^n, & \text{za } q^n = 8k+5 \text{ in } d^{2k+1} \equiv 1 \bmod q^n \\ \frac{1}{2}(4d)^{k+1}(q^n+1) \bmod q^n, & \text{za } q^n = 8k+5 \text{ in } d^{2k+1} \equiv -1 \bmod q^n \end{cases}$$

Več o tem se nahaja v ameriškem standardu IEEE P1363.

2.2.2 Obsegi karakteristike $p = 2$

V obsegu s karakteristiko 2 običajni pristop za reševanje kvadratne enačbe odpove. V končnem obsegu karakteristike 2 nekvadratov sploh ni in je enačba $X^2 = d$ rešljiva za vsak $d \in \mathrm{GF}(2^n)$. Ker v takem obsegu velja $-d = d$, ima pri vsakem $d \in \mathrm{GF}(2^n)$ 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 $\mathrm{GF}(2^n)$ rešljiva. Oglejmo si kvadratno enačbo oblike

$$aX^2 + bX + c = 0,\ a \neq 0,\ a, b, c \in \mathrm{GF}(2^n). \tag{2}$$

Če enačbo (2) pomnožimo z a^{-1}, dobimo

$$X^2 + uX + v = 0,\ u, v \in \mathrm{GF}(2^n). \tag{3}$$

Primer, ko je $u = 0$, smo že obravnavali, zato naj bo v nadaljevanju $u \neq 0$. Enačbo (3) pomnožimo z u^{-2} in uvedemo novo neznanko $Y = u^{-1}X$ ter dobimo

$$Y^2 + Y = w, \text{ kjer je } w = vu^{-2}. \tag{4}$$

Obstaja preprost kriterij za rešljivost zadnje enačbe, podan v naslednji trditvi.

Trditev 2.12 *Enačba (4) ima rešitev v obsegu* $\mathrm{GF}(2^n)$ *natanko tedaj, ko je sled elementa* w *enaka* 0.

Dokaz :
($\Rightarrow$) Naj ima enačba (4) rešitev y. Uporabimo sled na obeh straneh enačbe in dobimo

$$\mathrm{Tr}(w) = \mathrm{Tr}(y^2 + y) = \mathrm{Tr}(y^2) + \mathrm{Tr}(y) = \mathrm{Tr}(y) + \mathrm{Tr}(y) = 0.$$

Pri tem smo uporabili aditivnost sledi in lastnost $\mathrm{Tr}(y^2) = \mathrm{Tr}(y)$.
($\Leftarrow$) Naj bo $\mathrm{Tr}(w) = 0$. Opisali bomo eksplicitno konstrukcijo ene rešitve enačbe (4). Ta konstrukcija je praktično uporabna, kadar so elementi obsega v računalniku predstavljeni v normalni bazi, torej bazi oblike $\{\theta, \theta^2, \ldots, \theta^{2^{n-1}}\}$ za nek $\theta \in \mathrm{GF}(2^n)$. Rešitev y bomo predstavili v tej normalni bazi. Naj elementu y ustrezajo koeficienti $(y_0, y_1, \ldots, y_{n-1})$, kjer moramo elemente y_i še določiti. Elementu w pa naj ustreza predstavitev $(w_0, w_1, \ldots, w_{n-1})$. Poskusimo z nastavkom $y_0 = 0$. Enačba (4) dobi obliko

$$(y_{n-1}, 0, y_1, \ldots, y_{n-2}) + (0, y_1, y_2, \ldots, y_{n-1}) = (w_0, w_1, w_2, \ldots, w_{n-1}).$$

Iz drugega, tretjega, ..., zadnjega stolpca dobimo enačbe za $y_1, y_2, \ldots, y_{n-1}$:

$$y_1 = w_1,\ y_i = w_i + y_{i-1},\ i \in \{2, 3, \ldots, n-1\}. \tag{5}$$

Zdaj moramo le še ugotoviti, če je zadoščeno tudi enačbi v prvem stolpcu $y_{n-1} = w_0$. Uporabimo predpostavko, da je $\mathrm{Tr}(w) = 0$. Enačbe iz (5) seštejemo med sabo. Členi y_i, $i \in \{1, 2, \ldots, n-2\}$ se pokrajšajo in dobimo enačbo

$$y_{n-1} = \sum_{i=1}^{n-1} w_i = \mathrm{Tr}(w) + w_0 = w_0,$$

kar je ravno enačba prvega stolpca. Pri drugem enačaju v zgornji enakosti smo uporabili formulo: če je $a = \sum_{i=0}^{n-1} a_i \theta^{2^i}$, kjer je $a_i \in \mathrm{GF}(2)$, potem velja $\mathrm{Tr}(a) = \sum_{i=0}^{n-1} a_i \mathrm{Tr}(\theta^{2^i}) = \sum_{i=0}^{n-1} a_i \mathrm{Tr}(\theta) = \sum_{i=0}^{n-1} a_i$. □

Ker v primeru obsega karakteristike 2 sled slika v praobseg GF(2), je vrednost sledi nekega elementa lahko le 0 ali 1. Sled je neničeln funkcional, zato obstajajo elementi w z neničelno sledjo in iz izreka (2.9) sledi, da je takih w v $\mathrm{GF}(2^n)$ natanko $2^n - 2^{n-1}$. Torej v vsakem obsegu $\mathrm{GF}(2^n)$ obstajajo nerešljive kvadratne enačbe.

Trditev 2.13 *V vsakem končnem obsegu* $\mathrm{GF}(q^n)$ *obstajajo kvadratne enačbe s koeficienti iz tega obsega, ki v* $\mathrm{GF}(q^n)$ *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 uporabimo trditev (2.12). □

Tako na primer enačba $X^2 + X + \alpha = 0$ nima rešitve v GF(2^n), če je α generator kakšne normalne baze v GF(2^n).

3 NORMALNE BAZE

V tem poglavju se bomo posvetili normalnim bazam. Najprej si bomo ogledali osnovne pojme in aritmetiko v normalnih bazah, nato še porazdelitev normalnih elementov.

3.1 Osnovni pojmi

Naj bo p praštevilo in $q = p^m$, kjer je $m \geq 1$. GF(q) naj bo končen obseg s q elementi in GF(q^n) njegova n razsežna razširitev. Normalne baze končnega obsega GF(q^n) so posebna družina baz za vektorski prostor GF(q^n) nad GF(q).

Definicija 3.1 *Podmnožica N vektorskega prostora* GF(q^n) *nad* GF(q) *je* **normalna baza**, *če velja:*

1. *N je baza za vektorski prostor* GF(q^n) *nad* GF(q),
2. *$N = \{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ za nek $\alpha \in$* GF(q^n).

Pravimo, da α generira normalno bazo N oziroma je **normalni element** obsega GF(q^n). V obsegu je lahko več normalnih elementov, vendar pa α in α^{q^i} za vsak $i \in \{0, \ldots, n-1\}$ generirata enako normalno bazo, saj v obsegu GF(q^n) velja $\alpha^{q^n} = \alpha$. Zdaj bomo navedli izrek o obstoju normalnih baz, katerega dokaz se nahaja v Menezes et al. [2, 4.3].

Izrek 3.1 *V vsakem končnem obsegu* GF(q^n) *obstaja normalna baza.* □

Za vsak $i, j \in \{0, 1, \ldots, n-1\}$ je produkt $\alpha_i \alpha_j$ linearna kombinacija elementov $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ s koeficienti iz GF(q). Velja:

$$\alpha_0 \alpha_i = \sum_{j=0}^{n-1} t_{ij} \alpha_j, \ t_{ij} \in \mathrm{GF}(q)$$

in

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

kjer je $T = (t_{ij})$ matrika dimenzije $n \times n$ nad GF(q). Matriko T imenujemo **multiplikacijska tabela** normalne baze N ali multiplikacijska tabela normalnega elementa α. Število neničelnih elementov v T imenujemo **kompleksnost** normalne baze N in ga označimo s c_N. Obstaja mnogo baz vektorskega prostora GF(q^n) nad GF(q). Za nekatere baze so ustrezne multiplikacijske tabele T preprostejše kot za druge, v smislu, da imajo manj neničelnih elementov. Tako si lahko z izborom normalne baze nizke kompleksnosti poenostavimo množenje.

3.2 Aritmetika normalnih baz

Oglejmo si najprej seštevanje. Naj bo $N = \{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ normalna baza obsega GF(q^n). Potem lahko vsak element A iz GF(q^n) zapišemo kot

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

kjer je $a_i \in$ GF(q) za vsak $i \in \{0, \ldots, n-1\}$. Poljuben element A iz GF(q^n) lahko zapišemo kot $A = (a_0, a_1, \ldots, a_{n-1})$. Seštevanje je kar seštevanje po komponentah.

Nadaljevali bomo s potenciranjem. Element A^q ima pripadajoči vektor $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$. Koordinate A^q so torej le v desno ciklično zamaknjene koordinate vektorja A in zato je potenciranje učinkovito. To je zelo pomembno pri implementaciji kriptosistemov, kot so Diffie-Hellmanova izmenjava ključev ali ElGamalov kriptosistem, kjer je potrebno računati visoke potence elementov v končnih obsegih. Tudi q-korenjenje v normalnih bazah je enostavno, kajti koren elementa A je tisti element, ki ga dobimo s cikličnim premikom koeficientov elementa A v levo.

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

$$\alpha_i \alpha_j = \sum_{k=0}^{n-1} t_{i-j,k-j} \alpha_k,$$

kjer je $T = (t_{ij})$ multiplikacijska tabela normalne baze N. Potem je

$$c_k = \sum_{i,j=0}^{n-1} a_i b_j t_{i-j,k-j}, 0 \leq k \leq n-1.$$

Opisali bomo algoritem invertiranja, ki najprej privzame posebno obliko eksponenta n, nato pa njegovo posplošitev na poljubno naravno število. Najprej si bomo ogledali računanje inverza v primeru, ko je 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 $A^{-1} = (A^{2^{2^r}-1})^2$. Nato lahko zapišemo $2^{2^r}-1$ kot

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

Zdaj lahko opišemo algoritem, ki vrne multiplikativni inverz elementa $A \in \mathrm{GF}(2^n)^*$, kjer je $n = 2^r + 1$.

Algoritem
$C = A$
for $i = 0 : r - 1$ **do**
  $D = C^{2^{2^i}}$
  $C = C \cdot D$
end
$A^{-1} = C^2$

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 lahko posplošimo na vsako vrednost eksponenta n. Najprej zapišemo $n - 1 = \sum_{i=1}^{t} 2^{k_i}$, kjer velja $k_1 > k_2 > \ldots > k_t$. Ker je $A^{-1} = (A^{2^{n-1}-1})^2$, lahko inverz elementa A zapišemo kot

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

Pri izračunu $A^{2^{2^{k_1}}-1}$ potrebujemo tudi vse ostale vrednosti $A^{2^{2^{k_i}}-1}$ za $k_i < k_1$. Naj bo teža n število enic v binarni predstavitvi števila n in označimo jo z $W(n)$. V zgornjem računu je potrebno izvesti $\lfloor \log_2(n-1) \rfloor + W(n-1) - 1$ množenj v $\mathrm{GF}(2^n)$ in $n-1$ cikličnih zamikov.

3.2.1 Primer

Poiskali bomo inverz elementa v normalni bazi obsega $\mathrm{GF}(2^{173})$. Uporabili bomo metodo kvadriraj in množi, predstavljeno zgoraj. Naš 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 inverz $A^{-1} = A^{2^{173}-2} = (A^{2^{172}-1})^2$ elementa $A \in \mathrm{GF}(2^{173})$.

$$A^{2^2-1} = A^2 \cdot A$$
$$A^{2^4-1} = (A^3)^{2^2} \cdot A^3$$
$$A^{2^8-1} = (A^{15})^{2^4} \cdot A^{15}$$
$$A^{2^{16}-1} = (A^{255})^{2^8} \cdot A^{255}$$
$$A^{2^{32}-1} = (A^{65535})^{2^{16}} \cdot A^{65535}$$
$$A^{2^{64}-1} = (A^{4294967295})^{2^{32}} \cdot A^{4294967295}$$
$$A^{2^{128}-1} = (A^{18446744073709551615})^{2^{64}} \cdot A^{18446744073709551615}$$
$$A^{-1} = \left[(A^{2^4-1})\left((A^{2^8-1})\left[(A^{2^{32}-1})(A^{2^{128}-1})^{2^{32}}\right]^{2^8}\right)^{2^4}\right]^2.$$

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.

3.3 Porazdelitev normalnih elementov

V tem razdelku si bomo ogledali, kako so normalni elementi porazdeljeni po prostoru. Potrebovali bomo nekaj konceptov linearne algebre.

3.3.1 Algebraične osnove

Naj bo T linearna transformacija na končno dimenzionalnem vektorskem prostoru V nad obsegom F. Polinom $f(x) = \sum_{i=0}^{m} a_i x^i \in F[x]$ *anihilira* T, če velja $a_m T^m + \ldots + a_1 T + a_0 I = 0$, 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.

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 kot $Z(u,T)$. Če je $Z(u,T) = V$, potem u imenujemo *ciklični vektor prostora V za T*.

Za vsak vektor $u \in V$ monični polinom $g(x) \in F[x]$ najmanjše stopnje, da velja $g(T)u = 0$, imenujemo *T-red elementa u* ali *minimalni polinom elementa u*. 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 u (tak h, da je $h(T)u = 0$), tudi minimalni in karakteristični polinom za T.

Definicija 3.2 *Frobeniusova preslikava je linearna transformacija obsega* $\mathrm{GF}(q^n)$*, definirana kot* $\sigma : \eta \to \eta^q,\ \eta \in \mathrm{GF}(q^n)$.

Trditev 3.2 *Minimalni in karakteristični polinom preslikave* σ *sta identična, oba enaka* $x^n - 1$.

Dokaz : Vemo, da je $\sigma^n\eta = \eta^{q^n} = \eta$ za vsak $\eta \in \mathrm{GF}(q^n)$. Torej je $\sigma - I = 0$. Dokažimo, da je $x^n - 1$ minimalni polinom za σ.

Naj bo $f(x) = \sum_{i=0}^{n-1} f_i x^i \in \mathrm{GF}(q)[x]$ polinom stopnje manj od n, ki anihilira σ; torej tak, da velja $\sum_{i=0}^{n-1} f_i\sigma^i = 0$. Potem za vsak $\eta \in \mathrm{GF}(q^n)$ 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 $\mathrm{GF}(q^n)$. Torej je $x^n - 1$ minimalni polinom preslikave σ.

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

3.3.2 Normalni elementi

Naj bo $\alpha \in \mathrm{GF}(q^n)$ normalni element. Potem so $\alpha, \sigma\alpha, \sigma^2\alpha, \ldots, \sigma^{n-1}\alpha$ linearno neodvisni nad $\mathrm{GF}(q)$ in zato ne obstaja polinom stopnje manj kot n, ki anihilira α. Od tod sledi, da mora biti σ-red elementa α enak $x^n - 1$ in α ciklični vektor prostora $\mathrm{GF}(q^n)$ nad $\mathrm{GF}(q)$ za σ. Torej je $\alpha \in \mathrm{GF}(q^n)$ normalni element nad $\mathrm{GF}(q)$ natanko tedaj, ko je $\mathrm{Ord}_{\alpha,\sigma}(x) = x^n - 1$.

Naj bo $n = n_1p^e$, kjer je $\gcd(p, n_1) = 1$ in $e \geq 0$. Označimo $p^e = t$. Predpostavimo, da ima $x^n - 1$ v $\mathrm{GF}(q)[x]$ naslednjo faktorizacijo

$$x^n - 1 = (\varphi_1(x)\varphi_2(x)\ldots\varphi_r(x))^t, \tag{6}$$

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

$$\Phi_i(x) = (x^n - 1)/\varphi_i(x) \ za\ i = 1, 2, \ldots, r.$$

Izrek 3.3 *Element* $\alpha \in \mathrm{GF}(q^n)$ *je normalni element natanko tedaj, ko velja*

$$\Phi_i(\sigma)\alpha \neq 0 \ za\ i = 1, 2, \ldots, r.$$

Dokaz : Po definiciji je α normalen element nad GF(q) natanko tedaj, ko so $\alpha_i = \alpha^{q^i} = \sigma^i(\alpha),\ i \in \{0, 1, \ldots, n-1\}$ linearno neodvisni nad GF(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 izrek velja. □

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

Posledica 3.4 *Naj bo $n = p^e$. Potem je $\alpha \in \mathrm{GF}(q^n)$ normalni element nad* GF(q)*, če in samo če velja* $\mathrm{Tr}_{q^n|q}(\alpha) \neq 0$.

Dokaz : Ko je $n = p^e$, je $x^n - 1 = (x-1)^n$. Torej je v faktorizaciji (6) r enak 1, $\varphi_1(x) = x - 1$ in $\Phi_1(x) = x^{n-1} + \ldots + x + 1$. Po izreku (3.3) je $\alpha \in \mathrm{GF}(q^n)$ normalni element nad GF(q), če in samo če velja $\Phi_1(\sigma)\alpha = \sum_{i=0}^{n-1} \alpha^{q^i} = \mathrm{Tr}_{q^n|q}(\alpha) \neq 0$. □

4 OPTIMALNE NORMALNE BAZE

V tem poglavju bomo najprej povedali, kaj so optimalne normalne baze, nato se bomo posvetili njihovi konstrukciji in povezavi s polinomskimi bazami, na koncu pa bomo navedli izrek, ki nam pove, kdaj obstajajo optimalne normalne baze.

Normalne baze nizke kompleksnosti so zaželjene v implementaciji končnih obsegov. Omenili smo že, da z optimalnimi normalnimi bazami pospešimo množenje. Ko smo obravnavali množenje v končnih obsegih, smo definirali multiplikacijsko tabelo T normalne baze $N = \{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$. To je tista $n \times n$ matrika, katere elementi so koeficienti v produktu

$$\alpha\alpha_i = \sum_{j=0}^{n-1} t_{ij}\alpha_j,\ 0 \leq i \leq n-1,\ t_{ij} \in \mathrm{GF}(q). \tag{7}$$

Kot smo že povedali, število neničelnih elementov v matriki $T = (t_{ij})$ imenujemo kompleksnost normalne baze N in označimo s c_N.

Izrek 4.1 *Spodnja meja kompleksnosti za vsako normalno bazo obsega* GF(q^n) *je* $2n - 1$.

Dokaz : Naj bo $N = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ normalna baza obsega GF(q^n). Potem je $b = \sum_{i=0}^{n-1} \alpha_i = \mathrm{Tr}(\alpha) \in \mathrm{GF}(q)$. Če seštejemo enačbe (7) in primerjamo koeficente pri α_k, dobimo

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

Ker je $\alpha \neq 0$ in je $\{\alpha\alpha_i \mid 0 \leq i \leq n-1\}$ tudi baza, je matrika $T = (t_{ij})$ obrnljiva. Torej je za vsak j vsaj en neničeln t_{ij}. Za vsak $j \neq 0$ morata biti vsaj dva neničelna koeficienta t_{ij}, da se stolpec matrike T sešteje v 0. Torej obstaja vsaj $2n-1$ neničelnih elementov v T. 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, s koeficienti, ki so si aditivni inverzi. □

Definicija 4.1 *Normalna baza je* **optimalna**, *če je* $c_N = 2n-1$.

4.1 Konstrukcija optimalnih normalnih baz

Predstavili bomo konstrukcijo, ki so jo zasnovali Mullin, Onyszchuk, Vanstone in Wilson. Najprej pa bomo navedli izrek, iz katerega sledita konstrukciji optimalnih normalnih baz dveh različnih tipov. Za dokaz izreka glej npr. Gao, [3, 4.1].

Izrek 4.2 *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 $\mathrm{GF}(q^{nk})$ 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 $\mathrm{GF}(q^n)$ nad $\mathrm{GF}(q)$ s kompleksnostjo največ $(k+1)n-k$ ali $kn-1$, če je $k \equiv 0 \bmod p$, kjer je p karakteristika obsega $\mathrm{GF}(q)$.* □

Izrek 4.3 *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 korenov enote linearno neodvisnih in tvorijo optimalno normalno bazo obsega $\mathrm{GF}(q^n)$ nad $\mathrm{GF}(q)$.*

Dokaz : Izrek sledi iz (4.2) kot poseben primer, ko je $k = 1$. □

Oglejmo si multiplikacijsko tabelo te baze. Naj bo α $(n+1)$-i primitivni koren enote. Potem je α koren polinoma $x^n + \ldots + x + 1$. Ker pa je $n+1$ praštevilo, $n+1$ deli $q^n - 1$ in vsi $(n+1)$-i koreni enote so v $\mathrm{GF}(q^n)$. Ker je q primitiven v $\mathbb{Z}_{n+1}$, obstaja n različnih konjugirank 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 $\mathrm{GF}(q^n)$ nad $\mathrm{GF}(q)$. Velja

$$\alpha\alpha^i = \alpha^{i+1} \in N,\ 1 \leq i < n$$

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 T, 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 T so seveda enaki 0. Optimalno normalno bazo, dobljeno s to konstrukcijo, imenujemo **optimalna normalna baza tipa I**.

Izrek 4.4 *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 $\mathrm{GF}(2^n)$ nad $\mathrm{GF}(2)$, kjer je γ primitivni $(2n+1)$-i koren enote.

Dokaz : Izrek sledi iz (4.2) kot poseben primer, ko je $k = 2$ in $q = 2$. □

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

$$\gamma^{n+1} + \gamma^{-(n+1)} = \gamma^n + \gamma^{-n}. \tag{8}$$

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 $\mathrm{GF}(2^n)$. Matrika T, 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 GF(2). Obstajajo preprosta pravila za preverjanje hipotez iz izrekov 4.3 in 4.4. Strnimo jih.

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 $\mathrm{GF}(q^n)$.

Trditev 4.5 *Naj bo α neka ničla nekega nerazcepnega polinoma f stopnje n iz $\mathrm{GF}(q)[x]$. Množica $P = \{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ je baza vektorskega prostora $\mathrm{GF}(q^n)$ nad $\mathrm{GF}(q)$, 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 $\mathrm{GF}(q)[x]$, ki ima stopnjo manjšo od n. Zato so vsi elementi P linearno neodvisni. Ker je moč P enaka n, je P res baza. □

Množica P se imenuje **polinomska baza** vektorskega prostora $\mathrm{GF}(q^n)$ nad $\mathrm{GF}(q)$. Ker je $\mathrm{GF}(q)$ obseg, je $\mathrm{GF}(q)[x]$ glavni kolobar. Ideal, generiran z nerazcepnim elementom, je v glavnem kolobarju vedno maksimalen. Za nerazcepni polinom f iz definicije polinomske baze je faktorski kolobar $\mathrm{GF}(q)[x]/f(x)$ obseg. Moč tega obsega je $q^{\deg(f)} = q^n$, torej je ta obseg izomorfen obsegu $\mathrm{GF}(q^n)$. Povzemimo zgornje ugotovitve v naslednjo trditev, za dokaz glej Vidav [1, 9.1].

Trditev 4.6 *Naj bo $\mathrm{GF}(q)$ končen obseg in $\mathrm{GF}(q^n)$ njegova razširitev stopnje n. Potem v $\mathrm{GF}(q)[x]$ obstaja nerazcepen polinom $f(x)$ stopnje n in je $\mathrm{GF}(q^n) \cong \mathrm{GF}(q)[x]/f(x)$ obseg, kjer je $\mathrm{GF}(q)[x]/f(x)$ obseg polinomov nad obsegom $\mathrm{GF}(q)$, reduciranih po modulu polinoma $f(x)$.* □

4.2.1 Optimalne normalne baze tipa I

Ogledali si bomo minimalne polinome generatorjev optimalnih normalnih baz. Minimalni polinom generatorja optimalne normalne baze tipa I je kar $f(x) = x^n + \ldots + x + 1$, njegovo nerazcepnost pa nam zagotovi naslednji izrek, glej Vidav [1, 9.10].

Izrek 4.7 *Polinom $x^n + \ldots + x + 1$ je nerazcepen nad* GF(q) *natanko tedaj, ko je $n + 1$ praštevilo in q primitiven v $\mathbb{Z}_{n+1}$.* □

4.2.2 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 $f_n(x) = \prod_{j=1}^{n}(x - \gamma^j - \gamma^{-j}) = \sum_{i=0}^{n} m_i x^i$, $m_i \in$ GF(2). Če veljajo pogoji izreka (4.4), je polinom $f(x)$ minimalni polinom elementa $\alpha = \gamma + \gamma^{-1}$. Poiskali bomo eksplicitno formulo za $f_n(x)$ 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 (8) sledi, da velja

$$(\gamma^j)^n + (\gamma^j)^{-n} = (\gamma^j)^{n+1} + (\gamma^j)^{-(n+1)},\ j \in \{0, 1, \ldots, n\}. \tag{9}$$

Uporabili bomo Waringovo formulo (glej [12], [14, 1.3]):

$$A^n + B^n = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-1)^i (A+B)^{n-2i}(AB)^i,\ A, B \in \mathrm{GF}(2^n). \tag{10}$$

Iz (10) sledi, da za vsako naravno število k velja

$$(\gamma^j)^k + (\gamma^{-j})^k = (\gamma^j)^k + (\gamma^j)^{-k} = \sum_{i=0}^{\lfloor k/2 \rfloor} \frac{k}{k-i}\binom{k-i}{i}(-1)^i (\gamma^j + \gamma^{-j})^{k-2i}. \tag{11}$$

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

$$D_k(x) = \sum_{i=0}^{\lfloor k/2 \rfloor} \frac{k}{k-i}\binom{k-i}{i}(-1)^i x^{k-2i}. \tag{12}$$

Izkazalo se je, da so Dicksonovi polinomi pomembni tako v teoretični kot tudi v uporabni matematiki. Več o Dicksonovih polinomih se nahaja v [13]. Iz (11) in (12) sledi

$$D_k(\gamma^j + \gamma^{-j}) = (\gamma^j)^k + (\gamma^j)^{-k}. \tag{13}$$

Oglejmo si zdaj polinom $D_{n+1}(x) - D_n(x)$. Ta je po (13) enak

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

Potem iz (9) sledi, da je $\gamma^j + \gamma^{-j}$ za $j \in \{0, 1, \ldots, n\}$, koren polinoma $D_{n+1}(x) - D_n(x)$. Po definiciji mora biti $D_{n+1}(x) - D_n(x)$ stopnje $n+1$ in zato ima $n+1$ ničel. Ker so vsi $\gamma^j + \gamma^{-j}$ različni za $j \in \{0, 1, \ldots, n\}$, 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 4.8 *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 $n+1$.

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

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

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

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

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

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

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

Opomnimo še, da je $f_n(x)$ nerazcepen nad $\mathrm{GF}(q)$ natanko tedaj, ko je multiplikativna grupa $\mathbb{Z}_{2n+1}^*$ generirana z elementoma q in -1 ter $f_n(x)$ 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 $A \in \mathrm{GF}(2^n)$ 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.

Definicija 4.2 *Naj bo N optimalna normalna baza obsega $\mathrm{GF}(q^n)$ nad $\mathrm{GF}(q)$ in $a \in \mathrm{GF}(q)$. Potem je tudi $aN = \{a\alpha : \alpha \in N\}$ optimalna normalna baza obsega $\mathrm{GF}(q^n)$ nad $\mathrm{GF}(q)$. 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 (4.3) in (4.4). Leta 1992 sta Gao in Lenstra dokazala naslednji izrek, ki nam pove, kdaj obstajajo optimalne normalne baze.

Izrek 4.9 *Naj bo* $N = \{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ *optimalna normalna baza obsega* $\mathrm{GF}(q^n)$ *nad* $\mathrm{GF}(q)$. *Naj bo* $b = \mathrm{Tr}_{q^n|q}(\alpha)$ *sled elementa* α *v* $\mathrm{GF}(q)$. *Potem velja eden izmed naslednjih pogojev:*

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

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

Za dokaz izreka glej Gao [3, 4.2], za obširen dokaz nekoliko splošnejše verzije gornjega izreka pa Gao, Lenstra [4].

5 NADALJNI RAZISKOVALNI PROBLEMI

V prejšnjih poglavjih smo si ogledali normalne baze, optimalne normalne baze ter podali konstrukciji le-teh. V tem poglavju bomo izpostavili nekaj problemov, ki bi si zaslužili nadaljne raziskave. Za zaključek bomo podali še Lenstrov algoritem za konstrukcijo normalnih elementov.

Za dan nerazcepen polinom stopnje n nad $\mathrm{GF}(q)$ znamo deterministično skonstruirati normalno bazo obsega $\mathrm{GF}(q^n)$ nad $\mathrm{GF}(q)$ v polinomskem času. Tako problem konstrukcije normalne baze zreduciramo na naslednji problem.

Problem 1 *Poiskati deterministični algoritem polinomske časovne zahtevnosti (v* n *in* $\log n$*) za konstrukcijo nerazcepnega polinoma stopnje* n *v* $\mathrm{GF}(q)[x]$, *za dan končni obseg* $\mathrm{GF}(q)$ *in dano naravno število* n.

Ta problem je pomemben v teoriji končnih obsegov in računalniški algebri.

V kriptografiji je pomembno poznati ali primitiven element ali pa element visokega multiplikativnega reda v $\mathrm{GF}(2^n)$. V splošnem imajo generatorji optimalnih normalnih baz tipa II visok multiplikativni red in so dokaj pogosto primitivni. Ta fenomen je opazil Rybowicz.

Problem 2 *Naj bo* n *pozitivno število in* γ $(2n+1)$*-i primitivni koren enote v neki razširitvi obsega* $\mathrm{GF}(2)$. *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 $\mathrm{GF}(2^n)$. Naslednji problem je na nek način nasprotje zgornjega.

Problem 3 *Naj bo α element v neki razširitvi obsega* GF(2). *Za dan multiplikativni red α določi multiplikativni red elementa γ, kjer je $\gamma + \gamma^{-1} = \alpha$.*

Za implementacijo aritmetike v končnih obsegih želimo normalne baze čim nižje kompleksnosti. V prejšnjem poglavju smo določili vse optimalne normalne baze v končnih obsegih in videli, da vsi končni obsegi ne vsebujejo optimalnih normalnih baz. Naravno se poraja naslednje vprašanje.

Problem 4 *Recimo, da v obsegu* GF(q^n) *ne obstaja optimalna normalna baza. Kakšna je potem minimalna kompleksnost normalne baze obsega* GF(q^n) *in kako konstruirati normalno bazo minimalne kompleksnosti?*

Računalniški eksperimenti nakazujejo, da ne obstajajo normalne baze kompleksnosti med $2n-1$ in $3n-3$, kar pomeni, da je najmanjša možna kompleksnost normalne baze, ki ni optimalna, $3n-3$. Zanimivo bi bilo dokazati, da to res drži.

Za konec si bomo ogledali, kako deterministično skonstruiramo normalni element končnega obsega v polinomskem času.

5.1 Lenstrov algoritem

Opisali bomo Lenstrov algoritem, pri katerem moramo poiskati σ-red $\mathrm{Ord}_\theta(x)$ poljubnega elementa $\theta \in \mathrm{GF}(q^n)$. Stopnja $\mathrm{Ord}_\theta(x)$ je tak $k > 0$, da $\sigma^k\theta$ pripada linearni ogrinjači $\{\sigma^i\theta \mid 0 \le i < k\}$. Če je $\sigma^k\theta = \sum_{i=0}^{k-1} c_i\sigma^i\theta$ za ta k, potem je $\mathrm{Ord}_\theta(x) = x^k - \sum_{i=0}^{k-1} c_i x^i$. Torej lahko $\mathrm{Ord}_\theta(x)$ izračunamo v polinomskem času.

Za opis Lenstrovega algoritma bomo potrebovali dve lemi.

Lema 5.1 *Naj bo $\theta \in \mathrm{GF}(q^n)$, $\mathrm{Ord}_\theta(x) \neq x^n - 1$ in $g(x) = (x^n-1)/\mathrm{Ord}_\theta(x)$. Potem obstaja tak $\beta \in \mathrm{GF}(q^n)$, da je*

$$g(\sigma)\beta = \theta. \tag{14}$$

Dokaz : Naj bo γ normalni element obsega GF(q^n) nad GF(q). Potem obstaja tak $f(x) \in \mathrm{GF}(q)[x]$, 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 $\mathrm{Ord}_\theta(x)f(x)$ deljiv z $x^n - 1$ in zato $f(x)$ deljiv z $g(x)$. Naj bo $f(x) = g(x)h(x)$. Potem je $g(\sigma)(h(\sigma)\gamma) = \theta$. To dokazuje, da je $\beta = h(\sigma)\gamma$ rešitev enačbe (14). □

Lema 5.2 *Naj bo $\theta \in \mathrm{GF}(q^n)$, $\mathrm{Ord}_\theta(x) \neq x^n - 1$ in $g(x) = (x^n-1)/\mathrm{Ord}_\theta(x)$. Predpostavimo, da obstaja rešitev β enačbe (14), tako da je stopnja $\mathrm{Ord}_\beta(x)$ manjša ali kvečjemu enaka stopnji $\mathrm{Ord}_\theta(x)$. Potem obstaja tak neničeln element $\eta \in \mathrm{GF}(q^n)$, da je*

$$g(\sigma)\eta = 0. \tag{15}$$

Za tak η velja

$$\deg(\mathrm{Ord}_{\theta+\eta}(x)) > \deg(\mathrm{Ord}_{\theta}(x)). \tag{16}$$

Dokaz : Naj bo γ normalni element obsega $\mathrm{GF}(q^n)$ nad $\mathrm{GF}(q)$. Potem je $\eta = \mathrm{Ord}_\theta(\sigma)\gamma \neq 0$ rešitev enačbe (15). Dokazali bomo, da drži (16) za vsako neničelno rešitev η enačbe (15).

Iz (14) sledi, da $\mathrm{Ord}_\theta(x)$ deli $\mathrm{Ord}_\beta(x)$, torej nam hipoteza $\deg(\mathrm{Ord}_\beta(x)) \leq \deg(\mathrm{Ord}_\theta(x))$ implicira, da $\mathrm{Ord}_\beta(x) = \mathrm{Ord}_\theta(x)$. Zato mora biti polinom $g(x)$ tuj $\mathrm{Ord}_\theta(x)$. Ker $\mathrm{Ord}_\eta(x)$ deli $g(x)$, 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 (16) sledi iz $\eta \neq 0$. □

Zdaj lahko opišemo Lenstrov algoritem, ki vrne normalni element obsega $\mathrm{GF}(q^n)$ nad $\mathrm{GF}(q)$.

Algoritem
1. Vzamemo poljuben element $\theta \in \mathrm{GF}(q^n)$ in določimo $\mathrm{Ord}_\theta(x)$.
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 linearnih enačb $g(\sigma)\beta = \theta$ za β.
4. Določimo $\mathrm{Ord}_\beta(x)$. Če je stopnja $\mathrm{Ord}_\beta(x)$ večja od stopnje $\mathrm{Ord}_\theta(x)$, potem zamenjamo θ z β in se vrnemo na **2**. korak. V nasprotnem primeru pa poiščemo tak neničeln element η, da velja $g(\sigma)\eta = 0$, zamenjamo θ s $\theta + \eta$, določimo red novega θ ter se vrnemo na **2**. korak.

Pravilnost algoritma temelji na lemah 5.1 in 5.2, kajti z vsako zamenjavo θ se stopnja $\mathrm{Ord}_\theta(x)$ poveča vsaj za 1.

Literatura

[1] I. Vidav: *Algebra*, DMFA - založništvo, 2003

[2] A. J. Menezes, I. F. Blake, S. Gao, R. C. Mullin, S. A. Vanstone, T. Yaghoobian: *Applications of Finite Fields*, Kluwer Academic Publishers, 1993

[3] S. Gao: *Normal Bases over Finite Fields*, doktorska disertacija, University of Waterloo, 1993

[4] S. Gao, H. V. Lenstra: *Optimal Normal Bases*, Designs, Codes and Cryptography 2, 1992

[5] D. Hachenberger: *Finite Fields: Normal Bases and Completely Free elements*, Kluwer Academic Publishers, 1997

[6] A. J. Menezes, P. van Oorschot, S. Vanstone: *Handbook of Applied Cryptography*, CRC Press, 1996

[7] D. R. Stinson: *Cryptography: Theory and Practice*, CRC Press, 2002

[8] J. Barbič: *Schoofov algoritem*, diplomsko delo, Fakulteta za matematiko in fiziko, Univerza v Ljubljani, 2000

[9] V. Nastran: *Baze binarnih končnih obsegov*, diplomsko delo, Fakulteta za matematiko in fiziko, Univerza v Ljubljani, 2003

[10] J. Guajardo: *Itoh-Tsujii Inversion Algorithm*, Communication Security Group, Ruhr-Universität Bochum, 2003

[11] http://grouper.ieee.org/groups/1363/passwdPK/draft.html

[12] E. W. Weisstein: *CRC concise encyclopedia of mathematics*, CRC, 1999

[13] R. Lidl, G. Mullen, G. Turnwald: *Dickson Polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics, Vol. 65, Longman Scientific and Technical, 1993

[14] R. Lidl, H. Niederreiter: *Finite Fields*, Cambridge University Press, 1984