TIESINIŲ KODŲ DEKODAVIMAS

Rimantas Grigutis

1. Įvadas.

Nagrinėjamas tiesinis (n, k) kodas:

$$a = a_1a_2...a_k \longrightarrow c = c_1c_2...c_kc_{k+1}...c_n = a_1a_2...a_kc_{k+1}...c_n.$$

$H = (A \mid I_{n-k}) -$ kontrolinė matrica. Tai $(n-k)\times n$ matrica ir $rankH = n-k$.
$G = \left(I_k \mid -A^T\right) -$ generuojanti matrica. Tai $k \times n$ matrica ir $rankG = k$.
$C = \ker H = imG$ - kodo žodžių aibė (*kodas*). $C \subset F_q^n$ yra poerdvis.
• *Kodas C yra generuojančios matricos G eilučių vektorinė erdvė.*
Pagrindiniai sąryšiai:

$$Hc^T = 0;$$
$$c = aG;$$
$$GH^T = 0,$$

t.y. seka $0 \to F_q^k \xrightarrow{G} F_q^n \xrightarrow{H} F_q^{n-k} \to 0$ yra F_q modulių tiksli seka:
$imG = \ker H, G-$ monomorfizmas, H - epimorfizmas.

• Svarbi kodo C charakteristika yra minimalus *kodo atstumas* d_C, kuris yra $d_C \geq 2t + 1$, čia $t-$ ištaisomų klaidų skaičius.

Teorema. *$d_C \geq s + 1$ tada ir tik tada, kai bet kurie s kontrolinės matricos stulpeliai yra tiesiškai nepriklausomi.*

2. Tiesinio kodo dekodavimas.

Tegu $C \subset F_q^n$ yra (n, k) kodas virš F_q. dim $C = k$ ir $|C| = q^k$.
Faktorizuokime vektorinę erdvę F_q^n poerdviu C :

$$F_q^n/C = \left(a^{(0)} + C\right) \cup \left(a^{(1)} + C\right) \cup ... \cup \left(a^{(s)} + C\right),$$

čia $s = q^{n-k} - 1$.
Tegu kodavimo ir perdavimo schema yra:

$$a \longrightarrow c \rightsquigarrow y = a^{(i)} + z.$$

Tada *klaidos vektorius* $e := y - c = a^{(i)} + (z - c) \in a^{(i)} + C$.

Mūsų užduotis: rasti tokį $e \in a^{(i)} + C$, kad jo *svoris* $w(e)$ būtų minimalus. Tada dekoduojame $x = y - e$.

Apibrėšime visus vektorius, esančius vienoje ekvivalentumo klasėje, vienijančią chrakteristiką - *sindromą*.

Apibrėžimas. *Tegu H yra tiesinio (n, k) kodo C kontrolinė matrica. Vektorius $S(y) := Hy^T$ vadinamas vektoriaus y sindromu. Tai $(n - k)$ ilgio vektorius.*

• *Sindromo savybės.*

S1. $S(y) = 0$ tada ir tik tada, kai $y \in C$.

S2. $S(y) = S(z)$ tada ir tik tada, kai $y + C = z + C$.

3. Tiesinio kodo dekodavimo algoritmas.

Duota. Kodas $C \subset F_q^n$ yra (n, k) kodas virš F_q. dim $C = k$ ir $|C| = q^k$.

$H-$ kontrolinė matrica, $G-$ generuojanti matrica.

$y-$ gautas žodis.

Rasti a ir $x-$ siųstą žodį.

Algoritmas.

1. Skaičiuojame $S(y) = Hy^T$.

2. Ieškome klasės $y + C$ lyderio $b^{(i)}$, t.y. turinčio mažiausią svorį klasės $y + C$ elemento: $y = b^{(i)} + z$.

3. Dekoduojame: $x = y - b^{(i)} = z$.

4. Randame a, sprendžiant lygčių sistemą: $aG = z$.

Pavyzdys. Tegu C yra binarinis tiesinis $(4, 2)$ kodas, kurio kontrolinė ir generuojanti matricos yra:

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

Tegu gautas žodis $y = 1110$.

1. $S(y) = Hy^T = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

2. Klasės $y + C = \{1110;\ 0100;\ 1001;\ 0011\}$ lyderis yra $b = 0100 = y + 1010$.

3. Dekoduojame: $x = y - b = 1110 - 0100 = 1010 = z$

4. Randame $a : aG = z$

$$(\alpha\beta) \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} = (1010)$$
$$(\alpha\beta) = (10).$$

4. Cikliniai kodai.

Turime vektorinių erdvių virš F_q izomorfizmą:

$$F_q^n \approx F_q[x]/(x^n-1)$$
$$a=(a_0,a_1,...,a_{n-1}) \to a_0+a_1x+\cdots+a_{n-1}x^{n-1}$$

Tegu $g(x)=g_0+g_1x+\cdots g_{n-k}x^{n-k} \in F_q[x]$ dalijasi iš $x^n-1, \deg g(x)=n-k$. Tada galime apibrėžti tiesinį kodą $C=\{a\cdot g(x) \mid \deg a(x) \le k-1\}$, kurio bazė yra

$g(x), xg(x), x^2g(x), ..., x^{k-1}g(x)$.

Kodo C generuojanti matrica yra

$$G=\begin{pmatrix} g_0 & g_1 & ... & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & & g_{n-k} & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix}.$$

$h(x)=\dfrac{x^n-1}{g(x)}=h_0+h_1x+\cdots+h_kx^k$, tada kodo kontrolinė matrica

$$H=\begin{pmatrix} 0 & 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & & h_0 \\ 0 & 0 & 0 & h_k & h_{k-1} & & & h_0 & 0 \\ & & & & \cdots & & & & \\ h_k & h_{k-1} & \cdots & h_0 & 0 & 0 & & & 0 \end{pmatrix}.$$

• $C-$ žiedo $F_q[x]/(x^n-1)$ idealas, todėl $C=(g(x))$ ir vadinamas *ciklinių kodu.*. Polinomas $g(x)$ vadinamas *generuojančiu kodo C polinomu.* Tegu $\alpha_1, ..., \alpha_{n-k}$ generuojančio kodo polinomo šaknys. Tada kodo kontrolinė matrica

$$H=\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ & & & \cdots & \\ 1 & \alpha_{n-k} & \alpha_{n-k}^2 & \cdots & \alpha_{n-k}^{n-1} \end{pmatrix}$$

ir $f(x) \in C \Leftrightarrow f(\alpha_i)=0$ su visais $i=1,2,...,n-k$ ir $f \in \ker H$.

5. BCH kodai.

Tegu

$b > 0$ sveikas skaičius;

$\alpha \in F_{q^m}$ primytvioji $n-$ ojo laipsnio šaknis iš 1;

$m-$ mažiausias toks, kad $q^m \equiv 1 \pmod{n}$, t.y. $q^m - 1 \vdots n$.

Mes turime, kad $\alpha \in F_{q^m} \Rightarrow \alpha^{q^m-1} = 1 \Rightarrow$ elemento α eilė yra $q^m - 1$ daliklis.

BCH kodas su konstruktyviu atstumu d virš F_q konstruojamas taip:

1. Imami $\alpha^b, \alpha^{b+1}, ..., \alpha^{b+d-2}$ (viso $d-1$ elementas).
2. Randami šių elementų minimalūs polinomai $m^{(b)}(x), ..., m^{(b+d-1)}(x)$.
3. $g(x) := MBK\left(m^{(b)}(x), ..., m^{(b+d-1)}(x)\right)$.

Svarbūs atskiri atvejai:

$b = 1$ tai BCH siaurąja prasme;

$n = q^m - 1$ tai primityvusis BCH;

$n = q - 1$ tai Reed-Solomon'o kodas (RS kodas): tada $\alpha^{q-1} = 1$ ir $\alpha \in F_q$.

BCH kodo kontrolinė matrica yra:

$$H = \begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \dots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \dots & \alpha^{(n-1)(b+1)} \\ & & & \dots & \\ 1 & \alpha^{b+d-2} & \alpha^{2(b+d-2)} & \dots & \alpha^{(n-1)(b+d-2)} \end{pmatrix}$$

• Svarbu: $d_{BCH} \geq d$.

6. Primityvaus binarinio BCH kodo pavyzdys.(Hamming'o kodas)

$q=2, m=4, b=1, n=15, d=3.$

Tegu $\alpha-$ primityvusis kūno F_{2^4} elemantas, kurio minimalus polinomas yra $m(x)=x^4+x+1$.

Kodo kontrolinė matrica

$$H=(1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14})=$$
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Ši matrica gaunama išreiškus α^i elemantais $1,\alpha,\alpha^2,\alpha^3$. Tai Hamming'o $(15,11)$ kodas $d=3$, nes $m(\alpha^2)=0$. Šis kodas ištaiso 1 klaidą.

Tam kad *dekoduoti* $v\in F_2^{15}$ reikia suskaičiuoti v sindromą:

$$S(v)=Hv^T=v(\alpha)=r(\alpha),$$

čia $v(x)=m(x)a(x)+r(x)$ ir $\deg r(x)\le 3$.

Pavyzdys.

1. Tegu $v=010110001011101=x+x^3+x^4+x^8+x^{10}+x^{11}+x^{12}+x^{14}$. Tada $r(x)=1+x$ ir

$S(v)=Hv^T=(1100)^T=1+\alpha$.

2. Toliau ieškome klaidos vektoriaus $e, w(e)\le 1$, $S(e)=S(v)$. Tam ieškome tokio $j, 1\le j\le 14$, kad $\alpha^j=Hv^T$ ir randame $j=4$. Taigi klaida yra vektoriaus v $5-$ oje komponentėje ir todėl dekoduojame:

$$w=0101\mathbf{0}0001011101.$$

7. Binarinio BCH kodo pavyzdys su konstruktyviu $d=4,5$.

$q=2, n=15, d=4, b=1$.

Tegu α yra primityvaus polinomo $m(x)=x^4+x+1$ šaknis. Žinome, kad α^2 yra irgi polinomo $m(x)$ šaknis. Elementas α^3 yra polinomo $n(x)=x^4+x^3+x^2+x+1$ šaknis. Taigi BCH kodas siaurąja prasme su $d=4$ generuojamas polinomu:

$$\mathrm{g}(x)=m(x)n(x).$$

Turime taip pat, kad α^4 yra polinomo $m(x)$ šaknis, todėl tai BCH kodas su konstruktyviu $d=5$. Tai $(15,7)$ kodas su $d=5$.

8. BCH dekodavimo algoritmas.

Tegu *siunčiamas* žodis w yra užkoduotas BCH kodu su konstruktyviu atstumu $d \geq 2t+1$ ir atsirado ne daugiau t klaidų. Tegu gautas žodis v.

Algoritmas.

1.(Sindomas) Ieškome v sindromo:

$$S(v) = Hv^T = (S_b, S_{b+1}, ..., S_{b+d-2})^T .$$

Tegu

$$S_j = \sum_{i=1}^{r} c_i \gamma_i^j \ , \ b \leq j \leq b+d-2,$$

čia c_i- klaidos reikšmės, o $\gamma_i \in F_{q^m}$ - lokatoriai. Tikslas - rasti (c_i, γ_i).

2.(Klaidų skaičiaus r radimas) Ieškome tokį *maksimalų* $r \leq t$, kad sistema

$$S_{j+r} + S_{j+r-1}\tau_1 + \cdots + S_j\tau_r = 0, \, b \leq j \leq b+r-1$$

turėtų neišsigimusią matricą. Išsprendžiame šią sistemą ir τ_i išreikšime per S_j.

3.(Lokatorių γ_i radimas). Spręsdami lygtį:

$$s(x) = \prod_{i=1}^{r} (1 - \gamma_i x) = \sum_{i=1}^{r} \tau_i x^i$$

randame lokatorius γ_i. Sprendžiame skaičiuodami polinomo $s(x)$ elemento α laipsniuose.

4. (Klaidų reikšmių radimas). Spręsdami sistemą iš 1 punkto randame c_i.

Tada klaidos vektorius $e(x) = \sum c_i x^{a_i}$, kur $\gamma_i = \alpha^{a_i}$.

5. Dekodavimas: $w = v - e$.

Paaiškinimas. Turime $S(v) = Hv^T = (S_b, S_{b+1}, ..., S_{b+d-2})^T$ ir $S_j = v(\alpha^j) = e(\alpha^j)$ ir $e(x) = \sum_{i=1}^{r} c_i x^{a_i}$. Pažymėkime $\gamma_i = \alpha^{a_i} \in F_{q^m}$ (klaidos lokatoriai). Tada $S_j = e(\alpha^j) = \sum_{i=1}^{r} c_i \gamma_i^j$.

9. BCH dekodavimo pavyzdys.

0 (Kodo aprašymas).

Duotas binarinis BCH *su* konstruktyviu $d = 5$ ir ištaisančiu 1 ir 2 klaidas.

Tegu $b = 1, n = 15, q = 2$.

Tegu $\alpha \in F_{16}$ primityvusis elementas ir jo minimalus polinomas $m_1(x) = x^4 + x + 1$.

Tegu $m_i(x)$ yra elemento α^i minimalusis polinomas. Tada

$$m_1 = m_2 = m_4 = m_8 = 1 + x + x^4$$
$$m_3 = m_6 = m_{12} = m_9 = 1 + x + x^2 + x^3 + x^4.$$

taigi, BCH kodo generuojantis polinomas yra

$$g(x) = m_1(x)\, m_3(x) = 1 + x^4 + x^6 + x^7 + x^8.$$

Tai tiesinis $(15, 7)$ kodas su kontroliniu polinomu

$$h(x) = \frac{x^{15} - 1}{g(x)} = 1 + x^4 + x^6 + x^7.$$

Kodo bazė yar vektoriai atitinkantys polinomus

$$g, xg, x^2g, x^2g, x^3g, x^4g, x^5g, x^6g.$$

Kodo generuojanti matrica

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

1. Algoritmas.
Tegu gautasis po perdavimo žodis yra

$$v = 100100110000100$$
$$v(x) = 1 + x^3 + x^6 + x^7 + x^{12}.$$

$1^\bullet$ (v sindromo $S(v)$ skaičiavimas).

$$S(v) = (S_1, S_2, S_3, S_4), \text{ čia } S_i = v(\alpha^i) = w(\alpha^i) + e(\alpha^i) = e(\alpha^i)$$
$$S_1 = e(\alpha) = v(a) = 1$$
$$S_2 = e(\alpha^2) = v(\alpha^2) = 1$$
$$S_3 = e(\alpha^3) = v(\alpha^3) = \alpha^4$$
$$S_4 = e(\alpha^4) = v(\alpha^4) = 1.$$

$2^\bullet$(klaidų skaičiaus r nustatymas, $r \leq 2$).
Maksimali sistema turi pavidalą:

$$S_3 + S_2\tau_1 + S_1\tau_2 = 0$$
$$S_4 + S_3\tau_1 + S_2\tau_2 = 0$$

t.y. sistemos matrica $\begin{pmatrix} S_2 & S_1 \\ S_3 & S_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \alpha^4 & 1 \end{pmatrix}$ yra neišsigimusi.
Taigi $r = 2$ ir todėl yra ištaisomos 2 klaidos.
Sistemos sprendinys yra $\tau_1 = 1$; $\tau_2 = \alpha$ ir todėl klaidų lokatorių polinomas yra

$$s(x) = 1 + x + \alpha x^2.$$

$3^\bullet$ Polinomo $s(x)$ šaknimis yra $\alpha^8 = \gamma_1^{-1}$ ir $\alpha^6 = \gamma_2^{-1}$. Todėl $\gamma_1 = \alpha^7$ ir $\gamma_2 = \alpha^9$.
Taigi gavome, kad klaidos yra 8 ir 10 pozicijose.
Sprendžiame sistemą

$$\begin{cases} S_1 = c_1\gamma_1 + c_2\gamma_2 \\ S_2 = c_1\gamma_1^2 + c_2\gamma_2^2 \end{cases}$$
$$\begin{cases} 1 = c_1\alpha^7 + c_2\alpha^9 \\ 1 = c_1\alpha^{14} + c_2\alpha^{18} \end{cases}$$
$$c_1 = 1, c_2 = 1.$$

4• Klaidos vektorius $e(x) = c_1 x^{a_1} + c_2 x^{a_2} = x^7 + x^9$, nes $\gamma_1 = \alpha^7$ ir $\gamma_2 = \alpha^9$. Ištaisome klaidą:

$$w(x) = v(x) - e(x) = 1 + x^3 + x^6 + x^9 + x^{12} = 1001001001001 00$$

5• Pradinė informacija:

$$\frac{w(x)}{g(x)} = 1 + x^3 + x^4 = 1001100.$$

10. Papildymas.

$F_{2^4}^*$ Indeksų lentelė
($\alpha^4 + \alpha + 1 = 0$ ir $\alpha^{15} = 1$)

1	α	α	0010
2	α^2	α^2	0100
3	α^3	α^3	1000
4	α^4	$\alpha + 1$	0011
5	α^5	$\alpha^2 + \alpha$	0110
6	α^6	$\alpha^3 + \alpha^2$	1100
7	α^7	$\alpha^3 + \alpha + 1$	1011
8	α^8	$\alpha^2 + 1$	0101
9	α^9	$\alpha^3 + \alpha$	1010
10	α^{10}	$\alpha^2 + \alpha + 1$	0111
11	α^{11}	$\alpha^3 + \alpha^2 + \alpha$	1110
12	α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$	1111
13	α^{13}	$\alpha^3 + \alpha^2 + 1$	1101
14	α^{14}	$\alpha^3 + 1$	1001
15	α^{15}	1	0001