13. BAIGTINIŲ KŪNŲ ELEMENTŲ REIŠKIMAS

Yra keletas baigtinių kūnų elementų reiškimo būdų. Pirmasis iš jų remiasi tuo, kad faktoržiedis $GF(q)[x]/_{(f(x))}$, kai $f(x)$ yra neredukuojamas polinomas virš $GF(q)$, – kūnas. Antrasis – kad baigtinio kūno $GF(q)$ multiplikacinė grupė $GF(q)^*$ yra ciklinė ir kiekvienas nenulinis šio kūno elementas yra primityviojo elemento laipsnis. Pirmuoju atveju kūno elementai – tai polinomai virš $GF(q)$ ir todėl sudėties veiksmas šiems elementams atliekamas labai paprastai, o štai sandaugai suskaičiuoti reikia daug darbo. Antruoju atveju – viskas atvirkščiai: sandaugos veiksmas ciklinės grupės elementams – tai paprasčiausi veiksmai su laipsnio rodikliais, o štai šių elementų sudėtis reikalauja nemažai skaičiavimų. Laimei, yra glaudus abiejų reiškimo būdų ryšys, pateikiamas indeksų lentele. Pateiksime ir trečiąjį baigtinio kūno elementų reiškimo būdą, jungiantį pirmųjų dviejų tiek teigiamas, tiek neigiamas savybes.

1. Tegu $GF(q)$, $q = p^n$ yra baigtinis kūnas, p – pirminis. Tada egzistuoja (žr. 9.7 teiginį) neredukuojamas virš $GF(p)$ n-ojo laipsnio polinomas $f(x)$ ir

$$GF(q) = GF(p)[x]/_{(f(x))} = \{r(x) + (f(x)) \mid \deg\ r(x) < n\}.$$

Šiuo atveju kūno $GF(q)$ elementus tapatiname su ne aukštesnio negu $n-1$ laipsnio polinomais virš $GF(p)$, o abi operacijos su šiais polinomais atliekamos mod $f(x)$.

Tegu a yra polinomo $f(x)$ šaknis kuriame nors kūno $GF(p)$ plėtinyje. Iš 8.11 teiginio žinome, kad $GF(q)$ yra izomorfiškas $\big(GF(p)\big)(a)$ ir todėl

$$GF(q) = \{r(a) \mid r(x) \in GF(p)[x],\ f(a) = 0\}.$$

10.1 pavyzdys. Norint užrašyti kūno $GF(16) = GF(2^4)$ elementus, prireiks neredukuojamo virš $GF(2)$ ketvirtojo laipsnio polinomo. Visus tokius polinomus galima rasti išbraukus iš visų 4-ojo laipsnio polinomų virš $GF(2)$ sąrašo redukuojamus polinomus. Iš viso 4-ojo laipsnio polinomų virš $GF(2)$ yra $2^4 = 16$.

Redukuojamieji polinomai $f(x) = \alpha x^4 + \beta x^3 + \gamma x^2 + \delta x + e,\ \ \alpha, \beta, \gamma, \delta, e \in GF(2)$, yra vieno iš pavidalų

$$\begin{aligned}
&f(x) = \big(\alpha_0 + \alpha_1 x + \alpha_2 x^2 + 1 \cdot x^3\big)\big(\beta_0 + x\big),\\
&f(x) = \big(\gamma_0 + \gamma_1 x + x^2\big)\big(\delta_0 + \delta_1 x + x^2\big),\\
&\alpha_0, \alpha_1, \alpha_2, \beta_0, \gamma_0, \gamma_1, \delta_0, \delta_1 \in GF(2) = \{0, 1\}.
\end{aligned}$$

Kai $e = 0$, t.y. bent vienas elementas iš porų α_0, α_1 arba γ_0, γ_1 lygus nuliui, tai polinomas $f(x)$ yra redukuojamas. Tegu dabar $\alpha_0, \alpha_1, \gamma_0, \gamma_1$ – nenuliniai elementai.

Sudauginę polinomus

$$\begin{aligned}
&\big(x^3 + 1\big)\big(x + 1\big) = x^4 + x^3 + x + 1,\\
&\big(x^3 + x + 1\big)\big(x + 1\big) = x^4 + x^3 + x^2 + 1,\\
&\big(x^3 + x^2 + 1\big)\big(x + 1\big) = x^4 + x^2 + x + 1,\\
&\big(x^3 + x^2 + x + 1\big)\big(x + 1\big) = x^4 + 1,\\
&\big(x^2 + 1\big)\big(x^2 + 1\big) = x^4 + 1,\\
&\big(x^2 + 1\big)\big(x^2 + x + 1\big) = x^4 + x^3 + x + 1,\\
&\big(x^2 + x + 1\big)\big(x^2 + x + 1\big) = x^4 + x^2 + 1,
\end{aligned}$$

matome, kad tik trys polinomai $f_1(x) = x^4 + x + 1$, $f_2(x) = x^4 + x^3 + 1$ ir $f_3(x) = x^4 + x^3 + x^2 + x + 1$ yra neredukuojami virš $GF(2)$.

Pasirinkime vieną iš jų, pavyzdžiui, $f(x) = x^4 + x^3 + 1$. Tada

$$GF(2)[x]\big/\big(x^4 + x^3 + 1\big) = GF(16) = \big(GF(2)\big)(a);$$

čia a – polinomo $f(x)$ šaknis. Išvardysime šio kūno elementus.

Konstantos: 0, 1.

Tiesiniai elementai: a, $a + 1$.

Kvadratiniai elementai: a^2, $a^2 + 1$, $a^2 + a$, $a^2 + a + 1$.

Kubiniai elementai: a^3, $a^3 + 1$, $a^3 + a$, $a^3 + a + 1$, $a^3 + a^2$, $a^3 + a^2 + 1$, $a^3 + a^2 + a$, $a^3 + a^2 + a + 1$.

Taip išreikštų kūno $GF(16)$ elementų sudėtis – tai ne didesnio kaip 3-ojo laipsnio polinomų sudėtis virš $GF(2)$. Pavyzdžiui,

$$\big(a^3 + a + 1\big) + \big(a^2 + a\big) = a^3 + a^2 + 1 \qquad (2 = 0).$$

Dauginti kūno $GF(16)$elementus sunkiau, nes visą laiką reikia atsižvelgti į tai, kad $f(a) = a^4 + a^3 + 1 = 0$, t.y. $a^4 = a^3 + 1$ ($-1 = 1$ kūne $GF(2)$). Pavyzdžiui,

$$\begin{aligned} a^7 &= a^4 \cdot a^3 = \big(a^3 + 1\big)a^3 = a^6 + a^3 = a^4 \cdot a^2 + a^3 \\ &= \big(a^3 + 1\big)a^2 + a^3 = a^5 + a^2 + a^3 = a^4 a + a^2 + a^3 \\ &= \big(a^3 + 1\big)a + a^2 + a^3 = a^4 + a + a^2 + a^3 = a^3 + 1 + a + a^2 + a^3 \\ &= 1 + a + a^2. \end{aligned}$$

2. Tegu a yra primityvusis kūno $GF(q)$ elementas. Tada

$$GF(q) = \{0, 1 = a^0, a, \ldots, a^{q-2}\}.$$

Dviejų taip išreikštų kūno $GF(q)$ elementų sandauga apibrėžta lygybe

$$a^r \cdot a^s = a^{r+s \,(\mathrm{mod}\, q-1)}.$$

Šių elementų sudėtis apibrėžiama primityviajam elementui a parenkant minimalųjį polinomą $m(x)$ ir kiekvienam a laipsniui priskiriant vienintelį elementą

$$\alpha_0 + \alpha_1 a + \ldots + \alpha_{n-1} a^{n-1}, \quad n = \deg\, m(x).$$

Tada elementų sudėtis apibrėžiama kaip 10.1 pavyzdyje.

10.2 pavyzdys. Tegu $f(x) = x^4 + x^3 + 1$, kaip ir 10.1 pavyzdyje, neredukuojamas polinomas virš $GF(2)$. Tegu a – polinomo $f(x)$ šaknis. Elemento a eilė $\mathrm{ord}_{GF(16)^*}(a)$ kūno $GF(16)$ multiplikacinėje grupėje yra lygi grupės $GF(16)^*$ eilės $\big|GF(16)^*\big| = 16 - 1 = 15$ dalikliui. Taigi

$$\begin{aligned} &a^1 \neq 1, \\ &a^3 \neq 1, \\ &a^5 = a^4 \cdot a = \big(a^3 + 1\big)a = a^4 + a = a^3 + a + 1 \neq 1, \end{aligned}$$

todėl $a^{15} = 1$ ir $\mathrm{ord}_{GF(16)^*}(a) = 15$, t.y. a – primityvusis kūno $GF(16)$ elementas. Tad

$$GF(16) = \{0, 1, a, a^2, \ldots, a^{13}, a^{14}\}.$$

Dviejų kūno $GF(16)$ elementų reiškimo būdų ryšys pateikiamas vadinamąja indeksų lentele, kurioje kiekvienam kūno $GF(16)$ primityviojo elemento a laipsniui a^k priskiriamas šio kūno elementas, išreikštas polinomu. Pavyzdžiui,

$$a^4 = a^3 + 1,$$
$$a^5 = a^4 \cdot a = \left(a^3 + 1\right)a = a^4 + a = a^3 + a + 1,$$
$$a^6 = a^5 \cdot a = \left(a^3 + a + 1\right)a = a^4 + a^2 + a = a^3 + a^2 + a + 1 \text{ ir t. t.}$$

Indeksas	Laipsninis reiškimas	Polinominis reiškimas	Vektorinis reiškimas
$*$	0	0	$(0,0,0,0)$
0	1	1	$(0,0,0,1)$
1	a	a	$(0,0,1,0)$
2	a^2	a^2	$(0,1,0,0)$
3	a^3	a^3	$(1,0,0,0)$
4	a^4	a^3+1	$(1,0,0,1)$
5	a^5	a^3+a+1	$(1,0,1,1)$
6	a^6	a^3+a^2+a+1	$(1,1,1,1)$
7	a^7	a^2+a+1	$(0,1,1,1)$
8	a^8	a^3+a^2+a	$(1,1,1,0)$
9	a^9	a^2+1	$(0,1,0,1)$
10	a^{10}	a^3+a	$(1,0,1,0)$
11	a^{11}	a^3+a^2+1	$(1,1,0,1)$
12	a^{12}	$a+1$	$(0,0,1,1)$
13	a^{13}	a^2+a	$(0,1,1,0)$
14	a^{14}	a^3+a^2	$(1,1,0,0)$

Pastabos. 1. Neišskiriant 0, paprastai žymima $a^* = 0$, $a \in GF(q)$.

2. Iš paskutinio stulpelio matome, kad kūnas $GF(16)$ yra 4-matė vektorinė erdvė virš $GF(2)$, kurios bazė $\{1, a, a^2, a^3\}$, ir todėl šiame stulpelyje yra mūsų vektorinės erdvės elementų koordinatės nurodytoje bazėje.

Operacijas kūne $GF(16)$ iliustruosime pavyzdžiu:

$$\begin{aligned}
&\left(a^{10}+a^7+a^5+a^2+1\right)\left(a^4+a^3+a\right)\\
&=a^{14}+a^{11}+a^9+a^6+a^4+a^{13}+a^{10}\\
&+a^8+a^5+a^3+a^{11}+a^8+a^6+a^3+a\\
&=a^{14}+a^{13}+a^{10}+a^9+a^5+a^4+a\\
&=(1,1,0,0)+(0,1,1,0)+(1,0,1,0)+(0,1,0,1)\\
&+(1,0,1,1)+(1,0,0,1)+(0,0,1,0)=\\
&=(0,1,0,1)=a^9=a^2+1.
\end{aligned}$$

10.3 apibrėžimas. *Primityviojo kūno $GF(q)$ elemento minimalusis polinomas vadinamas primityviuoju polinomu.*

Primityvieji polinomai yra svarbūs, nes jų šaknų laipsniais reiškiami baigtinio kūno elementai. Tačiau šių polinomų paieška nėra paprasta ir ją aptarsime vėliau.

3. Trečias baigtinio kūno $GF(q)$ elementų reiškimo būdas – matricos.

Naudojamasi tiesinės algebros teiginiu apie tai, kad bet kurio polinomo $f(x)=\alpha_0+\alpha_1 x+\ldots+\alpha_{n-1}x^{n-1}+x^n$ (čia α_i – kūno K elementai) lydinčioji matrica

$$A=\begin{pmatrix}
0 & 0 & \ldots & 0 & -\alpha_0\\
1 & 0 & \ldots & 0 & -\alpha_1\\
0 & 1 & \ldots & 0 & -\alpha_2\\
\ldots & \ldots & \ldots & \ldots & \ldots\\
0 & 0 & \ldots & 1 & -\alpha_{n-1}
\end{pmatrix}$$

yra polinomo $f(x)$ šaknis: $f(A)=\alpha_0 I+\alpha_1 A+\ldots+\alpha_{n-1}A^{n-1}+A^n=0$.

Taigi turėdami n-ojo laipsnio neredukuojamą polinomą $f(x)$ virš kūno $GF(q)$, kurio lydinčioji matrica yra A, kūno $GF(q^n)$ elementus galime vaizduoti matricomis

$$\beta_0 I+\beta_1 A+\ldots+\beta_{n-1}A^{n-1},\quad \beta_0,\beta_1,\ldots,\beta_n\in GF(q).$$

Svarbiausia, kad kūno elementų aritmetiką galima suvesti į matricų aritmetiką, nepriklausomai nuo to, ar neredukuojamas $f(x)$ yra primityvusis, ar ne.

10.4 pavyzdys. Polinomas $f(x) = x^2 + 1$ yra neredukuojamas virš $GF(3)$ (nes neturi virš $GF(3)$ šaknų). Šio polinomo lydinčioji matrica yra

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

$$\begin{aligned} GF(9) &= \big(GF(3)\big)(A) \\ &= \left\{ 0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},\ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ 2I = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \right. \\ &\quad A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix},\ A + I = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix},\ A + 2I = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}, \\ &\quad \left. 2A = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix},\ 2A + I = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix},\ 2A + 2I = \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} \right\}. \end{aligned}$$

Operacijas iliustruosime pavyzdžiu:

$$(2A + 2I)(A + 2I) = \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} \cdot \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = 2I.$$

10.5 pavyzdys. Neredukuojamas virš $GF(3)$ polinomas $f(x) = x^2 + 2x + 2$ yra primityvusis polinomas, nes, kai $a^2 + 2a + 2 = 0$ (čia a yra $f(x)$ šaknis),

$$\begin{aligned} &a^2 = -2a - 2 = a + 1 \neq 1, \\ &a^4 = a^2 + 2a + 1 = 3a + 2 = 2 \neq 1, \\ &a^8 = 4 = 1, \\ &\operatorname{ord}_{GF(9)^*}(a) = |GF(9)^*|. \end{aligned}$$

Primityviojo polinomo $f(x)$ lydinčioji matrica yra

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

Tada

$$\begin{aligned} GF(9) = \left\{ 0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},\ C = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},\ C^2 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \right. \\ C^3 = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix},\ C^4 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix},\ C^5 = \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix}, \\ \left. C^6 = \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix},\ C^7 = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix},\ C^8 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}. \end{aligned}$$

Operacijas iliustruosime pavyzdžiu:

$$\begin{aligned}(C^7+2C^4)(C^3+C) &= \left(\begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix} + 2\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}\right)\\ &\quad\cdot\left(\begin{pmatrix}1 & 2\\ 2 & 0\end{pmatrix} + \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\right)\\ &= \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix} = C.\end{aligned}$$

Pastaba. Nors kūno elementus išreiškus matricomis operacijas atlikti paprasta, kai $\deg f(x)$ yra didelis, tenka naudoti didelio matavimo matricas.