15.JUNGTINIAI ELEMENTAI.MIOBIUSO FUNKCIJA

Žinodami, kad kiekvienas kūno $GF(q^n)$ elementas yra neredukuojamo polinomo virš $GF(q)$ šaknis (šis neredukuojamas polinomas yra polinomo $x^{q^n}-x$ daliklis ir nebūtinai šio polinomo laipsnis yra n), pateiksime apibrėžimą.

11.10 apibrėžimas. *Du elementai $a, b \in GF(q^n)$ vadinami jungtiniais virš kūno $GF(q)$, jeigu jie abu yra to paties neredukuojamo polinomo $f(x)$ virš $GF(q)$ šaknys.*

11.11 pastabos. *1. Polinomas $f(x)$ yra elementų a ir b minimalusis polinomas.*

2. Elemento $a \in GF(q^n)$ jungtiniai elementai virš $GF(q)$ yra

$$a, a^q, a^{g^2}, \ldots, a^{q^{m-1}};$$

čia m – toks mažiausias teigiamas sveikas skaičius, kad $a^{q^m} = a$.

3. Kūno $GF(q^n)$ primityviojo elemento a visi jungtiniai elementai virš kūno $GF(q)$ taip pat yra primityvieji kūno $GF(q^n)$ elementai.

11.12 pavyzdys. Tegu $a \in GF(16)$ yra polinomo $f(x) = x^4+x+1 \in GF(2)[x]$ šaknis. Elemento a jungtiniai elementai virš $GF(2)$ yra

$$a, a^2, a^4 = a+1, a^8 = a^2+1.$$

Visi šie elementai yra primityvieji kūno $GF(16)$ elementai (polinomas $f(x) = x^4+x+1$ – neredukuojamas polinomas virš $GF(2)$).

Pasirėmę 11.11 pastaba, pateiksime būdą elemento $a \in GF(q^n)$ minimaliajam polinomui virš $GF(q)$ rasti.

11.13 teiginys. *Elemento $a \in GF(q^n)$ minimalusis polinomas virš $GF(q)$ yra*

$$g(x) = (x-a)(x-a^q)\ldots(x-a^{q^{m-1}});$$

čia m – toks mažiausias teigiamas sveikas skaičius, kad $a^{q^m} = a$. Elementai $a, a^q, \ldots, a^{q^{m-1}}$ yra elemento a jungtiniai elementai, o polinomas g – minimalusis visų šių elementų polinomas virš kūno $GF(q)$.

11.14 pavyzdys. Rasime visų kūno $GF(16)$ elementų minimaliuosius polinomus virš $GF(2)$. Iš 11.7 pavyzdžio žinome, kad neredukuojamo polinomo $g(x) = x^4 + x^3 + 1$ šaknis a generuoja multiplikacinę grupę $GF(16)^*$, t.y. bet kuris nenulinis kūno $GF(16)$ elementas yra a laipsnis. Taip yra todėl, kad $\mathrm{ord}_{GF(16)^*} = \mathrm{ord}_{GF(2)}\big(g(x)\big) = 15$.

Pradėsime nuo jungtinių elementų klasių kūne $GF(16)$ išskyrimo.

Elemento a jungtiniai yra: a, a^2, a^4, a^8 $(a^{16} = a)$.

Elemento a^3 jungtiniai yra: a^3, a^6, a^{12}, $a^{24} = a^9$ $(a^{48} = a^3)$.

Elemento a^5 jungtiniai yra: a^5, a^{10} $(a^{20} = a^5)$.

Elemento a^7 jungtiniai yra: a^7, a^{14}, $a^{28} = a^{13}$, $a^{56} = a^{11}$ $(a^{112} = a^7)$.

Tegu $m_k(x)$ yra elemento a^k minimalusis polinomas. Tada $m_0(x) = x + 1$ ir

$$\begin{aligned} m_1(x) = m_2(x) = m_4(x) = m_8(x) &= (x-a)(x-a^2)(x-a^4)(x-a^8) \\ &= \big(x^2 - (a+a^2)x + a^3\big)\big(x^2 - (a^4+a^8)x + a^{12}\big) \\ &= (x^2 - a^{13}x + a^3)(x^2 - a^7 x + a^{12}) \\ &= x^4 - (a^7 + a^{13})x^3 + (a^3 + a^{12} + a^{20})x^2 - (a^{25} + a^{10})x + a^{15} \\ &= x^4 + x^3 + 1, \end{aligned}$$

nes, atsižvelgiant į 10.2 pavyzdžio lentelę,

$$\begin{aligned} &a + a^2 = (0,0,1,0) + (0,1,0,0) = (0,1,1,0) = a^{13}, \\ &a^4 + a^8 + (1,0,0,1,) + (1,1,1,0) = (0,1,1,1) = a^7, \\ &a^7 + a^{13} = (0,1,1,1) + (0,1,1,0) = (0,0,0,1) = 1, \\ &a^3 + a^{12} + a^{20} = a^+ a^{12} + a^5 = (1,0,0,0) + (0,0,1,1) + (1,0,1,1) \\ &= (0,0,0,0) = 0, \\ &a^{25} + a^{10} = a^{10} + a^{10} = 2a^{10} = 0, \\ &a^{15} = 1. \end{aligned}$$

Be to,

$$\begin{aligned} m_3(x) = m_6(x) = m_9(x) = m_{12}(x) &= (x-a^3)(x-a^6)(x-a^9)(x-a^{12}) \\ &= (x-a^3)(x-a^{12})(x^6-a^6)(x-a^9) \\ &= \left(x^2-(a^3+a^{12})+a^{15}\right)\left(x^2-(a^6+a^9)+a^{15}\right) \\ &= (x^2-a^5x+1)(x^2-a^{10}x+1) \\ &= x^4-(a^6+a^{10})x^3+(1+1+a^{15})x^2-(a^5+a^{10})+1 \\ &= x^4+x^3+x^2+x+1, \end{aligned}$$

$$m_5(x) = m_{10}(x) = (x-a^5)(x-a^{10}) = x^2-(a^5+a^{10})x+a^{15} = x^2+x+1,$$

$$\begin{aligned} m_7(x) = m_{11}(x) = m_{13}(x) = m_{14}(x) &= (x-a^7)(x-a^{11})(x-a^{13})(x-a^{14}) \\ &= \left(x^2-(a^{11}+a^{11})x+a^{18}\right)\left(x^2-(a^{13}+a^{14})x+a^{27}\right) \\ &= (x^2+a^{10}x+a^3)(x^2+a^{10}x+a^{12}) \\ &= x^4+(a^{10}+a^{10})x^3+(a^3+a^{12}+a^{20})x^2+(a^{22}+a^{13})x+a^{15} \\ &= x^4+x+1. \end{aligned}$$

Pastebėsime, kad elemento $a=0$ minimalusis polinomas yra x.

Galime pateikti tikslią fiksuoto laipsnio neredukuojamų virš $GF(q)$ polinomų kiekio formulę. Šiai formulei rasti pasitelksime vieną iš aritmetinių funkcijų – Miobiuso[1] funkciją.

11.15 apibrėžimas. *Funkciją $\mu : \mathbb{N} \to \mathbb{Z}$, kurios reikšmės*

$$\mu(n) = \begin{cases} 1, & \text{kai } n = 1, \\ (-1)^k, & \text{kai skaičiaus } n \text{ kanoninis skaidinys yra} \\ & n = p_1 p_2 \dots p_k, \quad p_i \neq p_j, \quad i \neq j, \\ 0, & \text{kai skaičius } n \text{ dalijasi iš pirminio skaičiaus kvadrato,} \end{cases}$$

vadiname Miobiuso funkcija.

Suformuluosime pagrindines Miobiuso funkcijos savybes.

11.16 teiginys. *1 (Miobiuso funkcijos multiplikatyvumas).*
Tegu $n, m \in \mathbb{N}$ ir DBD $(n,m) = 1$. *Tada $\mu(m \cdot n) = \mu(m) \cdot \mu(n)$.*

[1] A.–F. Möbius, 1790–1868, – vokiečių matematikas.

2. Jeigu $n \in \mathbb{N}$, tai

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1, & \text{kai } n = 1, \\ 0, & \text{kai } n > 0, \end{cases}$$

čia sumuojama pagal visus skaičiaus n daliklius d.

3 (Miobiuso apgręžimo formulė).

3.1 (adityvusis variantas). Tegu h ir H yra funkcijos, apibrėžtos natūraliesiems skaičiams su reikšmėmis adicinėje komutatyvioje grupėje A: $h, H : \mathbb{N} \to A$.

Lygybė

$$H(n) = \sum_{d \mid n} h(d), \quad \text{visiems } n \in \mathbb{N} \tag{$*$}$$

teisinga tada ir tik tada, kai

$$h(n) = \sum_{d \mid n} \mu\Big(\frac{n}{d}\Big) H(d) = \sum_{d \mid n} \mu(d)\, H\Big(\frac{n}{d}\Big), \quad \text{visiems } n \in \mathbb{N}. \tag{$**$}$$

3.2 (multiplikatyvusis variantas). Tegu h ir H yra funkcijos, apibrėžtos natūraliesiems skaičiams su reikšmėmis multiplikacinėje komutatyvioje grupėje B: $h, H : \mathbb{N} \to B$.

Lygybė

$$H(n) = \prod_{d \mid n} h(d), \quad \text{visiems } n \in \mathbb{N}$$

teisinga tada ir tik tada, kai

$$h(n) = \prod_{d \mid n} H(d)^{\mu(\frac{n}{d})} = \prod_{d \mid n} H\Big(\frac{n}{d}\Big)^{\mu(d)}, \quad \text{visiems } n \in \mathbb{N}.$$

Simbolis $\prod\limits_{d \mid n}$ yra multiplikacinis simbolio $\sum\limits_{d \mid n}$ variantas, reiškiantis, kad dauginama pagal visus skaičiaus n daliklius d.

Įrodymas. 1. Miobiuso funkcijos multiplikatyvumas išplaukia iš funkcijos apibrėžimo.

2. Aišku, kai $n = 1$, tai lygybė teisinga. Kai $n > 1$ ir skaičiaus n kanoninis skaidinys yra $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, tai

$$\sum_{d \mid n} \mu(d) = \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{1 \leqslant i_1 < i_2 \leqslant k} \mu\big(p_{i_1} p_{i_2}\big) + \ldots + \mu(p_1 p_2 \ldots p_k) =$$

$$= 1 + C_k^1 (-1) + C_k^2 (-1)^2 + \ldots + C_k^k (-1)^n = \big(1 + (-1)\big)^k = 0.$$

3.1. Tegu $d_1, d_2, \ldots, d_s$ yra visi skaičiaus n dalikliai.
Kai teisinga $(*)$, tai

$$\begin{aligned}\sum_{d \mid n} \mu\Big(\frac{n}{d}\Big)\, H(d) &= \sum_{d \mid n} \mu(d)\, H\Big(\frac{n}{d}\Big) = \sum_{d \mid n} \mu(d) \sum_{c \mid \frac{n}{d}} h(c) \\ &= \mu(d_1) \sum_{d_i \mid \frac{n}{d_1}} h(d_i) + \ldots + \mu(d_s) \sum_{d_i \mid \frac{n}{d_s}} h(d_i) \\ &= h(d_1) \sum_{d_i \mid \frac{n}{d_1}} \mu(d_i) + \ldots + h(d_s) \sum_{d_i \mid \frac{n}{d_s}} \mu(d_i) \\ &= \sum_{c \mid n} h(c) \sum_{d \mid \frac{n}{c}} \mu(d) = h(n).\end{aligned}$$

Paskutinė lygybė teisinga, nes

$$\sum_{d \mid \frac{n}{c}} \mu(d) \neq 0 \iff \frac{n}{c} = 1 \iff n = c.$$

Kai teisinga $(**)$, tai

$$\begin{aligned}\sum_{d \mid n} h(d) &= \sum_{d \mid n} \sum_{c \mid d} \mu(c)\, H\Big(\frac{d}{c}\Big) = \sum_{d \mid n} \sum_{c \mid d} \mu\Big(\frac{d}{c}\Big) H(c) \\ &= \sum_{c \mid d_1} \mu\Big(\frac{d_1}{c}\Big)\, H(c) + \ldots + \sum_{c \mid d_s} \mu\Big(\frac{d_s}{c}\Big)\, H(c) \\ &= \sum_{c \mid n} H(c) \cdot \sum_{d_i \mid \frac{n}{c}} \mu(d_i) = H(n).\end{aligned}$$

3.2. Įrodymas analogiškas 3.1 įrodymui.

$\triangle$

Grįžkime prie fiksuoto laipsnio neredukuojamų polinomų kiekio formulės.

11.17 teiginys. *Bet kuriam natūraliajam skaičiui $n \in \mathbb{N}$ visų neredukuojamų virš kūno $GF(q)$ polinomų, kurių laipsnis yra n daliklis, sandauga lygi $f_{q^n}(x) = x^{q^n} - x$.*

Įrodymas. Iš 11.2 teiginio žinome, kad polinomo $f_{q^n}(x) \in GF(q)\,[x]$ kanoniniame skaidinyje yra visi neredukuojami virš $GF(q)$ polinomai, kurių laipsniai yra skaičiaus n dalikliai. Kita vertus,

$$f'_{q^n}(x) = q^n\, x^{q^n-1} - 1 = -1 \neq 0,$$

t.y. polinomas $f_{q^n}(x)$ neturi kartotinių šaknų, ir todėl kiekvieno neredukuojamo polinomo $f_{q^n}(x)$ kartotinumas polinomo kanoniniame skaidinyje yra lygus 1.

$\triangle$

Neredukuojamų virš kūno $GF(q)$ d laipsnio polinomų skaičių žymėsime $N_q(d)$.

11.18 išvada. *Su visais natūraliaisiais skaičiais n teisinga lygybė*

$$q^n = \sum_{d\,|\,n} d\, N_q(d).$$

11.19 išvada. *Teisinga formulė*

$$N_q(n) = \frac{1}{n} \sum_{d\,|\,n} \mu\Big(\frac{n}{d}\Big) q^d = \frac{1}{n} \sum_{d\,|\,n} \mu(d)\, q^{\frac{n}{d}}.$$

Įrodymas. Šiai formulei gauti reikia funkcijoms $h, H : \mathbb{N} \to \mathbb{Z}$, apibrėžtoms lygybėmis $h(n) = n\, N_q(n)$ ir $H(n) = q^n$, pritaikyti adityvųjį Miobiuso apgręžimo variantą.

$\triangle$

11.20 pavyzdys. 18-ojo laipsnio neredukuojamų polinomų virš kūno $GF(q)$ skaičius yra

$$\begin{aligned} N_q(18) &= \frac{1}{18}\big(\mu(1)q^{18} + \mu(2)q^9 + \mu(3)q^6 + \mu(6)q^3 + \mu(9)q^2 + \mu(18)q\big) \\ &= \frac{1}{18}\big(q^{18} - q^9 - q^6 + q^3\big). \end{aligned}$$

4-ojo laipsnio neredukuojamų polinomų virš kūno $GF(2)$ skaičius yra

$$N_2(4) = \frac{1}{4}\big(\mu(1)2^4 + \mu(2)2^2 + \mu(4)2^1\big) = \frac{1}{4}\big(2^4 - 2^2\big) = 3$$

(palyginkite su 11.7 pavyzdžio lentele).

Taikydami Miobiuso apgręžimo formulę, galime rasti ne tik n-ojo laipsnio neredukuojamų polinomų virš $GF(q)$ skaičių, bet ir šių polinomų sandaugą, žymimą $I(q,n,x)$.

11.21 išvada. *Teisinga formulė*

$$I(q,n,x)=\prod_{d\mid n}\left(x^{q^d}-x\right)^{\mu\left(\frac{n}{d}\right)}=\prod_{d\mid n}\left(x^{q^{\frac{n}{d}}}-x\right)^{\mu(d)}.$$

Įrodymas. Remiantis 11.17 teiginiu,

$$x^{q^n}-x=\prod_{d\mid n}I(q,d,x).$$

Tegu funkcijos, apibrėžtos lygybėmis $h(n)=I(q,n,x)$ ir $H(n)=x^{q^n}-x$, $h,H:\mathbb{N}\to B$; čia B – multiplikacinė racionaliųjų funkcijų virš kūno $GF(q)$ grupė (t.y. funkcijų $f(x)=\frac{p_1(x)}{p_2(x)}$; čia $p_1(x)$ ir $p_2(x)$ polinomai virš $GF(q)$, $p_1(x)\,p_2(x)\neq 0$). Pritaikę funkcijoms h ir H multiplikatyviąją Miobiuso apgręžimo formulę, gausime norimą formulę.

△

11.22 pavyzdys.

$$\begin{aligned}I(2,4,x)&=\left(x^{16}-x\right)^{\mu(1)}\left(x^4-x\right)^{\mu(2)}\left(x^2-x\right)^{\mu(4)}\\&=\frac{x^{16}-x}{x^4-x}=\frac{x^{15}-1}{x^3-1}=x^{12}+x^9+x^6+x^3+1.\end{aligned}$$