2. Tiesiniai kodai

Nagrinėsime kodus, sudarytus iš specialios abėcėlės žodžių. Ši abėcėlė tai algebrinis kūnas $\mathbf{F}_q$, čia $q = p^n$ – pirminio skaičiaus laipsnis. Atskiru ir svarbiausiu atveju – $q = 2$.

2.1. Kodavimas tiesiniais kodais

Žodžių aibė $\mathbf{F}_q^n$ yra n-matė tiesinė erdvė virš kūno $\mathbf{F}_q$.
Dabar – pagrindinė šio skyriaus sąvoka.

2.1.1 apibrėžimas. *Kodą* $\mathbf{L}$, $\mathbf{L} \subset \mathbf{F}_q^n$, *vadinsime tiesiniu, jei* $\mathbf{L}$ *yra tiesinis* $\mathbf{F}_q^n$ *poerdvis. Jei* $\mathbf{L}$ *dimensija lygi* k, *o minimalus atstumas* d, *tai kodą* $\mathbf{L}$ *vadinsime* $[n, k, d]$, *arba tiesiog* $[n, k]$, *kodu.*

Kiekvienas $[n, k]$ kodas turi q^k elementų. Dažniausiai susidursime su dvinarės abėcėlės žodžių kodais, t. y. atveju $q = 2$.

Tegu $\mathbf{L}$ yra $[n, k]$ kodas. Kad jis būtų visiškai apibrėžtas, nebūtina išrašyti visus q^k jo žodžius. Pakanka nurodyti tuos žodžius $\mathbf{a}_1, \ldots, \mathbf{a}_k$, kurie sudaro $\mathbf{L}$ kaip tiesinio $\mathbf{F}_q^n$ poerdvio bazę.

2.1.2 apibrėžimas. *Tegu* $\mathbf{L}, \mathbf{L} \subset \mathbf{F}_q^n$, *yra tiesinis* $[n, k]$ *kodas. Kūno* $\mathbf{F}_q$ *elementų* $k \times n$ *matricą* G *vadinsime generuojančia kodo* $\mathbf{L}$ *matrica, jei* n *ilgio žodžiai, gauti išrašant matricos* G *eilučių elementus, sudaro kodo* $\mathbf{L}$ *bazę.*

Jeigu žinome $[n, k]$ kodo $\mathbf{L}$ generuojančią matricą G, tai visus kodo $\mathbf{L}$ žodžius ir tik juos gausime imdami generuojančios matricos eilučių kombinacijas:

$$\mathbf{L} = \{\mathbf{x}G : \mathbf{x} \in \mathbf{F}_q^k\};$$

čia $\mathbf{x}G$ reiškia žodžio, kaip vektoriaus-eilutės ir matricos sandaugą.

Stabtelkime ties šiuo sąryšiu. Atvaizdis

$$\mathbf{x} \to \mathbf{x}G$$

apibrėžia abipusiškai vienareikšmę erdvės $\mathbf{F}_q^k$ ir kodo $\mathbf{L}$ žodžių atitiktį. Tad šį priskyrimą galime interpretuoti kaip šaltinio informacijos, pateikiamos erdvės $\mathbf{F}_q^k$ žodžiais, kodavimą kodo $\mathbf{L}$ elementais.

Tik šitokią kodavimo procedūrą ir tenaudosime šiame skyriuje. Tačiau kodo generuojanti matrica nėra vienintelė. Skirtingas generuojančias matricas atitinka skirtingos kodavimo procedūros. Informacijos gavėjui turi būti pranešta, kokią generuojančią matricą naudoja siuntėjas. Tada pagal kodo žodį $\mathbf{y}$ gavėjas, pasinaudojęs sąryšiu $\mathbf{y} = \mathbf{x}G$, galės surasti šaltinio siųstą žodį $\mathbf{x}$.

Elementariaisiais matricos G pertvarkiais vadinsime šiuos veiksmus:

1) dviejų eilučių (arba stulpelių) keitimą vietomis;
2) eilutės daugybą iš $f \in \mathbf{F}_q$, $f \neq 0$;
3) eilutės keitimą jos bei kitos eilutės suma;
4) stulpelio daugybą iš $f \in \mathbf{F}_q$, $f \neq 0$.

Jei matrica G yra tiesinio $[n, k]$ kodo $\mathbf{L}$ generuojanti matrica, o matrica G' gaunama iš G, atlikus baigtinę elementariųjų pertvarkių seką, tai G' yra taip pat tam tikro tiesinio $[n, k]$ kodo $\mathbf{L}'$ generuojanti matrica. Prisiminę ekvivalenčių kodų apibrėžimą bei apmąstę, kaip keičiasi kodas $\mathbf{L}$, kai matricą G keičiame G', gauta, atlikus vieną elementarų pertvarkį, nesunkiai prieisime tokią išvadą.

2.1.1 teorema. *Jei* G *ir* G' *yra* $[n, k]$ *kodų* $\mathbf{L}, \mathbf{L}'$ *generuojančios matricos, ir* G' *galima gauti iš* G, *atlikus baigtinę elementariųjų pertvarkių seką, tai kodai* $\mathbf{L}, \mathbf{L}'$ *yra ekvivalentūs.*

Atitinkamais elementariaisiais pertvarkiais kontrolinę matricą galima pertvarkyti į tokio pavidalo matricą:

$$G' = \begin{pmatrix} 1 & 0 & \ldots & 0 & a_{1,1} & \ldots & a_{1,n-k} \\ 0 & 1 & \ldots & 0 & a_{2,1} & \ldots & a_{2,n-k} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 & a_{k,1} & \ldots & a_{k,n-k} \end{pmatrix} = (I_k, A);$$

• • • ◇ • • •

čia: I_k yra vienetinė $k \times k$ matrica, A – kūno $\mathbf{F}_q$ elementų $k \times (n-k)$ matrica. Susitarsime sakyti, jog gautoji matrica yra **standartinio pavidalo**.

2.1.2 teorema. *Kiekvienas $[n,k]$ kodas yra ekvivalentus $[n,k]$ kodui, turinčiam standartinio pavidalo generuojančią matricą.*

Bet kokį tiesinį kodą galime pakeisti jam ekvivalenčiu kodu, turinčiu standartinio pavidalo generuojančią matricą. Todėl pakanka nagrinėti tik tokius kodus. Pastebėkime, jog kodavimo procedūra, kai naudojama standartinio pavidalo generuojanti matrica $G = (I_k, A)$, atrodo šitaip:

$$\mathbf{x} \to \mathbf{xy}, \quad \mathbf{y} = \mathbf{x}A,$$

taigi koduojami žodžiai tiesiog pailginami, pridedant $n-k$ kontrolinių simbolių.

2.1.3 apibrėžimas. *Žodžio $\mathbf{x} \in \mathbf{F}_q^n$, $\mathbf{x} = x_1 \dots x_n$, svoriu vadinsime skaičių*

$$w(\mathbf{x}) = \sum_{x_i \neq 0} 1.$$

2.1.3 teorema. *Tegu d yra tiesinio kodo $\mathbf{L}$ minimalus atstumas. Tada*

$$d = \min\{w(\mathbf{x}) : \mathbf{x} \in \mathbf{L}, \mathbf{x} \neq 00\dots0\}.$$

2.2. Tiesinių kodų dekodavimas

Vienetinę $m \times m$ matricą žymėsime I_m, $k \times m$ matricą, sudarytą vien tik iš nulių, žymėsime $O_{k,m}$, indeksus k, m kartais praleisime. Jei A yra $m \times k$ matrica, tai $k \times m$ matricą, gautą sukeitus A stulpelius ir eilutes vietomis, žymėsime $A^\top$ (transponavimo operacija). Jei matricos A, B turi vienodą eilučių arba stulpelių skaičių, tai jungdami jas gausime didesnių matavimų matricas

$$(A, B) \text{ arba } \begin{pmatrix} A \\ B \end{pmatrix}.$$

Iš pradžių tokia lengvai patikrinama matricų tapatybė.

2.2.1 teorema. *Jei A yra $k \times m$ matrica, tai*

$$(I_k, A)\begin{pmatrix} -A \\ I_m \end{pmatrix} = O_{k,m}.$$

Tegu dabar $G = (I_k, A)$ yra tiesinio $[n,k]$ kodo $\mathbf{L}$ standartinio pavidalo generuojanti matrica. Sudarykime kitą matricą

$$H = (-A^T, I_{n-k}).$$

Tada

$$H^T = \begin{pmatrix} -A \\ I_{n-k} \end{pmatrix},$$

ir 2.2.1 teoremos lygybę galima užrašyti taip:

$$GH^T = O_{k,n-k}.$$

2.2.2 teorema. *Tegu $G = (I_k, A)$ yra tiesinio $[n,k]$ kodo $\mathbf{L}$ generuojanti matrica, $H = (-A^T, I_{n-k})$. Žodis $\mathbf{x} \in \mathbf{F}_q^n$ priklauso kodui $\mathbf{L}$ tada ir tik tada, kai*

$$\mathbf{x}H^T = O_{1,n-k}. \tag{2.2.1}$$

• • • ◇ • • •

Taigi (2.2.1) lygybė įgalina lengvai atpažinti kodo žodžius. Analogija su kontrolinio simbolio metodu, nagrinėtu ankstesniame skyriuje? Taip, žinoma.

2.2.1 apibrėžimas. *Tegu* $\mathbf{L}$ *yra tiesinis* $[n,k]$ *kodas.* $(n-k)\times n$ *matricą* H*, kuri tenkina sąlygą*

$$\mathbf{L}=\{\mathbf{x}:\mathbf{x}H^T=O_{1,n-k}\},$$

vadinsime kodo $\mathbf{L}$ *kontroline matrica (parity check matrix).*

Kodo kontrolinė matrica apibrėžta nevienareikšmiškai. Tačiau mokame pagal standartinio pavidalo generuojančią matricą G sudaryti specialią kontrolinę matricą H:

jei $G=(I_k,A)$*, tai* $H=(-A^T,I_{n-k})$*.*

2.2.3 teorema. *Tegu* H *yra tiesinio kodo* $\mathbf{L}$ *kontrolinė matrica. Jeigu egzistuoja* d *tiesiškai priklausomų* H *stulpelių, o bet kuri* $d-1$ *šios matricos stulpelių sistema yra tiesiškai nepriklausoma, tai kodo* $\mathbf{L}$ *minimalus atstumas lygus* d*.*

Dabar aptarsime, kaip atliekamas tiesinių kodų dekodavimas, taikant minimalaus atstumo taisyklę.

Tegu $\mathbf{L}\subset\mathbf{F}_q^n$ yra tiesinis $[n,k]$ kodas. Suskaidysime erdvę $\mathbf{F}_q^n$ aibėmis $\mathbf{L_x}=\mathbf{x}+\mathbf{L}$; čia $\mathbf{x}\in\mathbf{F}_q^n$. Aibės $\mathbf{L_x},\mathbf{L_y}$ arba nesikerta, arba sutampa; čia $\mathbf{x},\mathbf{y}\in\mathbf{F}_q^n$. Aibė

$$\mathbf{F}_q^n/\mathbf{L}=\{\mathbf{L_x}:\mathbf{x}\in\mathbf{F}_q^n\}$$

yra tiesinė erdvė, gauta faktorizavus $\mathbf{F}_q^n$ pagal poerdvį $\mathbf{L}$. Pastebėsime, $|\mathbf{F}_q^n/\mathbf{L}|=q^{n-k}$.

Tarkime, informacija koduojama naudojant kodą $\mathbf{L}$. Tegu kitame kanalo gale gautas žodis $\mathbf{x}$, kuris galbūt skiriasi nuo siųstojo. Taikydami minimalaus atstumo taisyklę, šį žodį dekoduosime kodo žodžiu $\mathbf{c}$, kuris tenkina sąlygą

$$h(\mathbf{c},\mathbf{x})=w(\mathbf{x}-\mathbf{c})=\min_{\mathbf{c}'\in\mathbf{L}}w(\mathbf{x}-\mathbf{c}').$$

Tačiau žodis $\mathbf{a}=\mathbf{x}-\mathbf{c}$ yra kurioje nors klasėje $\mathbf{L_b}$ – toje pat kaip $\mathbf{x}$. Vadinasi, dekoduojant reikia peržiūrėti klasę $\mathbf{L_b}$, kurioje atsidūrė gautas žodis $\mathbf{x}$, rasti joje mažiausią svorį turintį elementą $\mathbf{a}$ ir dekoduoti taip:

$$\mathbf{x}\to f(\mathbf{x})=\mathbf{x}-\mathbf{a}.$$

Šią procedūrą galime atlikti taip. Sunumeruokime kodo $\mathbf{L}$ žodžius taip, kad žodis $\mathbf{0}=00\ldots0$ būtų pirmas: $\mathbf{L}=\{\mathbf{c}_0,\mathbf{c}_1,\ldots,\mathbf{c}_N\},\mathbf{c}_0=\mathbf{0},N=q^k-1$. Visus $\mathbf{F}_q^n$ elementus išrašysime tokioje matricoje-lentelėje:

$$\begin{pmatrix}\mathbf{a}_0 & \mathbf{c}_1 & \mathbf{c}_2 & \ldots & \mathbf{c}_N\\ \mathbf{a}_1 & \mathbf{a}_1+\mathbf{c}_1 & \mathbf{a}_1+\mathbf{c}_2 & \ldots & \mathbf{a}_1+\mathbf{c}_N\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ \mathbf{a}_s & \mathbf{a}_s+\mathbf{c}_1 & \mathbf{a}_s+\mathbf{c}_2 & \ldots & \mathbf{a}_s+\mathbf{c}_N\end{pmatrix}. \tag{2.2.2}$$

Pirmo stulpelio žodžius $\mathbf{a}_i$ parenkame taip, kad būtų patenkintos sąlygos:

$$\mathbf{a}_0=\mathbf{0},\ w(\mathbf{a}_i)=\min\{w(\mathbf{a}):\mathbf{a}\in\mathbf{F}_q^n,\mathbf{a}\notin\bigcup_{j<i}\mathbf{L}_{\mathbf{a}_j}\},\ j\geq1.$$

Šis matricos sudarymo būdas garantuoja, jog kiekvienoje eilutėje išrašyti atitinkamos klasės $\mathbf{L_a}$ elementai, o pirmasis iš jų turi mažiausią svorį. (2.2.2) matricą vadinsime **standartine** kodo **L lentele**, o žodžius $\mathbf{a}_i$ – atitinkamų klasių **lyderiais**.

Turint standartinę kodo lentelę, dekodavimo algoritmą galima taip aprašyti:

- *randame, kurioje standartinės lentelės eilutėje yra gautasis žodis* $\mathbf{x}$*;*
- *randame šios eilutės lyderį* $\mathbf{a}$ *ir dekoduojame* $\mathbf{x}$ *žodžiu* $f(\mathbf{x})=\mathbf{x}-\mathbf{a}$ *.*

••• ◇ •••

Tačiau dekodavimą galima dar labiau suprastinti.

Tegu H yra kontrolinė kodo $\mathbf{L}$ matrica. Pastebėkime, jog sandaugos $\mathbf{x}H^T, \mathbf{x} \in \mathbf{F}_q^n$, reikšmė priklauso tik nuo to, kuriai aibės $\mathbf{F}_q^n/\mathbf{L}$ klasei priklauso $\mathbf{x}$. Jei $\mathbf{x}$ yra kodo $\mathbf{L}$ žodis, tai $\mathbf{x}H^T = \mathbf{0}, \mathbf{0} = 00\ldots0$.

2.2.2 apibrėžimas. *Tegu H yra kodo $\mathbf{L}$ kontrolinė matrica, $\mathbf{x} \in \mathbf{F}_q^n$. Žodžio $\mathbf{x}$ sindromu*[1] *vadinsime $\mathbf{F}_q^n$ elementą $s(\mathbf{x}) = \mathbf{x}H^T$.*

Skirtingoms klasėms priklausančius žodžius atitinka skirtingi sindromai. Tad dekoduojant pagal minimalaus atstumo taisyklę, pakanka turėti prieš akis tokią lentelę:

Sindromai	$\mathbf{s}_1$	$\mathbf{s}_2$	$\ldots$	$\mathbf{s}_N$
Lyderiai	$\mathbf{a}_1$	$\mathbf{a}_2$	$\ldots$	$\mathbf{a}_N$.

Dabar pirmąją užrašyto dekodavimo algoritmo dalį galime formuluoti taip:

- *randame gautojo žodžio sindromą.*

Sindromui rasti pakanka mokėti padauginti vektorių iš kontrolinės matricos.

2.3. Hammingo kodai

Tiesinis kodas vienareikšmiškai apibrėžiamas tiek generuojančia, tiek kontroline matrica. Tuo pasiremsime sudarydami Hamingo kodus[1] .

Ieškosime kodų, kurių minimalus atstumas $d = 3$. Taigi apsiribosime tuo, kad tokie kodai taiso tik vieną klaidą, tačiau sieksime, kad jie būtų kiek įmanoma didesni. Fiksuosime dar vieną ieškomų kodų parametrą – kontrolinės matricos eilučių skaičių.

Taigi ieškosime daugiausiai abėcėlės $\mathbf{F}_q$ žodžių turinčio tiesinio kodo, jeigu iš anksto duotas kontrolinės matricos eilučių skaičius r ir minimalus atstumas $d = 3$. Taigi kontrolinė matrica H turi turėti r eilučių, o bet kurie du jos stulpeliai turi būti tiesiškai nepriklausomi. Tai reiškia, kad nei vienas stulpelis negali būti gaunamas iš kito, padauginus pastarąjį iš $\alpha \in \mathbf{F}_q$. Sudarysime H imdami tiek stulpelių, kiek tik yra įmanoma.

Pasirinkime iš aibės $V_1 = \mathbf{F}_q^r$ nenulinį žodį $\mathbf{s}_1$ ir sudarykime iš jo elementų pirmąjį H stulpelį. Apibrėškime aibę

$$V_2 = V_1 \backslash \{\alpha \mathbf{s}_1 : \alpha \in \mathbf{F}_q\}.$$

Antrąjį H stulpelį sudarykime iš pasirinkto aibės V_2 žodžio elementų. Bendra stulpelių pasirinkimo taisyklė tokia:

- *jeigu m-asis matricos H stulpelis sudarytas iš žodžio $\mathbf{s}_m \in V_m$ komponenčių, sudarykime aibę*

$$V_{m+1} = V_m \backslash \{\alpha \mathbf{s}_m : \alpha \in \mathbf{F}_q\},$$

ir, jeigu ši aibė nėra tuščia, pasirinkime iš jos žodį $\mathbf{s}_{m+1}$. Jeigu $V_{m+1} = \emptyset$, matricos H sudarymą užbaikime.

Gautos matricos H eilutės yra tiesiškai nepriklausomos, t. y. matricos rangas lygus r. Kiek stulpelių parenkama tokiu būdu? Kadangi

$$|V_1| = q^r, \quad |V_m| = q^r - 1 - (m-1)(q-1), \quad m \geq 2,$$

tai iš viso galima parinkti $n = (q^r - 1)/(q - 1)$ stulpelių. Taigi matrica H yra kontrolinė tiesinio $[n, n-r, 3]$ kodo matrica.

2.3.1 apibrėžimas. *Tegu $r \geq 1$, $n = (q^r - 1)/(q - 1)$. Tiesinius $[n, n-r, 3]$ kodus iš $\mathbf{F}_q$ abėcėlės žodžių vadinsime Hamingo kodais ir žymėsime $\mathbf{H}_q(r)$.*

2.3.1 teorema. *Hamingo kodai yra tobuli.*

[1] Syndrome – požymių visuma, sankaupa (graikiškai).

[1] Juos nepriklausomai vienas nuo kito sukūrė Marcel Golay (1949) ir Richard Hamming (1950).

Kodai $\mathbf{H}_2(r)$ yra geriausiai žinomi Hamingo kodai. Jų kontrolines matricas labai paprasta sudaryti. Surašykime pirmųjų 2^r-1 natūraliųjų skaičių skleidinių dvejetainėje sistemoje elementus į matricos stulpelius. Gautoji $r\times(2^r-1)$ matrica yra kontrolinė kodo $\mathbf{H}_2(r)$ matrica.

Pavyzdžiui, kontrolinė kodo $\mathbf{H}_2(3)$ matrica yra

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

Dvinarių Hamingo kodų dekodavimas taip pat labai paprastas. Imkime jau minėtu būdu sudarytą $\mathbf{H}_2(r)$ kodo kontrolinę matricą H. Jeigu siųstas kodo žodis $\mathbf{c}$ siuntimo metu buvo i-oje pozicijoje iškraipytas, tai gautasis žodis yra $\mathbf{x}=\mathbf{c}+\mathbf{e}_i$; čia $\mathbf{e}_i$ yra žodis, kurio visos komponentės, išskyrus i-ąją, lygios nuliui. Raskime $\mathbf{x}$ sindromą:

$$\mathbf{x}H^\perp=\mathbf{e}_iH^\perp.$$

Sindromas $\mathbf{e}_iH^\perp$ sudarytas iš tų pačių simbolių kaip ir matricos H i-asis stulpelis. Perskaitę $\mathbf{e}_iH^\perp$ kaip natūralųjį skaičių, užrašytą dvejetainėje sistemoje, gauname reikšmę i, t. y. neteisingai perduotos žodžio komponentės numerį. Tokiu būdu gavėjas gali atstatyti tą kodo žodį, kuris buvo siųstas. Tačiau norėdamas atkurti pradinį šaltinio žodį, gavėjas turi žinoti kokią generuojančią matricą koduodamas naudojo siuntėjas.

2.4. Naujų kodų sudarymo būdai

Iš jau sudarytų kodų galima konstruoti naujus. Visų pirma naują kodą galima sudaryti pasinaudojus seno kodo kontroline matrica.

2.4.1 apibrėžimas. *Tegu* $\mathbf{L}$ *yra tiesinis kodas su kontroline matrica* H*. Kodą, kuriam matrica* H *yra generuojanti, vadinsime kodu, dualiu* $\mathbf{L}$ *ir žymėsime* $\mathbf{L}^\top$*. Jei* $\mathbf{L}=\mathbf{L}^\top$*, kodą* $\mathbf{L}$ *vadinsime savidualiu.*

Štai dar vienas būdas sudaryti naują kodą iš jau sukonstruoto.

2.4.2 apibrėžimas. *Tegu* $\mathbf{L}$ *yra tiesinis kodas. Jo plėtiniu (extended code) vadinsime kodą*

$$\mathbf{L}^*=\{c_1c_2\dots c_nc_{n+1}:c_1c_2\dots c_n\in\mathbf{L},c_1+c_2+\dots+c_n+c_{n+1}=00...0.\}$$

Plėtinys yra taip pat tiesinis kodas. Jei $\mathbf{L}$ yra dvinaris kodas, o jo minimalus atstumas d yra nelyginis, tai plėtinio minimalus atstumas yra $d+1$.

Dar dvi operacijos: kodo sutrumpinimas (*puncturing*): visi kodo žodžiai sutrumpinami, nubraukiant tą pačią komponentę; kodo sumažinimas (*shortening*): surenkami tuo pačiu simboliu besibaigią kodo žodžiai ir naujas kodas sudaromas iš šių žodžių, nubraukiant paskutinį simbolį.

2.4.3 apibrėžimas. *Tegu* $\mathbf{L}_1,\mathbf{L}_2$ *yra du tiesiniai kodai iš tos pačios abėcėlės žodžių. Kodu* $\mathbf{L}_1|\mathbf{L}_2$ *vadinsime tiesinį kodą*

$$\mathbf{L}_1|\mathbf{L}_2=\{x|x+y:x\in\mathbf{L}_1,y\in\mathbf{L}_2\}.$$

Ši konstrukcija kodavimo teorijoje dar vadinama $u|u+v$ konstrukcija.

2.4.1 teorema. *Jei* $\mathbf{L}_1,\mathbf{L}_2$ *yra du tiesiniai kodai iš tos pačios abėcėlės žodžių,* d_1,d_2 *– jų minimalūs atstumai, tai kodo* $\mathbf{L}_1|\mathbf{L}_2$ *dimensija lygi kodų* $\mathbf{L}_1,\mathbf{L}_2$ *dimensijų sumai, o minimalus atstumas yra* $d=\min(2d_1,d_2)$.

2.4.4 apibrėžimas. *(Helgert, Stinaff, 1973) Tegu* $\mathbf{L}$ *yra dvinaris* $[n,k,d]$ *kodas, kurio generuojanti matrica yra*

$$G=\left(\begin{array}{cccc|ccc}1&1&\dots&1&0&\dots&0\\&&G_1&&&G_2&\end{array}\right),$$

čia pirmieji d *pirmosios eilutės elementai lygūs vienetui. Tiesinis kodas* $[n-d,k-1]$ *, kurio generuojanti matrica yra* G_2*, vadinamas liekanų kodu (residual code).*

Pastebėkime, kad kiekvieno kodo generuojančią matricą galima elementariais pertvarkiais suvesti į apibrėžime naudojamą formą.

• • • ◇ • • •

2.4.2 teorema. *Tegu* **L** *yra dvinaris* $[n, k, d]$ *tiesinis kodas. Tada jo liekanų kodo minimalus atstumas* d' *tenkina nelygybę* $d' \geq d/2$.

Tegu x yra **L'** žodis, tada x yra tam tikra matricos G_2 eilučių tiesinė kombinacija. Jei y yra analogiška matricos G_1 eilučių kombinacija, tai $y|x \in \mathbf{L}$. Tegu

$$y'|x = y|x + 11\ldots1|00...0 \in \mathbf{L}.$$

Taigi $y|x, y'|x \in \mathbf{L}$ ir

$$\begin{aligned} w(y|x) =& w(y) + w(x) \geq d, \\ w(y'|x) =& w(y') + w(x) \geq d. \end{aligned}$$

Tačiau arba $w(y) \geq d/2$ arba $w(y') \geq d/2$. Tada bet kokiam **L'** žodžiui x teisinga nelygybė $w(x) \geq d/2$, taigi minimaliam kodo atstumui $d' \geq d/2$.

2.4.3 teorema. *Tegu* **L** *yra dvinaris* $[n, k, d]$ *tiesinis kodas. Tada jo liekanų kodo minimalus atstumas* d' *tenkina nelygybę* $d' \geq d/2$.

Pakanka pastebėti, kad kiekvieną G_2 matricos eilučių tiesinę kombinaciją atitinka du kodo **L** žodžiai, iš kurių vienas turi $\leq d/2$ vienetų pirmosiose d pozicijose. Tada bet kurio liekanų kodo žodžio svoris nemažesnis už $d/2$.

2.5. Kodo žodžių svorių pasiskirstymas

Svarbu žinoti, kokie žodžiai sudaro kodą. Viena iš kodo žodžio x charakteristikų – jo svoris $w(x)$. Apibrėšime funkciją, kuri „saugo“ informaciją apie kodo žodžių svorius.

2.5.1 apibrėžimas. *Tegu* **C** *yra* n *ilgio abėcėlės* F_q *žodžių kodas,* $A_i = |\{c \in \mathbf{C} : w(c) = i\}|$. *Funkciją*

$$w_{\mathbf{C}}(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$$

vadinsime kodo **C** *svorių funkcija, o skaičių* A_i *seką – kodo svorių skirstiniu.*

Pastebėsime, kad svorių pasiskirstymo funkciją galima ir taip užrašyti:

$$w_{\mathbf{C}}(x, y) = \sum_{c \in \mathbf{C}} x^{n-w(c)} y^{w(c)}.$$

Dažnai naudojamas kitas svorių pasiskirstymo funkcijos variantas

$$w_{\mathbf{C}}(z) = w_{\mathbf{C}}(1, z) = \sum_{i=0}^{n} A_i z^i = \sum_{c \in \mathbf{C}} z^{w(c)}.$$

Kartais svorių pasiskirstymo funkciją galima palyginti nesunkiai surasti.

2.5.1 teorema. *Hamingo kodo* $\mathbf{H} = \mathbf{H}_2(r)$ *svorių pasiskirstymo funkcijos koeficientai tenkina rekurenčiąją lygybę*

$$iA_i = C_n^{i-1} - A_{i-1} - (n - i + 2)A_{i-2}, \quad (i \geq 2, n = 2^r - 1),$$

o svorių pasiskirstymo funkcija lygi

$$w_{\mathbf{H}}(z) = \frac{1}{n+1}(1+z)^n + \frac{n}{n+1}(1+z)^{(n-1)/2}(1-z)^{(n+1)/2}.$$

Įrodymas. Įrodysime rekurentinį sąryšį. Kiekvieną **H** žodį x su svoriu $w(x) = m$ atitinka kontrolinės matricos H m stulpelių tiesinė kombinacija, kuri lygi nuliniam stulpeliui. Ir atvirkščiai: jei sudėję m kontrolinės matricos stulpelių gauname nulinį stulpelį, tai šią sumą atitinka vienintelis kodo žodis su svoriu m. Parinkime $i - 1$ matricos H stulpelių, tai galima padaryti C_n^{i-1} būdų. Galimi trys atvejai:

1) stulpelių suma yra nulinis stulpelis;

2) stulpelių suma lygi vienam iš pasirinktų stulpelių;
2) stulpelių suma lygi vienam iš nepasirinktų stulpelių.

Skirtingų pasirinkimų, atitinkančių 1) yra A_{i-1}, atitinkančių 2) – $(n-i+2)A_{i-2}$ ir atitinkančių atvejį 3) – iA_i. Taigi

$$C_n^{i-1} = A_{i-1} + (n-i+2)A_{i-2} + iA_i.$$

Vienas pagrindinių rezultatų apie kodo svorių funkciją yra MacWilliams[2] tapatybė, kurią suformuluosime teoremoje.

2.5.2 teorema. *Tegu* $\mathbf{L}$ *yra tiesinis abėcėlės* F_q *žodžių kodas,* $\mathbf{L}^\top$ *dualus jo kodas. Tada abiejų kodų svorių pasiskirstymo funkcijas sieja tapatybė*

$$w_{\mathbf{L}^\top}(x,y) = \frac{1}{|\mathbf{L}|} w_{\mathbf{L}}(x+(q-1)y, x-y).$$

Įrodysime šią tapatybę dvinarės ($q=2$) abėcėlės atveju. Įrodymui prireiks kelių pagalbinių teiginių ir sąvokų.

Abėcėlės F_q tiesinio kodo $\mathbf{L}$ žodžiams x, y apibrėšime skaliarinę sandaugą. Tegu $x = x_1 \dots x_n, y = y_1 \dots y_n$, tada

$$(x,y) = x_1y_1 + x_2y_2 + \ldots + x_ny_n.$$

Toliau $\mathbf{L}$ žymi tiesinį abėcėlės F_2 žodžių kodą.

2.5.3 teorema. *Teisinga lygybė*

$$\sum_{u\in\mathbf{L}} (-1)^{(u,v)} = \begin{cases} |\mathbf{L}|, & \text{jei } v \in \mathbf{L}^\top, \\ 0, & \text{jei } v \notin \mathbf{L}^\top. \end{cases}$$

2.5.4 teorema. *Tegu* G *yra bet kokia komutatyvi grupė adityviai užrašomos operacijos atžvilgiu,* $f : \mathrm{F}_2^n \to G$,

$$\widehat{f}(u) = \sum_{v\in\mathrm{F}_2^n} (-1)^{(u,v)} f(v).$$

Tada bet kokiam tiesiniam kodui $\mathbf{L} \subset \mathrm{F}_2^n$ *teisinga lygybė*

$$\sum_{u\in\mathbf{L}^\top} f(u) = \frac{1}{|\mathbf{L}|} \sum_{u\in\mathbf{L}} \widehat{f}(u).$$

Įrodymas. Pakeisdami sumavimo tvarką ir pasiremdami anksčiau įrodytu teiginiu, gausime

$$\sum_{u\in\mathbf{L}} \widehat{f}(u) = \sum_{v\in\mathrm{F}_2^n} f(v) \sum_{u\in\mathbf{L}} (-1)^{(u,v)} =$$

$$\sum_{v\in\mathbf{L}^\top} f(v) \sum_{u\in\mathbf{L}} (-1)^{(u,v)} + \sum_{v\notin\mathbf{L}^\top} f(v) \sum_{u\in\mathbf{L}} (-1)^{(u,v)} = |\mathbf{L}| \sum_{v\in\mathbf{L}^\top} f(v).$$

Pastaba. Funkcija $\widehat{f}(u)$ vadinama funkcijos $f(u)$ Hadamardo transformacija.

2.5.2 teoremos įrodymas. Apibrėškime funkciją $f : \mathrm{F}_2^n \to R[x,y]$, čia $R[x,y]$ – dviejų kintamųjų daugianarių žiedas:

$$f(u) = x^{n-w(u)} y^{w(u)}$$

[2] F. J. MacWilliams, tai moteris.

ir pastebėkime, kad bet kokiam kodui $\mathbf{L}$

$$\sum_{u\in\mathbf{L}} f(u) = w_{\mathbf{L}}(x,y).$$

Pasinaudoję ką tik įrodytu teiginiu gausime

$$w_{\mathbf{L}^\top}(x,y) = \sum_{u\in\mathbf{L}^\top} f(u) = \frac{1}{|\mathbf{L}|}\sum_{u\in\mathbf{L}} \widehat{f}(u). \tag{2.5.1}$$

Skaičiuosime funkciją $\widehat{f}(u)$. Tegu $u = u_1u_2\dots u_n, v = v_1v_2\dots v_n$. Tada

$$\widehat{f}(u) = \sum_{v\in\mathrm{F}_2^n} (-1)^{(u,v)} x^{n-w(u)} y^{w(u)} = \sum_{v_1=0}^{1}\dots\sum_{v_n=0}^{1}\prod_{i=1}^{n}(-1)^{u_iv_i}x^{1-v_i}y^{v_i} =$$

$$\prod_{i=1}^{n}\Big(\sum_{w=0}^{1}(-1)^{u_iw}x^{1-w}y^w\Big).$$

Dabar pastebėkime, kad vidinė suma lygi:

$$\sum_{w=0}^{1}(-1)^{u_iw}x^{i-w}y^w = \begin{cases} x+y, & \text{jei } u_i=0,\\ x-y, & \text{jei } u_i=1.\end{cases}$$

Taigi

$$\widehat{f}(u) = (x+y)^{n-w(u)}(x-y)^{w(u)}.$$

Įstatydami šią reikšmę į (2.5.1), gausime MacWilliams tapatybę.

2.6. Maksimalaus atstumo tiesiniai kodai

1.3 skyriuje apibrėžėme maksimalaus kodo sąvoką; tokių kodų sudarymo arba bent jau jų parametrų nustatymo uždavinį vadinome pagrindine (teorine) kodavimo problema. Šiame skyrelyje tirsime atvejus, kai maksimalius kodus galima rasti tiesinių kodų klasėje.

Priminsime, jog $(n, A_q(n,d), d)$ žymėjome maksimalaus kodo parametrus; čia: n – kodo žodžių ilgis, d – minimalus atstumas, $A_q(n,d)$ – žodžių skaičius, o q – naudojamos abėcėlės simbolių skaičius. Singletono įvertis pateikia viršutinį $A_q(n,d)$ rėžį:

$$A_q(n,d) \le q^{n-d+1}. \tag{2.6.1}$$

Tegu dabar $\mathbf{L}$ yra tiesinis $[n,k]$ kodas iš abėcėlės $\mathbf{F}_q$ žodžių; tada jo žodžių skaičius lygus q^k. Pasirėmę (2.6.1), gausime

$$q^k \le q^{n-d+1}, \text{ arba } d \le n-k+1. \tag{2.6.2}$$

Jeigu iš tiesų galioja lygybės, tai kodas $\mathbf{L}$ yra, žinoma, maksimalus.

2.6.1 apibrėžimas. *Tiesinį $[n,k]$ kodą $\mathbf{L}$ vadinsime maksimalaus atstumo kodu*[3]*, jei jo minimaliam atstumui d galioja lygybė $d = n-k+1$.*

Sąvokos ,,maksimalus tiesinis kodas“ ir ,,maksimalaus atstumo tiesinis kodas“ nėra tapačios. Tad išties negalime tvirtinti, jog, tirdami maksimalaus atstumo kodus, nagrinėjame pagrindinę kodavimo problemą tiesinių kodų klasėje.

Pasiremdami kontrolinės matricos ir kodo minimalaus atstumo sąryšiu, gausime tokią maksimalaus atstumo kodų charakteristiką.

[3] Maximum distance separable, arba MDS, kodas angliškoje literatūroje.

2.6.1 teorema. *Tegu* $\mathbf{L}$ *yra tiesinis* $[n,k]$ *kodas, o* H *– jo kontrolinė matrica. Tada* $\mathbf{L}$ *yra maksimalaus atstumo kodas tuo ir tik tuo atveju, kai bet kurie* $n-k$ *matricos* H *stulpeliai yra tiesiškai nepriklausomi.*

Įrodymas. 2.2.3 teorema tvirtina, kad minimalus kodo $\mathbf{L}$ atstumas lygus d tada ir tik tada, kai egzistuoja d tiesiškai priklausomų kontrolinės matricos stulpelių, tačiau bet kurie $d-1$ jos stulpelių yra tiesiškai nepriklausomi. Kontrolinės matricos H matavimai yra $(n-k)\times n$. Bet kurie $n-k+1$ matricos stulpeliai sudaro tiesiškai priklausomą sistemą – juk matricos H rangas lygus $n-k$. Todėl sąlyga $d=n-k+1$ yra ekvivalenti reikalavimui, kad bet kurie $d-1=n-k$ stulpelių sudarytų tiesiškai nepriklausomą sistemą.

Teorema įrodyta.

Kaip netrukus įsitikinsime, maksimalaus atstumo kodai egzistuoja poromis.

Jei $\mathbf{L}$ yra tiesinis $[n,k]$ kodas su generuojančia matrica G ir kontroline matrica H, tai dualaus kodo generuojanti matrica yra H, o kontrolinė G.

Priminsime, kad kodai $\mathbf{L},\mathbf{L}^\perp$ nebūtinai skirtingi. Jeigu galioja lygybė $\mathbf{L}=\mathbf{L}^\perp$, tai kodas $\mathbf{L}$ vadinamas **savidualiu**. Suprantama, kad savidualūs kodai gali egzistuoti tik tada, kai n yra lyginis. Kad kodas būtų savidualus, jo generuojanti matrica turi būti kartu ir kontrolinė.

Pavyzdys. Dvinaris kodas su generuojančia matrica

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

yra savidualus, nes $GG^\perp=O_{1,6}$.

2.6.2 teorema. *Tegu* $\mathbf{L}$ *yra maksimalaus atstumo kodas. Tada ir* $\mathbf{L}^\perp$ *yra taip pat maksimalaus atstumo kodas.*

Įrodymas. Tegu G,H yra atitinkamai $[n,k]$ kodo $\mathbf{L}$ generuojanti bei kontrolinė matricos. Bet kurie skirtingi $n-k$ matricos H stulpeliai sudaro tiesiškai nepriklausomą sistemą. Tada bet kuris šios matricos $n-k$ eilės minoras nelygus nuliui. Iš matricos H eilučių elementų sudarykime žodžius $\mathbf{a}_1,\dots,\mathbf{a}_m, m=n-k$. Bet kuris kitas kodo $\mathbf{L}^\perp$ žodis $\mathbf{x}$ yra šių žodžių tiesinė kombinacija:

$$\mathbf{x}=\alpha_1\mathbf{a}_1+\ldots+\alpha_m\mathbf{a}_m,\quad \alpha_i\in\mathbf{F}_q. \tag{2.6.3}$$

Pagal (2.6.3) lygybę atlikime matricos H pertvarkius; dėl apibrėžtumo tarkime, $\alpha_1\neq 0$. Padauginkime pirmąją eilutę iš α_1, po to dauginkime i-ąją eilutę iš $\alpha_i, (i\geq 2)$ ir pridėkime prie pirmosios. Atlikę šiuos veiksmus, pirmojoje eilutėje gausime žodžio $\mathbf{x}$ iš (2.6.3) simbolius. Jokio H matricos $n-k$ minoro reikšmė netapo lygi nuliui, nes pakito tik daugikliu $\alpha_1\neq 0$. Taigi žodyje $\mathbf{x}$ negali būti $n-k$ komponenčių, lygių nuliui. Tai reiškia, jog kiekvieno žodžio $\mathbf{x}\in\mathbf{L}^\perp$ svoris $w(\mathbf{x})\geq n-(n-k-1)=k+1$. Todėl $d\geq k+1$, tačiau (2.6.2) nelygybė $\mathbf{L}^\perp$ kodui tvirtina, kad $d\leq k+1$. Taigi $d=k+1=n-(n-k)+1$, o tai reiškia, jog kodas $\mathbf{L}^\perp$ yra maksimalaus atstumo kodas.

Derindami abiejų teoremų tvirtinimus, nesunkiai gausime tokią išvadą.

Išvada. *Jei* $[n,k]$ *kodo* $\mathbf{L}$ *generuojanti matrica yra* G*, tai* $\mathbf{L}$ *yra maksimalaus atstumo kodas tada ir tik tada, kai bet kurie* k *matricos* G *stulpeliai yra tiesiškai nepriklausomi.*

Kai ką jau žinome apie maksimalaus atstumo kodus, tik nežinome, ar egzistuoja vien žinios apie juos, ar ir patys kodai? Tačiau nesunku įžvelgti, kad bet kokio kūno $\mathbf{F}_q$ atveju egzistuoja $[n,n,1],[n,1,n]$ ir $[n,n-1,2]$ kodai. Visi jie yra maksimalaus atstumo kodai, juos vadinsime tiesiog **trivialiais**. Ištirsime netrivialių maksimalaus atstumo kodų egzistavimo sąlygas.

2.6.3 teorema. *Maksimalaus atstumo* $[n,k]$ *kodų, tenkinančių sąlygą* $1<k\leq n-q$*, nėra.*

Įrodymas. Tarkime priešingai: yra maksimalaus atstumo $[n,k]$ kodas $\mathbf{L}$, tenkinantis nelygybę $1<k\leq n-q$.

Tegu $G=(I_k,A)$ yra šio kodo standartinio pavidalo generuojanti matrica. Atlikę šios matricos elementariuosius pertvarkius, gauname naujas matricas, kurias atitinka kodai, ekvivalentūs $\mathbf{L}$, taigi maksimalaus

atstumo kodai. Įrodysime, jog egzistuoja tam tikra elementariųjų pertvarkių seka, kurios rezultatas – matrica, atitinkanti nemaksimalaus atstumo kodą.

Kadangi $\mathbf{L}$ yra maksimalaus atstumo kodas, tai pagal 2.6.1 teoremą bet kurie k matricos G stulpeliai sudaro tiesiškai nepriklausomą sistemą. Iš šio fakto iškart išplaukia, jog nei vienas matricos A elementas nelygus nuliui. Išties, jei kuriame nors A stulpelyje būtų nulis, tai tas stulpelis galėtų būti išreikštas I_k matricos $k-1$ stulpelių tiesine kombinacija.

Padauginę matricos A stulpelius iš atitinkamų nenulinių $\mathbf{F}_q$ elementų, galime pasiekti, kad gautoji matrica būtų tokia:

$$G' = (I_k, A'), \quad A' = \begin{pmatrix} 1 & 1 & \dots & 1 \\ a'_{21} & a'_{22} & \dots & a'_{2,n-k} \\ \vdots & \vdots & \ddots & \vdots \\ a'_{k1} & a'_{k2} & \dots & a'_{k,n-k} \end{pmatrix}.$$

Visi matricos A' elementai taip pat nenuliniai. Imkime antrąją A' eilutę. Kadangi joje yra $n-k \geq q$ elementų, tai bent du iš jų bus vienodi, tarkime, lygūs α. Padauginę antrąją matricos G' eilutę iš α^{-1} ir pridėję prie pirmosios, gausime eilutę, kurioje yra ne mažiau kaip k nulių. Bet tai reiškia, jog atitinkamo kodo $\mathbf{L}'$ žodžio svoris ne didesnis už $n-k$. Tačiau toks kodas nėra maksimalaus atstumo kodas.

Pasinaudoję tuo, kad maksimalaus atstumo kodo dualus kodas irgi yra maksimalaus atstumo kodas gausime tokį tvirtinimą.

2.6.4 teorema. *Jei* $\mathbf{L}$ *yra netrivialus maksimalaus atstumo* $[n,k]$ *kodas, tai*

$$n-q+1 \leq k \leq q-1.$$

Iš šio teiginio gauname, jog dvinaris kodas ($q=2$) yra maksimalaus atstumo kodas tada ir tik tada, kai jis trivialus. Tačiau kitoms q reikšmėms netrivialūs maksimalaus atstumo kodai egzistuoja.

Tegu $\alpha_1, \dots, \alpha_s$ yra skirtingi ir nelygūs nuliui kūno $\mathbf{F}_q$ elementai. Sudarykime gerai tiesinėje algebroje žinomą Vandermondo (A.T. Vandermonde) determinantą:

$$V(\alpha_1, \alpha_2, \dots, \alpha_s) = \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_s \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_s^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{s-1} & \alpha_2^{s-1} & \dots & \alpha_s^{s-1} \end{pmatrix},$$

$$V(\alpha_1, \alpha_2, \dots, \alpha_s) = \prod_{1 \leq i < j \leq s} (\alpha_j - \alpha_i).$$

Imkime dabar visus nenulinius $\mathbf{F}_q$ elementus, fiksuokime $k, 1 \leq k \leq q$, ir sudarykime $(q-k+1) \times (q+1)$ matricą H:

$$H = \begin{pmatrix} 1 & 1 & \dots & 1 & 1 & 0 \\ \alpha_1 & \alpha_2 & \dots & \alpha_{q-1} & 0 & 0 \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_{q-1}^2 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \alpha_1^{q-k} & \alpha_2^{q-k} & \dots & \alpha_{q-1}^{q-k} & 0 & 1 \end{pmatrix}.$$

Remdamiesi Vandermondo determinanto išraiška, nesunkiai įsitikinsime, jog bet kurie $q-k+1$ matricos H stulpeliai yra tiesiškai nepriklausomi. Tai reiškia (žr. 2.6.1 teoremą), jog H yra kontrolinė maksimalaus atstumo $[q+1,k]$ kodo matrica. Jei $k=1$ arba $k=q$, šis kodas yra trivialus, tačiau kitais atvejais – ne. Pasirėmę 2.6.2 teorema, taip pat galime teigti, kad H yra maksimalaus atstumo $[q+1, q-k+1]$ kodo generuojanti matrica.

• • • ◇ • • •

2.7. Golay kodai

Sukonstruosime tiesinį dvinarį $[24, 12, 8]$ kodą, kurį žymėsime $\mathbf{G}_{24}$. Jis unikalus štai kokia prasme.

2.7.1 teorema. *Bet kuris dvinaris* $(24, 2^{12}, 8)$ *kodas ekvivalentus tiesiniam* $[24, 12, 8]$ *kodui* $\mathbf{G}_{24}$.

Be to, sutrumpinant $\mathbf{G}_{24}$ kodą vienu simboliu gaunamas tiesinis $[23, 12, 7]$ kodas, kuris yra tobulas.

Yra keletas $\mathbf{G}_{24}$ sudarymo būdų. Panagrinėkime, kaip $\mathbf{G}_{24}$ gali būti gaunamas iš Hammingo kodo $\mathbf{H} = \mathbf{H}_2(3)$. Aprašysime tik pačią konstrukciją, neįrodinėdami, kad sudarytas kodas yra $[24, 12, 8]$ kodas.

Tegu $\mathbf{H}^*$ yra kodas, kurį gauname iš $\mathbf{H}$ užrašydami jo žodžius iš dešinės į kairę, tegu $\overline{\mathbf{H}}, \overline{\mathbf{H}^*}$ yra kodų $\mathbf{H}$, $\mathbf{H}^*$ plėtiniai. Sudarykime žodžių aibę

$$\mathrm{a|0|a}, \quad \mathrm{0|b|b}, \quad \mathrm{x|x|x}, \tag{2.6.1}$$

čia 0 yra žodis sudarytas iš 8 nulių, a,b „perbėga“ kodo $\overline{\mathbf{H}}$, o x – kodo $\overline{\mathbf{H}^*}$ bazės žodžius. Galima parodyti, kad (2.6.1) sistemos žodžiai yra tiesiškai nepriklausomi. Jų tiesinės kombinacijos sudaro poerdvį, kuris ir yra Golay kodas $\mathbf{G}_{24}$.

Galima $\mathbf{G}_{24}$ kodą apibrėžti tiesiog užrašant jo generuojančią matricą.

2.7.1 apibrėžimas. *Tiesinį dvinarį* $[24, 12]$ *kodą, kurio generuojanti matrica yra* $G = (I_{12}, A)$,

$$A = \begin{pmatrix} \diamond & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & * & 1 & 1 & 1 & \diamond & \diamond & \diamond & 1 & \diamond \\ 1 & 1 & \diamond & 1 & 1 & 1 & \diamond & \diamond & \diamond & 1 & \diamond & 1 \\ 1 & \diamond & 1 & 1 & 1 & \diamond & \diamond & \diamond & 1 & \diamond & 1 & 1 \\ 1 & 1 & 1 & 1 & \diamond & \diamond & \diamond & 1 & \diamond & 1 & 1 & \diamond \\ 1 & 1 & 1 & \diamond & \diamond & \diamond & 1 & \diamond & 1 & 1 & \diamond & 1 \\ 1 & 1 & \diamond & \diamond & \diamond & 1 & \diamond & 1 & 1 & \diamond & 1 & 1 \\ 1 & \diamond & \diamond & \diamond & 1 & \diamond & 1 & 1 & \diamond & 1 & 1 & 1 \\ 1 & \diamond & \diamond & 1 & \diamond & 1 & 1 & \diamond & 1 & 1 & 1 & \diamond \\ 1 & \diamond & 1 & \diamond & 1 & 1 & \diamond & 1 & 1 & 1 & \diamond & \diamond \\ 1 & 1 & \diamond & 1 & 1 & \diamond & 1 & 1 & 1 & \diamond & \diamond & \diamond \\ 1 & \diamond & 1 & 1 & \diamond & 1 & 1 & 1 & \diamond & \diamond & \diamond & 1 \end{pmatrix}, \quad \diamond = 0,$$

vadinsime Golay kodu $\mathbf{G}_{24}$.

$\mathbf{G}_{24}$ kodo savybes lengviausia įrodinėti remiantis specialia generuojančios matricos struktūra.

Išbraukime matricoje A j-ąjį stulpelį ir pažymėkime gautąją matricą A_j. Sudarykime matricą $G_j = (I_{12}, A_j)$. Tegu $\mathbf{L}_j$ yra tiesinis $[23, 12]$ kodas, kurio generuojanti matrica yra G_j. Iš tikrųjų visi šie kodai yra ekvivalentūs.

2.7.2 apibrėžimas. *Tiesinį dvinarį* $[23, 12]$ *kodą, kurio generuojanti matrica yra* $G = (I_{12}, A_1)$, *vadinsime Golay kodu* $\mathbf{G}_{23}$.

2.7.3 apibrėžimas. *Tiesinį trinarį* $[12, 6]$ *kodą, kurio generuojanti matrica yra* $G = (I_6, B)$,

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

vadinsime Golay kodu $\mathbf{G}_{12}$.

Tokiu pat būdu, kaip ir dvinarių kodų atveju, iš Golay kodo $\mathbf{G}_{12}$ gauname Golay kodą $\mathbf{G}_{11}$, kuris yra tiesinis $[11, 6]$ kodas.

Taigi turime visą Golėjaus kodų ketvertą. Panagrinėsime kodo $\mathbf{G}_{24}$ savybes.

• • • ◇ • • •

2.7.2 teorema. *Teisingi tokie tvirtinimai:*

1) kodas $\mathbf{G}_{24}$ *yra savidualus;*

2) matrica $G' = (A, I_{12})$ *irgi yra kodo* $\mathbf{G}_{24}$ *generuojanti matrica;*

3) kodo $\mathbf{G}_{24}$ *žodžių svoriai dalijasi iš 4;*

4) nėra $\mathbf{G}_{24}$ *žodžio, kurio svoris lygus 4.*

Įrodymas. 1. Du aibės $\mathbf{F}_q^n$ žodžius **x,y** vadinsime ortogonaliais, jeigu užrašę juos kaip matricos eilutes turėsime $\mathbf{x} \cdot \mathbf{y}^\perp = 0$. Tiesinio kodo generuojančios matricos ir kontrolinės matricos eilutės yra ortogonalios. Tada bet kokio tiesinio kodo $\mathbf{L}$ ir jam dualaus kodo $\mathbf{L}^\perp$ žodžiai irgi ortogonalūs. Kodą $\mathbf{L}^\perp$ galima apibrėžti kaip žodžių, ortogonalių kodo $\mathbf{L}$ žodžiams, aibę.

Nesunku patikrinti, jog visos matricos G eilutės yra tarpusavyje ir pačios sau ortogonalios: jei $\mathbf{e}_i$ yra i-oji eilutė, $\mathbf{e}_i^\perp$ – iš tų pačių elementų sudarytas stulpelis, tai $\mathbf{e}_i\mathbf{e}_j^\perp = 0$ visoms poroms i, j. Iš to išplaukia, kad $\mathbf{G}_{24} \subset \mathbf{G}_{24}^\perp$. Tačiau iš tiesų privalo galioti lygybė, nes abiejų kodų dimensijos yra vienodos.

2. Matrica $H = (-A^\perp, I_{12})$ generuoja kodą, kuris yra dualus $\mathbf{G}_{24}$, taigi, atsižvelgus į 1), tą patį kodą $\mathbf{G}_{24}$. Tačiau $A^\perp = A = -A$, todėl $H = G'$. Teiginys įrodytas.

3. Tegu $\mathbf{r}$ yra kodo $\mathbf{G}_{24}$ žodis, sudarytas iš matricos G r-osios eilutės elementų. Nesunku patikrinti, kad bet kokiam r atitinkamo žodžio svoris $w(\mathbf{r})$ dalijasi iš 4. Tegu **r,s** yra du kodo žodžiai. Žodį, kuris gaunamas iš **r,s** , sudauginus atitinkamas jų komponentes, žymėsime $\mathbf{r} \cdot \mathbf{s}$, o sudėjus – $\mathbf{r} + \mathbf{s}$. Nesunku įsitikinti, jog svoriams galioja tokia lygybė:

$$w(\mathbf{r} + \mathbf{s}) = w(\mathbf{r}) + w(\mathbf{s}) - 2w(\mathbf{r} \cdot \mathbf{s}).$$

Vėlgi tiesiogiai tikrinant, galima nustatyti, jog, parinkus bet kurią eilučių porą, žodžio $\mathbf{r} \cdot \mathbf{s}$ svoris dalijasi iš 2. Bet tada $w(\mathbf{r} + \mathbf{s})$ dalijasi iš 4. Teiginys įrodytas.

4. Tarkime, kad egzistuoja kodo $\mathbf{G}_{24}$ žodis $\mathbf{x}$, kad $w(\mathbf{x}) = 4$. Kadangi abi matricos G, G' generuoja tą patį kodą $\mathbf{G}_{24}$, tai $\mathbf{x}$ galime nagrinėti kaip matricos G arba G' eilučių tiesinę kombinaciją. Pažymėję **l,r** atitinkamai kairiąją ir dešiniąją žodžio $\mathbf{x}$ puses (sudarytas iš 12 simbolių), gausime $w(\mathbf{x}) = w(\mathbf{l}) + w(\mathbf{r})$. Pastebėsime, jog atvejis $w(\mathbf{l}) = 0$ arba $w(\mathbf{r}) = 0$ yra negalimas. Jei $w(\mathbf{l}) = 1$, tai $w(\mathbf{r}) = 3$; $\mathbf{x}$ turi būti viena iš matricos G eilučių, bet eilutės su dešinės pusės svoriu, lygiu 3, nėra. Analogiškai gauname, jog atvejis $w(\mathbf{l}) = 3$, $w(\mathbf{r}) = 1$ taip pat neįmanomas. Lieka atvejis $w(\mathbf{l}) = w(\mathbf{r}) = 2$. Bet tokiu atveju $\mathbf{x}$ yra dviejų skirtingų matricos G eilučių suma. Tiesiogiai tikrinant, galime nustatyti, jog $w(\mathbf{u} + \mathbf{v}) \neq 4$ jokioms dviem skirtingoms G eilutėms **u,v**. Teiginys įrodytas.

Pastebėję, kad kodo $\mathbf{G}_{24}$ žodžiai $\mathbf{x}$ su svoriu $w(\mathbf{x}) = 8$ egzistuoja (pavyzdžiui, antroji matricos G eilutė), ir prisiminę, jog minimalus tiesinio kodo atstumas lygus mažiausiajam iš kodo žodžių svorių, gauname tokį teiginį.

2.7.3 teorema. $\mathbf{G}_{24}$ *yra* $[24, 12, 8]$ *kodas.*

Paminėsime, jog Golėjaus kodų $\mathbf{G}_{23}, \mathbf{G}_{12}, \mathbf{G}_{11}$ minimalūs atstumai lygūs atitinkamai 7, 6, 5. Šie kodai kaip ir $\mathbf{G}_{24}$ irgi turi 2.6.1 teoremoje minimą vienaties savybę.

Dabar aptarsime kodo $\mathbf{G}_{24}$ dekodavimo būdą. Kadangi minimalus kodo atstumas lygus 8, tai dekoduojant galima ištaisyti ne daugiau kaip 3 klaidas. Naudojant sindromus, reikėtų sudaryti lentelę iš $2^{24}/2^{12} = 4096$ sindromų bei juos atitinkančių lyderių.

Laimei, specialios matricų G, G' savybės leidžia dekodavimo procedūrą žymiai suprastinti. Jeigu siunčiant kodo žodį $\mathbf{c}$ įvyko iškraipymas $\mathbf{e}$[3] , tai gautasis žodis yra $\mathbf{x} = \mathbf{c} + \mathbf{e}$. Nurodysime metodą, kuris leidžia teisingai nustatyti nežinomą $\mathbf{e}$, kai $w(\mathbf{e}) \leq 3$. Radę $\mathbf{e}$, gautą žodį $\mathbf{x}$ dekoduosime žodžiu $\mathbf{x} - \mathbf{e}$. Žinoma, taikydami dekodavimo taisyklę iš anksto nežinome, ar $w(\mathbf{e}) \leq 3$. Jeigu metodas „neveikia“, tai ši sąlyga nėra patenkinta, o dekoduoti teisingai tokiu atveju iš pat pradžių nepažadėjome!

Kairiąją iškraipymo $\mathbf{e}$ dalį, sudarytą iš 12 pirmųjų simbolių, pažymėję $\mathbf{e}_1$, o dešiniąją – $\mathbf{e}_2$, gauname

$$\mathbf{e} = \mathbf{e}_1\mathbf{e}_2, \quad w(\mathbf{e}) = w(\mathbf{e}_1) + w(\mathbf{e}_2) \leq 3.$$

[3] Žodį $\mathbf{e}$ sudaro nuliai tose pozicijose, kurios perduotos teisingai, ir vienetai ten, kur įvyko perdavimo klaidos.

Galimi atvejai:

1) $w(\mathbf{e}_1) = 0$;
2) $w(\mathbf{e}_2) = 0$;
3) $w(\mathbf{e}_1) > 0,\ w(\mathbf{e}_2) > 0$.

Iš pradžių ištirsime, kaip pagal gautą žodį nustatyti, kuris iš 1), 2), 3) atvejų įvyko. Kadangi abi generuojančios matricos $G = (I_{12}, A), G' = (A, I_{12})$ yra kartu ir kontrolinės, tai galime nagrinėti du gauto žodžio $\mathbf{x}$ sindromus:

$$\mathbf{s}_1 = (\mathbf{x} + \mathbf{e})G^{\perp} = \mathbf{e}G^{\perp} = \mathbf{e}_1\mathbf{e}_2\begin{pmatrix} I_{12} \\ A \end{pmatrix} = \mathbf{e}_1 + \mathbf{e}_2 A, \tag{5.6.1}$$

$$\mathbf{s}_2 = (\mathbf{x} + \mathbf{e})G'^{\perp} = \mathbf{e}G'^{\perp} = \mathbf{e}_1\mathbf{e}_2\begin{pmatrix} A \\ I_{12} \end{pmatrix} = \mathbf{e}_1 A + \mathbf{e}_2. \tag{5.6.2}$$

Jeigu $w(\mathbf{e}_1) = 0$, iš (5.6.2) gauname $w(\mathbf{e}) = w(\mathbf{e}_2) = w(\mathbf{s}_2) \leq 3$. Jeigu $w(\mathbf{e}_2) = 0$, tai analogiškai iš (5.6.1) gauname $w(\mathbf{e}) = w(\mathbf{e}_1) = w(\mathbf{s}_1) \leq 3$. Jei $w(\mathbf{e}_1) > 0,\ w(\mathbf{e}_2) > 0$, tai $w(\mathbf{s}_1) > 5,\ w(\mathbf{s}_2) > 5$ (speciali matricos A struktūra!).

Taigi pagal sindromų svorius $w(\mathbf{s}_1), w(\mathbf{s}_2)$ galima nustatyti, kuris iš 1), 2), 3) atvejų įvyko.

Jei $w(\mathbf{s}_1) \leq 3$, tai $w(\mathbf{e}_2) = 0$, ir $\mathbf{e} = \mathbf{e}_1\mathbf{o} = \mathbf{s}_1\mathbf{o}$; čia $\mathbf{o}$ yra žodis, sudarytas iš 12 nulių. Analogiškai, jei $w(\mathbf{s}_2) \leq 3$, tai $\mathbf{e} = \mathbf{o}\mathbf{s}_2$.

Tad 1), 2) atvejais dekodavimas nesukelia didelių sunkumų. Lieka ištirti dekodavimą tuo atveju, kai $w(\mathbf{s}_1) > 5,\ w(\mathbf{s}_2) > 5$, t. y. 3) atveju. Jį suskaidysime į dvi galimybes:

a) $w(\mathbf{e}_1) = 1,\ w(\mathbf{e}_2) = 1$ arba 2;
b) $w(\mathbf{e}_1) = 2,\ w(\mathbf{e}_2) = 1$.

Pastebėsime, jog a) atveju pakanka rasti $\mathbf{e}_1$. Išties, suradę šį vektorių, galime manyti, jog gautasis žodis yra $\mathbf{x}' = \mathbf{x} - \mathbf{e}_1\mathbf{o}$ ir dekoduoti jau aptartu būdu. Analogiška pastaba teisinga ir b) atvejui.

Pakaks išnagrinėti a) atvejį. Tegu iškraipymas įvyko j-ojoje pozicijoje, $1 \leq j \leq 12$. Tada $\mathbf{e}_1 = \varepsilon_j$; čia ε_j žymime žodį iš 12 simbolių, kurių tik j-asis yra vienetas, kiti – nuliai. Sudarykime 12 naujų žodžių

$$\mathbf{x} + \varepsilon_1\mathbf{o}, \ldots, \mathbf{x} + \varepsilon_{12}\mathbf{o}$$

ir 12 juos atitinkančių sindromų

$$\mathbf{s}_i = (\mathbf{x} + \varepsilon_i\mathbf{o})\begin{pmatrix} A \\ I_{12} \end{pmatrix} = (\mathbf{e} + \varepsilon_i\mathbf{o})\begin{pmatrix} A \\ I_{12} \end{pmatrix} =$$

$$= (\varepsilon_j\mathbf{e}_2 + \varepsilon_i\mathbf{o})\begin{pmatrix} A \\ I_{12} \end{pmatrix} = \varepsilon_j A + \mathbf{e}_2 + \varepsilon_i A.$$

Jeigu $i \neq j$, tai

$$w(\mathbf{s}_i) \geq w(\varepsilon_j A + \varepsilon_i A) - w(\mathbf{e}_2) \geq$$

$$\geq w(\varepsilon_j A) + w(\varepsilon_i A) - 2w(\varepsilon_j A \cdot \varepsilon_i A) - w(\mathbf{e}_2) \geq 7 + 7 - 2 \cdot 4 - 2 = 4.$$

Jeigu $i = j$, tai $\varepsilon_j A + \varepsilon_i A = 0$ ir $w(\mathbf{s}_i) = w(\mathbf{e}_2) \leq 2$.

Taigi peržiūrėję sindromų svorius, pamatysime, kad visi jie, išskyrus vieną, yra ne mažesni už 4. Imdami tą j, kuriam $w(\mathbf{s}_j) \leq 2$, rasime $\mathbf{e}_1 = \varepsilon_j$. Jeigu svorių seka kitokia, tai susidūrėme su b) atveju. Tenka ieškoti $\mathbf{e}_2 = \varepsilon_j$. Dabar teks peržiūrėti sindromus

$$\mathbf{s}'_i = (\mathbf{x} + \mathbf{o}\varepsilon_i)\begin{pmatrix} I_{12} \\ A \end{pmatrix}.$$

Radę j, kuriam $w(\mathbf{s}'_j) \leq 2$, gausime $\mathbf{e}_2 = \varepsilon_j$. Jeigu vėl nepavyks (bet ne todėl, kad klaidingai skaičiavome!), teks konstatuoti, kad žodis yra pernelyg iškraipytas, kad galėtume jį atkurti.

• • • ◇ • • •

2.8. Reedo-Mullerio kodai

Rydo–Mulerio kodus (I. S. Reed, D. E. Muller) galima apibrėžti įvairiai. Mūsų tekste pasirinktas algebrinis-geometrinis požiūris.

Tarkime, tiesinės erdvės $\mathbf{F}_2^m$ žodžiai kokiu nors būdu sunumeruoti:

$$\mathbf{F}_2^m = \{\mathbf{a}_1, \ldots, \mathbf{a}_n\}, \quad n = 2^m.$$

Galime, pavyzdžiui, žvelgti į žodį $\mathbf{a} \in \mathbf{F}_2^m$ kaip į sveikojo skaičiaus $0 \le l < 2^m$ išraišką dvejetainėje sistemoje ir sutvarkyti žodžius atitinkamų skaičių didėjimo tvarka.

Žymėkime $x_i(\mathbf{a})$ i-ąją žodžio $\mathbf{a}$ komponentę. Tada aibės

$$H_i = \{\mathbf{a} : \mathbf{a} \in \mathbf{F}_2^m, x_i(\mathbf{a}) = 0\}, \quad i = 1, \ldots, m,$$

yra tiesinės erdvės $\mathbf{F}_2^m$ poerdviai.

Apibrėšime abipusiškai vienareikšmę $\mathbf{F}_2^m$ poaibių ir erdvės $\mathbf{F}_2^n$, $n = 2^m$, žodžių atitiktį. Jei $D \subset \mathbf{F}_2^m$, tai priskirsime: $D \to \mathbf{v}(D)$; čia žodžio $\mathbf{v}(D) \in \mathbf{F}_2^n$ komponentės apibrėžiamos taip:

$$x_i(\mathbf{v}(D)) = \begin{cases} 0, & \text{jei } \mathbf{a}_i \notin D, \\ 1, & \text{jei } \mathbf{a}_i \in D. \end{cases}$$

Taigi žodyje $\mathbf{v}(D)$ vienetukai žymi, kurie žodžiai įeina į D; $\mathbf{v}(D)$ yra tarsi poaibio D „inventorizacijos“ dokumentas. Visą erdvę $\mathbf{F}_2^m$ atitinka žodis $\mathbf{v}_0 = 11\ldots1$. Pastebėsime, jog galioja tokia lygybė:

$$\mathbf{v}(D) \cdot \mathbf{v}(E) = \mathbf{v}(D \cap E). \tag{2.8.1}$$

Priminsime, jog žodį, kurį gauname iš $\mathbf{a}, \mathbf{b} \in \mathbf{F}_2^n$ sudauginę atitinkamas komponentes, žymime $\mathbf{a} \cdot \mathbf{b}$.

2.8.1 apibrėžimas. *Tegu $m \ge 1,\ r \le n,\ n = 2^m$. Rydo–Mulerio $\mathbf{RM}(m, r)$ kodu vadinsime tiesinį $\mathbf{F}_2^n$ poerdvį, kurį generuoja žodžiai*

$$\mathbf{v}_0,\ \mathbf{v}_{i_1} \cdot \ldots \cdot \mathbf{v}_{i_s}; \tag{2.8.2}$$

čia $\mathbf{v}_0 = 11\ldots1,\ \mathbf{v}_i = \mathbf{v}(H_i),\ 1 \le i_1 < \ldots < i_s \le m,\ s \le r\ i = 1, \ldots, m$.

Vektorių, kurie užrašyti (2.8.2), skaičius lygus

$$k(m, r) = 1 + \binom{m}{1} + \binom{m}{2} + \ldots + \binom{m}{r}.$$

Kaip netrukus pamatysime, visi šie vektoriai yra tiesiškai nepriklausomi. Taigi $\mathbf{RM}(m, r)$ kodo generuojančią matricą gausime, išrašę šių vektorių elementus į matricos eilutes. Iš pradžių pastebėkime tokią žodžių $\mathbf{v}_i$ savybę. Imkime poerdvių H_i pildinius

$$H_i^c = \{\mathbf{a} : \mathbf{a} \in \mathbf{F}_2^m, x_i(\mathbf{a}) = 1\}, \quad i = 1, \ldots, m.$$

Nesunku pastebėti, jog

$$\mathbf{v}(H_i^c) = \mathbf{v}_0 + \mathbf{v}_i. \tag{2.8.3}$$

2.8.1 teorema. *$\mathbf{RM}(m, r)$ kodo dimensija lygi $k(m, r)$, o (2.8.2) vektoriai sudaro jo bazę.*

Įrodymas. Imkime (2.8.2) vektorių sistemoje $r = m$. Tada gausime lygiai $n = 2^m$ vektorių; tokia yra ir visos erdvės $\mathbf{F}_2^n$ dimensija. Jeigu parodysime, jog kiekvieną $\mathbf{F}_2^n$ vektorių galima išreikšti šiais n vektorių, tai galėsime teigti, kad jie sudaro tiesiškai nepriklausomą sistemą. Tada bet kokiam r (2.8.2) vektoriai irgi bus tiesiškai nepriklausomi, nes sudarys tiesiškai nepriklausomos sistemos posistemę.

Pakanka parodyti, kad kiekvieną $\mathbf{F}_2^n$ standartinės bazės vektorių galima išreikšti (2.8.2) vektorių tiesine kombinacija. Pavyzdžiui, imkime standartinės bazės vektorių $\mathbf{e}_i$, kuris sudarytas iš nulių visose pozicijose,

išskyrus i-ąją, lygią vienetui. Prisiminę erdvės $\mathbf{F}_2^m$ poaibių ir $\mathbf{F}_2^n$ žodžių atitiktį, galime rašyti: $\mathbf{e}_i = \mathbf{v}(D)$; čia $D = \{\mathbf{a}_i\}$. Tegu $\mathbf{a}_i = a_1 \dots a_m$. Žymėdami $H_i(0) = H_i$ ir $H_i(1) = H_i^c$, gausime

$$D = \{\mathbf{a}_i\} = H_1(a_1) \cap \dots \cap H_m(a_m).$$

Pasirėmę (2.8.1), gausime

$$\mathbf{e}_i = \mathbf{v}(D) = \mathbf{v}(H_1(a_1)) \cdot \dots \cdot \mathbf{v}(H_m(a_m)).$$

Tačiau $\mathbf{v}(H_i(a_i))$ lygūs arba $\mathbf{v}_i$, arba $\mathbf{v}_0 + \mathbf{v}_i$. Todėl $\mathbf{e}_i$ yra (2.8.2) sistemos vektorių tiesinė kombinacija.

Pavyzdys. Užrašysime $\mathbf{RM}(3,2)$ kodo bazę, o kartu ir kodo generuojančią matricą. Iš pradžių išrašykime erdvės $\mathbf{F}_2^3$ žodžius, o pagal juos konstruokime ir bazės vektorius.

	$\mathbf{a}_1$	$\mathbf{a}_2$	$\mathbf{a}_3$	$\mathbf{a}_4$	$\mathbf{a}_5$	$\mathbf{a}_6$	$\mathbf{a}_7$	$\mathbf{a}_8$
	000	001	010	011	100	101	110	111
$\mathbf{v}_0$	1	1	1	1	1	1	1	1
$\mathbf{v}_1$	1	1	1	1	0	0	0	0
$\mathbf{v}_2$	1	1	0	0	1	1	0	0
$\mathbf{v}_3$	1	0	1	0	1	0	1	0
$\mathbf{v}_1 \cdot \mathbf{v}_2$	1	1	0	0	0	0	0	0
$\mathbf{v}_1 \cdot \mathbf{v}_3$	1	0	1	0	0	0	0	0
$\mathbf{v}_2 \cdot \mathbf{v}_3$	1	0	0	0	0	0	0	0

Fiksuotam m gavome ištisą Rydo–Mulerio kodų koloniją, kurios nariai yra $\mathbf{RM}(m,r)$, $r = 0, \dots, m$. Akivaizdu, kad $\mathbf{RM}(m,0) = \{00\dots0, 11\dots1\}$, $\mathbf{RM}(m,m) = \mathbf{F}_2^n$. Nustatysime, kokie struktūriniai ryšiai sieja skirtingų m reikšmių Rydo–Mulerio kodus. Jie gali būti gaunami vienas po kito, naudojantis $u|u+v$ konstrukcija (žr. 2.4 skyrelį).

2.8.2 teorema. *Jeigu* $0 < r < m$, *tai*

$$\mathbf{RM}(m,r) = \mathbf{RM}(m-1,r)|\mathbf{RM}(m-1,r-1).$$

Įrodymas. Kadangi

$$\mathbf{RM}(m-1,r-1) \subset \mathbf{RM}(m-1,r),$$

tai kodas $\mathbf{R} = \mathbf{RM}(m-1,r)|\mathbf{RM}(m-1,r-1)$ apibrėžtas korektiškai.

Prisiminsime, jog kodo $\mathbf{RM}(m,r)$ dimensija lygi

$$k(m,r) = 1 + \binom{m}{1} + \binom{m}{2} + \dots + \binom{m}{r}.$$

Iš 2.8.2 teoremos išplaukia, kad kodo $\mathbf{R}$ dimensija lygi

$$k(m-1,r) + k(m-1,r-1) = k(m,r).$$

Taigi teorema bus teisinga, jeigu parodysime, jog bet kurį kodo $\mathbf{RM}(m,r)$ bazės vektorių $\mathbf{v}$ galima išreikšti tokiu būdu:

$$\mathbf{v} = \mathbf{x}|\mathbf{x}+\mathbf{y}, \quad \mathbf{x} \in \mathbf{RM}(m-1,r), \quad \mathbf{y} \in \mathbf{RM}(m-1,r-1). \tag{2.8.4}$$

Šiuos sąryšius įrodinėsime stipriai pasiremdami specialia $\mathbf{RM}(k,l)$ kodų bazių konstrukcija.

Interpretuodami $\mathbf{F}_2^k$ elementus kaip sveikųjų skaičių dvejetaines išraiškas, sunumeruosime $\mathbf{F}_2^k$ elementus šių skaičių didėjimo tvarka. Taigi

$$\mathbf{F}_2^{m-1} = \{\mathbf{a}_1, \dots, \mathbf{a}_n\}, \quad n = 2^{m-1};$$

$$\mathbf{F}_2^m = \{0\mathbf{a}_1, \dots, 0\mathbf{a}_n, 1\mathbf{a}_1, \dots, 1\mathbf{a}_n\} = \{\mathbf{b}_1, \dots, \mathbf{b}_{2n}\},$$

• • • ◇ • • •

čia $\mathbf{a}_1 = 00\ldots0, \mathbf{a}_2 = 00\ldots1, \ldots, \mathbf{a}_n = 11\ldots1$.

Erdvės $\mathbf{F}_2^{m-1}$ poerdvius $H_i' = \{\mathbf{a} : \mathbf{a} \in \mathbf{F}_2^{m-1}, x_i(\mathbf{a}) = 0\}$ atitinkančius $\mathbf{RM}(m-1,r)$ vektorius $\mathbf{v}(H_i')$ žymėsime $\mathbf{v}_i'$, $1 \le i \le\le m-1$ (žr. 2.8.1 apibrėžimą). Analogiškai $\mathbf{RM}(m,r)$ kodo vektorius $\mathbf{v}(H_i)$, $H_i = \{\mathbf{b} : \mathbf{b} \in \mathbf{F}_2^m, x_i(\mathbf{b}) = 0\}$, žymėsime $\mathbf{v}_i$, $i = 1,\ldots,m$. Be to, žymėsime $\mathbf{v}_0' = 11\ldots1, \mathbf{v}_0' \in \mathbf{RM}(m-1,r)$ ir $\mathbf{v}_0 = \mathbf{v}_0'|\mathbf{v}_0'$,
$\mathbf{v}_0 \in \mathbf{RM}(m,r)$.

Įsitikinkime, kad teisingi šie sąryšiai:

$$\mathbf{v}_0 = \mathbf{v}_0'|\mathbf{v}_0', \quad \mathbf{v}_1 = 11\ldots1|00\ldots0 = \mathbf{v}_0'|00\ldots0,$$

$$\mathbf{v}_i = \mathbf{v}_{i-1}'|\mathbf{v}_{i-1}', \quad 1 < i \le m. \tag{2.8.5}$$

2.8.1 teorema tvirtina, kad $\mathbf{RM}(m,r)$ kodo bazę sudaro vektoriai

$$\mathbf{v}_0,\ \mathbf{v}_{i_1} \cdot \ldots \cdot \mathbf{v}_{i_s}, \quad 1 \le i_1 < \ldots < i_s \le m, \quad s \le r.$$

Reikia parodyti, kad kiekvienas jų gali būti išreikštas (2.8.4) pavidalu. Jau įsitikinome, kad $\mathbf{v}_0 = \mathbf{v}_0'|\mathbf{v}_0'$. Imkime $\mathbf{v} = \mathbf{v}_{i_1} \cdot \ldots \cdot \mathbf{v}_{i_s}$.

Jei $i_1 > 1$, tai iš (2.8.5) gauname

$$\mathbf{v} = \mathbf{v}_{i_1-1}' \cdot \ldots \cdot \mathbf{v}_{i_s-1}'|\mathbf{v}_{i_1-1}' \cdot \ldots \cdot \mathbf{v}_{i_s-1}' = \mathbf{v}'|\mathbf{v}', \quad \mathbf{v}' \in \mathbf{RM}(m-1,r).$$

Jei $i_1 = 1$, tai

$$\mathbf{v} = \mathbf{v}_{i_1-1}' \cdot \ldots \cdot \mathbf{v}_{i_s-1}'|00\ldots0 = \mathbf{v}'|\mathbf{v}' + \mathbf{v}';$$

čia $\mathbf{v}' = \mathbf{v}_{i_1-1}' \cdot \ldots \cdot \mathbf{v}_{i_s-1}' \in \mathbf{RM}(m-1,r-1)$.

Teorema įrodyta.

Remdamiesi įrodytu teiginiu, rasime minimalius Rydo–Mulerio kodų atstumus.

2.8.3 teorema. *Minimalus kodo* $\mathbf{RM}(m,r)$ *atstumas lygus* 2^{m-r} .

Įrodymas. Teorema akivaizdžiai teisinga, kai $r = 0$ arba m. Taigi teorema teisinga su visais galimais r, jei $m = 1$.

Toliau pasinaudosime matematine indukcija. Tarkime, teorema teisinga su visais galimais r , kai $m < k$. Tegu $m = k$. Kadangi su visais $1 \le i_1 < \ldots < i_r \le m$

$$w(\mathbf{v}_{i_1} \cdot \ldots \cdot \mathbf{v}_{i_r}) = 2^{k-r},$$

tai kodo $\mathbf{RM}(k,r)$ minimalus atstumas $d_{k,r}$ turi tenkinti nelygybę $d_{k,r} \le 2^{k-r}$. Tačiau $\mathbf{RM}(k,r) = \mathbf{RM}(k-1,r)|\mathbf{RM}(k-1,r-1)$. Todėl pagal 2.4.2 teoremos teiginį bei indukcijos prielaidą su visais $0 < r < k$, $d_{k,r} = \min\{2d_{k-1,r}, d_{k-1,r-1}\} = 2^{k-r}$. Atvejus $r = 0, k$ jau aptarėme. Teorema įrodyta.

Verta panagrinėti Rydo–Mulerio kodų dekodavimą , nes tai puiki proga pasinaudoti kitokiu tiesinių kodų dekodavimo metodu negu tas, kurį aptarėme anksčiau. Naudosime *loginės daugumos*[4] taisyklę.

Tarkime informacija koduojama Rydo–Mulerio $\mathbf{RM}(m,r)$ kodu: kanalu siunčiami žodžiai $\mathbf{c} = c_1\ldots c_n$, $n = 2^m$,

$$\mathbf{c} = \sum_{\substack{1 \le i_1 < \ldots i_s \le m \\ s \le r}} a(i_1,\ldots,i_s)\mathbf{v}_{i_1} \cdot \ldots \cdot \mathbf{v}_{i_s}; \tag{2.8.6}$$

čia $a_(i_1,\ldots,i_s) = 0$ arba 1. Kanalas galbūt iškraipo siunčiamus simbolius ir gautas žodis yra $\mathbf{d} = d_1\ldots d_n$, $n = 2^m$. Naudodamiesi šiuo žodžiu, rasime teisingas koeficientų $a(i_1,\ldots,i_s)$ reikšmes, taigi atstatysime siųstąjį žodį $\mathbf{c}$, jeigu įvykusių iškraipymų nėra daugiau kaip $0.5(2^{m-r}-1)$. Procedūra tokia: kiekvienam koeficientui $a(i_1,\ldots,i_r)$ sudarysime lygiai 2^{m-r} išraiškų

$$a(i_1,\ldots,i_r) = \sum_{i \in I_j} c_i, \quad j = 1,\ldots,2^{m-r}, \tag{2.8.7}$$

[4] Majority logic decoding (angliškoje literatūroje).

tokių kad $|I_j| = 2^r,\ I_i \cap I_j = \emptyset$, jei $i \neq j$. Jeigu iškraipyta ne daugiau kaip $0.5(2^{m-r}-1)$ žodžio $\mathbf{c}$ simbolių, tai ne daugiau kaip $0.5(2^{m-r}-1)$ (5.8.6) lygybių nebebus teisingos. Tačiau ne mažiau kaip $0.5(2^{m-r}+$ $+1)$, t. y. daugiau kaip pusė liks galioti. Tikrąją koeficiento reikšmę rasime suskaičiavę, kokių simbolių – vienetų ar nulių – yra daugiau sekoje

$$\sum_{i\in I_j} d_i, \quad j = 1, \ldots, 2^{m-r}.$$

Daugiau kartų pasikartojęs simbolis ir bus koeficiento $a(i_1, \ldots, i_r)$ reikšmė. Šitokiu būdu suradę visus koeficientus $a(i_1, \ldots, i_r)$, galime iš gautojo žodžio $\mathbf{d}$ atimti atitinkamus r-os eilės narius, ir manyti, kad gautasis skirtumas yra žodis, gautas siunčiant kodo $\mathbf{RM}(m, r-1)$ žodį. Tada analogiškai galime ieškoti koeficientų $a(i_1, \ldots, i_{r-1})$.

Tačiau kaip sudaryti lygybes (2.8.7)? Sudaryti jas nesudėtinga, tačiau tenka perspėti, jog suprasti visas detales galima tik jaučiantis Rydo–Mulerio kodų šeimoje kaip namuose, t. y. susikūrus labai aiškų mintinį konstrukcijos vaizdą.

Apibrėšime dviejų žodžių $\mathbf{a} = a_1 \ldots a_n, \mathbf{b} = b_1 \ldots b_n$ skaliarinę sandaugą:

$$(\mathbf{a}, \mathbf{b}) = a_1 b_1 + \ldots + a_n b_n;$$

čia sudėtis imama kūne $\mathbf{F}_2$. Pastebėsime, jog

$$(\mathbf{v}(D), \mathbf{v}(E)) \equiv |D \cap E| (\mathrm{mod}\ 2). \tag{2.8.8}$$

Kaip ir anksčiau, naudosime žymenis

$$H_i(0) = H_i = \{\mathbf{a} : \mathbf{a} \in \mathbf{F}_2^m, x_i(\mathbf{a}) = 0\},\ H_i(1) = H_i^c,\ i = 1, \ldots, m.$$

Fiksuokime rinkinį $1 \leq i_1 < \ldots < i_r \leq m$. Tegu $\{l_1, \ldots, l_{m-r}\} = \{1, \ldots, m\} \backslash \{i_1, \ldots, i_r\}$; čia $l_1 < \ldots < l_{m-r}$. Kiekvienam nulių ir vienetų rinkiniui $\langle t \rangle = \langle t_1, \ldots, t_{m-r} \rangle$ apibrėžkime

$$\mathbf{w}_{\langle t \rangle} = \mathbf{v}(H_{l_1}(t_1) \cap \ldots \cap H_{l_{m-r}}(t_{m-r})).$$

Iš viso turime 2^{m-r} žodžių $\mathbf{w}_{\langle t \rangle}$. Svarbi įžvalga: kiekviename žodyje $\mathbf{w}_{\langle t \rangle}$ yra lygiai 2^r vienetų ir nėra vieneto, kuris būtų toje pat pozicijoje skirtingiems $\mathbf{w}_{\langle t \rangle}, \mathbf{w}_{\langle t' \rangle}$. Tegu $\mathbf{v} = \mathbf{v}_{j_1} \cdot \ldots \cdot \mathbf{v}_{j_s}$. Tada bet kokiam $\langle t \rangle$

$$(\mathbf{v}, \mathbf{w}_{\langle t \rangle}) = \begin{cases} 0, & \text{jei } \{j_1, \ldots, j_s\} \neq \{i_1, \ldots, i_r\}, \\ 1, & \text{jei } \{j_1, \ldots, j_s\} = \{i_1, \ldots, i_r\}. \end{cases} \tag{2.8.9}$$

Šį sąryšį galima išsiaiškinti, remiantis (2.8.8) bei Rydo–Mulerio kodo konstrukcijos ypatybėmis; būtina aiškiai suvokti, kokie elementai įeina į atitinkamą aibę $D \cap E$. Padauginę (2.8.6) iš $\mathbf{w}_{\langle t \rangle}$) ir turėdami galvoje (2.8.9) lygybes, gausime

$$(\mathbf{c}, \mathbf{w}_{\langle t \rangle}) = a(i_1, \ldots, i_r).$$

Tačiau tai ir yra ieškotos (2.8.7) lygybės!

Pavyzdys. Panagrinėsime $\mathbf{RM}(3, 1)$ dekodavimą. Prisiminkime kodo sudarymo lentelę:

	$\mathbf{a}_1$	$\mathbf{a}_2$	$\mathbf{a}_3$	$\mathbf{a}_4$	$\mathbf{a}_5$	$\mathbf{a}_6$	$\mathbf{a}_7$	$\mathbf{a}_8$
	000	001	010	011	100	101	110	111
$\mathbf{v}_0$	1	1	1	1	1	1	1	1
$\mathbf{v}_1$	1	1	1	1	0	0	0	0
$\mathbf{v}_2$	1	1	0	0	1	1	0	0
$\mathbf{v}_3$	1	0	1	0	1	0	1	0

.

Šio kodo žodžiai užrašomi taip:

$$\mathbf{c} = a(0)\mathbf{v}_0 + a(1)\mathbf{v}_1 + a(2)\mathbf{v}_2 + a(3)\mathbf{v}_3.$$

$\bullet\bullet\bullet \diamond \bullet\bullet\bullet$

Lygybių sistemą sudarysime $a(3)$ koeficientui. Rinkinius $\langle t\rangle = \langle 0,0\rangle, \langle 0,1\rangle,\ \langle 1,0\rangle,\ \langle 1,1\rangle$ atitinka žodžiai

$$\mathbf{w}_{\langle t\rangle} = 11000000, 00110000, 00001100, 00000011.$$

Todėl (2.8.7) lygybės atrodys taip:

$$\begin{aligned} a(3) &= c_1 + c_2, \\ a(3) &= c_3 + c_4, \\ a(3) &= c_5 + c_6, \\ a(3) &= c_7 + c_8. \end{aligned} \tag{2.8.10}$$

Tarkime, buvo siųstas žodis $\mathbf{c} = \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3 = 10010110$, tačiau vienas simbolis buvo iškraipytas ir gautasis žodis yra $\mathbf{d} = 11010110$. Pagal gautąjį žodį suradę dešines (2.8.10) lygybių puses, gauname 0,1,1,1. Taigi $a(3) = 1$.

• • • ◇ • • •