II dalis
Tiesiniai kodai

1 Kai kurių algebrinių struktūrų priminimas

Šiame skyriuje prisiminsime kai kurias sąvokas, jums žinomas iš algebros kurso.

1.1 Kūnas

Visų pirma prisiminkime *kūno* (kartais dar vadinamo *lauku*) apibrėžimą.

- *Grupė* $(B, \times)$ — tai netuščia aibė B, kurioje apibrėžta operacija $\times$, tenkinanti tokias savybes:
  - asociatyvumo, t. y.
$$\forall a, b, c \in B \quad (a \times b) \times c = a \times (b \times c),$$
  - egzistuoja neutralus elementas $i \in B$, t. y. toks, kad
$$a \times i = i \times a = a,$$
  -
$$\forall a \in B, \exists \overline{a} \in B : a \times \overline{a} = \overline{a} \times a = i.$$
- Grupė vadinama *komutatyviąja*, arba *Abelio*, jei operacija $\times$ yra komutatyvi, t. y.
$$\forall a, b \in B \quad a \times b = b \times a.$$
- *Kūnas* $(A, +, \cdot)$ — tai aibė A, sudaryta bent iš dviejų elementų, kurioje apibrėžtos sudėties „+“ ir daugybos „$\cdot$“ operacijos, tenkinančios savybes:
  - $(A, +)$ — komutatyvioji grupė (neutralų elementą sudėties atžvilgiu žymėsime „0“ ir vadinsime *nuliu*, $\overline{a}$ žymėsime $-a$),
  - $(A \backslash \{0\}, \cdot)$ — grupė (neutralų elementą daugybos atžvilgiu žymėsime „1“ ir vadinsime *vienetu*, $\overline{a}$ žymėsime a^{-1} arba $1/a$),
  - visiems $a, b, c \in A$ galioja distributyvumo dėsniai:
    - $a \cdot (b + c) = a \cdot b + a \cdot c$,
    - $(a + b) \cdot c = a \cdot c + b \cdot c$.

Pastaba. Galima parodyti, kad jei A yra kūnas, tai $0 \cdot a = 0 \ \ \forall a \in A$.

Pavyzdys. Jei p - pirminis skaičius, tai sveikųjų skaičių moduliu p aibė sudaro baigtinį kūną iš p elementų
$$\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\},$$
vadinamą *pirminiu kūnu*. Jame operacijos atliekamos moduliu p (t.y. atlikus veiksmą dalinama iš p ir imama liekana). Pavyzdžiui, kūne $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ gauname, kad $3 + 4 = 2$, nes $3 + 4 = 7 \equiv 2 \bmod 5$. Taip pat *dvinariame kūne* $\mathbb{F}_2 = \{0, 1\}$ gauname, kad $1 + 1 = 0$. □

1.2 Tiesinė erdvė

Tegu A — kūnas, $n \geqslant 1$ — sveikasis skaičius. Aibė $V \subset A^n$ vadinama *tiesine erdve virš* A, jei

$$v, u \in V \Rightarrow av + bu \in V \ \forall\, a, b \in A.$$

1.1 pavyzdys. Pagal apibrėžimą nesunku patikrinti, kad $V = \{000, 011, 101, 110\}$ yra tiesinė erdvė virš $\mathbb{F}_2$. □

Pastabos. 1. Nulinis vektorius visada priklauso tiesinei erdvei V, nes pagal apibrėžimą bet kuri erdvės V vektorių u ir v tiesinė kombinacija priklauso V, tuo pačiu ir $0 \cdot u + 0 \cdot v = 0 \in V$.

2. Dvinariu atveju tiesinės erdvės apibrėžimo sąlyga tampa

$$v, u \in V \Rightarrow v + u \in V. \tag{1}$$

Iš tikrųjų, dvinariu atveju a ir b gali įgyti tik dvi reikšmes — 0 ir 1, todėl tėra keturios galimos tiesinės kombinacijos:

$$\begin{aligned} 0 \cdot u + 0 \cdot v &= 0, \\ 0 \cdot u + 1 \cdot v &= v, \\ 1 \cdot u + 0 \cdot v &= u, \\ 1 \cdot u + 1 \cdot v &= u + v. \end{aligned}$$

Antra ir trečia priklauso V pagal sąlygą, todėl lieka patikrinti, ar $0 \in V$ ir ar teisinga (1) sąlyga. Bet pastebėkime, kad sąlyga $0 \in V$ išplaukia iš (1) sąlygos, nes iš pastarosios gauname, kad $0 = u + u \in V$. Todėl lieka tik (1) sąlyga.

Tiesinės erdvės V vektorių rinkinys $u_1, \ldots, u_s$ vadinamas *tiesiškai nepriklausomu*, jei

$$(a_1u_1 + \cdots + a_su_s = 0, a_i \in A \ \forall i) \Rightarrow (a_1 = \cdots = a_s = 0).$$

Šį apibrėžimą galima suformuluoti ir iš kitos pusės: tiesinės erdvės V vektorių rinkinys $u_1, \ldots, u_s$ vadinamas tiesiškai nepriklausomu, jei bet kokia tiesinė jų kombinacija su bent vienu nenuliniu koeficientu yra nenulinis vektorius:

$$(a_i \in A \ \forall i \ \text{ ir } \ \exists i : a_i \neq 0, 1 \leqslant i \leqslant s) \Rightarrow (a_1u_1 + \cdots + a_su_s \neq 0).$$

1.2 užduotis. Įrodykite, kad galioja šios savybės.

1. Rinkinys iš vieno vektoriaus yra tiesiškai priklausomas tada ir tik tada, kai tas vektorius yra nulinis vektorius.

2. Jei nulinis vektorius priklauso vektorių rinkiniui, tai tas vektorių rinkinys yra tiesiškai priklausomas.

3. Vektorių rinkinys yra tiesiškai priklausomas tada ir tik tada, kai kuris nors to rinkinio vektorius yra likusių vektorių tiesinė kombinacija.

4. Dviejų nenulinių vektorių u, v rinkinys yra tiesiškai priklausomas tada ir tik tada, kai egzistuoja $a \in A$ toks, kad $u = av$.

5. Dviejų dvinarių nenulinių vektorių u, v rinkinys yra tiesiškai priklausomas tada ir tik tada, kai tie vektoriai lygūs.

6. Jei vektorių aibė yra tiesiškai nepriklausoma, tai bet koks netuščias jos poaibis irgi yra tiesiškai nepriklausomas.

Tiesinės erdvės V tiesiškai nepriklausomų vektorių rinkinys $u_1, \ldots, u_s$ vadinamas erdvės V *baze*, jei kiekvieną erdvės V vektorių galima išreikšti vektorių $u_1, \ldots, u_s$ tiesine kombinacija, t.y.

$$\forall v \in V \ \exists a_1, \ldots, a_s \in A : v = a_1 u_1 + \cdots + a_s u_s.$$

Pavyzdys. Tiesinės erdvės iš 1.1 pavyzdžio bazė yra $\{011, 101\}$. Be to, aibės $\{011, 110\}$ ir $\{101, 110\}$ taip pat yra šios erdvės bazės. □

Teorema. *Tarkime, $V \subset A^n$ yra tiesinė erdvė. Tada V turi bazę, sudarytą iš ne daugiau kaip n vektorių. Jei ji sudaryta iš s vektorių, tai:*

1. *Bet koks vektorių iš V rinkinys, sudarytas iš $s+1$ vektoriaus, yra tiesiškai priklausomas.*

2. *Kiekviena V bazė yra sudaryta iš s vektorių.*

3. *Bet kurie s tiesiškai nepriklausomi V vektoriai sudaro V bazę.*

4. *Kiekvienas tiesinės erdvės V vektorius* vienareikšmiškai *išreiškiamas bazės vektorių tiesine kombinacija.*

Erdvės V *dimensija*, žymima $\dim V$, yra bazės vektorių skaičius s.

1.3 Baigtiniai kūnai

Šiame poskyryje prisiminsime baigtinių kūnų (dar vadinamų Galua kūnais, angl. finite fields, Galois fields) pagrindines sąvokas, nes ateityje nagrinėsime kodus, apibrėžtus virš baigtinės abėcėlės, turinčios kūno struktūrą.

- Kūną, turintį baigtinį skaičių elementų, vadinsime *baigtiniu kūnu*. Baigtinį kūną, turintį q elementų, žymėsime $\mathbb{F}_q$ (angliškoj literatūroj jis dažnai žymimas $GF(q)$). Pavyzdžiui, pirminis kūnas $\mathbb{F}_p$ yra baigtinis.

- Baigtinis kūnas iš q elementų egzistuoja tada ir tik tada, kai $q = p^m$, kur p — pirminis, $m \geqslant 1$. Visi baigtiniai kūnai, turintys q elementų, yra izomorfiški, todėl galima laikyti, kad toks kūnas yra vienintelis.

- Tarkime, $q = p^m$, kur p — pirminis, $m \geqslant 1$. Jei $m = 1$, tai $q = p$ ir $\mathbb{F}_q$ yra pirminis kūnas, t. y. sveikųjų skaičių moduliu q aibė. Jei $m > 1$, tai $\mathbb{F}_q$ nėra sveikųjų skaičių moduliu q aibė, t. y. veiksmai su kūno $\mathbb{F}_q$ elementais atliekami kitaip, nei sveikųjų skaičių moduliu q aibėje. Tuo pačiu gauname, kad jei r nėra pirminis, sveikųjų skaičių moduliu r aibė nėra kūnas.

- Visi baigtiniai kūnai yra komutatyvūs, t.y. daugyba yra komutatyvi.

- Mažiausias toks sveikas skaičius s, kad $\underbrace{1+\cdots+1}_{s}=0$, kur 0 ir 1 yra atitinkamai kūno K nulis ir vienetas, vadinamas kūno K *charakteristika*. Jei toks skaičius neegzistuoja (pavyzdžiui, realiųjų skaičių kūne), kūno charakteristika laikoma lygia nuliui. Baigtinio kūno $\mathbb{F}_{p^m}$ charakteristika yra p. Jei p yra kūno K charakteristika, tai

$$p\beta = 0 \text{ visiems } \beta \in K. \tag{2}$$

  Pavyzdžiui, $2\beta = 0$ visiems $\beta \in \mathbb{F}_2$.

- Iš (2) lygybės gauname, kad

$$(\beta+\gamma)^p = \beta^p + \gamma^p \ \forall \beta, \gamma \in \mathbb{F}_{p^m}. \tag{3}$$

  Pagal indukciją taip pat gauname

$$(\beta+\gamma)^{p^i} = \beta^{p^i} + \gamma^{p^i} \ \forall \beta, \gamma \in \mathbb{F}_{p^m} \ \forall i \geqslant 1. \tag{4}$$

1.3.1 Nepirminiai kūnai

- Pirminis kūnas[2] $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ yra kūno $\mathbb{F}_{p^m}$ poaibis. Kūnas $\mathbb{F}_{p^m}$ yra tiesinė erdvė virš $\mathbb{F}_p$, $\dim \mathbb{F}_{p^m} = m$. Jei β_0, β_1, $\cdots$,β_{m-1} yra erdvės $\mathbb{F}_{p^m}$ bazė virš $\mathbb{F}_p$, tai

$$\mathbb{F}_{p^m} = \{a_0\beta_0 + a_1\beta_1 + \cdots + a_{m-1}\beta_{m-1} \mid a_i \in \mathbb{F}_p \ \forall i\}.$$

- Aibė $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ yra ciklinė multiplikacinė grupė, t.y.

$$\exists \alpha \in \mathbb{F}_q^* : \mathbb{F}_q^* = \{1, \alpha, \alpha^2, \cdots, \alpha^{q-2}\}, \alpha^{q-1} = 1.$$

  Toks α yra vadinamas *primityviu kūno* $\mathbb{F}_q$ *elementu* (jis nebūtinai yra vienintelis). Ši baigtinio kūno elementų išraiška leidžia lengvai dauginti ir dalinti: dauginant (dalinant) du ciklinės grupės elementus pakanka sudėti (atimti) jų laipsnių rodiklius (moduliu $q-1$).

- Jei $\alpha \in \mathbb{F}_{p^m}$ yra primityvus elementas, tai $\{1, \alpha, \alpha^2, \cdots, \alpha^{m-1}\}$ yra kūno $\mathbb{F}_{p^m}$ bazė virš $\mathbb{F}_p$, todėl

$$\mathbb{F}_{p^m} = \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} \mid a_i \in \mathbb{F}_p \ \forall i\}.$$

  Ši baigtinio kūno elementų išraiška leidžia lengvai sudėti ir atimti: sudedame (atimame) panariui koeficientus prie α laipsnių. Koeficientus sudėti (atimti) mokame, nes jie priklauso kūnui $\mathbb{F}_p$. Praktikoje į elementą $a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}$ patogu žiūrėti kaip į vektorių $(a_0, a_1, \ldots, a_{m-1}) \in \mathbb{F}_p^m$, ir veiksmus atlikti su vektoriais.

  Jei galėtume nesunkiai pereiti nuo vienos baigtinio kūno elementų išraiškos prie kitos, tai galėtume elementus ir sudėti (atimti), ir dauginti (dalinti). Netrukus pamatysime, kaip tai padaryti. Bet prieš tai — dar viena baigtinio kūno elementų išraiška.

- Jei $f(x)$ yra pirminis m-tojo laipsnio polinomas virš $\mathbb{F}_p$, tai $\mathbb{F}_{p^m}$ yra izomorfiškas faktoržiedžiui $\mathbb{F}_p[x]/(f(x))$ (prisiminkime, kad faktoržiedis $\mathbb{F}_p[x]/(f(x))$ yra polinomų virš $\mathbb{F}_p$ dalybos iš $f(x)$ liekanų aibė, kurioje veiksmai atliekami moduliu $f(x)$). Taigi, galime laikyti, kad

$$\mathbb{F}_{p^m} = \{g(x) = g_0 + g_1x + \cdots + g_{m-1}x^{m-1} \mid g_i \in \mathbb{F}_p \ \forall i\},$$

  ir veiksmai atliekami $\bmod f(x)$.

[2]Tekstas smulkesniu šriftu yra neprivalomas.

- Visiems p — pirminiams ir $m \geqslant 1$ egzistuoja toks pirminis m-tojo laipsnio polinomas $f(x) \in \mathbb{F}_p[x]$, kurio šaknis yra kūno $\mathbb{F}_{p^m}$ primityvus elementas α, t.y. $f(\alpha) = 0$. Toks polinomas vadinamas *primityviu polinomu* (jis nebūtinai yra vienintelis).
- Primityvus polinomas $f(x)$ leidžia susieti dvi baigtinio kūno $\mathbb{F}_{p^m}$ elementų išraiškas, tiksliau, leidžia primityvaus elemento laipsnius $\alpha^m, \alpha^{m+1}, \ldots, \alpha^{p^m-2}$ išreikšti bazės $1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{m-1}$ vektorių tiesine kombinacija. Iš tikro, tegu $f(x) = f_0 + f_1 x + \cdots + f_m x^m$, $f_i \in \mathbb{F}_p$ $\forall i$. Kadangi $f(\alpha) = 0$, tai $f_0 + f_1\alpha + \cdots + f_m\alpha^m = 0$. Iš čia gauname, kad $\alpha^m = -\frac{1}{f_m}(f_0 + f_1\alpha + \cdots + f_{m-1}\alpha^{m-1})$ — išreiškėme bazės vektorių tiesine kombinacija. Aukštesnius α laipsnius išreiškiame taip pat, pavyzdžiui, $\alpha^{m+1} = \alpha^m\alpha$, įstatome gautą α^m išraišką ir t.t.
- Nors primityvių polinomų yra ne vienas ir visi jie gali būti naudojami veiksmams su baigtinio kūno elementais, yra tam tikri „standartiniai“ primityvūs polinomai, kurie paprastai ir yra naudojami. 1 lentelėje pateikiame kelis jų pavyzdžius mažiems p ir m.

p	Primityvūs polinomai	p	Primityvūs polinomai
2	$x+1$	3	x^4+x^3+2
	x^2+x+1		$x^5+x^4+x^2+1$
	x^3+x+1		x^6+x^5+2
	x^4+x+1	5	x^2+x+2
	x^5+x^2+1		x^3+x^2+2
	x^6+x+1		x^4+x^3+x+3
	x^7+x+1	7	x^2+x+3
	$x^8+x^4+x^3+x^2+1$		x^3+x^2+x+2
	x^9+x^4+1	11	x^2+x+7
	$x^{10}+x^3+1$	13	x^2+x+2
3	$x+1$	17	x^2+x+10
	x^2+x+2	19	x^2+x+2
	x^3+2x^2+1	23	$x^2+22x+19$

1 lentelė: Primityvūs polinomai

1.3 pavyzdys. Sudarykime kūną $\mathbb{F}_8$. Matome, kad $p = 2$, $m = 3$ (nes $8 = 2^3$). Žinome, kad $\mathbb{F}_8^* = \{1, \alpha, \alpha^2, \cdots, \alpha^6\}$, $\alpha^7 = 1$, kur α yra kūno $\mathbb{F}_8$ primityvus elementas. Tai leidžia dauginti kūno $\mathbb{F}_8$ elementus, pavyzdžiui, $\alpha^2\alpha^3 = \alpha^5$, $\alpha^3\alpha^6 = \alpha^9 = \alpha^7\alpha^2 = \alpha^2$ (kad $\alpha^9 = \alpha^2$, galėjome pasakyti iš karto, nes rodiklių skaičiavimai vyksta moduliu $q-1$, t.y. mod7). Be abejo, $0 \cdot \alpha^i = 0$ $\forall i$.

Be to, žinome, kad $\{1, \alpha, \alpha^2\}$ yra kūno $\mathbb{F}_8$ bazė virš $\mathbb{F}_2$, todėl

$$\begin{aligned}\mathbb{F}_8 &= \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_i \in \mathbb{F}_2 \ \forall i\} \\ &= \{0, 1, \alpha, 1+\alpha, \alpha^2, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2\}.\end{aligned}$$

Tai leidžia lengvai sudėti ir atimti, pavyzdžiui, $(1+\alpha)+(\alpha+\alpha^2) = 1+2\alpha+\alpha^2 = 1+\alpha^2$ (nes kūno $\mathbb{F}_8$ charakteristika yra $p = 2$, t.y. $1+1 = 2 = 0$ ir $-1 = 1$).

Kad galėtume pereiti nuo vienos išraiškos prie kitos, pasinaudosime primityviu polinomu iš 1 lentelės. Matome, kad, kai $p = 2$ ir $m = 3$, galime naudoti primityvų polinomą $f(x) = x^3 + x + 1$. Primityvus elementas α yra jo šaknis, t.y. $f(\alpha) = 0$, todėl $\alpha^3 + \alpha + 1 = 0$. Iš čia $\alpha^3 = -\alpha - 1 = \alpha + 1$ — išreiškėme bazės vektorių tiesine kombinacija.

Tada

$$\begin{aligned}\alpha^4 &= \alpha^3\alpha = (\alpha+1)\alpha = \alpha^2 + \alpha, \\ \alpha^5 &= \alpha^4\alpha = (\alpha^2+\alpha)\alpha = \alpha^3 + \alpha^2 = \alpha + 1 + \alpha^2, \\ \alpha^6 &= \alpha^5\alpha = (\alpha+1+\alpha^2)\alpha = \alpha^2 + \alpha + \alpha^3 = \alpha^2 + \alpha + \alpha + 1 = \alpha^2 + 1.\end{aligned}$$

Žinome, kad $\alpha^7 = 1$. Patikrinkime, ar iš tikrųjų:

$$\alpha^7 = \alpha^6\alpha = (\alpha^2+1)\alpha = \alpha^3 + \alpha = \alpha + 1 + \alpha = 1.$$

0	0	000
1	1	100
α	α	010
α^2	α^2	001
α^3	$1+\alpha$	110
α^4	$\alpha+\alpha^2$	011
α^5	$1+\alpha+\alpha^2$	111
α^6	$1+\alpha^2$	101

2 lentelė: Kūno $\mathbb{F}_8$ elementai

Taigi, dabar, atlikdami veiksmus su kūno $\mathbb{F}_8$ elementais, lengvai galime pereiti nuo vienos išraiškos prie kitos. Pavyzdžiui, $\alpha^4+\alpha^6=(\alpha^2+\alpha)+(\alpha^2+1)=\alpha+1=\alpha^3$.

Kaip buvo pastebėta, į elementą $a_0+a_1\alpha+a_2\alpha^2$ patogu žiūrėti kaip į vektorių $(a_0,a_1,a_2)\in\mathbb{F}_2^3$, ir veiksmus atlikti su vektoriais. Pavyzdžiui, elementą $\alpha^2+\alpha$ atitinka vektorius 011. Programuojant veiksmus su nedideliais baigtiniais kūnais, patogu pasidaryti lentelę, kuri susietų primityvaus elemento α laipsnius su tokiais vektoriais. Tada du elementai bus sudauginami, sudedant jų laipsnių rodiklius, o norint sudėti du elementus, lentelėje bus surandami juos atitinkantys vektoriai, sudedami (moduliu p), o rezultatas vėl paverčiamas α laipsniu. Pavyzdžiui, $\alpha^4+\alpha^6\to 011+101=110\to\alpha^3$.

Reziumuodami 2 lentelėje pateikiame kūno $\mathbb{F}_8$ elementų išraiškas. Pirmame stulpelyje yra primityvaus elemento α laipsnis, antrame — jo išraiška bazės $\{1,\alpha,\alpha^2\}$ vektorių tiesine kombinacija, ir trečiame — atitinkamas vektorius iš $\mathbb{F}_2^3$. □

1.4 pavyzdys. Panagrinėkime kūną $\mathbb{F}_9$. Kadangi $9=3^2$, tai $p=3$ ir $m=2$. Taigi, $\mathbb{F}_3=\{0,1,2\}$ yra kūno $\mathbb{F}_9$ poaibis ($2+2=4=1$, $3=0$, $-1=2$, $-2=1$). Taip pat žinome, kad $\mathbb{F}_9^*=\{1,\alpha,\alpha^2,\cdots,\alpha^7\}, \alpha^8=1$, kur α yra kūno $\mathbb{F}_9$ primityvus elementas. Be to, $\{1,\alpha\}$ yra kūno $\mathbb{F}_9$ bazė virš $\mathbb{F}_3$, todėl

$$\begin{aligned}\mathbb{F}_9 &= \{a_0+a_1\alpha \mid a_i\in\mathbb{F}_3\ \forall i\}\\ &= \{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}.\end{aligned}$$

Primityvus polinomas (iš 1 lentelės) būtų $f(x)=x^2+x+2$, taigi, $\alpha^2+\alpha+2=0$ ir $\alpha^2=-\alpha-2=2\alpha+1$. Toliau

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

Dabar galime atlikti veiksmus su kūno $\mathbb{F}_9$ elementais. Pavyzdžiui, $\alpha^3\alpha^6=\alpha^9=\alpha$, $(\alpha^2)^{-1}=\alpha^{-2}=\alpha^6$ (nes rodiklių veiksmai atliekami moduliu 8), $\alpha^6-\alpha^3=(\alpha+2)-(2\alpha+2)=\alpha+2-2\alpha-2=-\alpha=2\alpha=\alpha^5$, ir pan.

3 lentelėje pateikiame kūno $\mathbb{F}_9$ elementus. □

2 Tiesinio kodo apibrėžimas ir savybės

Pradedame nagrinėti didelę kodų šeimą, vadinamą tiesiniais kodais. Praktiškai visos svarbesnės kodų šeimos yra tiesinių kodų šeimos pošeimiai. Šiame skyriuje nagrinėsime savybes, bendras visiems tiesiniams kodams, o vėliau pereisime prie atskirų tiesinių kodų pošeimių.

0	0	00
1	1	10
α	α	01
α^2	$1+2\alpha$	12
α^3	$2+2\alpha$	22
α^4	2	20
α^5	2α	02
α^6	$2+\alpha$	21
α^7	$1+\alpha$	11

3 lentelė: Kūno $\mathbb{F}_9$ elementai

2.1 Tiesinio kodo apibrėžimas

Nuo šiol abėcėlė bus $A = \mathbb{F}_q$, $q = p$, p — pirminis[3], t. y. abėcėlė bus pirminis kūnas $\mathbb{F}_p$. Tegu $n \geq 1$.

2.1 apibrėžimas. *Kodą $C \subset \mathbb{F}_q^n$ vadinsime* tiesiniu*, jei C yra tiesinė erdvė. Tiesinio kodo dimensijos k ir ilgio n santykį $\frac{k}{n}$ vadinsime tiesinio kodo* koeficientu.

Jei tiesinio kodo C ilgis yra n, dimensija k, minimalus atstumas d, tai visas kodas žymimas $C[n,k,d]$ arba tiesiog $[n,k,d]$. Jei minimalus atstumas nesvarbus arba nežinomas, žymima $C[n,k]$ arba $[n,k]$.

Taigi, tiesinis kodas yra tiesiog tiesinė erdvė. Todėl galime pasinaudoti visomis tiesinių erdvių savybėmis. Pavyzdžiui, žinome, kad tiesinė erdvė turi bazę.

2.2 pavyzdys. Imkime tiesinį erdvės $\mathbb{F}_3^4$ poerdvį C, generuotą vektorių 2102 ir 1120. Tai reiškia, kad šie vektoriai sudaro poerdvio bazę, o visi kiti išreiškiami jų tiesinėmis kombinacijomis:

$$\begin{aligned}
0\cdot 2102 + 0\cdot 1120 &= 0000,\\
0\cdot 2102 + 1\cdot 1120 &= 1120,\\
0\cdot 2102 + 2\cdot 1120 &= 2210,\\
1\cdot 2102 + 0\cdot 1120 &= 2102,\\
1\cdot 2102 + 1\cdot 1120 &= 0222,\\
1\cdot 2102 + 2\cdot 1120 &= 1012,\\
2\cdot 2102 + 0\cdot 1120 &= 1201,\\
2\cdot 2102 + 1\cdot 1120 &= 2021,\\
2\cdot 2102 + 2\cdot 1120 &= 0111.
\end{aligned}$$

Taigi, tiesinis kodas $C = \{0000, 1120, 2210, 2102, 0222, 1012, 1201, 2021, 0111\}$. □

2.3 teorema. *1. Tiesinio $[n,k]$ kodo virš $\mathbb{F}_q$ dydis yra q^k.*

2. Tiesinio kodo minimalus atstumas yra lygus minimaliam svoriui.

Teoremos įrodymas paliekamas skaitytojui kaip užduotis.

[3]Visa čia išdėstyta teorija tinka ir nepirminiams kūnams. Toliau yra pateikti ir keli (neprivalomi) pavyzdžiai virš nepirminių kūnų.

2.4 pavyzdys. 2.2 pavyzdžio kodas yra $[4, 2]$ kodas virš $\mathbb{F}_3$, todėl pagal teoremos pirmą dalį, jo dydis turi būti $3^2 = 9$. Tą mes ir matėme. □

Pagal teoremos antrą dalį, tiesinio kodo minimalus atstumas randamas žymiai paprasčiau, negu netiesinio kodo. Užtenka surasti minimalų svorį, kuris ir bus minimalus atstumas.

2.5 pavyzdys. Kodo iš 2.2 pavyzdžio minimalų atstumą rasime taip. Randame jo minimalų svorį: mažiausio svorio nenulinis žodis yra svorio 3 žodis (tiesą pasakius, visų šio kodo nenulinių žodžių svoris yra 3). Todėl šio kodo minimalus atstumas irgi yra trys. □

2.2 Generuojanti matrica

Tegu $C[n, k]$ yra tiesinis kodas virš $\mathbb{F}_q$. Kad jis būtų visiškai apibrėžtas, nebūtina išrašyti visus q^k jo žodžius. Pakanka nurodyti jo bazę. Kodavimo teorijoje dažnai patogiau bazę užrašyti ne kaip vektorių rinkinį, o kaip matricą.

Apibrėžimas. *Tiesinio kodo $C[n, k]$ virš $\mathbb{F}_q$* generuojančia matrica *vadiname $k \times n$ matricą virš $\mathbb{F}_q$, kurios eilutės sudaro kodo C bazę.*

2.6 pavyzdys. 2.2 pavyzdžio kodo viena iš generuojančių matricų yra

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

□

Pastabos. 1. Generuojančios matricos eilučių skaičius lygus kodo dimensijai.

2. Tiesinis kodas gali turėti kelias generuojančias matricas, nes jis gali turėti kelias skirtingas bazes, o ir tos pačios bazės vektorius išrikiavę kita tvarka, gausime kitą generuojančią matricą.

Jei turime kokio nors tiesinio kodo $C[n, k]$ virš $\mathbb{F}_q$ generuojančią matricą G, tai visus kodo C žodžius ir tiktai juos gausime imdami generuojančios matricos G eilučių tiesines kombinacijas. Nesunku pastebėti, kad matricos G eilučių $G_1, \ldots, G_k$ tiesinė kombinacija su koeficientais $x_1, \ldots, x_k$ yra lygi vektoriaus-eilutės $x = (x_1, \ldots, x_k)$ ir matricos G sandaugai xG, t.y. $(x_1, \ldots, x_k)G = x_1G_1 + \cdots + x_kG_k$.

Pavyzdys.

$$(x_1, x_2)\begin{pmatrix} 2 & 1 & 0 & 2 \\ 1 & 1 & 2 & 0 \end{pmatrix} = (2x_1 + x_2, x_1 + x_2, 2x_2, 2x_1) = x_1(2102) + x_2(1120).$$ □

Todėl $C = \{xG \mid x \in \mathbb{F}_q^k\}$.

Atvaizdis $x \mapsto xG$ apibrėžia abipusiškai vienareikšmę erdvės $\mathbb{F}_q^k$ ir tiesinio kodo C žodžių atitiktį. Todėl šį atvaizdį galima interpretuoti kaip šaltinio informacijos, pateikiamos erdvės $\mathbb{F}_q^k$ žodžiais, kodavimą kodo C žodžiais.

Taigi, kodavimas tiesiniu kodu visai paprastas — ilgio k informacijos vektorių x virš $\mathbb{F}_q$ dauginame iš kodo C generuojančios matricos G ir gauname užkoduotą žodį $xG \in C$.

Pavyzdys. Kodavimui naudojame dvinarį tiesinį $[4, 3]$ kodą, kurio generuojanti matrica yra

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

Tarkime, šaltinis perduoda tokį dvinarį srautą: $110\ 010\ 001\ 111\ 101\ 010\cdots$ (čia patogumo dėlei srautą iškart suskaidome ilgio $k = 3$ vektoriais). Tada užkoduota seka, kurią siųsime kanalu, bus tokia: $1011\ 0111\ 1010\ 0001\ 0110\ 0111\cdots$ □

Kadangi generuojančios matricos G eilutės yra tiesiškai nepriklausomos, tai jos rangas yra lygus eilučių skaičiui k. Iš algebros žinome, kad tada iš matricos galime išrinkti tokius k stulpelių, iš kurių sudarytos kvadratinės matricos determinantas būtų nelygus 0. Tarkime, $s_1, s_2, \ldots, s_k$ yra tokių stulpelių numeriai, išrikiuoti didėjančia tvarka.

Tada

1) sukeisdami matricos G eilutes vietomis,

2) daugindami jas iš nenulinių kūno $\mathbb{F}_q$ elementų,

3) pridėdami prie kurios nors G eilutės kitą G eilutę, padaugintą iš kūno $\mathbb{F}_q$ elemento,

galime gauti tokio pavidalo matricą:

$$G' = \begin{pmatrix} \cdots & 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots \\ \cdots & 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 & \cdots \\ \cdots & 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 & \cdots \\ & \vdots & & \vdots & & \vdots & \ddots & \vdots & \\ \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 & \cdots \end{pmatrix} \tag{5}$$

Čia vienetinės matricos stulpelius gauname būtent $s_1, s_2, \ldots, s_k$ pozicijose. Gautoji matrica taip pat yra kodo C generuojanti matrica, nes atliekant išvardintas matricų operacijas jos rangas nesumažėja ir jos eilutės išlieka kode C.

2.7 pastaba. Atkreipkite dėmesį, kad veiksmus galima atlikti tik su generuojančios matricos eilutėmis, jokiu būdu ne su stulpeliais.

2.8 pavyzdys. Pertvarkykime 2.6 pavyzdžio generuojančią matricą.

$$\begin{pmatrix} 2 & 1 & 0 & 2 \\ 1 & 1 & 2 & 0 \end{pmatrix} \begin{matrix} \cdot 2 \\ \cdot 1 \downarrow \end{matrix} \sim \begin{pmatrix} 1 & 2 & 0 & 1 \\ 0 & 2 & 2 & 2 \end{pmatrix} \begin{matrix} \cdot 2 \\ \cdot 2 \uparrow \end{matrix} \sim \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

Kad gautume pirmame stulpelyje pirmą vienetinės matricos stulpelį, pirmos matricos pirmą eilutę padauginome iš 2, o taip pat pridėjome prie antros. Gauname antrą matricą. Tada antrą antros matricos eilutę padauginome iš 2, o taip pat padauginę iš 2 pridėjome prie pirmos, kad gautume antrame stulpelyje antrą vienetinės matricos stulpelį (žr. trečią matricą). Taigi, vienetinę matricą gauname pirmame ir antrame stulpeliuose, t.y. šiuo atveju $k = 2$, o $s_1 = 1$ ir $s_2 = 2$. □

Teorema. *Du tiesiniai $[n, k]$ kodai virš $\mathbb{F}_q$ yra lygūs tada ir tik tada, kai jų generuojančias matricas galima suvesti į tą pačią (5) pavidalo matricą su tais pačiais stulpeliais $s_1, \ldots, s_k$.*

Įrodykite šį teiginį savarankiškai.

Tai būdas patikrinti, ar, esant duotoms dviems generuojančioms matricoms, jos generuoja tą patį kodą ar ne. Užtenka pasirinkti $s_1, \dots, s_k$, suvesti matricas į (5) lygybės pavidalą ir patikrinti, ar gauname tą pačią matricą.

2.9 pavyzdys. Tegu

$$G = \begin{pmatrix} 2 & 1 & 0 & 2 \\ 1 & 1 & 2 & 0 \end{pmatrix} \quad \text{ir} \quad G' = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}.$$

2.8 pavyzdyje matėme, kad matricoje G vienetinę matricą galima gauti pirmame ir antrame stulpeliuose:

$$G \sim \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

Pabandykime ir matricos G' pirmame ir antrame stulpeliuose gauti vienetinę matricą.

$$G' = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix} \begin{matrix} \cdot 2 \\ \\ \end{matrix} \begin{matrix} \cdot 1 \\ \downarrow \end{matrix} \sim \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \begin{matrix} \cdot 1 \\ \\ \end{matrix} \begin{matrix} \cdot 2 \\ \uparrow \end{matrix} \sim \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

Gavome tą pačią matricą. Taigi, matricos G ir G' generuoja tą patį tiesinį kodą. □

2.10 apibrėžimas. *Matricą*

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots \\ 0 & 1 & \cdots & 0 & \cdots \\ \vdots & \vdots & \ddots & \vdots & \cdots \\ 0 & 0 & \cdots & 1 & \cdots \end{pmatrix}$$

vadinsime standartinio pavidalo *matrica.*

Tai $k \times n$ matrica ($k \leqslant n$), kurios pirmuose k stulpelių stovi vienetinė matrica, o likusi matricos dalis yra bet kokia. Standartinio pavidalo matricą paprastai žymėsime taip: $G = (I|A)$, čia I — vienetinė $k \times k$ matrica, A — kokia nors $k \times (n-k)$ matrica.

Teorema. *Bet kuris tiesinis kodas yra ekvivalentus tiesiniam kodui, turinčiam standartinio pavidalo generuojančią matricą.*

Įrodymas. Kaip matėme, bet kurią generuojančią matricą galime suvesti į (5) lygybės pavidalą. Paskui sukeičiame gautos matricos stulpelius taip, kad kiekvienam i s_i-tasis stulpelis atsidurtų i-tojoje pozicijoje, kad gautume standartinio pavidalo matricą. Gauta standartinio pavidalo matrica jau galbūt nebebus pradinio kodo generuojanti matrica, bet jinai bus ekvivalentaus kodo generuojanti matrica, nes jinai generuos kodą, kuris nuo pradinio skirsis tik koordinačių perstata. □

Ši teorema tvirtina, kad paprastai užtenka nagrinėti kodus, turinčius standartinio pavidalo generuojančią matricą, nes visi kiti kodai yra jiems ekvivalentūs.

2.11 pavyzdys. Turime tiesinį $[5, 3]$ kodą C virš $\mathbb{F}_q$, generuotą matricos G. Raskime kodą, ekvivalentų kodui C, turintį standartinio pavidalo generuojančią matricą.

1. Tegu $q = 5$, t.y. $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$, čia skaičiuojama moduliu 5 (taigi, $-1 = 4$, $5 = 0$, $6 = 1$ ir t.t.). Tegu

$$G = \begin{pmatrix} 4 & 3 & 1 & 4 & 3 \\ 3 & 1 & 2 & 0 & 4 \\ 4 & 1 & 4 & 2 & 4 \end{pmatrix}.$$

Bandome suvesti G į standartinį pavidalą. Bandydami ir rasime tiesiškai nepriklausomų stulpelių numerius s_1, s_2, s_3. Naudosime standartines matricų eilučių operacijas, išvardintas 32 puslapyje prieš (5) lygybę. Trumpai prisiminkime, kaip jos taikomos. Taigi, pirmą matricos G stulpelį norime perdaryti į pirmą vienetinės matricos stulpelį, t.y. pirmoje koordinatėje norime gauti 1, kitur — 0.

Kad vietoj 4 gautume 1, pirmą eilutę turime padalinti iš 4, arba, kitaip sakant, padauginti iš 4^{-1}. Bet kas tai yra elemento 4 atvirkštinis elementas 4^{-1}? Tai toks elementas, kurį padauginę iš 4, gauname 1 (prisiminkime, kad visos operacijos atliekamos moduliu 5). Nesunkiai įsitikiname, kad $4^{-1} = 4$, nes $4 \cdot 4 = 16 \equiv 1 \pmod 5$. Taigi, pirmą eilutę dauginame iš 4.

Toliau, antroje pirmo stulpelio pozicijoje reikia vietoj 3 gauti 0. Tam pirmą eilutę, padaugintą iš kažkokio skaičiaus h, pridėsime prie antros. Kam lygus h? Jį galime rasti iš lygybės $4h + 3 = 0$ (pirmos eilutės pirmą elementą dauginame iš h, pridedame prie antros eilutės pirmo elemento, ir gauname 0), t.y. $h = (-3)4^{-1} = 2 \cdot 4 = 8 = 3$. Be abejo, h galėjome rasti ir kitaip: iš pradžių pirmą eilutę padaliname iš 4, kad gautume pirmoje pozicijoje 1, o tada padauginame iš -3. Tada aišku, kad pridėję pirmą eilutę prie antros, pirmoje pozicijoje gausime 0, nes sudėsime -3 iš pirmos eilutės su 3 iš antros. Bet ir tokiu būdu gausime tą patį h, nes jei daliname iš 4 ir dauginame iš -3, tai $h = 4^{-1}(-3) = 3$. Taigi, pirmą eilutę padauginame iš 3 ir pridedame prie antros. Lygiai taip pat apskaičiuojame, iš ko reikia padauginti pirmą eilutę, kad pridėję ją prie trečios, gautume 0 pirmoje pozicijoje. Gauname:

$$G = \begin{pmatrix} 4 & 3 & 1 & 4 & 3 \\ 3 & 1 & 2 & 0 & 4 \\ 4 & 1 & 4 & 2 & 4 \end{pmatrix} \begin{matrix} \cdot 4 \\ \\ \cdot 4 \end{matrix} \begin{matrix} \cdot 3 \\ \downarrow \\ \\ \end{matrix} \begin{matrix} \\ \\ \downarrow \end{matrix} \sim \begin{pmatrix} 1 & 2 & 4 & 1 & 2 \\ 0 & 0 & 0 & 2 & 3 \\ 0 & 3 & 3 & 3 & 1 \end{pmatrix}.$$

Dabar antrame stulpelyje norime gauti antrą vienetinės matricos stulpelį, t.y. atitinkamai 0, 1 ir 0. Bet antro stulpelio antroje pozicijoje dabar stovi 0 — kad ir iš ko daugintume antrą eilutę, vistiek negausime 1. Tokiu atveju ieškome eilutės, kurios antroje pozicijoje yra ne nulis. Viršuje (virš antros eilutės) ieškoti negalime, nes ten jau sutvarkyta (jau pirmos eilutės pirmoje pozicijoje stovi 1, todėl pirmos eilutės perkelti kitur negalime), galime ieškoti tik apačioje (po antra eilute). Matome, kad trečia eilutė tinka, todėl sukeičiame antrą ir trečią eilutes vietomis:

$$G \sim \begin{pmatrix} 1 & 2 & 4 & 1 & 2 \\ 0 & 0 & 0 & 2 & 3 \\ 0 & 3 & 3 & 3 & 1 \end{pmatrix} \begin{matrix} \\ \updownarrow \\ \\ \end{matrix} \sim \begin{pmatrix} 1 & 2 & 4 & 1 & 2 \\ 0 & 3 & 3 & 3 & 1 \\ 0 & 0 & 0 & 2 & 3 \end{pmatrix}.$$

Gauname antrą vienetinės matricos stulpelį:

$$G \sim \begin{pmatrix} 1 & 2 & 4 & 1 & 2 \\ 0 & 3 & 3 & 3 & 1 \\ 0 & 0 & 0 & 2 & 3 \end{pmatrix} \begin{matrix} \cdot 2 \\ \\ \cdot 0 \end{matrix} \begin{matrix} \cdot 1 \\ \uparrow \\ \downarrow \end{matrix} \sim \begin{pmatrix} 1 & 0 & 2 & 4 & 3 \\ 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & 2 & 3 \end{pmatrix}.$$

Vėl ta pati problema — trečio stulpelio trečioje pozicijoje nepavyks padaryti 1, ir ieškoti eilutės, su kuria būtų galima sukeisti trečią eilutę, nebėra kur (ieškoti galime tik apačioje,

t.y. po trečia eilute). Tai reiškia, kad pirmi trys stulpeliai yra tiesiškai priklausomi, ir juose padaryti vienetinės matricos nepavyks. Nieko tokio, kažkur vistiek pavyks, tai renkamės kitą stulpelį. Imkime kitą stulpelį — einant iš eilės, ketvirtą, — ir bandykime jame gauti vienetinės matricos trečią stulpelį. Tai visai nesunku:

$$G \sim \begin{pmatrix} 1 & 0 & 2 & 4 & 3 \\ 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & 2 & 3 \end{pmatrix} \begin{matrix} \\ \\ \cdot 3 \end{matrix} \quad \begin{matrix} \\ \\ \cdot 2 \uparrow \end{matrix} \quad \begin{matrix} \\ \\ \cdot 3 \uparrow \end{matrix} \sim \begin{pmatrix} 1 & 0 & 2 & 0 & 2 \\ 0 & 1 & 1 & 0 & 3 \\ 0 & 0 & 0 & 1 & 4 \end{pmatrix}.$$

Gavome (5) lygybės pavidalo matricą su vienetinės matricos stulpeliais 1, 2 ir 4 pozicijose. Sukėlę šiuos stulpelius į pradžią (t.y. sukeitę trečią ir ketvirtą stulpelius vietomis), gauname standartinio pavidalo generuojančią matricą

$$G' = \begin{pmatrix} 1 & 0 & 0 & 2 & 2 \\ 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 1 & 0 & 4 \end{pmatrix},$$

kuri nėra kodo C generuojanti matrica (kaip matėme, kodas C neturi standartinio pavidalo generuojančios matricos, nes jo generuojančios matricos pirmi trys stulpeliai yra tiesiškai priklausomi), bet generuoja ekvivalentų kodą C', kuris nuo kodo C skiriasi tik tuo, kad jame trečia ir ketvirta koordinatė yra sukeistos vietomis.

2. Tegu $q = 9$. Skaičiavimams naudosime kūno $\mathbb{F}_9$ lentelę iš 30 puslapio (3 lentelė, 1.4 pavyzdys).

   Tegu

$$G = \begin{pmatrix} \alpha^2 & \alpha & \alpha^6 & \alpha^4 & \alpha^3 \\ 1 & \alpha^2 & \alpha^5 & \alpha^3 & \alpha \\ \alpha^6 & \alpha^2 & \alpha^3 & \alpha^4 & 1 \end{pmatrix}$$

   ir $x = (\alpha^2, \alpha^4, \alpha)$. Lygiai taip pat, kaip pereitame pavyzdyje apskaičiuojame, iš ko reikia dauginti pirmą eilutę, kad gautume pirmą vienetinės matricos stulpelį. Pavyzdžiui, kad vietoj α^2 gautume 1, pirmą eilutę dauginame iš $\left(\alpha^2\right)^{-1} = \alpha^{-2} = \alpha^6$. Kad gautume 0 vietoj 1 antros eilutės pirmoje pozicijoje, pirmą eilutę padauginame iš tokio h, kad $\alpha^2 h + 1 = 0$, t.y. $h = (-1)\left(\alpha^2\right)^{-1} = 2\alpha^{-2} = \alpha^4\alpha^6 = \alpha^1 0 = \alpha^2$ (galima buvo skaičiuoti ir taip: $2\alpha^{-2} = 2\alpha^6 = 2(\alpha + 2) = 2\alpha + 1 = \alpha^2$), ir pridedame prie antros. Taip pat, kad gautume 0 vietoj α^6 trečios eilutės pirmoje pozicijoje, pirmą eilutę padauginame iš tokio h, kad $\alpha^2 h + \alpha^6 = 0$, t.y. $h = (-\alpha^6)\left(\alpha^2\right)^{-1} = 2\alpha^6\alpha^{-2} = \alpha^4\alpha^6\alpha^6 = \alpha^1 6 = 1$, ir pridedame prie trečios. Ir t.t.

$$\begin{aligned} G &= \begin{pmatrix} \alpha^2 & \alpha & \alpha^6 & \alpha^4 & \alpha^3 \\ 1 & \alpha^2 & \alpha^5 & \alpha^3 & \alpha \\ \alpha^6 & \alpha^2 & \alpha^3 & \alpha^4 & 1 \end{pmatrix} \begin{matrix} \cdot\alpha^6 \\ \\ \\ \end{matrix} \quad \begin{matrix} \cdot\alpha^2 \downarrow \\ \\ \\ \end{matrix} \quad \begin{matrix} \cdot 1 \\ \\ \downarrow \end{matrix} \\ &\sim \begin{pmatrix} 1 & \alpha^7 & \alpha^4 & \alpha^2 & \alpha \\ 0 & \alpha & \alpha^2 & 1 & 0 \\ 0 & 1 & 1 & 1 & \alpha^5 \end{pmatrix} \begin{matrix} \cdot\alpha^7 \\ \\ \\ \end{matrix} \quad \begin{matrix} \cdot\alpha^2 \uparrow \\ \\ \\ \end{matrix} \quad \begin{matrix} \cdot\alpha^3 \\ \\ \downarrow \end{matrix} \\ &\sim \begin{pmatrix} 1 & 0 & 1 & \alpha^6 & \alpha \\ 0 & 1 & \alpha & \alpha^7 & 0 \\ 0 & 0 & \alpha^2 & \alpha^5 & \alpha^5 \end{pmatrix} \begin{matrix} \\ \\ \cdot\alpha^6 \end{matrix} \quad \begin{matrix} \\ \\ \cdot\alpha^3 \uparrow \end{matrix} \quad \begin{matrix} \\ \\ \cdot\alpha^2 \uparrow \end{matrix} \\ &\sim \begin{pmatrix} 1 & 0 & 0 & \alpha^5 & \alpha^2 \\ 0 & 1 & 0 & \alpha^6 & 1 \\ 0 & 0 & 1 & \alpha^3 & \alpha^3 \end{pmatrix} = G' \end{aligned}$$

   Matome, kad kodas C turi standartinio pavidalo generuojančią matricą. Kadangi kodas visada yra sau ekvivalentus (su tapačiąja perstata σ gauname, kad $\sigma(C) = C$), tai gavome ekvivalentų kodą C' (šiuo atveju $C' = C$), turintį standartinio pavidalo generuojančią matricą.

□

Pastebėkime, kad kodavimo procedūra $x \mapsto xG$, kai naudojama standartinio pavidalo generuojanti matrica $G = (I|A)$, yra paprastesnė. Iš tikro, jei $x = (x_1, \ldots, x_k)$, tai

$$xG = x(I|A) = (xI|xA) = (x|xA) = (x_1, \ldots, x_k, c_{k+1}, \ldots, c_n),$$

kur $(c_{k+1}, \ldots, c_n) = xA$. Taigi, koduojant prie ilgio k vektoriaus x tiesiog prijungiame $n-k$ kontrolinių simbolių $(c_{k+1}, \ldots, c_n)$, gautų dauginant x iš matricos A. Vėliau matysime, kad standartinio pavidalo generuojanti matrica supaprastina ir dekodavimą.

2.12 pavyzdys. Vektorių x užkoduokime, naudodami 2.11 pavyzdyje gautas standartinio pavidalo generuojančias matricas.

1. Tegu $x = (142)$. Koduodami vektorių x kodu C' iš 2.11 pavyzdžio pirmos dalies, gauname kodo žodį $xG' = (14212)$. Matome, kad iš tikro užkoduotame vektoriuje pirmos $k = 3$ koordinatės yra iš pradinio vektoriaus x.

2. Užkodavę vektorių $x = (\alpha^2, \alpha^4, \alpha)$ kodu C' iš 2.11 pavyzdžio antros dalies, gauname $xG' = (\alpha^2, \alpha^4, \alpha, 1, 0)$.

□

2.13 pavyzdys. Rasti I dalies 2 skyriuje duotų paprastų pavyzdžių generuojančias matricas.

1. *Pakartojimo kodas R_n.* Tai dvinaris kodas. Priminsiu, kad 0 užkoduojame $00\cdots0$, 1 — $11\cdots1$ (pakartojame 0 ar 1 n kartų). Jei šis kodas yra tiesinis, tai jo generuojanti matrica G bus tokia, kad $0 \cdot G = 00\cdots0$ ir $1 \cdot G = 11\cdots1$. Taigi, G bus $1 \times n$ matrica. Nesunku pastebėti, kad $G = (11\cdots1)$.

2. *Kontrolinio simbolio kodas.* Irgi dvinaris kodas. Pranešimą $x = (x_1, x_2, \ldots, x_k)$ užkoduojame vektoriumi $c = (x_1, x_2, \ldots, x_k, x_{k+1})$, kur $x_{k+1} \equiv \sum_{i=1}^{k} x_i \pmod 2$. Jei užrašytume kūno $\mathbb{F}_2$ operacijomis, tai gautume

$$x_{k+1} = \sum_{i=1}^{k} x_i. \tag{6}$$

Taigi, jei šis kodas yra tiesinis, tai jo generuojanti matrica G tenkins $xG = c$. Matome, kad tai $k \times (k+1)$ matrica. Aišku, kad ji yra standartinio pavidalo, nes pirmos k kodo žodžio c koordinatės lygios vektoriui x. Taigi, pirmuose k matricos G stulpelių stovi $k \times k$ vienetinė matrica. Lieka išsiaiškinti, kaip atrodo $(k+1)$-asis matricos G stulpelis. Prisiminę, kaip dauginamas vektorius ir matrica, matome, kad jei matricos G $(k+1)$-asis stulpelis yra $(g_1, g_2, \ldots, g_k)^T$ (čia ir toliau y^T yra transponuotas vektorius ar matrica y), tai vektoriaus xG $(k+1)$-oji koordinatė yra lygi $\sum_{i=1}^{k} g_i x_i$. Matome, kad (6) lygybėje esančią sumą gauname tada, kai visi g_i yra lygūs 1. Taigi, $(k+1)$-asis matricos G stulpelis yra sudarytas tik iš vienetų. Todėl kontrolinio simbolio kodas yra tiesinis, ir jo generuojanti matrica yra

$$G = \begin{pmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & 1 & \cdots & 0 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 1 \end{pmatrix}.$$

3. *ISBN kodas.* Vektorių $(a_1, a_2, \ldots, a_9)$, sudarytą iš dešimtainių skaitmenų, užkoduojame vektoriumi $(a_1, a_2, \ldots, a_{10})$, kur $a_{10} \equiv \sum_{i=1}^{9} i a_i \pmod{11}$, t.y.

$$a_{10} = \sum_{i=1}^{9} i a_i \tag{7}$$

kūne $\mathbb{F}_{11}$. Vėlgi matome, kad matrica G yra standartinio pavidalo, o paskutinis — dešimtas — stulpelis pagal (7) lygybę yra $(1, 2, \ldots, 9)^T$. Taigi, matrica bus

$$G = \begin{pmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & 1 & \cdots & 0 & 2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 9 \end{pmatrix}.$$

4. *Asmens kodo* kodavimui naudojamą matricą galime gauti analogiškai, kaip ir ISBN kodui. Paliekama skaitytojui.

5. *Kodas $[t^2 + 2t, t^2]$, kai $t = 2$.* Tai $[8, 4]$ dvinaris kodas. Nesunku pastebėti, kad jis vektorių $x = (x_1, x_2, x_3, x_4)$ užkoduoja vektoriumi $c = (x_1, x_2, x_1 + x_2, x_3, x_4, x_3 + x_4, x_1 + x_3, x_2 + x_4)$. Taip pat, kaip anksčiau, randame generuojančios matricos G stulpelius. Pavyzdžiui, kadangi sandaugos xG rezultato c trečia koordinatė yra $x_1 + x_2 = 1 \cdot x_1 + 1 \cdot x_2 + 0 \cdot x_3 + 0 \cdot x_4$, tai trečias matricos G stulpelis bus $(1, 1, 0, 0)^T$. Taigi, kodo generuojanti matrica bus

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

6. $[7, 4]$ *Hemingo kodas.* Tai $[7, 4]$ dvinaris kodas. Nesunku pastebėti, kad jis vektorių $x = (x_1, x_2, x_3, x_4)$ užkoduoja vektoriumi $c = (x_1, x_2, x_3, x_4, x_1 + x_2 + x_3, x_2 + x_3 + x_4, x_1 + x_3 + x_4)$. Taigi, kodo generuojanti matrica bus

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

□

2.3 Dualus kodas ir kontrolinė matrica

2.3.1 Dualus kodas

Tegu $x = (x_1, \ldots, x_n)$ ir $y = (y_1, \ldots, y_n)$ yra erdvės $\mathbb{F}_q^n$ vektoriai. Jų *skaliarine sandauga* vadinsime įprastą vektorių skaliarinę sandaugą, t.y.

$$x \cdot y = x_1 y_1 + \cdots + x_n y_n,$$

čia $x \cdot y \in \mathbb{F}_q$, t.y. sandaugos ir sumos operacijos atliekamos kūne $\mathbb{F}_q$. Vektoriai vadinami *ortogonaliais (statmenais)*, jei jų skaliarinė sandauga lygi nuliui. Pavyzdžiui, vektoriai 111 ir 101 yra ortogonalūs virš baigtinio kūno $\mathbb{F}_2$, nes

$$111 \cdot 101 = 1 \cdot 1 + 1 \cdot 0 + 1 \cdot 1 = 1 + 0 + 1 = 0.$$

Apibrėžimas. *Tegu $C[n,k]$ yra tiesinis kodas virš $\mathbb{F}_q$. Kodo C* dualus kodas, *žymimas $C^\perp$, yra kodo C ortogonali erdvė, t.y. aibė vektorių, ortogonalių kiekvienam kodo C žodžiui:*

$$C^\perp = \{x \in \mathbb{F}_q^n : x \cdot y = 0 \ \forall y \in C\}.$$

2.14 pavyzdys. Tarkime, dvinaris tiesinis kodas $C[3,2]$ yra generuotas matricos

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

Kaip 2.2 pavyzdyje galime gauti, kad $C = \{000, 110, 101, 011\}$. Kodo C dualus kodas $C^\perp$ bus sudarytas iš tų erdvės $\mathbb{F}_2^3$ vektorių (jų yra aštuoni: $000, 001, 010, 011, 100, 101, 110, 111$), kurie ortogonalūs kiekvienam kodo C vektoriui. Nesunkiai patikriname, kad tik du vektoriai tenkina šią sąlygą: $C^\perp = \{000, 111\}$. □

Pastaba. Ortogonalumo sąvoka erdvėse virš baigtinių kūnų skiriasi nuo ortogonalumo sąvokos virš realiųjų skaičių kūno. Pavyzdžiui, erdvėje $\mathbb{R}^n$ tik nulinis vektorius yra ortogonalus pats sau, todėl bet kurios $\mathbb{R}^n$ erdvės ir jos ortogonalios erdvės sankirta visada yra $\{0\}$ (pavyzdžiui, plokštumos ir jai statmenos tiesės). Erdvėse virš baigtinių kūnų ši savybė nebegalioja, pavyzdžiui, vektorius $x = (1, 1, 0, \ldots, 0) \in \mathbb{F}_2^n$ yra ortogonalus pats sau, nes $x \cdot x = 1 + 1 = 0$, todėl gali būti, kad $x \in C$ ir $x \in C^\perp$. Gali netgi būti, kad visi kodo C vektoriai yra ortogonalūs visiems kodo vektoriams, todėl $C \subseteq C^\perp$.

2.15 teorema. *Tiesinio kodo $C[n,k]$ dualus kodas yra tiesinis $[n, n-k]$ kodas.*

Be įrodymo.

2.16 pavyzdys. Iš tiesų, 2.14 pavyzdžio dualus kodas $C^\perp = \{000, 111\}$ yra tiesinis $[3,1]$ kodas, jo generuojanti matrica yra $G^\perp = (111)$. □

2.17 teiginys. *Bet kuriam tiesiniam kodui C turime, kad $(C^\perp)^\perp = C$.*

Įrodymas. Visų pirma parodysime, kad $C \subseteq (C^\perp)^\perp$. Tarkime, $x \in C$. Bet kuris kodo C žodis yra ortogonalus bet kuriam kodo $C^\perp$ žodžiui, todėl $x \cdot y = 0 \ \forall y \in C^\perp$. Bet tai savo ruožtu reiškia, kad $x \in (C^\perp)^\perp$. Todėl $C \subseteq (C^\perp)^\perp$.

Iš kitos pusės, ką tik matėme, kad jei C yra $[n,k]$ kodas, tai $C^\perp$ yra tiesinis $[n, n-k]$ kodas. Analogiškai gauname, kad $(C^\perp)^\perp$ yra $[n, n-(n-k)]$, t.y. $[n,k]$ kodas.

Taigi, $C \subseteq (C^\perp)^\perp$ ir $\dim C = \dim(C^\perp)^\perp$, todėl $C = (C^\perp)^\perp$. □

Taigi, įrodėme, kad jei $C^\perp = D$, tai $D^\perp = C$. Todėl visus tiesinius kodus galima suskirstyti į poras, kur kiekvienoje poroje kodai yra vienas kitam dualūs.

Pavyzdys. 2.14 pavyzdyje matėme, kad kodo $C = \{000, 110, 101, 011\}$ dualus kodas yra $C^\perp = \{000, 111\}$. Lygiai taip pat nesunkiai galime įsitikinti, kad kodo $C^\perp$ dualus kodas yra $(C^\perp)^\perp = \{000, 110, 101, 011\} = C$. □

2.3.2 Ekvivalenčių kodų dualūs kodai

Ekvivalenčių kodų dualūs kodai taip pat ekvivalentūs. Ir netgi daugiau, jie ekvivalentūs su ta pačia perstata. Tiksliau, galioja toks teiginys.

2.18 teiginys. *Jei C ir C' yra ekvivalentūs kodai, ir σ yra tokia perstata, kad $C' = \sigma(C)$, tai $C'^{\perp} = \sigma(C^{\perp})$.*

Įrodymas.

$$\begin{aligned}
& x \in C'^{\perp} \\
\iff \quad & x \cdot y = 0 \ \forall y \in C' = \sigma(C) && (8)\\
\iff \quad & x \cdot \sigma(c) = 0 \ \forall c \in C && (9)\\
\iff \quad & \sigma^{-1}(x) \cdot c = 0 \ \forall c \in C && (10)\\
\iff \quad & \sigma^{-1}(x) \in C^{\perp} \\
\iff \quad & x \in \sigma(C^{\perp}).
\end{aligned}$$

Ką ir reikėjo įrodyti. Pakomentuosime įrodymą. (8) ir (9) yra ekvivalentūs, nes jei $y \in \sigma(C)$, tai egzistuoja toks $c \in C$, kad $y = \sigma(c)$, ir c perbėga C tada ir tik tada, kai $y = \sigma(c)$ perbėga $\sigma(C)$. (9) ir (10) yra ekvivalentūs, nes skaliarinė sandauga nepasikeičia, jei abiejų vektorių koordinates perstatome, naudodami tą pačią perstatą. Šiuo atveju naudojome perstatą σ^{-1} ir pasinaudojome tuo, kad $\sigma^{-1}(\sigma(c)) = c$. □

2.3.3 Kontrolinės matricos apibrėžimas ir savybės

Apibrėžimas. *Tiesinio kodo* kontroline matrica *vadiname jo dualaus kodo generuojančią matricą.*

Kaip ir generuojančią matricą, taip ir kontrolinę matricą kodas gali turėti ne vieną.

Tiesinio kodo kontrolinė matrica, kaip ir generuojanti matrica, vienareikšmiškai apibrėžia kodą. Kartais yra patogiau nurodyti kodą pateikiant kontrolinę, o ne generuojančią matricą, nes kontrolinė matrica leidžia nesunkiai patikrinti, ar duotas vektorius priklauso kodui (todėl ir vadinasi „kontroline“). Iš tikro, galioja toks teiginys.

Čia ir toliau y^T žymi transponuotą vektorių ar matricą y.

2.19 teiginys. *Tarkime, H yra tiesinio kodo $C[n,k]$ virš $\mathbb{F}_q$ kontrolinė matrica, $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$. Vektorius $x \in C$ tada ir tik tada, kai $Hx^T = 0$.*

Įrodymas. Atkreipkime dėmesį, kad jei $H_1, \ldots, H_{n-k}$ pažymėtume matricos H eilutes, tai

$$Hx^T = (H_1 \cdot x, \ldots, H_{n-k} \cdot x)^T, \tag{11}$$

čia $H_i \cdot x$ yra vektorių skaliarinė sandauga.

Visų pirma parodykime, kad jei $Hx^T = 0$, tai $x \in C$. Pagal (11) lygybę, $Hx^T = 0$ reiškia, kad vektorius x yra ortogonalus kiekvienai matricos H eilutei. Bet tokiu atveju vektorius x yra ortogonalus kiekvienam kodo $C^{\perp}$ vektoriui y, nes y gali būti išreikštas kodo $C^{\perp}$ bazės vektorių (t.y. matricos H eilučių) tiesine kombinacija $y = a_1 H_1 + \cdots + a_{n-k} H_{n-k}$, ir tada

$$y \cdot x = (a_1 H_1 + \cdots + a_{n-k} H_{n-k}) \cdot x = a_1 (H_1 \cdot x) + \cdots + a_{n-k} (H_{n-k} \cdot x) = 0 + \cdots + 0 = 0.$$

Todėl pagal dualaus kodo apibrėžimą $x \in (C^\perp)^\perp = C$.

Dabar įrodysime į kitą pusę. Kadangi $C = (C^\perp)^\perp$, tai $x \in C$ reiškia, kad $x \in (C^\perp)^\perp$. Pagal dualaus kodo apibrėžimą, vektorius x yra ortogonalus kiekvienam kodo $C^\perp$ vektoriui, o tuo pačiu ir matricos H eilutėms $H_1, \ldots, H_{n-k}$, todėl $Hx^T = 0$. □

Nesunku pastebėti, kad, kadangi H yra $(n-k) \times n$ matrica, x^T yra n ilgio vektorius-stulpelis, tai Hx^T yra $n-k$ ilgio vektorius-stulpelis.

Pavyzdys. Tarkime, dvinario tiesinio kodo C kontrolinė matrica yra

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

Patikrinkime, pavyzdžiui, ar vektorius $x = (010)$ priklauso kodui C:

$$Hx^T = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Todėl $x \notin C$. □

2.3.4 Kontrolinės matricos radimas

Dabar parodysime, kaip nesunkiai galima rasti kodo kontrolinę matricą. Žymėkime I_k vienetinę $k \times k$ matricą. Jei B ir B' yra tiek pat eilučių turinčios matricos, tai $(B|B')$ bus matrica, gauta sujungus abi matricas į vieną (tiesiog prie matricos B stulpelių prijungiame matricos B' stulpelius). Jei B ir B' yra atitinkamai $k \times n_1$ ir $k \times n_2$ matricos, tai $(B|B')$ bus $k \times (n_1 + n_2)$ matrica.

2.20 teiginys. *Jei $G = (I_k|A)$ yra kodo C generuojanti matrica, tai $H = (-A^T|I_{n-k})$ yra kodo C kontrolinė matrica.*

Be įrodymo.

Taigi, suvedę kodo generuojančią matricą į standartinį pavidalą, galime rasti kontrolinę matricą.

2.21 pavyzdys. Rasime 2.6 pavyzdžio kodo C kontrolinę matricą H. Tam turime suvesti generuojančią matricą G į standartinį pavidalą ir pasinaudoti 2.20 teiginiu. Matrica G jau buvo suvesta į standartinį pavidalą 2.8 pavyzdyje:

$$G = \begin{pmatrix} 2 & 1 & 0 & 2 \\ 1 & 1 & 2 & 0 \end{pmatrix} \sim \left(\begin{array}{cc|cc} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{array}\right).$$

Todėl kontrolinė matrica

$$H = \left(\begin{array}{cc|cc} -1 & -1 & 1 & 0 \\ -2 & -1 & 0 & 1 \end{array}\right) = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}.$$ □

2.20 teiginys leidžia rasti kontrolinę matricą, jei kodas turi standartinio pavidalo generuojančią matricą. Jei kodas neturi standartinio pavidalo generuojančios matricos, pasinaudojame tuo, kad kiekvienas kodas ekvivalentus kodui, turinčiam standartinio pavidalo generuojančią matricą, ir 2.18 teiginiu.

2.22 pavyzdys. Matėme, kad 2.11 pavyzdžio pirmos dalies kodas C neturi standartinio pavidalo generuojančios matricos. Raskime jo kontrolinę matricą.

Prisiminkime, kad bandydami suvesti kodo C generuojančią matricą G į standartinį pavidalą, gavome vienetinės matricos stulpelius 1, 2 ir 4 pozicijose:

$$G = \begin{pmatrix} 4 & 3 & 1 & 4 & 3 \\ 3 & 1 & 2 & 0 & 4 \\ 4 & 1 & 4 & 2 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 2 & 0 & 2 \\ 0 & 1 & 1 & 0 & 3 \\ 0 & 0 & 0 & 1 & 4 \end{pmatrix}.$$

Pritaikę kodui C perstatą

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix},$$

gauname kodui C ekvivalentų kodą $C' = \sigma(C)$, kurio generuojanti matrica

$$G' = \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 2 & 2 \\ 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 1 & 0 & 4 \end{array}\right)$$

yra standartinio pavidalo. Pasinaudoję 2.20 teiginiu, galime rasti kodo C' kontrolinę matricą:

$$H' = \left(\begin{array}{ccc|cc} -2 & -1 & 0 & 1 & 0 \\ -2 & -3 & -4 & 0 & 1 \end{array}\right) = \begin{pmatrix} 3 & 4 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 1 \end{pmatrix}.$$

Kadangi $C' = \sigma(C)$, tai pagal 2.18 teiginį $C'^{\perp} = \sigma(C^{\perp})$, t.y. $C^{\perp} = \sigma^{-1}(C'^{\perp})$. Taigi, pritaikę kodui $C'^{\perp}$ atvirkštinę perstatą

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix},$$

gausime mūsų ieškomą dualų kodą $C^{\perp}$. Tai reiškia, kad matrica

$$H = \begin{pmatrix} 3 & 4 & 1 & 0 & 0 \\ 3 & 2 & 0 & 1 & 1 \end{pmatrix},$$

gauta sukeitus matricos H' stulpelius pagal perstatą σ^{-1}, bus kodo $C^{\perp}$ generuojanti matrica, t.y. kodo C kontrolinė matrica. □

2.23 užduotis. Rasti I dalies 2 skyriuje duotų paprastų pavyzdžių kontrolines matricas (pasinaudoti 2.13 pavyzdžiu).

Pastaba. Tarkime, turime tiesinio kodo C kontrolinę matricą H ir norime rasti generuojančią matricą G. Matrica H yra kodo $C^{\perp}$ generuojanti matrica. Pagal 2.17 teiginį $(C^{\perp})^{\perp} = C$, todėl matrica G yra kodo $C^{\perp}$ kontrolinė matrica. Taigi, matricą G galime rasti pasinaudoję 2.20 teiginiu: suvedame matricą H į standartinį pavidalą ir randame G.

2.24 pavyzdys. Jei tiesinio kodo virš $\mathbb{F}_3$ kontrolinė matrica yra

$$H = \begin{pmatrix} 2 & 1 & 0 & 2 \\ 1 & 1 & 2 & 0 \end{pmatrix},$$

tai generuojančią matricą G randame lygiai taip pat, kaip 2.21 pavyzdyje. Gauname, kad

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

□

Matėme, kad rasti tiesinio kodo kontrolinę matricą nėra sunku. Taip pat, kaip rodo kitas teiginys, nėra sunku ir nustatyti, ar duota matrica yra duoto kodo kontrolinė matrica, ar ne.

2.25 teiginys. *Tegu C yra tiesinis $[n,k]$ kodas virš $\mathbb{F}_q$, generuotas matricos G, o H yra matrica virš $\mathbb{F}_q$. Matrica H yra kodo C kontrolinė matrica tada ir tik tada, kai H yra $(n-k)\times n$ matrica, jos rangas yra $n-k$, ir $GH^T=0$ (čia 0 yra $k\times(n-k)$ matrica, sudaryta vien iš nulių).*

2.26 užduotis. Įrodyti teiginį.

Sprendimas. Pastebėsime, kad sandaugos $U=GH^T$ i-tojoje eilutėje bei j-ajame stulpelyje stovintis elementas u_{ij} yra matricos G i-tosios eilutės ir matricos H j-osios eilutės skaliarinė sandauga.

" $\Longrightarrow$ " Išplaukia iš 2.15 teoremos (dualaus kodo dimensija, kartu ir kontrolinės matricos eilučių skaičius, yra $n-k$), generuojančios matricos apibrėžimo (kontrolinės matricos visos eilutės yra tiesiškai nepriklausomi vektoriai, todėl jos rangas yra $n-k$), ir iš to, kad visi kodo C žodžiai (įskaitant ir jo generuojančios matricos G eilutes) yra ortogonalūs visiems kodo $C^\perp$ žodžiams (tuo pačiu ir jo generuojančios matricos H eilutėms).

" $\Longleftarrow$ " Kadangi $(n-k)\times n$ matricos H rangas yra $n-k$, tai jos eilutės yra tiesiškai nepriklausomos. Pažymėkime D matricos H generuotą kodą. Kaip ir 2.19 teiginio įrodyme, gauname, kad, kadangi $GH^T=0$, tai visi kodo C žodžiai yra ortogonalūs visiems kodo D žodžiams, todėl $D\subseteq C^\perp$. Be to, $\dim D=n-k=\dim C^\perp$. Todėl $D=C^\perp$ ir H yra kodo C kontrolinė matrica. □

Pavyzdys. Tegu $C[3,1]$ yra dvinaris tiesinis kodas, generuotas matricos $G=(111)$. Patikrinkime, ar matrica

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

yra kodo C kontrolinė matrica. Iš tikro, nesunku įsitikinti, kad matrica H tenkina teiginio reikalavimus: tai 2×3 dvinarė matrica, jos rangas yra 2, ir $GH^T=0$. □

2.3.5 Kontrolinė matrica ir minimalus atstumas

Kodo kontrolinė matrica gali praversti ir nustatant kodo minimalų atstumą.

2.27 teorema. *Tegu H yra tiesinio kodo C kontrolinė matrica. Kodo C minimalus atstumas yra lygus d tada ir tik tada, kai egzistuoja d tiesiškai priklausomų matricos H stulpelių, o bet kuri $d-1$ šios matricos stulpelių sistema yra tiesiškai nepriklausoma.*

Be įrodymo.

Kitaip tariant, kodo C minimalus atstumas d yra toks mažiausias skaičius, kad egzistuoja d tiesiškai priklausomų kodo C kontrolinės matricos H stulpelių.

Pavyzdys. Tegu $C[3,1]$ yra dvinaris tiesinis kodas, kurio kontrolinė matrica yra

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

Norėdami rasti kodo C minimalų atstumą, pradėdami nuo $d=1$ ieškokime tokio d, kad egzistuotų d tiesiškai priklausomų matricos H stulpelių.

Tegu $d=1$. Ar egzistuoja d tiesiškai priklausomų matricos H stulpelių? Kaip matėme 1.2 poskyryje, aibė iš vieno vektoriaus yra tiesiškai priklausoma tik tada, kai tas vektorius yra nulinis. Matrica H nulinių stulpelių neturi, tai visos aibės iš vieno stulpelio yra tiesiškai nepriklausomos. Todėl kodo C minimalus atstumas nėra 1.

Tegu $d = 2$. Ar egzistuoja d tiesiškai priklausomų matricos H stulpelių? Kaip matėme 1.2 poskyryje, dviejų dvinarių vektorių rinkinys yra tiesiškai priklausomas tada ir tik tada, kai tie vektoriai yra lygūs. Bet matrica H lygių stulpelių neturi, tai visos aibės iš dviejų stulpelių yra tiesiškai nepriklausomos. Todėl kodo C minimalus atstumas nėra 2.

Lieka patikrinti $d = 3$. Ar egzistuoja d tiesiškai priklausomų matricos H stulpelių? Taip, nes matome, kad trečias stulpelis yra pirmų dviejų suma, o tai ir reiškia, kad šie trys stulpeliai yra tiesiškai priklausomi. Todėl kodo C minimalus atstumas yra 3.

Ir iš tikro, nesunku įsitikinti, kad kodo C generuojanti matrica yra $G = (111)$, todėl $C = \{000, 111\}$ — aišku, kad mažiausias atstumas tarp skirtingų kodo C žodžių yra 3. □

2.3.6 Savidualūs kodai

Apibrėžimas. *Jei $C \subseteq C^\perp$, kodas C vadinamas* silpnai savidualiu. *Jei $C = C^\perp$, kodas C vadinamas* (griežtai) savidualiu.

Pavyzdys. Dvinaris pakartojimo kodas R_n yra silpnai savidualus tada ir tik tada, kai n yra lyginis. Iš tikrųjų, $R_n = \{0\cdots0, 1\cdots1\}$, kur žodžių ilgis yra n. Kada R_n yra silpnai savidualus, t. y. kada $R_n \subseteq R_n^\perp$? Aišku, kad $0\cdots0$ visada priklauso $R_n^\perp$, nes $R_n^\perp$ yra tiesinis kodas. Lieka panagrinėti, kada $1\cdots1 \in R_n^\perp$. Pagal dualaus kodo apibrėžimą, $1\cdots1 \in R_n^\perp$ reiškia, kad $1\cdots1$ yra ortogonalus visiems kodo $R_n = \{0\cdots0, 1\cdots1\}$ žodžiams. Žodžiui $0\cdots0$ jis bus ortogonalus visada. Belieka nustatyti, kada jis bus ortogonalus žodžiui $1\cdots1$, t. y. sau pačiam. Aišku, kad $1\cdots1$ bus ortogonalus sau pačiam tada ir tik tada, kai n yra lyginis.

Kai $n = 2$, tai dvinaris pakartojimo kodas $R_2 = \{00, 11\}$ yra savidualus. Patikrinkite patys. □

2.28 teiginys. *Tegu $C[n, k]$ yra tiesinis kodas, generuotas matricos G.*

1. *Kodas C yra silpnai savidualus tada ir tik tada, kai $GG^T = 0$.*
2. *Kodas C yra savidualus tada ir tik tada, kai $k = n/2$ ir $GG^T = 0$.*
3. *Kodas C yra savidualus tada ir tik tada, kai G yra kodo C kontrolinė matrica.*

2.29 užduotis. Įrodyti teiginį.

Sprendimas. 1. Tarkime, tiesinis kodas C yra silpnai savidualus. Tada pagal apibrėžimą $C \subseteq C^\perp$. Taigi, visi kodo C žodžiai yra ortogonalūs visiems kodo C žodžiams (įskaitant ir patiems sau). Tuo pačiu ir visos generuojančios matricos G eilutės yra ortogonalios visoms G eilutėms, todėl $GG^T = 0$.

Tarkime, kad $GG^T = 0$, t.y. visos generuojančios matricos G eilutės yra ortogonalios visoms G eilutėms. Kaip ir 2.19 teiginio įrodyme, gauname, kad visi kodo C žodžiai yra ortogonalūs visiems kodo C žodžiams, todėl $C \subseteq C^\perp$ ir C yra silpnai savidualus.

2. Tarkime, tiesinis $[n, k]$ kodas C yra savidualus. Tada pagal apibrėžimą $C = C^\perp$, todėl $\dim C = \dim C^\perp$. Bet $\dim C^\perp = n - \dim C$, todėl $\dim C = n - \dim C$, t.y. $k = \dim C = n/2$. Be to, C yra silpnai savidualus, todėl pagal 1 dalį $GG^T = 0$.

   Tarkime, turime tokį tiesinį $[n, k]$ kodą C, generuotą matricos G, kurio dimensija $k = n/2$ ir $GG^T = 0$. Pagal 1 dalį C yra silpnai savidualus, t.y. $C \subseteq C^\perp$. Be to, $\dim C^\perp = n - k = n - n/2 = n/2 = \dim C$, todėl $C = C^\perp$ ir kodas C yra savidualus.

3. Tarkime, tiesinis $[n, k]$ kodas C, generuotas matricos G, yra savidualus. Pagal 2 dalį $k = n/2$ ir $GG^T = 0$. Todėl pagal 2.25 teiginį matrica G yra kodo C kontrolinė matrica.

   Tarkime, turime tiesinį kodą C, kurio generuojanti matrica G yra ir kontrolinė kodo C matrica. Tai reiškia, kad $k = n - k$, todėl $k = n/2$. Be to, pagal 2.25 teiginį $GG^T = 0$, todėl pagal 2 dalį kodas C yra savidualus.□

Pavyzdžiai. 1. Tegu $C[4,1]$ yra dvinaris tiesinis kodas, generuotas matricos $G = (1111)$. Pagal teiginio 1 dalį jis yra silpnai savidualus, nes $GG^T = 0$.

2. Tegu $C[4,2]$ yra dvinaris tiesinis kodas, generuotas matricos

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

Pagal teiginio 2 dalį jis yra savidualus, nes $k = 2 = 4/2 = n/2$ ir $GG^T = 0$. □

3 Tiesinių kodų dekodavimas

Tegu $C[n,k,d]$ yra tiesinis kodas virš $\mathbb{F}_q$ (taigi, $C \subset \mathbb{F}_q^n$), generuotas matricos G. Pranešimo $m \in \mathbb{F}_q^k$ kodavimas-dekodavimas gali būti parodytas tokia schema:

$$m \in \mathbb{F}_q^k \xrightarrow{\text{kodavimas}} c = mG \in C \subset \mathbb{F}_q^n \xrightarrow{\text{kanalas}} y = c + e \in \mathbb{F}_q^n \xrightarrow{\text{dekodavimas}} c' \in C \xrightarrow{c'=m'G} m' \in \mathbb{F}_q^k$$

Kanale prie kodo žodžio c pridedamas klaidų vektorius $e \in \mathbb{F}_q^n$, ir iš kanalo gauname vektorių $y = c + e \in \mathbb{F}_q^n$. Dekodavimo metu paprastai visų pirma randame klaidų vektorių $e' \in \mathbb{F}_q^n$ (tikimės, kad $e' = e$), atėmę jį iš y gauname kodo žodį $c' = y - e' \in C$, o tada randame pranešimą $m' \in \mathbb{F}_q^k$, kuris užkoduojamas kodo žodžiu c'. Pranešimas m' randamas pasinaudojus tuo, kad $c' = m'G$. Tai tiesinių lygčių sistema, kuri, jei $c' \in C$, turi lygiai vieną sprendinį. Jei teisingai nustatėme klaidų vektorių (t.y. jei $e' = e$), tai rasime ir teisingą pranešimą (t.y. gausime $m' = m$), o jei ne, tai ne.

Šiame skyriuje pateikiame vieną dekodavimo procedūrą, kuri tinka bet kuriam tiesiniam kodui. Tai dekodavimas, naudojantis standartinę lentelę. Ši procedūra leidžia rasti kodo žodį $c' \in C$, esantį arčiausiai iš kanalo išėjusio vektoriaus y, t.y. realizuoja minimalaus atstumo dekodavimo taisyklę. Tokiu būdu ši procedūra leidžia ištaisyti visas klaidas, jei jų skaičius neviršija $t = [(d-1)/2]$ (o kartais leidžia ištaisyti ir kai viršija).

3.1 Klasės

3.1 apibrėžimas. *Tegu $C[n,k,d]$ yra tiesinis kodas virš $\mathbb{F}_q$. Tegu $a \in \mathbb{F}_q^n$.* Klase *vadinsime aibę*

$$a + C = \{a + x : x \in C\}.$$

3.2 pavyzdys. Tegu $C = \{000, 111\}$ yra dvinaris tiesinis kodas (tai pakartojimo kodas R_3). Raskime visas klases. 4 lentelėje surašyti visi vektoriai $a \in \mathbb{F}_2^3$ ir atitinkamos klasės $a + C$. Matome, kad $000 + C = 111 + C = \{000, 111\}$ ir t.t. Taigi, iš viso yra 4 klasės $\{000, 111\}$, $\{001, 110\}$, $\{010, 101\}$ ir $\{100, 011\}$. Matome, kad viena iš klasių yra pats kodas. □

3.3 teiginys. *1. Kiekvienas vektorius $b \in \mathbb{F}_q^n$ priklauso kuriai nors klasei. Tiksliau, $b \in b + C$.*

2. Vektoriai $a, b \in \mathbb{F}_q^n$ priklauso tai pačiai klasei tada ir tik tada, kai $a - b \in C$.

3. Kiekvienai klasei priklauso q^k vektorių.

a	$a+C$
000	$\{000, 111\}$
001	$\{001, 110\}$
010	$\{010, 101\}$
100	$\{100, 011\}$
011	$\{011, 100\}$
101	$\{101, 010\}$
110	$\{110, 001\}$
111	$\{111, 000\}$

4 lentelė: Klasių pavyzdys

4. *Klasės arba nesikerta, arba sutampa.*

5. *Tarkime, kad kodo C minimalus atstumas yra d. Tada kiekvienoje klasėje egzistuoja ne daugiau kaip vienas žodis, kurio svoris yra mažesnis už $d/2$.*

3.4 užduotis. Įrodyti teiginį.

Sprendimas. 1. Kadangi C yra tiesinis kodas, tai $0 \in C$, todėl $b = b + 0 \in b + C$.

2. "$\Rightarrow$": Tarkime, $a, b \in c+C$. Tada egzistuoja tokie $c_1, c_2 \in C$, kad $a = c+c_1$ ir $b = c+c_2$. Taigi, $a-b = c_1-c_2$. Bet C yra tiesinis kodas, todėl $c_1 - c_2 \in C$.

   "$\Leftarrow$": Tarkime, $a - b \in C$. Tada $a \in b + C$. Bet $b \in b + C$, todėl a ir b priklauso tai pačiai klasei.

3. Žinome, kad $|C| = q^k$ (teorema iš 2.1 poskyrio). Aišku, kad klasės $a + C$ vektorių skaičius irgi neviršija q^k. Be to, jis negali būti ir mažesnis, nes jei $c_1, c_2 \in C, c_1 \neq c_2$, tai $a + c_1 \neq a + c_2$.

4. Imkime dvi klases: $a+C$ ir $b+C$. Jei jos nesikerta — teiginys įrodytas. Tarkime, kad jos kertasi, t.y. kad jų sankirta nėra tuščia. Reikia parodyti, kad jos sutampa. Tegu $v \in a+C$ ir $v \in b+C$. Tada $v = a+c_1$, $c_1 \in C$, ir $v = b + c_2$, $c_2 \in C$, todėl $a + c_1 = b + c_2$, t.y. $a = b + c_2 - c_1 \in b + C$ (vėlgi todėl, kad kodas C tiesinis, gauname, kad $c_2 - c_1 \in C$). Taigi, $a + C \subseteq b + C$. Lygiai taip pat išreiškę b per a gausime $b + C \subseteq a + C$. Vadinasi, $a + C = b + C$.

5. Tarkime x ir y priklauso tai pačiai klasei $x+C$, ir $w(x) < \frac{d}{2}$, $w(y) < \frac{d}{2}$. Pagal trikampio nelygybę, $w(x-y) = d(x, y) \leqslant d(x, 0) + d(0, y) = w(x) + w(y) < \frac{d}{2} + \frac{d}{2} = d$. Bet šio teiginio antras punktas rodo, kad $x - y \in C$. Taigi, radome kodo C žodį $x - y$, kurio svoris mažesnis už kodo minimalų atstumą d. Taip gali būti tik tuo atveju, kai $x - y = 0$. Taigi, $x = y$. □

Teiginys tvirtina, kad erdvę $\mathbb{F}_q^n$ galima padalinti į r tarpusavyje nesikertančių klasių:

$$\mathbb{F}_q^n = (a_0 + C) \cup (a_1 + C) \cup \cdots \cup (a_{r-1} + C),$$

kur $r = \left|\mathbb{F}_q^n\right| / |C| = q^n/q^k = q^{n-k}$. Taip pat laikysime, kad $a_0 = 0$, todėl pirmoji klasė $a_0 + C = 0 + C = C$.

3.2 Dekodavimas

3.5 teiginys. *Galimų klaidų vektorių aibė sutampa su klase, kurioje yra iš kanalo gautas vektorius.*

Įrodymas. Tarkime, pranešimą $m \in \mathbb{F}_q^k$ užkoduojame kodu C, generuotu matricos G, gauname $c = mG \in C$. Iš kanalo gauname vektorių $y = c + e \in \mathbb{F}_q^n$. Tada klaidų vektorius $e = y - c \in y + C$, nes $-c \in C$. Taigi, klaidų vektorius e priklauso tai pačiai klasei, kaip ir iš kanalo gautas vektorius y. Iš kitos pusės, bet kuris šios klasės vektorius galėtų būti klaidų vektoriumi. Iš tikrųjų, tarkime, $z \in y + C$. Galėjo būti, kad į kanalą buvo pasiųstas kodo žodis $y - z \in C$ (pagal 3.3 teiginio 2 dalį), kanale prie jo buvo pridėtas klaidų vektorius z. Tokiu atveju iš kanalo iš tiesų gauname y.□

Tarkime, kad dekodavimui naudojame minimalaus atstumo dekodavimo taisyklę, t.y. dekoduojame tuo kodo žodžiu $x \in C$, kuris yra arčiausiai iš kanalo gauto vektoriaus $y \in \mathbb{F}_q^n$, t.y. kuris tenkina sąlygą $d(x, y) = \min_{z \in C} d(z, y)$. Taigi, nusprendžiame, kad toks $x \in C$ yra tas vektorius, kuris buvo išsiųstas į kanalą, ir klaidų vektoriumi laikome $e = y - x$ (nes $y = x + e$).

Tą patį gausime ir darydami kitaip: ieškokime tokio klaidų vektoriaus e, kurio svoris būtų mažiausias. Tokiu atveju skirtumo $e = y - x$ svoris $w(y - x)$, o tuo pačiu ir atstumas tarp x ir y (nes $w(y - x) = d(x, y)$) irgi bus mažiausias. Taigi, taip darydami irgi naudojame minimalaus atstumo dekodavimo taisyklę. Prisiminę, kad klaidų vektorius priklauso vektoriaus y klasei, gauname tokią dekodavimo procedūrą:

> *Klasėje, kuriai priklauso iš kanalo gautas vektorius y, randame mažiausio svorio vektorių e (laikome jį klaidų vektoriumi), ir dekoduojame kodo C žodžiu $y - e$.*

3.6 apibrėžimas. *Mažiausio svorio klasės vektorius vadinamas klasės* lyderiu. *Jei klasėje yra keli mažiausio svorio vektoriai, tai klasės lyderiu vadinsime kurį nors vieną iš jų.*

3.3 Standartinė lentelė

Taigi, norėdami dekoduoti, turime rasti klasės lyderį. Paprasčiausia yra visų klasių lyderius susirasti iš anksto, o dekodavimo metu tik pažiūrėti, kuriai klasei priklauso iš kanalo išėjęs vektorius, ir pasinaudoti jos lyderiu. Tai galime atlikti, sudarę standartinę lentelę.

Tarkime, $C[n, k, d]$ yra tiesinis kodas virš $\mathbb{F}_q$, generuotas matricos G. Sudarysime tokią lentelę. Pirmoje eilutėje surašome visus galimus pranešimų erdvės $\mathbb{F}_q^k$ žodžius $m_0, m_1, \ldots, m_{N-1}$, čia $N = q^k$. Tegu $m_0 = 00\cdots0$ — nulinis vektorius. Į antrą eilutę surašome atitinkamus kodo C žodžius, t.y. $c_0 = 0, c_1, \ldots, c_{N-1}$, kur $c_i = m_i G$, $i = 0, 1, \ldots, N-1$. Trečiąją ir kitas lentelės eilutes užpildome taip: pasirenkame tokį mažiausio svorio vektorių $a \in \mathbb{F}_q^n$, kurio dar nebuvo prieš tai užrašytose eilutėse, ir jį užrašome pirmojoje vietoje, o paskui likusius klasės $a + C$ žodžius $a + c_1, a + c_2, \ldots, a + c_{N-1}$. Taip darome, kol užrašome visus erdvės $\mathbb{F}_q^n$ žodžius. Gauname tokią lentelę:

Pranešimai:	0	m_1	m_2	$\cdots$	m_{N-1}
Kodas:	0	c_1	c_2	$\cdots$	c_{N-1}
Klasės:	a_1	$a_1 + c_1$	$a_1 + c_2$	$\cdots$	$a_1 + c_{N-1}$
	a_2	$a_2 + c_1$	$a_2 + c_2$	$\cdots$	$a_2 + c_{N-1}$
	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
	a_{r-1}	$a_{r-1} + c_1$	$a_{r-1} + c_2$	$\cdots$	$a_{r-1} + c_{N-1}$

Čia r yra klasių skaičius. Ši lentelė vadinama *standartine kodo C lentele*. Jos sudarymo būdas garantuoja, kad kiekvienoje eilutėje išrašyti atitinkamos klasės $a_i + C$, $i = 0, 1, \ldots, r-1$, vektoriai, o pirmasis iš jų yra klasės lyderis.

Turėdami standartinę kodo lentelę, dekoduojame iš kanalo gautą vektorių $y \in \mathbb{F}_q^n$ taip:

1. Randame, kurioje standartinės lentelės eilutėje yra y (jis tikrai kažkur bus, nes lentelėje yra visi erdvės $\mathbb{F}_q^n$ vektoriai).

2. Nusprendžiame, kad šios eilutės pradžioje stovintis klasės lyderis a yra klaidų vektorius, ir dekoduojame vektorių y žodžiu $y - a$, t.y. žodžiu, kuris yra vektoriaus y stulpelio viršuje.

3.7 pavyzdys. Tarkime, kodas C yra dvinaris tiesinis $[5, 2, 3]$ kodas, generuotas matricos

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

Jo standartinė lentelė bus, pavyzdžiui, tokia:

Pranešimai:	00	10	01	11
Kodas:	00000	10110	01011	11101
Klasės:	10000	00110	11011	01101
	01000	11110	00011	10101
	00100	10010	01111	11001
	00010	10100	01001	11111
	00001	10111	01010	11100
	00101	10011	01110	11000
	01100	11010	00111	10001

Kodo C standartinė lentelė gali būti ir kitokia. Tai priklauso nuo to, kokia tvarka išrikiuoti pranešimai. Tėra reikalaujama, kad pirmoje vietoje stovėtų nulinis pranešimas, o likę gali būti išrikiuoti bet kaip. Pakeitus pranešimų išrikiavimo tvarką, keistųsi vietomis standartinės lentelės stulpeliai.

Standartinės lentelės eilutės, kuriose surašyti klasių vektoriai, irgi gali keistis vietomis. Pavyzdžiui, sudarinėdami šią standartinę lentelę, į pirmos klasės pirmą poziciją rašome bet kurį mažiausio svorio vektorių, kurio dar nėra lentelėje. Nulinio svorio vektorius 00000 lentelėje jau yra (tai kodo žodis). Bet nėra nei vieno svorio 1 žodžio. Tai galime iš jų rinktis bet kurį. Pasirinkome 10000, išrašėme jo klasę. Vėl galime rinktis bet kurį iš likusių svorio 1 žodžių, ir t.t. Kai baigiasi svorio 1 žodžiai, renkamės iš dar neužrašytų svorio 2 žodžių. Ir t.t. Taip darome, kol užrašome visus erdvės $\mathbb{F}_2^5$ žodžius. Žinome, kad klasių yra $r = q^{n-k} = 2^{5-2} = 8$, tai lentelėje bus 8 eilutės su erdvės $\mathbb{F}_2^5$ žodžiais.

Žymėkime y iš kanalo gautą vektorių. Tarkime, $y = 11001$. Randame jį lentelėje, jis yra paskutiniame stulpelyje. Jo klasės lyderį 00100 (esantį vektoriaus y eilutės pirmoje vietoje) laikysime klaidų vektoriumi, ir dekoduojame žodžiu 11101.

Jei $y = 01011$, randame jį tarp kodo žodžių, padarome išvadą, kad klaidų nebuvo, ir dekoduojame tuo pačiu žodžiu 01011.

Tarkime, $y = 10011$. Randame jį priešpaskutinėje eilutėje. Klaidų vektoriumi laikome tos klasės lyderį 00101, ir dekoduojame kodo žodžiu 10110.

Pastebėkime, kad paskutinėse dviejose klasėse nebėra lyderio vienareikšmiškumo. Pavyzdžiui, priešpaskutinės klasės lyderiu galėjome rinktis vektorių 11000. Tokiu atveju vektorių $y = 10011$ būtume dekodavę kitu kodo žodžiu $10011 - 11000 = 01011$. Taip yra dėl to, kad klasėje, esančioje priešpaskutinėje lentelės eilutėje, mažiausias vektoriaus svoris yra 2. Tai reiškia, kad jei y priklauso tai klasei, tai kanale įvyko bent dvi klaidos. O tiek ištaisyti kodas negali, nes tai $t = [(d-1)/2] = [(3-1)/2] = 1$ klaidą taisantis kodas. Ir tikrai, vektorius $y = 10011$ vienodu atstumu nutolęs nuo

dviejų kodo žodžių — 10110 ir 01011, todėl dekoduoti galime bet kuriuo iš jų. Ir dekoduojame būtent taip, kad klaidos vektorius būtų standartinės lentelės sudarymo metu pasirinktas klasės lyderis. □

3.4 Sindromai ir sumažinta standartinė lentelė

Be abejo, standartinės lentelės metodas tinka dekoduoti naudojant tik labai mažus tiesinius kodus, nes atmintyje reikia saugoti visus erdvės $\mathbb{F}_q^n$ žodžius. Naudojamos atminties kiekį būtų galima sumažinti, jei turėtume galimybę nesunkiai nustatyti, kuriai klasei priklauso iš kanalo gautas vektorius. Tokiu atveju pakaktų pasinaudoti tik pirmuoju lentelės stulpeliu. Tai leidžia padaryti sindromas.

3.8 apibrėžimas. *Tegu H yra tiesinio kodo C kontrolinė matrica, $y \in \mathbb{F}_q^n$. Žodžio y* sindromu *vadiname vektorių $s(y) = Hy^T \in \mathbb{F}_q^{n-k}$.*

3.9 pavyzdys. Jei tiesinio kodo virš $\mathbb{F}_3$ kontrolinė matrica yra

$$H = \begin{pmatrix} 2 & 1 & 0 & 2 \\ 1 & 1 & 2 & 0 \end{pmatrix},$$

tai vektoriaus $y = 2221$ sindromas

$$s(y) = Hy^T = \begin{pmatrix} 2 & 1 & 0 & 2 \\ 1 & 1 & 2 & 0 \end{pmatrix} \begin{pmatrix} 2 \\ 2 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}.$$

□

3.10 teiginys. *Tegu H yra tiesinio kodo C kontrolinė matrica. Tegu $y \in \mathbb{F}_q^n$.*

1. *Vektorius $y \in C$ tada ir tik tada, kai $s(y) = 0$.*
2. *Du vektoriai priklauso tai pačiai klasei tada ir tik tada, kai jų sindromai lygūs.*
3. *Tegu $q = 2$ (t.y. C yra dvinaris kodas), o y yra iš kanalo gautas galbūt iškraipytas vektorius. Tada $s(y)$ yra lygus sumai tų kontrolinės matricos H stulpelių, kur įvyko klaidos.*

Įrodymas. 1. Išplaukia iš 2.19 teiginio ir sindromo apibrėžimo.

2. Jei vektoriai y ir z priklauso tai pačiai klasei, tai pagal 3.3 teiginio 2 dalį $y - z \in C$. Tada pagal 2.19 teiginį $H(y-z)^T = 0$, t.y. $Hy^T = Hz^T$, todėl $s(y) = s(z)$. Į kitą pusę įrodymas analogiškas.

3. Tarkime, $y = x + e$, kur $x \in C$ — į kanalą pasiųstas kodo žodis, $e = (e_1, \ldots, e_n) \in \mathbb{F}_q^n$ — klaidų vektorius. Kadangi $q = 2$, tai e_i gali būti tik 0 ar 1. Be to, $x \in C$, todėl $Hx^T = 0$ (2.19 teiginys). Žymėkime H_i, $i = 1, \ldots, n$, matricos H stulpelius. Tada

$$s(y) = Hy^T = H(x+e)^T = Hx^T + He^T = He^T = \sum_{i=1}^{n} e_i H_i = \sum_{\substack{1 \leqslant i \leqslant n \\ e_i = 1}} H_i.$$

Paskutinė suma yra sudaryta iš tų kontrolinės matricos stulpelių H_i, kuriems atitinkamas $e_i = 1$, t.y. kur įvyko klaidos. □

Paskutinio teiginio 2 dalis rodo, kad tarp sindromų aibės ir klasių aibės egzistuoja abipusiškai vienareikšmė atitiktis. Todėl kiekvienos standartinės lentelės eilutės gale galime prirašyti sindromą, atitinkantį toje eilutėje išrašytą klasę.

Gavę iš kanalo vektorių y, apskaičiuojame jo sindromą $s(y)$, kuris ir parodo, kurioje standartinės lentelės eilutėje y yra. Taigi, norint dekoduoti, pakanka turėti tokią *sumažintą standartinę lentelę*:

Klasių lyderiai	Sindromai
0	0
a_1	s_1
a_2	s_2
$\vdots$	$\vdots$
a_{r-1}	s_{r-1}

Gavę iš kanalo vektorių y, apskaičiuojame jo sindromą $s(y)$, randame $s_i = s(y)$ sumažintoje standartinėje lentelėje, nusprendžiame, kad atitinkamas klasės lyderis a_i yra klaidų vektorius ir dekoduojame vektorių y kodo žodžiu $y - a_i$.

Sumažintą standartinę lentelę sudarome taip: imame visus erdvės $\mathbb{F}_q^n$ žodžius y, pradedant nuo mažiausio svorio vektorių, ir skaičiuojame jų sindromus $s(y)$. Jei gauname naują sindromą, tai y ir $s(y)$ dedame į lentelę. Taip darome, kol gauname visas q^{n-k} klases.

3.11 pavyzdys. Imkime kodą iš 2.24 pavyzdžio. Kaip matėme, tai kodas virš $\mathbb{F}_3$, kurio generuojanti ir kontrolinė matricos yra atitinkamai

$$G = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix} \quad \text{ir} \quad H = \begin{pmatrix} 2 & 1 & 0 & 2 \\ 1 & 1 & 2 & 0 \end{pmatrix}.$$

Sudarysime sumažintą standartinę lentelę. Mūsų atveju klasių bus $3^{4-2} = 9$. Pradedame nuo svorio 0 vektoriaus $y = 0000$, kurio sindromas $s(y) = Hy^T = 00^T$, čia 00^T yra nulinis vektorius-stulpelis (transponuotas vektorius-eilutė). Toliau eina svorio 1 vektoriai $1000, \ldots, 0001, 2000, \ldots,$ 0002, kurių sindromai yra atitinkamai $21^T, \ldots, 10^T$ (žr. lentelę). Visi jie skirtingi, dėl to visus juos dedame į lentelę. Gauname 9 eilutes, kiek ir turėjome gauti. Lentelę sudarėme. Kad jos sudarymo principas būtų aiškesnis, pažiūrėkime, ką būtume darę toliau, jei būtume radę dar ne visas eilutes. Toliau imtume svorio 2 vektorius. Pavyzdžiui, pradėtume nuo vektoriaus 1100, kurio sindromas yra 02^T. Toks sindromas lentelėje jau yra, todėl vektorių 1100 atmetame (nes lentelėje jau turime jo klasės lyderį 0010). Taip bandytume visus kitus svorio 2 vektorius, paskui svorio 3 ir t. t., kol galų gale gautume tiek klasių, kiek turime gauti.

Gauname tokią sumažintą standartinę lentelę (paprastumo dėlei vektorius-stulpelius rašysime kaip atitinkamus vektorius-eilutes):

Klasių lyderiai	Sindromai
0000	00
1000	21
0100	11
0010	02
0001	20
2000	12
0200	22
0020	01
0002	10

Tarkime, iš kanalo gauname vektorių $y = 2221$. Apskaičiuojame jo sindromą $s(y) = 22^T$. Randame jį sumažintoje standartinėje lentelėje. Atitinkamą klasės lyderį 0200 laikome klaidų vektoriumi ir dekoduojame kodo žodžiu $2221 - 0200 = 2021$. □

3.5 Ribotas dekodavimas ir nepilna sumažinta standartinė lentelė

Visgi matome, kad tokią standartinę lentelę (sumažintą ar ne) sudaryti galime tik nedideliems q ir n, nes turime peržiūrėti didelę dalį (ar visus) erdvės $\mathbb{F}_q^n$ žodžius. Tai būtų žymiai lengviau padaryti, jei apsiribotume nedideliu ištaisomų klaidų skaičiumi. Pavyzdžiui, norime ištaisyti visas klaidas, jei jų skaičius neviršija kažkokio iš anksto pasirinkto pakankamai nedidelio skaičiaus K. Jei viršija — ką gi, ištaisyti negalėsime, teks, pavyzdžiui, prašyti atsiųsti iš naujo. Tai galima būtų daryti taip.

3.3 teiginio 5 dalyje gavome, kad kiekvienoje klasėje egzistuoja ne daugiau kaip vienas žodis, kurio svoris yra mažesnis už $d/2$, kur d yra kodo C minimalus atstumas. Taigi jei klasėje egzistuoja nors vienas žodis, kurio svoris mažesnis už $d/2$, tai visų kitų klasės žodžių svoriai yra nemažesni už $d/2$, todėl šis žodis ir yra klasės lyderis.

Kadangi visi erdvės $\mathbb{F}_q^n$ žodžiai priklauso kuriai nors klasei, tai visi erdvės žodžiai, kurių svoris mažesnis už $d/2$, yra savo klasių lyderiai. Visiems tokiems žodžiams galima apskaičiuoti sindromus ir sudaryti *nepilną sumažintą standartinę lentelę* vien iš jų. Arba net iš dar mažiau žodžių: pasirenkame $K < d/2$, ir į nepilną sumažintą lentelę sudedame tik žodžius, kurių svoris nedidesnis už K, ir jų sindromus.

Dekoduojame tada taip: iš kanalo gavę vektorių y, apskaičiuojame jo sindromą $s(y)$, tada nepilnoje sumažintoje standartinėje lentelėje ieškome klasės lyderio a_i, kurio sindromas $s_i = s(y)$. Jei randame, tai vektorių y dekoduojame žodžiu $y - a_i$, o jei nerandame, tai reiškia, kad kanale įvyko daugiau nei K klaidų, ir mūsų naudojamas algoritmas neturi galimybių jų ištaisyti.

3.12 pavyzdys. Grįžkime prie kodo C, pateikto 3.7 pavyzdyje. Prisiminkime, kad tai dvinaris tiesinis $[5, 2, 3]$ kodas, generuotas matricos

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

Nesunkiai galime rasti, kad kodas $C = \{00000, 10110, 01011, 11101\}$, todėl jo minimalus atstumas $d = 3$. Pasirinkime $K = 1$, $K < d/2$. Norint sudaryti sumažintą standartinę lentelę, dar reikia žinoti kodo C kontrolinę matricą H. Ją taip pat nesunkiai galime rasti:

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

Nepilnoje sumažintoje standartinėje lentelėje bus tik klasių lyderiai, kurių svoris nedidesnis už K, ir jų sindromai (paprastumo dėlei vektorius-stulpelius rašysime kaip atitinkamus vektorius-eilutes):

Klasių lyderiai	Sindromai
00000	000
10000	110
01000	011
00100	100
00010	010
00001	001

Tarkime, iš kanalo gauname vektorių $y = 11001$. Apskaičiuojame jo sindromą $s(y) = 100^T$. Randame jį nepilnoje sumažintoje standartinėje lentelėje. Atitinkamą klasės lyderį 00100 laikome klaidų vektoriumi ir dekoduojame kodo žodžiu $11001 - 00100 = 11101$.

Tarkime, iš kanalo gauname vektorių $y = 10011$. Apskaičiuojame jo sindromą $s(y) = 101^T$. Tokio sindromo nepilnoje sumažintoje standartinėje lentelėje nėra. Tai reiškia, kad kanale įvyko daugiau nei $K = 1$ klaida, ir mūsų naudojamas algoritmas neturi galimybių jų ištaisyti. Bet šiuo atveju tai nedidelis trūkumas, nes bet kokiu atveju kodas C garantuotai gali ištaisyti tik $[(d-1)/2] = 1$ klaidą, t. y. nors pilna standartinė lentelė ir galėtų ištaisyti dvi klaidas, bet mes vistiek nebūtume garantuoti, kad ištaisė teisingai. □

Nepilna sumažinta standartinė lentelė žymiai lengviau sudaroma, todėl gali būti naudojama didesniems tiesiniams kodams, užtat jos klaidų taisymo galimybės yra ribotos.

Reziumuojant reikia pasakyti, kad yra parodyta, kad tiesinių kodų dekodavimo uždavinys yra NP-pilnas, t. y. vilties rasti polinominio laiko dekodavimo algoritmą, tinkantį visiems tiesiniams kodams, yra labai mažai. Todėl ieškoma tokių tiesinių kodų šeimos pošeimių, kuriems egzistuotų greitas polinominio laiko dekodavimo algoritmas. Kelias tokias šeimas (Hemingo kodus, Rydo-Miulerio kodus) mes ir panagrinėsime kituose skyriuose.

4 Dvinariai Hemingo kodai

4.1 Apibrėžimas ir savybės

Hemingo vieną klaidą taisantys kodai yra svarbi klaidas taisančių tiesinių kodų šeima. Jais naudojantis, lengva ir užkoduoti, ir dekoduoti. Mes aptarsime tik dvinarius Hemingo kodus.

4.1 apibrėžimas. *Tegu $r \geqslant 2$.* Dvinaris Hemingo kodas $\mathbf{H}_2(r)$ *yra dvinaris tiesinis ilgio $n = 2^r - 1$ kodas, kurio kontrolinės matricos stulpeliai yra visi galimi ilgio r dvinariai skirtingi nenuliniai vektoriai.*

4.2 pastaba. Apibrėžimas nenustato, kuria tvarka tie stulpeliai turi būti išrikiuoti. Kad ir kaip jie būtų išrikiuoti, gautas kodas bus vadinamas Hemingo kodu. Taigi egzistuoja ištisa šeima dvinarių ilgio $2^r - 1$ ekvivalenčių Hemingo kodų.

4.3 pavyzdžiai. 1. Tegu $r = 2$. Pagal apibrėžimą, Hemingo kodas $\mathbf{H}_2(2)$ yra dvinaris tiesinis ilgio $n = 2^2 - 1 = 3$ kodas, kurio kontrolinės matricos H stulpeliai yra visi galimi ilgio 2 dvinariai skirtingi nenuliniai vektoriai, t. y. vektoriai 10, 01 ir 11, todėl kontrolinė matrica yra, pavyzdžiui, tokia:

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

2. Tegu $r = 3$. Pagal apibrėžimą, Hemingo kodas $\mathbf{H}_2(3)$ yra dvinaris tiesinis ilgio $n = 2^3 - 1 = 7$ kodas, kurio kontrolinės matricos H stulpeliai yra visi galimi ilgio 3 dvinariai skirtingi nenuliniai vektoriai, todėl kontrolinė matrica yra, pavyzdžiui, tokia:

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

□

4.4 teiginys. *Dvinario Hemingo kodo minimalus atstumas* $d = 3$.

Įrodymas. Pagal 2.27 teoremą kodo minimalus atstumas lygus d, jei jo kontrolinės matricos H bet kurie $d-1$ stulpeliai yra tiesiškai nepriklausomi ir egzistuoja d tiesiškai priklausomų stulpelių.

Kadangi dvinario Hemingo kodo kontrolinės matricos visi stulpeliai yra nenuliniai ir skirtingi, tai bet kuri stulpelių pora yra tiesiškai nepriklausoma. Be to, į matricą įeina visi galimi ilgio r nenuliniai dvinariai vektoriai, taigi bet kurių dviejų matricos H stulpelių suma taip pat yra matricos H stulpelis, nelygus nei vienam iš tų dviejų stulpelių, todėl šie trys stulpeliai yra tiesiškai priklausomi. Pagal 2.27 teoremą kodo minimalus atstumas $d = 3$. □

Taigi, dvinaris Hemingo kodas $\mathbf{H}_2(r)$ yra tiesinis $[2^r - 1, 2^r - r - 1, 3]$ kodas.

4.5 teiginys. *Tegu* $r \geqslant 2$. *Bet kuris dvinaris tiesinis* $[2^r-1, 2^r-r-1, 3]$ *kodas yra Hemingo kodas* $\mathbf{H}_2(r)$.

Įrodyti patiems.

4.6 pavyzdys. Kurso pradžioje, I dalies 2.6 poskyryje (5 psl.) apibrėžtas $[7, 4]$ Hemingo kodas - tai dvinaris Hemingo kodas $\mathbf{H}_2(3)$. Iš tikrųjų, 2.13 pavyzdžio 6 dalyje (37 psl.) matėme, kad jo generuojanti matrica yra

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

Pagal 2.20 teiginį gauname jo kontrolinę matricą:

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

Matome, kad kontrolinės matricos H stulpeliai iš tikrųjų yra visi galimi ilgio 3 dvinariai skirtingi nenuliniai vektoriai. □

4.2 Dekodavimas

Kadangi Hemingo kodo minimalus atstumas $d = 3$, tai $t = [(d-1)/2] = 1$, todėl Hemingo kodas taiso visas pavienes klaidas.

Pagal 3.10 teiginio 3 dalį, iš kanalo gauto vektoriaus y sindromas lygus Hemingo kodo kontrolinės matricos H stulpelių, atitinkančių klaidų pozicijas, sumai. Tarkime, įvyko lygiai viena klaida. Tada vektoriaus y sindromas yra lygus tam kontrolinės matricos H stulpeliui, kur įvyko klaida, todėl apskaičiavus sindromą užtenka rasti, kuris matricos H stulpelis yra jam lygus ir ištaisyti klaidą tą stulpelį atitinkančioje vektoriaus pozicijoje. Formaliai dvinario Hemingo kodo $\mathbf{H}_2(r)$, $r \geqslant 2$, dekodavimo algoritmą galime užrašyti taip:

- Tarkime, iš kanalo gavome vektorių $y = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$, kur $n = 2^r - 1$. Apskaičiuojame jo sindromą $s = s(y) \in \mathbb{F}_2^r$.
- Jei $s = 0$, tai $y \in C$ — algoritmas išveda y.

- Jei $s \neq 0$, tai s yra kuris nors kontrolinės matricos H stulpelis, tarkime, j-asis, $1 \leqslant j \leqslant n$ — algoritmas išveda $(y_1, \ldots, y_{j-1}, y_j + 1, y_{j+1}, \ldots, y_n)$.

Beje, šį algoritmą galima efektyviai realizuoti, jei kontrolinės matricos H stulpeliai išrikiuoti tokia tvarka: i-tasis stulpelis — skaičiaus i dvejetainė išraiška (jei reikia, papildyta nuliais), kur žemiausias narys yra kairėje, pavyzdžiui, vieneto dvejetainė išraiška yra $10\cdots0$. T.y.

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & \cdots \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & \cdots \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \tag{12}$$

Tada, apskaičiavus sindromą s, užtenka konvertuoti s iš dvejetainės į dešimtainę sistemą ir gauname klaidos pozicijos numerį j. Tokiu atveju nereikia perbėgti visos matricos H, lyginant kiekvieną jos stulpelį su sindromu s.

4.7 pavyzdys. Naudodamiesi dvinariu Hemingo kodu $\mathbf{H}_2(3)$, kurio kontrolinė matrica H yra (12) pavidalo, dekoduosime seką 0000010 1100110 0110100.

Kontrolinė matrica bus

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

Pažymėkime $y_1 = 0000010$. Sindromas $s(y_1) = 011^T$. Pavertę šią dvejetainę išraišką į dešimtainę gauname $j = 6$, t.y. klaida yra šeštoje pozicijoje. Todėl dekoduojame vektoriumi 0000000.

Toliau, tegu $y_2 = 1100110$. Tada $s(y_2) = 000^T$. Klaidų nėra, dekoduojame 1100110.

Na, ir $y_3 = 0110100$. Tada $s(y_3) = 001^T$, todėl $j = 4$ ir dekoduojame 0111100. □

5 Pirmos eilės Rydo-Miulerio kodai

5.1 Apibrėžimas ir savybės

5.1 apibrėžimas. *Tegu $m \geqslant 2$.*

1. *Funkcija $f : \mathbb{F}_2^m \to \mathbb{F}_2$ vadinama* logine funkcija *(arba* Būlio funkcija*).*
2. *Loginė funkcija*
$$f(x_1, x_2, \ldots, x_m) = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_m x_m + \mu,$$
kur $\lambda_1, \lambda_2, \ldots, \lambda_m, \mu \in \mathbb{F}_2$, vadinama afiniąja.

5.2 pavyzdys. Tegu $m = 3$. Funkcija $s(x_1, x_2, x_3) = x_1x_2 + x_1 + 1$ yra loginė funkcija. Jinai nėra afinioji, nes įeina kintamųjų sandauga x_1x_2. Funkcija $s'(x_1, x_2, x_3) = x_1 + x_3 + 1$ yra afinioji loginė funkcija. □

Kiekvienai loginei funkcijai galima sudaryti reikšmių lentelę, kurioje kintamųjų reikšmių rinkiniai išrikiuoti kaip 5.3 pavyzdyje.

5.3 pavyzdys. Paskutinio pavyzdžio loginės funkcijos $s(x_1, x_2, x_3) = x_1x_2 + x_1 + 1$ reikšmių lentelė yra tokia:

x_1	x_2	x_3	$s(x_1, x_2, x_3)$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

□

Loginės funkcijos įgyjamų reikšmių rinkinį iš reikšmių lentelės galima užrašyti ilgio 2^m vektoriumi. Pavyzdžiui, 5.3 pavyzdžio loginę funkciją $s(x_1, x_2, x_3) = x_1x_2 + x_1 + 1$ atitinka vektorius $\overrightarrow{s} = (s_0, \ldots, s_7) = (1, 1, 1, 1, 0, 0, 1, 1)$.

Formaliai tai galima užrašyti taip: loginę funkciją f atitinka vektorius $\overrightarrow{f} = (f_0, \ldots, f_{2^m-1})$, kur $f_i = f(b_1, b_2, \ldots, b_m)$, o $b_1, \ldots, b_m$ yra skaičiaus i dvejetainė išraiška (papildyta nuliais, jei reikia), t.y. $i = \sum_{j=0}^{m-1} b_{m-j}2^j$. Čia dvejetainės išraiškos žemiausias narys yra dešinėje, pavyzdžiui, vieneto dvejetainė išraiška yra $0 \cdots 01$. Taigi,

$$\begin{aligned} f_0 &= f(0, \ldots, 0, 0), \\ f_1 &= f(0, \ldots, 0, 1), \\ f_2 &= f(0, \ldots, 1, 0), \\ f_3 &= f(0, \ldots, 1, 1), \\ &\cdots \\ f_{2^m-1} &= f(1, \ldots, 1, 1). \end{aligned}$$

5.4 teiginys. *Jei f ir g yra loginės funkcijos, tai $\overrightarrow{f + g} = \overrightarrow{f} + \overrightarrow{g}$.*

5.5 užduotis. Įrodyti šį teiginį.

5.6 apibrėžimas. *Tegu $m \geqslant 2$.* Pirmos eilės dvinaris Rydo-Miulerio (Reed-Muller) kodas*, žymimas $RM(1, m)$, yra vektorių, atitinkančių afiniąsias logines funkcijas $f : \mathbb{F}_2^m \to \mathbb{F}_2$, aibė.*

Taigi, kodo $RM(1, m)$ ilgis n yra lygus vektorių ilgiui, t.y. $n = 2^m$. Afiniųjų loginių funkcijų yra 2^{m+1} (kiekvienam λ_i, $i = 1, \ldots, m$, parinkti turime dvi galimybes, kaip ir μ). Be to, visas afiniąsias logines funkcijas atitinka skirtingi vektoriai (įrodykite patys). Taigi, kodo dydis (t. y. kodo žodžių skaičius) $|RM(1, m)|$ irgi yra 2^{m+1}.

5.7 pavyzdys. Išrašykime visus kodo $RM(1, 3)$ žodžius. Tam reikės rasti visas galimas afiniąsias logines funkcijas $\mathbb{F}_2^3 \to \mathbb{F}_2$ ir sudaryti kiekvienos iš jų reikšmių lentelę. 5 lentelėje pateikiamos visos afiniosios loginės funkcijos ir jas atitinkantys vektoriai. Kairėje yra afiniosios loginės funkcijos f, kurių laisvasis narys μ lygus nuliui, o dešinėje jas atitinkančios $f + 1$, t.y. atitinkamos afiniosios loginės funkcijos su $\mu = 1$. Visi išvardinti $2^{3+1} = 16$ vektorių ir sudaro $RM(1, 3)$ kodą. □

Funkcija	Vektorius	Funkcija	Vektorius
0	00000000	1	11111111
x_1	00001111	x_1+1	11110000
x_2	00110011	x_2+1	11001100
x_3	01010101	x_3+1	10101010
x_1+x_2	00111100	x_1+x_2+1	11000011
x_1+x_3	01011010	x_1+x_3+1	10100101
x_2+x_3	01100110	x_2+x_3+1	10011001
$x_1+x_2+x_3$	01101001	$x_1+x_2+x_3+1$	10010110

5 lentelė: $RM(1,3)$ kodo žodžiai

Jei $\vec{f},\vec{g}\in RM(1,m)$, tai $\vec{f}+\vec{g}=\overrightarrow{f+g}$. Bet $f+g$ irgi yra afinioji loginė funkcija, todėl $\overrightarrow{f+g}\in RM(1,m)$. Taigi, $RM(1,m)$ yra tiesinis kodas. Kadangi tai dvinaris kodas, ir $|RM(1,m)|=2^{m+1}$, tai kodo dimensija yra $m+1$. Reziumuojant, $RM(1,m)$ yra tiesinis $[2^m,m+1]$ kodas.

Raskime kodo $RM(1,m)$ generuojančią matricą.

5.8 teiginys. *Tegu $m\geqslant 2$. Matrica, kurios eilutės yra funkcijas $x_1,x_2,\ldots,x_m$ ir 1 atitinkantys vektoriai $\vec{x_1},\vec{x_2},\ldots,\vec{x_m},\vec{1}$, yra kodo $RM(1,m)$ generuojanti matrica.*

Įrodymas. Kad įrodytume, kad tikrai tokia matrica yra kodo $RM(1,m)$ generuojanti matrica, turime parodyti, kad vektoriai $\vec{x_1},\vec{x_2},\ldots,\vec{x_m},\vec{1}$ sudaro kodo $RM(1,m)$ bazę, t. y. reikia parodyti, kad jie priklauso kodui $RM(1,m)$ ir yra tiesiškai nepriklausomi. Kadangi jų skaičius yra lygus kodo $RM(1,m)$ dimensijai, tai ir gausime, kad jie sudaro bazę.

Kadangi visi šie vektoriai atitinka afiniąsias funkcijas, jie priklauso $RM(1,m)$. Lieka parodyti, kad jie tiesiškai nepriklausomi. Imkime jų tiesinę kombinaciją $\sum_{i=1}^m\lambda_i\vec{x_i}+\mu\cdot\vec{1}$ su koeficientais $\lambda_1,\ldots,\lambda_m,\mu\in\mathbb{F}_2$ ir prilyginkime ją nuliui. Parodysime, kad tokiu atveju visi koeficientai yra lygūs nuliui. Kadangi $\vec{f}+\vec{g}=\overrightarrow{f+g}$ bet kurioms dviems loginėms funkcijoms f ir g, tai $\sum_{i=1}^m\lambda_i\vec{x_i}+\mu\cdot\vec{1}=\overrightarrow{\sum_{i=1}^m\lambda_ix_i+\mu}$. Todėl $\overrightarrow{\sum_{i=1}^m\lambda_ix_i+\mu}$ irgi yra nulinis vektorius. Bet tėra viena afinioji funkcija, kurią atitinka nulinis vektorius — tai nulinė funkcija, todėl funkcija $\sum_{i=1}^m\lambda_ix_i+\mu$ ir yra nulinė funkcija, ir jos visi koeficientai $\lambda_1,\ldots,\lambda_m,\mu$ yra lygūs nuliui. Taigi, parodėme, kad jei vektorių $\vec{x_1},\vec{x_2},\ldots,\vec{x_m},\vec{1}$ tiesinė kombinacija yra lygi nuliui, tai visi tos tiesinės kombinacijos koeficientai yra lygūs nuliui. Tai ir reiškia, kad vektoriai yra tiesiškai nepriklausomi. □

5.9 pavyzdys. Kodo $RM(1,3)$ generuojančios matricos eilutės yra vektoriai $\vec{x_1},\vec{x_2},\vec{x_3},\vec{1}$. Loginės funkcijos 1 reikšmių lentelė yra tokia:

x_1	x_2	x_3	1
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

Pirmas stulpelis yra funkciją x_1 atitinkantis vektorius $\vec{x}_1$, antras — $\vec{x}_2$, trečias — $\vec{x}_3$, ir ketvirtas — $\vec{1}$. Todėl kodo $RM(1,3)$ generuojanti matrica bus tiesiog transponuota ši reikšmių lentelė:

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

□

Žinome, kad koduodami tiesiniu kodu dauginame informacijos vektorių iš jo generuojančios matricos G, t. y. jei informacijos vektorius yra u, tai užkoduotas vektorius yra uG. Pasirodo, kad jei kodavimui Rydo-Miulerio kodu naudosime 5.8 teiginyje apibrėžtą generuojančią matricą, tai kodavimo procedūrą galėsime užrašyti ir kitaip. Atkreipkite dėmesį, kad informacijos vektoriaus u ilgis yra lygus kodo dimensijai, kuri šiuo atveju yra $m+1$.

5.10 teiginys. *Pažymėkime informacijos vektoriaus u koordinates $\lambda_1, \ldots, \lambda_m$ ir μ, t.y. $u = (\lambda_1, \ldots, \lambda_m, \mu)$. Tegu G yra 5.8 teiginyje apibrėžta Rydo-Miulerio kodo generuojanti matrica. Tada $uG = \vec{f}$, kur $\vec{f}$ yra vektorius, atitinkantis loginę funkciją $f(x) = \sum_{i=1}^{m} \lambda_i x_i + \mu$.*

Įrodymas. Matricos G eilutės yra $\vec{x_1}, \vec{x_2}, \ldots, \vec{x_m}, \vec{1}$, todėl

$$\begin{aligned} uG &= \lambda_1\vec{x_1} + \cdots + \lambda_m\vec{x_m} + \mu\vec{1} \\ &= \overrightarrow{\lambda_1 x_1 + \cdots + \lambda_m x_m + \mu} \\ &= \vec{f}. \end{aligned}$$

□

Taigi, užkoduotas vektorius yra $\vec{f}$.

5.11 pavyzdys. Tarkime, $m = 3$. Daugindami informacijos vektorių $u = (\lambda_1, \lambda_2, \lambda_3, \mu)$ iš 5.8 teiginyje pateiktos kodo $RM(1,m)$ generuojančios matricos G (žr. 5.9 pavyzdį), gauname

$$\begin{aligned} &(\lambda_1, \lambda_2, \lambda_3, \mu) \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \\ &= (\mu, \lambda_3+\mu, \lambda_2+\mu, \lambda_2+\lambda_3+\mu, \lambda_1+\mu, \lambda_1+\lambda_3+\mu, \lambda_1+\lambda_2+\mu, \lambda_1+\lambda_2+\lambda_3+\mu) \\ &= (f(0,0,0), f(0,0,1), f(0,1,0), f(0,1,1), f(1,0,0), f(1,0,1), f(1,1,0), f(1,1,1)) \\ &= \vec{f}. \end{aligned}$$

□

5.2 Dekodavimas

Operatorių Δ_i apibrėžkime taip:

$$\Delta_i : f(x) \mapsto \Delta_i f(x) = f(x + a_i) + f(x),$$

kur $f(x)$ — loginė funkcija, $1 \leqslant i \leqslant m$, ir

$$a_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{F}_2^m,$$

čia vienetas yra i-tojoje pozicijoje. Kitaip tariant,

$$\Delta_i f(x_1, \ldots, x_m) = f(x_1, \ldots, x_{i-1}, x_i + 1, x_{i+1}, \ldots, x_m) + f(x_1, \ldots, x_m).$$

5.12 pavyzdys. Tegu $m = 3$ ir $f(x_1, x_2, x_3) = x_1 + x_3$. Prisiminkime, kad skaičiuojama virš kūno $\mathbb{F}_2$. Tada

$$\begin{aligned}
\Delta_1 f &= f(x_1 + 1, x_2, x_3) + f(x_1, x_2, x_3) = (x_1 + 1 + x_3) + (x_1 + x_3) = 1,\\
\Delta_2 f &= f(x_1, x_2 + 1, x_3) + f(x_1, x_2, x_3) = (x_1 + x_3) + (x_1 + x_3) = 0,\\
\Delta_3 f &= f(x_1, x_2, x_3 + 1) + f(x_1, x_2, x_3) = 1.
\end{aligned}$$

Tegu dabar $f(x_1, x_2, x_3) = x_1x_2 + x_3$. Gauname, kad

$$\begin{aligned}
\Delta_1 f &= f(x_1 + 1, x_2, x_3) + f(x_1, x_2, x_3) = ((x_1 + 1)x_2 + x_3) + (x_1x_2 + x_3) = x_2,\\
\Delta_2 f &= f(x_1, x_2 + 1, x_3) + f(x_1, x_2, x_3) = (x_1(x_2 + 1) + x_3) + (x_1x_2 + x_3) = x_1,\\
\Delta_3 f &= f(x_1, x_2, x_3 + 1) + f(x_1, x_2, x_3) = 1.
\end{aligned}$$

□

5.13 teiginys. *Jei f yra afinioji loginė funkcija, tai $\Delta_i f$ yra konstanta. Tiksliau, jei*

$$f(x_1, \ldots, x_m) = \sum_{i=1}^{m} \lambda_i x_i + \mu,$$

tai

$$\Delta_i f(x) = \lambda_i.$$

5.14 užduotis. Įrodyti teiginį.

Taigi, $\overrightarrow{\Delta_i f} = \vec{\lambda}_i = \lambda_i (1, 1, \ldots, 1)$.

Tarkime, kad į kanalą pasiuntėme kodo $RM(1, m)$ žodį $\vec{f}$, atitinkantį afiniąją loginę funkciją $f(x) = \sum_{i=1}^{m} \lambda_i x_i + \mu$. Tarkime, kad iš kanalo gavome vektorių $\vec{g}$, atitinkantį (nebūtinai afiniąją) loginę funkciją g. Žinome, kad $\vec{g} = \vec{f} + \vec{e}$, kur $\vec{e}$ — klaidų vektorius, atitinkantis loginę funkciją e. Kadangi $\vec{f} + \vec{e} = \overrightarrow{f + e} = \vec{g}$, tai $g = f + e$.

Padarykime tokią *prielaidą*: klaidų skaičius vektoriuje mažesnis už ketvirtadalį vektoriaus ilgio, t. y. $w(\vec{e}) < \frac{2^m}{4} = 2^{m-2}$. Parodysime, kad tokiu atveju galima ištaisyti visas klaidas.

Tegu $1 \leqslant i \leqslant m$. Tada

$$\begin{aligned}
\Delta_i g &= g(x + a_i) + g(x)\\
&= f(x + a_i) + e(x + a_i) + f(x) + e(x)\\
&= \Delta_i f + \Delta_i e\\
&= \lambda_i + \Delta_i e,
\end{aligned}$$

todėl

$$\overrightarrow{\Delta_i g} = \lambda_i (1, \ldots, 1) + \overrightarrow{\Delta_i e}. \tag{13}$$

Įvertinkime vektoriaus $\overrightarrow{\Delta_i e}$ svorį $w(\overrightarrow{\Delta_i e})$. Tai leis įvertinti vektoriaus $\overrightarrow{\Delta_i g}$ svorį.

Visų pirma pastebėkime, kad kai $x = (x_1, x_2, \ldots, x_m)$ perbėga visų galimų tokių vektorių erdvę $\mathbb{F}_2^m$, tai $x + a_i$ taip pat perbėga visą šią erdvę $\mathbb{F}_2^m$, todėl atvaizdis $\mathbb{F}_2^m \to \mathbb{F}_2^m$, $x \mapsto x + a_i$ yra bijekcija (keitinys, perstata).

Kadangi skaičiuojant vektoriaus $\overrightarrow{e(x)}$ reikšmes x perbėga visą erdvę $\mathbb{F}_2^m$, tai skaičiuojant $\overrightarrow{e(x + a_i)}$ gauname tas pačias reikšmes, tik išrikiuotas kita tvarka.

5.15 pavyzdys. Tegu $m = 3$, $a_2 = (0, 1, 0)$ ir $\overrightarrow{e(x)} = (e_0, e_1, e_2, e_3, e_4, e_5, e_6, e_7)$. Pateiktoje lentelėje matome, kad, kai x perbėga $\mathbb{F}_2^3$, $x + a_2$ irgi perbėga $\mathbb{F}_2^3$. Todėl $e(x + a_2)$ įgyja tas pačias reikšmes, kaip $e(x)$, tik kita eilės tvarka. Pavyzdžiui, jei $x = 101$, tai $e(x + a_2) = e(101 + 010) = e(111) = e_7$, ir pan.

x	$x + a_2$	$e(x)$	$e(x + a_2)$
000	010	e_0	e_2
001	011	e_1	e_3
010	000	e_2	e_0
011	001	e_3	e_1
100	110	e_4	e_6
101	111	e_5	e_7
110	100	e_6	e_4
111	101	e_7	e_5

□

Taigi, vektorius $\overrightarrow{e(x + a_i)}$ ir $\overrightarrow{e(x)}$ sudaro tie patys elementai, tik skirtingai išrikiuoti, todėl jų svoriai sutampa: $w(\overrightarrow{e(x + a_i)}) = w(\overrightarrow{e(x)})$.

Pasinaudoję trikampio nelygybe ir mūsų prielaida, gauname:

$$w(\overrightarrow{\Delta_i e}) = w(\overrightarrow{e(x + a_i)} + \overrightarrow{e(x)}) \leqslant w(\overrightarrow{e(x + a_i)}) + w(\overrightarrow{e(x)}) = 2w(\overrightarrow{e(x)}) < 2 \cdot 2^{m-2} = 2^{m-1}.$$

Kadangi vektoriaus $\overrightarrow{\Delta_i e}$ ilgis yra 2^m, tai matome, kad vienetai stovi mažiau nei pusėje jo pozicijų. Grįžkime prie (13) lygybės.

- Jei $\lambda_i = 0$, tai $\overrightarrow{\Delta_i g} = \overrightarrow{\Delta_i e}$, todėl $w(\overrightarrow{\Delta_i g}) = w(\overrightarrow{\Delta_i e}) < 2^{m-1}$.
- Jei $\lambda_i = 1$, tai

$$w(\overrightarrow{\Delta_i g}) = w((1, 1, \ldots, 1) + \overrightarrow{\Delta_i e}) = 2^m - w(\overrightarrow{\Delta_i e}) > 2^m - 2^{m-1} = 2^{m-1}(2 - 1) = 2^{m-1}.$$

Tai mums leidžia nustatyti λ_i kiekvienam $i = 1, \ldots, m$ tokiu būdu. Gavę iš kanalo vektorių $\vec{g}$ apskaičiuojame vektoriaus $\overrightarrow{\Delta_i g}$ svorį $w(\overrightarrow{\Delta_i g})$.

- Jei $w(\overrightarrow{\Delta_i g}) < 2^{m-1}$, tai padarome išvadą, kad $\lambda_i = 0$.
- Jei $w(\overrightarrow{\Delta_i g}) > 2^{m-1}$, tai padarome išvadą, kad $\lambda_i = 1$.

Belieka nustatyti μ. Pažymėkime

$$h(x) = g(x) + \sum_{i=1}^{m} \lambda_i x_i.$$

Tada

$$h(x) = f(x) + e(x) + \sum_{i=1}^{m} \lambda_i x_i = \sum_{i=1}^{m} \lambda_i x_i + \mu + e(x) + \sum_{i=1}^{m} \lambda_i x_i = \mu + e(x).$$

Todėl

$$\overrightarrow{h(x)} = \mu\,(1, 1, \ldots, 1) + \overrightarrow{e(x)}.$$

Vėl gauname, kad:

- jei $\mu = 0$, tai $w(\overrightarrow{h(x)}) = w(\overrightarrow{e(x)}) < 2^{m-2}$,
- jei $\mu = 1$, tai $w(\overrightarrow{h(x)}) = 2^m - w(\overrightarrow{e(x)}) > 2^m - 2^{m-2} = 2^{m-2}(4-1) = 3 \cdot 2^{m-2}$.

Taigi, radę visus λ_i, apskaičiuojame vektoriaus

$$\overrightarrow{h(x)} = \overrightarrow{g(x)} + \overrightarrow{\sum_{i=1}^{m} \lambda_i x_i}$$

svorį $w(\overrightarrow{h(x)})$, ir:

- jei $w(\overrightarrow{h(x)}) < 2^{m-2}$, tai nusprendžiame, kad $\mu = 0$,
- jei $w(\overrightarrow{h(x)}) > 3 \cdot 2^{m-2}$, tai $\mu = 1$.

Jei $w(\overrightarrow{\Delta_i g})$ ar $w(\overrightarrow{h(x)})$ netenkina tų sąlygų, tai reiškia, kad klaidų kanale buvo padaryta daugiau, nei numatyta prielaidoje, ir šis algoritmas jų nebegali ištaisyti.

5.16 pavyzdys. Tegu $m = 3$. Dekodavimo algoritmas taisys mažiau, nei $2^{m-2} = 2^{3-2} = 2$ klaidas, t. y. galės ištaisyti tik vieną klaidą.

Tarkime, pranešimas yra $(\lambda_1, \lambda_2, \lambda_3, \mu) = (1, 0, 1, 1)$. Jį reikia užkoduoti. Užkoduotas vektorius bus vektorius $\vec{f}$, atitinkantis loginę funkciją $f(x) = \lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3 + \mu = x_1 + x_3 + 1$. Sudarome funkcijos f reikšmių lentelę ir gauname, kad $\vec{f} = (1, 0, 1, 0, 0, 1, 0, 1)$. Šį kodo $RM(1, 3)$ žodį ir siunčiame į kanalą.

Tarkime, kanale buvo padaryta viena klaida. Tarkime, klaida buvo padaryta ketvirtojoje pozicijoje, t. y. klaidų vektorius yra $\vec{e} = (0, 0, 0, 1, 0, 0, 0, 0)$. Klaidų vektorių atitinkančios funkcijos rasti nereikia, bet įdomumo dėlei pastebėkime, kad tai funkcija $e(x_1, x_2, x_3) = (1 + x_1)x_2x_3$, nes iš vektoriaus $\vec{e}$ matome, kad funkcija e įgyja reikšmę 1 tik su kintamųjų reikšmių rinkiniu $(0, 1, 1)$ (prisiminkime iš diskrečiosios matematikos kurso, kad gauti loginės funkcijos išraišką turėdami jos teisingumo reikšmių lentelę galime sudarydami jos normaliąsias formas — normaliąją konjunkcinę ar disjunkcinę formas).

Iš kanalo gauname vektorių $\vec{g} = \vec{f} + \vec{e} = (1, 0, 1, 1, 0, 1, 0, 1)$. Dekoduodami nustatysime λ_1, λ_2, λ_3 ir μ reikšmes, t. y. surasime pradinį pranešimą $(\lambda_1, \lambda_2, \lambda_3, \mu)$.

Pradėsime nuo λ_1 radimo. Reikia apskaičiuoti $\overrightarrow{\Delta_1 g} = \overrightarrow{g(x)} + \overrightarrow{g(x + a_1)}$. Kam lygus $\overrightarrow{g(x + a_1)}$? Kaip ir 5.15 pavyzdyje sudarome lentelę, pagal kurią nustatome, kokiu būdu sukeisti vektoriaus $\overrightarrow{g(x)}$ koordinates, kad gautume vektorių $\overrightarrow{g(x + a_1)}$.

x	$x + a_1$	$g(x)$	$g(x + a_1)$	$x + a_2$	$g(x + a_2)$	$x + a_3$	$g(x + a_3)$
000	100	g_0	g_4	010	g_2	001	g_1
001	101	g_1	g_5	011	g_3	000	g_0
010	110	g_2	g_6	000	g_0	011	g_3
011	111	g_3	g_7	001	g_1	010	g_2
100	000	g_4	g_0	110	g_6	101	g_5
101	001	g_5	g_1	111	g_7	100	g_4
110	010	g_6	g_2	100	g_4	111	g_7
111	011	g_7	g_3	101	g_5	110	g_6

Matome, kad jei

$$\overrightarrow{g(x)} = (g_0, g_1, \ldots, g_7) = (1,0,1,1,0,1,0,1),$$

tai

$$\overrightarrow{g(x+a_1)} = (g_4, g_5, g_6, g_7, g_0, g_1, g_2, g_3) = (0,1,0,1,1,0,1,1).$$

Todėl

$$\overrightarrow{\Delta_1 g} = \overrightarrow{g(x)} + \overrightarrow{g(x+a_1)} = (1,1,1,0,1,1,1,0).$$

Taigi, $w(\overrightarrow{\Delta_1 g}) = 6 > 2^{m-1} = 4$, todėl nusprendžiame, kad $\lambda_1 = 1$.

Analogiškai

$$\overrightarrow{g(x+a_2)} = (g_2, g_3, g_0, g_1, g_6, g_7, g_4, g_5) = (1,1,1,0,0,1,0,1),$$

todėl

$$\overrightarrow{\Delta_2 g} = \overrightarrow{g(x)} + \overrightarrow{g(x+a_2)} = (0,1,0,1,0,0,0,0).$$

Taigi, $w(\overrightarrow{\Delta_2 g}) = 2 < 4$, todėl nusprendžiame, kad $\lambda_2 = 0$.

Taip pat ir

$$\overrightarrow{g(x+a_3)} = (g_1, g_0, g_3, g_2, g_5, g_4, g_7, g_6) = (0,1,1,1,1,0,1,0),$$

todėl

$$\overrightarrow{\Delta_3 g} = \overrightarrow{g(x)} + \overrightarrow{g(x+a_3)} = (1,1,0,0,1,1,1,1).$$

Taigi, $w(\overrightarrow{\Delta_3 g}) = 6 > 4$, todėl nusprendžiame, kad $\lambda_3 = 1$.

Liko rasti μ. Sudarome funkciją $f'(x) = \lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3 = x_1 + x_3$, randame ją atitinkantį vektorių $\overrightarrow{f'(x)} = (0,1,0,1,1,0,1,0)$. Tada

$$\overrightarrow{h(x)} = \overrightarrow{g(x)} + \overrightarrow{f'(x)} = (1,1,1,0,1,1,1,1).$$

Kadangi $w(\overrightarrow{h(x)}) = 7 > 3 \cdot 2^{m-2} = 3 \cdot 2 = 6$, tai nusprendžiame, kad $\mu = 1$.

Taigi, dekodavę gauname, kad pradinis pranešimas buvo $(\lambda_1, \lambda_2, \lambda_3, \mu) = (1,0,1,1)$, t.y. padaryta klaida buvo ištaisyta. Įdomumo dėlei dar galime rasti klaidų vektorių

$$\overrightarrow{e(x)} = \overrightarrow{h(x)} + \mu\,(1,1,\ldots,1) = (0,0,0,1,0,0,0,0)$$

ir išsiųstą kodo žodį $\vec{f} = \vec{g} - \vec{e} = (1,0,1,0,0,1,0,1)$. □

5.3 Minimalus atstumas

5.17 teiginys. *Kodo $RM(1,m)$ minimalus atstumas yra 2^{m-1}.*

Be įrodymo.

6 Naujų kodų sudarymo būdai

Iš jau turimų kodų galima sudaryti naujus, stengiantis pagerinti jų parametrus.

6.1 Plėtinys

6.1 apibrėžimas. *Tegu C yra ilgio n kodas (nebūtinai tiesinis) virš $\mathbb{F}_q$. Jo* plėtiniu *vadinsime kodą*

$$C^+ = \{(x_1, x_2, \ldots, x_n, x_{n+1}) \in \mathbb{F}_q^{n+1} : (x_1, x_2, \ldots, x_n) \in C, \sum_{j=1}^{n+1} x_j = 0\}.$$

Taigi, plėtinys yra kodas, gaunamas tiesiog prie kiekvieno kodo C žodžio prijungus po tokį simbolį x_{n+1}, kad gauto žodžio koordinačių suma būtų lygi nuliui.

6.2 pavyzdys. Jei $C = \{1200, 1001, 0112\}$ yra kodas virš $\mathbb{F}_3$, tai $C^+ = \{12000, 10011, 01122\}$. Jei $C' = \{1100, 1000, 1110\}$ yra dvinaris kodas, tai $C'^+ = \{11000, 10001, 11101\}$. □

Matome, kad plėtinio sudarymas kai kuriais atvejais leidžia labai paprastai padidinti kodo minimalų atstumą (6.2 pavyzdyje kodo C minimalus atstumas $d = 2$, o jo plėtinio C^+ minimalus atstumas $d^+ = 3$).

6.3 teiginys. *Jei C yra tiesinis kodas, generuotas matricos G, tai jo plėtinys C^+ irgi yra tiesinis kodas, ir jo generuojanti matrica yra $G^+ = (G|b)$, kur b yra toks vektorius-stulpelis, kad kiekvienos G^+ eilutės elementų suma lygi* 0.

Įrodyti savarankiškai.

6.4 pavyzdys. Jei dvinaris kodas C yra generuotas matricos

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix},$$

tai jo plėtinio C^+ generuojanti matrica yra

$$G^+ = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$ □

6.5 užduotys. 1. Įrodykite tokius teiginius.

a) Jei C yra (n, M, d) kodas, tai jo plėtinys C^+ yra $(n+1, M, d^+)$ kodas, kur $d \leqslant d^+ \leqslant d+1$.

b) Jei C yra dvinaris kodas, kurio minimalus atstumas yra d, tai plėtinio minimalus atstumas

$$d^+ = \begin{cases} d, & \text{jei } d \text{ — lyginis,} \\ d+1, & \text{jei } d \text{ — nelyginis.} \end{cases}$$

c) Jei tiesinio kodo C kontrolinė matrica yra H, tai plėtinio C^+ kontrolinė matrica yra

$$H^+ = \left(\begin{array}{ccc|c} & & & 0 \\ & H & & \vdots \\ & & & 0 \\ \hline 1 & \cdots & 1 & 1 \end{array}\right).$$

2. Matome, kad plėtinio minimalus atstumas d^+ gali būti vienetu didesnis, negu pradinio kodo minimalus atstumas d. Bet sunku pasakyti, ar plėtinio minimalus atstumas bus didesnis už kodo minimalų atstumą, ar ne. Pavyzdžiui, jei kodai C_1 ir C_2 virš $\mathbb{F}_3$ yra generuoti atitinkamai matricų

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \text{ ir } G_2 = \begin{pmatrix} 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 2 \end{pmatrix},$$

tai plėtinio C_1^+ minimalus atstumas didesnis, nei kodo C_1, o plėtinio C_2^+ — ne. Iš tiesų, įsitikinkite, kad kodų C_1, C_2, C_2^+ minimalus atstumas yra 2, o kodo C_1^+ — 3.

6.2 Sutrumpintas kodas

6.6 apibrėžimas. *Tegu C yra ilgio n kodas virš $\mathbb{F}_q$, J yra indeksų aibės $\{1, \ldots, n\}$ poaibis. Kodo C aibėje J* sutrumpintu kodu *vadinsime kodą*

$$C_J = \{(x_i)_{i\in\{1,\ldots,n\}\setminus J} \in \mathbb{F}_q^{n-|J|} : (x_i)_{i\in\{1,\ldots,n\}} \in C \text{ su kuriais nors } x_i \in \mathbb{F}_q, i \in J\}.$$

Kai nenurodome, kokioje aibėje trumpiname, kodo C sutrumpintu kodu *vadiname kodą $C_{\{n\}}$.*

Taigi, kodo C aibėje J sutrumpintas kodas gaunamas tiesiog iš kiekvieno kodo C žodžio pašalinus koordinates, priklausančias aibei J. Gauname ilgio $n - |J|$ kodą. Jei nenurodoma, kokioje aibėje trumpiname, tai šaliname paskutinę (n-tąją) koordinatę, gauname $n - 1$ ilgio kodą.

6.7 pavyzdys. Jei $C = \{120020, 100121, 011201\}$ yra kodas virš $\mathbb{F}_3$, tai jo aibėje $\{2, 4, 6\}$ sutrumpintas kodas gaunamas iš kiekvieno kodo C žodžio pašalinus antrą, ketvirtą ir šeštą koordinates: $C_{\{2,4,6\}} = \{102, 010\}$. Kadangi sutrumpinę žodžius 120020 ir 100121 gauname tą patį žodį 102, tai sutrumpintame kode žodžių bus mažiau, nei pradiniame. Kodo C sutrumpintas kodas gaunamas iš kiekvieno kodo C žodžio pašalinus paskutinę koordinatę: $C_{\{6\}} = \{12002, 10012, 01120\}$. □

6.8 teiginys. *Jei kodas C yra tiesinis, tai jo aibėje J sutrumpintas kodas irgi yra tiesinis, ir jo generuojanti matrica gaunama iš kodo C generuojančios matricos pašalinus stulpelius, kurių numeriai priklauso aibei J.*

6.9 pavyzdys. Jei dvinaris kodas C yra generuotas matricos

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix},$$

tai jo aibėje $\{1, 4, 5\}$ sutrumpinto kodo generuojančią matricą G' gausime, pašalinę iš matricos G pirmą, ketvirtą ir penktą stulpelius:

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

Kodo C sutrumpinto kodo generuojančią matricą G' gausime, pašalinę iš matricos G paskutinį stulpelį:

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

□

Aibėje J sutrumpintų kodų dimensija gali sumažėti, dėl to reikia patikrinti, ar pašalinę generuojančios matricos stulpelius negausime tiesiškai priklausomų eilučių. Jei gauname, tai paliekame tik maksimalią tiesiškai nepriklausomų eilučių aibę, likusias eilutes pašalindami.

6.10 pavyzdys. Tarkime, dvinaris kodas C yra generuotas matricos

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

Pašalinę paskutinį jos stulpelį, gauname matricą

$$G'' = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix},$$

kurios eilutės tiesiškai priklausomos (pirmos dvi eilutės lygios). Pašaliname vieną iš tų lygių eilučių ir gauname sutrumpinto kodo generuojančią matricą

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

□

6.11 užduotys. Įrodykite tokius teiginius.

1. Jei C yra (n, M, d) kodas virš $\mathbb{F}_q$, tai jo sutrumpintas kodas C' yra $(n-1, M', d')$ kodas virš $\mathbb{F}_q$, kur $d - 1 \leqslant d' \leqslant d$, $M/q \leqslant M' \leqslant M$. Jei $d \geqslant 2$, tai $M' = M$.

2. Tegu C yra tiesinis $[n, k, d]$ kodas virš $\mathbb{F}_q$, kurio kontrolinė matrica yra H. Tada jo sutrumpintas kodas C' yra tiesinis $[n-1, k', d']$ kodas, kur $d-1 \leqslant d' \leqslant d$, $k-1 \leqslant k' \leqslant k$. Jei $d \geqslant 2$, tai $k' = k$. Kodo C' kontrolinė matrica H' gaunama taip: jei matricos H paskutinis stulpelis yra nulinis, H' gaunama iš H pašalinant paskutinį stulpelį, o jei ne, tai reikia suvesti H į tokį pavidalą, kad tik vienos eilutės paskutinėje pozicijoje būtų nenulinis elementas, ir pašalinti tą eilutę bei paskutinį stulpelį iš H.

6.3 Sumažintas kodas

6.12 apibrėžimas. *Tegu C yra ilgio n kodas virš $\mathbb{F}_q$, J yra indeksų aibės $\{1, \ldots, n\}$ poaibis. Kodo C* aibėje J sumažintu kodu *vadinsime kodą*

$$C_{\setminus J} = \{(x_i)_{i \in \{1,\ldots,n\} \setminus J} \in \mathbb{F}_q^{n-|J|} : (x_i)_{i \in \{1,\ldots,n\}} \in C \text{ toks, kad } x_i = 0 \ \forall i \in J\}.$$

Kai nenurodome, kokioje aibėje mažiname, kodo C sumažintu kodu *vadiname kodą $C_{\setminus \{n\}}$.*

Taigi, kodo C aibėje J sumažintą kodą gauname, išrinkę kodo C žodžius, kurių koordinatėse, priklausančiose aibei J, yra nuliai, ir pašalinę tas koordinates. Gauname ilgio $n - |J|$ kodą. Jei nenurodoma, kokioje aibėje mažiname, tai šaliname paskutinę (n-tąją) koordinatę iš tų kodo C žodžių, kurių paskutinė koordinatė lygi nuliui. Gauname $n-1$ ilgio kodą.

6.13 pavyzdys. Jei $C = \{120020, 100120, 011200, 210222\}$ yra kodas virš $\mathbb{F}_3$, tai jo aibėje $\{3, 6\}$ sumažintas kodas gaunamas taip. Visų pirma išrenkame kodo C žodžius, kurių trečioje ir šeštoje vietoje yra nuliai. Tokių žodžių aibė bus $\{120020, 100120\}$. Tada iš jų pašaliname trečią ir šeštą koordinates: $C_{\setminus\{3,6\}} = \{1202, 1012\}$. Kodo C sumažintas kodas bus $C_{\setminus\{6\}} = \{12002, 10012, 01120\}$. □

6.14 teiginys. *Jei kodas C yra tiesinis, tai jo aibėje J sumažintas kodas irgi yra tiesinis, ir jo kontrolinė matrica gaunama iš kodo C kontrolinės matricos pašalinus stulpelius, kurių numeriai priklauso aibei J.*

Taigi, dabar šaliname ne generuojančios matricos, kaip trumpindami kodą, o kontrolinės matricos stulpelius. Kaip šalinti stulpelius, matėme 6.9 pavyzdyje, tik jame dabar žodžius „generuojanti matrica“ reikėtų pakeisti į „kontrolinė matrica“.

Kaip ir sutrumpintiems kodams, galime gauti, kad pašalinus stulpelius matricoje atsiras tiesiškai priklausomų eilučių. Tokiu atveju paliekame tik maksimalią tiesiškai nepriklausomų eilučių aibę, likusias eilutes pašalindami.

6.15 užduotys. Įrodykite tokius teiginius.

1. Jei C yra (n, M, d) kodas virš $\mathbb{F}_q$, tai jo sumažintas kodas C' yra $(n-1, M', d')$ kodas virš $\mathbb{F}_q$, kur $0 \leqslant M' \leqslant M$, $d' \geqslant d$.

2. Tegu C yra tiesinis $[n, k, d]$ kodas virš $\mathbb{F}_q$. Jo sumažintas kodas C' taip pat yra tiesinis kodas. Jei kodo C žodžių paskutinėje pozicijoje yra tik nuliai, tai C' yra $[n-1, k, d]$ kodas. Priešingu atveju C' yra $[n-1, k-1, d']$ kodas, kur $d' \geqslant d$.