Kodavimo teorija

Vilius Stakėnas

2010 metų ruduo

Tiesinių kodų poros

Tiesinis kodas

Priminimas:

Apibrėžimas. Tiesinį erdvės $\mathbb{F}_q^n$ žodžių poerdvį $\mathbb{L} \subset \mathbb{F}_q^n$ vadiname tiesiniu kodu.
Jeigu šio kodo dimensija yra k, o minimalus atstumas d, sakome, kad tai yra $[n, k, d]$ kodas.

Dualus poerdvis

Apibrėžimas. Tegu $\mathbf{x} = x_1x_2 \dots x_n$, $\mathbf{y} = y_1y_2 \dots y_n$ yra du erdvės $\mathbb{F}_q^n$ žodžiai. Jų vidine sandauga vadinsime $\mathbb{F}_q$ elementą, apibrėžiamą lygybe

$$\mathbf{x} \cdot \mathbf{y} = x_1y_1 + \ldots + x_ny_n.$$

Teorema. Tegu $\mathbb{L}$ yra tiesinis poerdvis. Žodžių aibė

$$\mathbb{L}^\perp = \{\mathbf{y} \in \mathbb{F}_q^n : \mathbf{x} \cdot \mathbf{y} = 0 \text{ su visais } \mathbf{x} \in \mathbb{L}\}$$

taip pat yra tiesinis poerdvis. Poerdvių dimensijos susijusios lygybe

$$\dim(\mathbb{L}) + \dim\left(\mathbb{L}^\perp\right) = n.$$

Dualus kodas

Apibrėžimas. Tegu $\mathbb{L} \subset \mathbb{F}_q^n$ yra tiesinis kodas. Tiesinį poerdvį $\mathbb{L}^\perp$ vadinsime kodu, dualiu kodui $\mathbb{L}$.

Beveik akivaizdu, kad

$$\left(\mathbb{L}^\perp\right)^\perp = \mathbb{L}.$$

Kodų bazės

Tiesinį poerdvį $\mathbb{L}$ galime nusakyti naudodami jo bazę arba – jam dualaus poerdvio bazę.

Teorema. Tegu $\mathbb{L}$ yra tiesinis poerdvis, $\dim(\mathbb{L}) = k$, o $\mathbf{h}_1, \ldots, \mathbf{h}_{n-k}$ yra dualaus poerdvio $\mathbb{L}^\perp$ bazė. Tada

$$\mathbb{L} = \{\mathbf{x} \in \mathbb{F}_q^n : \mathbf{x} \cdot \mathbf{h}_1 = \mathbf{x} \cdot \mathbf{h}_2 = \ldots = \mathbf{x} \cdot \mathbf{h}_{n-k} = 0\}.$$

Kodų bazės

Sąlygas galime užrašyti tiesinėmis lygtimis. Jeigu dualaus poerdvio bazės žodžiai yra

$$\mathbf{h}_1 = h_{11}h_{12}\ldots h_{1n},\ \ldots,\ \mathbf{h}_{n-k} = h_{n-k,1}h_{n-k,2}\ldots h_{n-k,n},$$

tai poerdvis $\mathbb{L}$ yra sudarytas iš tų žodžių $\mathbf{x}$, kurių komponentės $x_1x_2\ldots x_n$ tenkina tokias lygybes:

$$\begin{aligned}
&h_{11}x_1 + h_{12}x_2 + \ldots + h_{1n}x_n = 0,\\
&h_{21}x_1 + h_{22}x_2 + \ldots + h_{2n}x_n = 0,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&h_{n-k,1}x_1 + h_{n-k,2}x_2 + \ldots + h_{n-k,n}x_n = 0.
\end{aligned}$$

Kodai su kontroliniu simboliu

Sudarykime matricą iš vienos eilutės:

$$H = (h_1\ h_2\ldots h_n), \quad h_j \in \mathbb{F}_p, \quad h_j \neq 0.$$

Ši matrica yra kontrolinė $[n, n-1]$ kodo $\mathbb{K}$ matrica. Kodui priklauso tie žodžiai $\mathbf{x} = x_1x_2\ldots x_n$, kurie tenkina lygybę

$$h_1x_1 + h_2x_2 + \ldots + h_nx_n = 0.$$

Kodai su kontroliniu simboliu

Kodavimas šiuo kodu – informacinių simbolių eilutės papildymas dar vienu (kontroliniu) simboliu:

$$x_1x_2\ldots x_{n-1} \mapsto x_1x_2\ldots x_{n-1}x_n,$$
$$x_n = -(h_1h_n^{-1}x_1 + \ldots + h_{n-1}h_n^{-1}x_{n-1}).$$

Minimalus kodo $\mathbb{K}$ atstumas yra $d = 2$, taigi jis negali ištaisyti nei vienos klaidos. Tačiau visada gali vieną klaidą aptikti!

Kodo, dualaus kodui su kontroliniu simboliu parametrus taip pat nesunku nustatyti. Jie tokie – $[n, 1, n]$.

Brūkšniniai kodai

Juodų ir baltų juostų seka užrašomi atitinkamos abėcėlės simboliai. Pavyzdžiui, knygų žymėjimo sistema ISBN – tai kodas su abėcėle

$$\mathcal{A} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X\},$$

čia X žymi skaičių 10. Informacija apie knygą užrašoma devyniais šios abėcėlės simboliais: pirmoji simbolių grupė žymi šalį, antroji – leidyklą, trečioji – knygą. Devynių simbolių žodis papildomas dešimtuoju – kontroliniu. Kontrolinė lygybė tokia:

$$X \cdot x_1 + 9 \cdot x_2 + 8 \cdot x_3 + 7 \cdot x_4 + 6 \cdot x_5 + \ldots + 2 \cdot x_9 + 1 \cdot x_{10} \equiv 0 \pmod{11}.$$

Pavyzdžiui, ISBN - 9986-16-180-0 yra knygos, išleistos Lietuvoje (9986 – Lietuvos kodas), „Tyto alba“ leidykloje (leidyklos kodas – 16).

EAN (European Article Numeration)

Abėcėlė:

$$\mathcal{A} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

Prekės žymimos trylikos skaitmenų kodu. Kontrolinė lygybė

$$1 \cdot x_1 + 3 \cdot x_2 + \ldots + 3 \cdot x_{12} + 1 \cdot x_{13} \equiv 0 \pmod{10}.$$

0.1 Hammingo kodų šeima

Hammingo kodas

Dvejetainis Hammingo kodas taiso vieną klaidą. Jo minimalus atstumas $d = 3$
Ieškosime daugiau tokių kodų.
Fiksuosime dar vieną ieškomų kodų parametrą – dualaus kodo dimensiją.

Ieškosime daugiausiai abėcėlės $\mathbb{F}_q$ žodžių turinčio tiesinio kodo, jeigu iš anksto duota jo dualaus kodo dimensija r ir minimalus atstumas $d = 3$.
Tokio kodo 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 $\alpha \in \mathbb{F}_q$.

Kontrolinės matricos sudarymas

Sudarysime H, imdami tiek stulpelių, kiek tik yra įmanoma.
Pasirinkime iš aibės $V_1 = \mathbb{F}_q^r$ nenulinį žodį $\mathbf{s}_1$ ir sudarykime iš jo elementų pirmąjį H stulpelį. Apibrėžkime aibę

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

Antrąjį H stulpelį sudarykime iš pasirinkto aibės V_2 žodžio elementų.

Kontrolinės matricos sudarymas

Bendra stulpelių pasirinkimo taisyklė tokia:

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

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

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

Kontrolinė matrica

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

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

tai iš viso galima parinkti $n = (q^r - 1)/(q-1)$ stulpelių.

Taigi matrica H yra kontrolinė tiesinio $[n, n-r, 3]$ kodo matrica.

Hammingo kodai

Apibrėžimas. Tegu $r \geq 1, \; n = (q^r - 1)/(q-1)$. Tiesinius $[n, n-r, 3]$ kodus iš $\mathbb{F}_q$ abėcėlės žodžių vadinsime Hammingo kodais ir žymėsime $\mathbb{H}_q(r)$.

Teorema. Hammingo kodai yra tobuli.

Dvejetainiai Hammingo kodai

Kodai $\mathbb{H}_2(r)$ yra geriausiai žinomi Hammingo kodai, $\mathbb{H}_2(3)$ – tai klasikinis mūsų nagrinėtas Hammingo kodas.

Kodų $\mathbb{H}_2(r)$ 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 $\mathbb{H}_2(r)$ matrica.
Pavyzdžiui, kontrolinė kodo $\mathbb{H}_2(3)$ matrica yra

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

Hammingo kodų dekodavimas

$\mathbb{H}_2(r)$ kodo kontrolinė matrica H, sudaryta aprašytuoju būdu.
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:

$$\mathbf{x}H^T = \mathbf{e}_i H^\top.$$

Sindromas $\mathbf{e}_i H^T$ sudarytas iš tų pačių simbolių kaip ir matricos H i-asis stulpelis.

Simplekso kodai

Kodai, dualūs Hammingo kodams vadinami, simplekso kodais.
Pažymėkime $\mathbb{S}_q(r) = \mathbb{H}_2(r)^\perp$.

Teorema. Simplekso kodų $\mathbb{S}_q(r)$ parametrai yra

$$\left[\frac{q^r - 1}{q - 1}, r, q^{r-1}\right].$$

Atstumas tarp bet kurių kodo $\mathbb{S}_q(r)$ žodžių lygus q^{r-1}.

Jeigu atstumas tarp bet kurių dviejų tam tikros aibės taškų yra pastovus, tai tokia aibė geometrijoje vadinama simpleksu.

Tikimybės

Tegu p yra simbolio iškraipymo tikimybė simetriniame kanale

$$P(\mathbb{S}_2(r) \text{ žodžio iškraipymai bus nepastebėti}) = (2^r - 1)p^{2^{r-1}}(1-p)^{2^{r-1}-1}.$$

Kodo $\mathbb{H}_2(r)$ žodžio teisingo dekodavimo tikimybė:

$$P(\mathbb{H}_2(r) \text{ žodis bus dekoduotas teisingai}) = (1-p)^{2^r-1} + (2^r - 1)p(1-p)^{2^r-2}.$$

Kodo žodžių svoriai

Hammingo kodo $\mathbb{H}_2(r)$ žodžių svorių skirstinys:

$$A_i = |\{\mathbf{c} \in \mathbb{H}_2(r) : w(\mathbf{c}) = i\}|, \quad i = 0, 1, \ldots, n.$$

Žinome, kad $A_0 = 1, A_1 = A_2 = 0$. Kitus dydžius galima skaičiuoti pasinaudojant rekurentiniu sąryšiu.

Teorema. Hammingo kodo $\mathbb{H}_2(r)$ dydžiai A_i tenkina rekurenčiąją lygybę

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

Kodo žodžių svoriai

Apibrėžimas. Tegu $\mathbb{C}$ yra n ilgio abėcėlės $\mathbb{F}_q$ žodžių kodas, $A_i = |\{\mathbf{c} \in \mathbb{C} : w(\mathbf{c}) = i\}|$. Funkciją

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

vadinsime kodo $\mathbb{C}$ svorių funkcija, o skaičių A_i seką – kodo svorių skirstiniu. Svorių pasiskirstymo funkciją galima ir taip užrašyti:

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

MacWilliams tapatybė

Teorema. Tegu $\mathbb{L}$ yra tiesinis abėcėlės $\mathbb{F}_q$ žodžių kodas, $\mathbb{L}^{\perp}$ jo dualus kodas. Tada abiejų kodų svorių pasiskirstymo funkcijas sieja tapatybė

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

Jei $q = 2$, tai tapatybė virsta tokia:

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