Kodavimo teorija

Vilius Stakėnas

2010 metų ruduo

Reedo-Mullerio kodai

Kosminiai kodai

Ši kodų šeima pasitarnavo kosmonautikai. Jais buvo naudojamasi 1969-1977 metais palaikant ryšį su kosminėmis stotimis.

Ir šiaip tai labai įdomūs kūriniai.

Dvejetainės abėcėlės kodai

Galima sukonstruoti Reedo-Mullerio kodus iš bet kokios abėcėlės $\mathbb{F}_p$ žodžių.

Paprasčiausias ir svarbiausias – dvejetainės abėcėlės atvejis.

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

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

Žodžių poerdviai

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

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

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

Žodžių atitiktis

Apibrėšime abipusiškai vienareikšmę $\mathbb{F}_2^m$ poaibių ir erdvės $\mathbb{F}_2^n$, $n = 2^m$, žodžių atitiktį.

Jei $D \subset \mathbb{F}_2^m$, tai priskirsime: $D \to \mathbf{v}(D)$; čia žodžio $\mathbf{v}(D) \in \mathbb{F}_2^n$ komponentės apibrėžiamos taip:

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

Inventorizacijos dokumentas

Žodyje $\mathbf{v}(D)$ vienetukai žymi, kurie žodžiai įeina į D; $\mathbf{v}(D)$ yra tarsi poaibio D „inventorizacijos“ dokumentas.

Pavyzdžiui, jei $m = 3, D = \{\mathbf{a}_1, \mathbf{a}_3, \mathbf{a}_5\}$, tai $\mathbf{v}(D) = 10101000$.

Visą erdvę $\mathbb{F}_2^m$ atitinka žodis $\mathbf{v}_0 = 11 \ldots 1$.

Teisinga tokia lygybė:

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

Čia $\cdot$ žymi žodžių daugybą, pvz. $101 \cdot 011 = 001$.

Reedo-Mullerio kodai

Apibrėžimas. Tegu $m \geq 1,\ r \leq m,\ n = 2^m$. Reedo–Mullerio $\mathbf{RM}(m, r)$ kodu vadinsime tiesinį $\mathbb{F}_2^n$ poerdvį, kurį generuoja žodžiai

$$\mathbf{v}_0,\ \mathbf{v}_{i_1} \cdot \ldots \cdot \mathbf{v}_{i_s};\ 1 \leq i_1 < \ldots < i_s \leq m,\ s \leq r, \tag{1}$$

čia

$$\mathbf{v}_0 = 11 \ldots 1,\ \mathbf{v}_i = \mathbf{v}(H_i),\ i = 1, \ldots, m.$$

Žodžių, kurie užrašyti (1), skaičius lygus

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

Kodo dimensija

Teorema. $\mathbf{RM}(m, r)$ kodo dimensija lygi $k(m, r)$, o žodžiai

$$\mathbf{v}_0,\ \mathbf{v}_{i_1} \cdot \ldots \cdot \mathbf{v}_{i_s};\ 1 \leq i_1 < \ldots < i_s \leq m,\ s \leq r,$$

sudaro jo bazę.

Įrodymas.

Iš pradžių pastebėkime tokią žodžių $\mathbf{v}_i$ savybę. Imkime poerdvių H_i pildinius

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

Nesunku pastebėti, jog

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

Įrodymas

Imkime

$$\mathbf{v}_0,\ \mathbf{v}_{i_1} \cdot \ldots \cdot \mathbf{v}_{i_s};\ 1 \leq i_1 < \ldots < i_s \leq m,\ s \leq r, \tag{2}$$

žodžių sistemoje $r = m$. Tada gausime lygiai $n = 2^m$ žodžių; tokia yra ir visos erdvės $\mathbb{F}_2^n$ dimensija.

Jeigu parodysime, jog kiekvieną $\mathbb{F}_2^n$ žodį galima išreikšti šiais n žodžiais, tai galėsime teigti, kad jie sudaro tiesiškai nepriklausomą sistemą.

Tada bet kokiam r (2) žodžiai irgi bus tiesiškai nepriklausomi, nes sudarys tiesiškai nepriklausomos sistemos posistemę.

Įrodymas

Pakanka parodyti, kad kiekvieną $\mathbb{F}_2^n$ standartinės bazės žodį galima išreikšti (2) žodžių tiesine kombinacija.

Įrodymas

Imkime standartinės bazės žodį $\mathbf{e}_i$, kuris sudarytas iš nulių visose pozicijose, išskyrus i-ąją, lygią vienetui.

Prisiminę erdvės $\mathbb{F}_2^m$ poaibių ir $\mathbb{F}_2^n$ žodžių atitiktį, galime rašyti: $\mathbf{e}_i = \mathbf{v}(D)$; čia $D = \{\mathbf{a}_i\}$.

Tegu $\mathbf{a}_i = a_1 \ldots a_m$. Žymėdami $H_i(0) = H_i$ ir $H_i(1) = H_i^c$, gausime

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

Įrodymas

Pasirėmę savybe

$$\mathbf{v}(U \cap V) = \mathbf{v}(U) \cdot \mathbf{v}(V),$$

gausime

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

Tačiau $\mathbf{v}(H_i(a_i))$ lygus arba $\mathbf{v}_i$, arba $\mathbf{v}_0 + \mathbf{v}_i$. Todėl $\mathbf{e}_i$ yra (2) sistemos žodžių tiesinė kombinacija.

$\mathbf{RM}(3, 2)$

	$\mathbf{a}_1$	$\mathbf{a}_2$	$\mathbf{a}_3$	$\mathbf{a}_4$	$\mathbf{a}_5$	$\mathbf{a}_6$	$\mathbf{a}_7$	$\mathbf{a}_8$
	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	1	0	0	0

Reedo-Mullerio kodų kolonija

Fiksuotam m gavome ištisą Reedo–Mullerio kodų koloniją, kurios nariai yra $\mathbf{RM}(m, r),\ r = 0, \ldots, m$.

Akivaizdu, kad

$$\mathbf{RM}(m, 0) = \{00 \ldots 0, 11 \ldots 1\},\ \mathbf{RM}(m, m) = \mathbb{F}_2^n.$$

Reedo-Mullerio kodo žodžių svoriai

Pastebėkime, kad visų Reedo-Mullerio kodo $\mathbf{RM}(m,r)$, kai $r<m$, žodžių svoriai yra lyginiai. Iš tikrųjų:

$$w(\mathbf{v}_0)=n=2^m,\quad w(\mathbf{v}_{i_1}\cdot\ldots\cdot\mathbf{v}_{i_s})=2^{m-s}.$$

Uždara šeima

$$1+\binom{m}{2}+\ldots+\binom{m}{r}+\binom{m}{r+1}+\ldots+\binom{m}{m-1}+1=2^m=n.$$

Pasinaudoję binominių koeficientų sąryšiu $\binom{m}{k}=\binom{m}{m-k}$ galime šią lygybę užrašyti panaudodami Reedo-Mullerio kodų dimensijas:

$$k(m,r)+k(m,m-r-1)=\dim(\mathbf{RM}(m,r))+\dim(\mathbf{RM}(m,m-r-1))=n.$$

Teorema. Su visomis m,r $(m<r)$ reikšmėmis teisingas sąryšis $\mathbf{RM}(m,r)^\perp=\mathbf{RM}(m,m-r-1)$.

Įrodymas

Kad teiginys būtų teisingas, reikia, kad būtų patenkintos dvi sąlygos:

- kodų $\mathbf{RM}(m,r),\mathbf{RM}(m,m-r-1)$ bazių žodžių skaliarinės sandaugos turi būti lygios nuliui moduliu 2;
- dimensijų suma lygi n.

Tačiau pastarąją lygybę jau nustatėme!

Įrodymas

Tegu $\mathbf{u} = \mathbf{v}_{i_1} \cdot \ldots \mathbf{v}_{i_s}$ ir $\mathbf{b} = \mathbf{v}_{j_1} \cdot \ldots \mathbf{v}_{j_t}$ yra šių kodų bazių žodžiai, $s + t \leq r + m - r - 1 < m$. Sudauginę juos gausime žodį

$$\mathbf{c} = \mathbf{v}_{l_1} \cdot \ldots \mathbf{v}_{l_z}, \quad z < m.$$

Tačiau

$$(\mathbf{a}, \mathbf{b}) = w(\mathbf{c}) \equiv 0 \ (\text{mod } 2).$$

Taigi ir pirmoji dualumo sąlyga yra teisinga.

Kitas požiūris

Kitaip pažvelkime į žodžių erdvės

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

ir $\mathbb{F}_2^n$ sąryšį.
Į kiekvieną žodį $\mathbf{f} \in \mathbb{F}_2^n$ galime žvelgti kaip į tam tikros funkcijos $f : \mathbb{F}_2^m \to \mathbb{F}_2$ reikšmių lentelę:

$$\text{jei } \mathbb{F} = y_1 y_2 \ldots y_n, \text{ tai } f(\mathbf{a}_1) = y_1, \ldots, f(\mathbf{a}_n) = y_n.$$

Kadangi šios funkcijos įgyja tik dvi reikšmes, galime jas interpretuoti kaip logines funkcijas.

Loginės funkcijos

Pažymėję $\mathbf{a} = x_1 x_2 \ldots x_m, \ \mathbf{a} \in \mathbb{F}_2^m$ galime suvokti $\mathbb{F}_2^n$ žodžius kaip logines funkcijas

$$f(x_1, x_2, \ldots, x_m).$$

Šios funkcijos sudaro tiesinę erdvę. Kokios funkcijos atitinka Reedo-Mullerio kodo bazės žodžius?

Reedo-Mullerio kodų žodžiai – loginiai daugianariai

Nesunku suprasti, kad

$$\begin{aligned} \mathbf{v}_0 &\mapsto 1,\ \mathbf{v}_i \mapsto= 1 + x_i,\ i = 1, 2, \ldots, m \\ \mathbf{v}_{i_1} \cdot \mathbf{v}_{i_2} \cdot \ldots \cdot \mathbf{v}_{i_s} &\mapsto (1 + x_{i_1})(1 + x_{i_2}) \cdots (1 + x_{i_s}) \\ &= 1 + x_{i_1} + \ldots + x_{i_1} x_{i_2} \cdot \ldots x_{i_s}. \end{aligned}$$

Taigi kodą $\mathbf{RM}(m, r)$ galime interpretuoti, kaip nedidesnio kaip r laipsnio „loginių daugianarių“ erdvę!

Minimalus atstumas

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

Kad minimalus kodo atstumas negali būti didesnis už 2^{m-r}, rodo kodo bazės žodžio svoris:

$$w(\mathbf{v}_1 \cdot \mathbf{v}_2 \cdot \ldots \cdot \mathbf{v}_r) = 2^{m-r}.$$

Norėdami įrodyti, kad ne mažesnis, turėtume kiek pasidarbuoti...

Reedo-Mullerio kodų dekodavimas

Naudosime loginės daugumos metodą – savotišką sprendimų priėmimą „balsavimo" būdu. Tarkime, informacija koduojama Reedo–Mullerio $\mathbf{RM}(m, r)$ kodu: kanalu siunčiami žodžiai $\mathbf{c} = c_1 \ldots c_n,\ n = 2^m$,

$$\mathbf{c} = a(0)\mathbf{v}_0 + \sum_{\substack{1 \le i_1 < \ldots i_s \le m \\ s \le r}} a(i_1, \ldots, i_s)\mathbf{v}_{i_1} \cdot \ldots \cdot \mathbf{v}_{i_s}; \tag{3}$$

čia $a(0), a(i_1, \ldots, i_s) = 0$ arba 1.

Dekodavimas

Kanalas galbūt iškraipė siunčiamus simbolius; pažymėkime gautąjį žodį $\mathbf{d} = d_1 \dots d_n, n = 2^m$.

Naudodamiesi šiuo žodžiu, rasime teisingas koeficientų $a(0), a(i_1, \dots, i_s)$ reikšmes, taigi atstatysime siųstąjį žodį $\mathbf{c}$, jeigu įvykusių iškraipymų nėra daugiau kaip $(2^{m-r} - 1)/2$.

Pasirengimas

Kiekvienam koeficientui $a(i_1, \dots, i_r)$ sudarysime lygiai 2^{m-r} išraiškų

$$a(i_1, \dots, i_r) = \sum_{i \in I_j} c_i, \quad j = 1, \dots, 2^{m-r}, \tag{4}$$

tokių, kad $|I_j| = 2^r,\ I_i \cap I_j = \emptyset$, jei $i \neq j$. Šios sąlygos reiškia, kad kievienoje iš (4) yra lygiai po 2^r dėmenų ir kiekvienas siunčiamo žodžio simbolis c_i pasirodo tik vienoje lygybėje.

Dekodavimas

Jeigu iškraipyta ne daugiau kaip $(2^{m-r} - 1)/2$ žodžio $\mathbf{c}$ simbolių, tai ne daugiau kaip $(2^{m-r} - 1)/2$ lygybių

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

nebebus teisingos.
Tačiau ne mažiau kaip $(2^{m-r} + 1)/2$, t. y. daugiau kaip pusė liks galioti.

Dekodavimas

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.

Dekodavimas

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.

Dekodavimas

Analogiškai galime ieškoti koeficientų $a(i_1, \ldots, i_{r-1})$.

Suradę visus koeficientus $a(i_1, \ldots, i_s)$ ir iš gautojo žodžio atėmę atitinkamus dėmenis gausime žodį $\mathbf{d}_0$, kurį galėsime interpretuoti, kaip gautą siunčiant kanalu $a(0)\mathbf{v}_0$.

Ar $a(0) = 0$, ar $a(0) = 1$ galėsime nuspręsti, suskaičiavę, ko daugiau – vienetų ar nulių yra žodyje $\mathbf{d}_0$.

Lygybių sudarymas

Dekodavimui reikalingoms lygybėms sudaryti pasinaudosime skaliarine žodžių $\mathbf{a} = a_1 \dots a_n, \mathbf{b} = b_1 \dots b_n$ daugyba:

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

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

$$(\mathbf{v}(D), \mathbf{v}(E)) \equiv |D \cap E| \pmod 2. \tag{5}$$

Žodžių rinkinys

$$\begin{aligned} H_i(0) &= H_i = \{\mathbf{a} : \mathbf{a} \in \mathbb{F}_2^m, x_i(\mathbf{a}) = 0\}, \\ H_i(1) &= H_i^c = \{\mathbf{a} : \mathbf{a} \in \mathbb{F}_2^m, x_i(\mathbf{a}) = 1\}, \ i = 1, \dots, m. \end{aligned}$$

Fiksuokime rinkinį $1 \le i_1 < \dots < i_r \le m$. Tegu

$$\{l_1, \dots, l_{m-r}\} = \{1, \dots, m\} \backslash \{i_1, \dots, i_r\};$$ čia $l_1 < \dots < l_{m-r}$.

Žodžių rinkinys

Kiekvienam nulių ir vienetų rinkiniui $t = t_1 \dots t_{m-r}$ apibrėžkime

$$\mathbf{w}_t = \mathbf{v}(H_{l_1}(t_1) \cap \dots \cap H_{l_{m-r}}(t_{m-r})).$$

Iš viso turime 2^{m-r} žodžių $\mathbf{w}_t$.
Svarbi įžvalga: kiekviename žodyje $\mathbf{w}_t$ yra lygiai 2^r vienetų ir nėra vieneto, kuris būtų toje pat pozicijoje skirtingiems $\mathbf{w}_t, \mathbf{w}_{t'}$.

Lygybės

Tegu $\mathbf{v} = \mathbf{v}_{j_1} \cdot \ldots \cdot \mathbf{v}_{j_s}$. Tada bet kokiam t

$$(\mathbf{v}, \mathbf{w}_t) = \begin{cases} 0, & \text{jei} \{j_1, \ldots, j_s\} \neq \{i_1, \ldots, i_r\}, \\ 1, & \text{jei } \{j_1, \ldots, j_s\} = \{i_1, \ldots, i_r\}. \end{cases}$$

Šį sąryšį galima išsiaiškinti, remiantis Reedo–Mullerio kodo konstrukcijos ypatybėmis; būtina aiškiai suvokti, kokie elementai įeina į atitinkamą aibę $D \cap E$.

Lygybės

Padauginę

$$\mathbf{c} = a(0)\mathbf{v}_0 + \sum_{\substack{1 \leq i_1 < \ldots i_s \leq m \\ s \leq r}} a(i_1, \ldots, i_s)\mathbf{v}_{i_1} \cdot \ldots \cdot \mathbf{v}_{i_s};$$

skaliariškai iš $\mathbf{w}_t$ ir atsižvelgdami į nustatytas lygybes, gausime

$$(\mathbf{c}, \mathbf{w}_t) = a(i_1, \ldots, i_r).$$

Tačiau tai ir yra loginės daugumos metodo lygybės!

Pavyzdys: $\mathrm{RM}(3,1)$ dekodavimas

Kodo lentelė

	$\mathbf{a}_1$	$\mathbf{a}_2$	$\mathbf{a}_3$	$\mathbf{a}_4$	$\mathbf{a}_5$	$\mathbf{a}_6$	$\mathbf{a}_7$	$\mathbf{a}_8$
	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:

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

Dekodavimas

Lygybių sistemą sudarysime $a(3)$ koeficientui. Rinkinius $t = 00, 01, 10, 11$ atitinka žodžiai

$$\mathbf{w}_t = 11000000, 00110000, 00001100, 00000011.$$

Todėl dekodavimo lygybės atrodys taip:

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

Dekodavimas

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 naudodamiesi dekodavimo lygybėmis gauname reikšmes $0, 1, 1, 1$. Taigi $a(3) = 1$.