Kodavimo teorija

Vilius Stakėnas

2010 metų ruduo

Tiesiniai kodai **2**
Abėcėlės 3
Tiesinis kodas 4
Generuojanti matrica 5
Kodavimas tiesiniais kodais 6
Elementarieji pertvarkiai 7
Tiesinių kodų ekvivalentumas 8
Standartinio pavidalo matricos 9
Standartinio pavidalo matricos 10
Minimalus kodo atstumas 11
Kodo matricos 12
Kontrolinė kodo matrica 13
Tiesinių kodų dekodavimas 14
Tiesinių kodų dekodavimas 15
Kodo lentelė 16
Žodžio sindromas 17

Tiesiniai kodai

Abėcėlės

Nagrinėsime kodus, sudarytus iš specialios abėcėlės žodžių.

Ši abėcėlė tai algebrinis kūnas $\mathbb{F}_q$, čia $q = p^n$ – pirminio skaičiaus laipsnis. Atskiru ir svarbiausiu atveju – $q = 2$.

Žodžių aibė $\mathbb{F}_q^n$ yra n-matė tiesinė erdvė virš kūno $\mathbb{F}_q$.

Tiesinis kodas

Apibrėžimas. Kodą $\mathbb{L},\ \mathbb{L} \subset \mathbb{F}_q^n$, vadinsime tiesiniu, jei $\mathbb{L}$ yra tiesinis $\mathbb{F}_q^n$ poerdvis. Jei $\mathbb{L}$ dimensija lygi k, o minimalus atstumas d, tai kodą $\mathbb{L}$ 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 $q = 2$.

Generuojanti matrica

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

Tada

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

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

Kodavimas tiesiniais kodais

Atvaizdis

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

apibrėžia abipusiškai vienareikšmę erdvės $\mathbb{F}_q^k$ ir kodo $\mathbb{L}$ žodžių atitiktį.

Ši atitiktis - šaltinio informacijos, pateikiamos erdvės $\mathbb{F}_q^k$ žodžiais, kodavimas kodo $\mathbb{L}$ elementais.

Elementarieji pertvarkiai

Elementariaisiais matricos G pertvarkiais vadinsime šiuos veiksmus:

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

Tiesinių kodų ekvivalentumas

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

Standartinio pavidalo matricos

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

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

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

Standartinio pavidalo matricos

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

Minimalus kodo atstumas

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

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

Teorema. Tegu d yra tiesinio kodo $\mathbb{L}$ minimalus atstumas. Tada

$$d = \min\{w(\mathbf{x}) : \mathbf{x} \in \mathbb{L}, \mathbf{x} \neq 00 \dots 0\}.$$

Kodo matricos

Teorema. Jei A yra $k \times m$ matrica, tai

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

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

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

Kontrolinė kodo matrica

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

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

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

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

Tiesinių kodų dekodavimas

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

Tiesinių kodų dekodavimas

Informacija koduojama naudojant kodą $\mathbb{L}$. 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

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

Žodis $\mathbf{a} = \mathbf{x} - \mathbf{c}$ yra kurioje nors klasėje $\mathbf{L}_b$ – toje pat kaip $\mathbf{x}$. Dekoduojant reikia peržiūrėti klasę $\mathbb{L}_\mathbf{b}$, kurioje atsidūrė gautas žodis $\mathbf{x}$, rasti joje mažiausią svorį turintį elementą $\mathbf{a}$ ir dekoduoti taip:

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

Kodo lentelė

$$\begin{pmatrix} \mathbf{a}_0 & \mathbf{c}_1 & \mathbf{c}_2 & \dots & \mathbf{c}_N \\ \mathbf{a}_1 & \mathbf{a}_1 + \mathbf{c}_1 & \mathbf{a}_1 + \mathbf{c}_2 & \dots & \mathbf{a}_1 + \mathbf{c}_N \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_s & \mathbf{a}_s + \mathbf{c}_1 & \mathbf{a}_s + \mathbf{c}_2 & \dots & \mathbf{a}_s + \mathbf{c}_N \end{pmatrix}$$

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

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

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

Žodžio sindromas

Apibrėžimas. Tegu H yra kodo $\mathbb{L}$ kontrolinė matrica, $\mathbf{x} \in \mathbb{F}_q^n$. Žodžio **x** sindromu vadinsime $\mathbb{F}_q^n$ elementą

$$s(\mathbf{x}) = \mathbf{x}H^T.$$

$$\begin{pmatrix} Sindromai & \mathbf{s}_1 & \mathbf{s}_2 & \dots & \mathbf{s}_N \\ Lyderiai & \mathbf{a}_1 & \mathbf{a}_2 & \dots & \mathbf{a}_N. \end{pmatrix}$$

Dekodavimas: *randame gautojo žodžio sindromą.*
Sindromui rasti pakanka mokėti padauginti vektorių iš kontrolinės matricos.