Kodavimo teorija

Vilius Stakėnas

2010 metų ruduo

Maksimalaus atstumo kodai 2 / 17

Maksimalus kodas

Priminimas:

Apibrėžimas. Kodą $\mathbf{C}$ iš $\mathbb{F}_q^n$ žodžių, kurio minimalus atstumas d, vadinamas maksimaliu, jeigu nėra tą patį minimalų atstumą ir daugiau žodžių turinčio kodo $\mathbf{C}^* \subset \mathbb{F}_q^n$.

Maksimalaus kodo parametrai: $(n, A_q(n,d), d)$.

3 / 17

Singletono įvertis

Singletono įvertis pateikia viršutinį $A_q(n,d)$ rėžį:

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

4 / 17

Maksimalaus atstumo kodai

Tegu dabar $\mathbb{L}$ yra tiesinis $[n,k]$ kodas iš abėcėlės $\mathbb{F}_q$ žodžių; tada jo žodžių skaičius lygus q^k. Iš Singletono įverčio gauname

$$q^k \leq q^{n-d+1} \text{ arba } d \leq n-k+1.$$

Jeigu galioja lygybės, tai kodas $\mathbb{L}$ yra maksimalus.

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

Angliškoje literatūroje - Maximum distance separable, arba MDS kodas.

5 / 17

Maksimalaus atstumo kodai

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

Maksimalaus atstumo kodai

Teorema. Tegu $\mathbb{L}$ yra maksimalaus atstumo kodas. Tada ir $\mathbb{L}^{\perp}$ yra taip pat maksimalaus atstumo kodas.

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

Trivialūs maksimalaus atstumo kodai

Egzistuoja $[n, n, 1], [n, 1, n]$ ir $[n, n - 1, 2]$ kodai iš abėcėlės $\mathbb{F}_q$ žodžių. Visi jie yra maksimalaus atstumo kodai, juos vadinsime tiesiog **trivialiais**.

Maksimalaus atstumo kodai

Ištirsime netrivialių maksimalaus atstumo kodų egzistavimo sąlygas.

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

Įrodymas

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

Tegu $G = (I_k, A)$ yra šio kodo standartinio pavidalo generuojanti matrica.

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

Įrodymas

Kadangi yra maksimalaus atstumo kodas, tai bet kurie k matricos G stulpeliai sudaro tiesiškai nepriklausomą sistemą.
Todė nei vienas matricos A elementas nelygus nuliui.
Padauginę matricos A stulpelius iš atitinkamų nenulinių $\mathbb{F}_q$ elementų, galime pasiekti, kad gautoji matrica būtų tokia:

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

Kadangi $q \leq n - k$, tai antroje A' eilutėje bent du elementai bus vienodi.
Dauginkime antrąją G' eilutę iš $-a'_{21}$ ir pridėkime prie pirmosios. Gautoje eilutėje bus k nulių!

Maksimalaus atstumo kodų parametrai

Teorema. Jei $\mathbb{L}$ 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.

Vandermondo determinantas

Tegu $\alpha_1, \ldots, \alpha_s$ yra skirtingi ir nelygūs nuliui kūno $\mathbb{F}_q$ elementai. Sudarykime Vandermondo determinantą:

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

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

Reedo-Solomono kodai

Apibrėžimas. Tegu $\mathbb{F}_q = \{\alpha_1, \alpha_2, \ldots, \alpha_q\}$ (apibrėžtumo dėlei tarkime, $\alpha_q = 0$), o $1 \le k \le q$ yra natūralusis skaičius. Tiesinį kodą, kurio generuojanti matrica yra

$$G_k = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_q \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_q^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & \alpha_q^{k-1} \end{pmatrix},$$

vadinsime Reedo-Solomono kodu ir žymėsime $\mathbf{RS}_{q,k}$.

Reedo-Solomono kodai

Teorema. Visi $\mathbf{RS}_{q,k}$ kodai yra maksimalaus atstumo kodai.
Jei $1 \le k_1 < k_2 \le q$, tai $\mathbf{RS}_{q,k_1} \subset \mathbf{RS}_{q,k_2}$.
Su visomis k reikšmėmis teisinga lygybė $\mathbf{RS}_{q,k}^{\perp} = \mathbf{RS}_{q,q-k}$.

Reedo-Solomono kodai

Generuojančią kodo $\mathbf{RS}_{q,k}$ matricą G_k (paskutinį jos stulpelį sudaro elementai $1, 0, 0, \ldots, 0$) papildykime dar vienu stulpeliu:

$$G_k^* = \begin{pmatrix} 1 & 1 & \ldots & 1 & 0 \\ \alpha_1 & \alpha_2 & \ldots & 0 & 0 \\ \alpha_1^2 & \alpha_2^2 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & 0 & 1 \end{pmatrix}.$$

Reedo-Solomono kodai

Pasinaudoję Vandermondo determinantu, galime įsitikinti, kad bet kurie k stulpeliai yra tiesiškai nepriklausomi. Taigi G_k^* taip pat yra maksimalaus atstumo kodo generuojanti matrica.

Šio kodo parametrai yra $[q+1, k, q-k+2]$. Pažymėkime šį kodą $\mathbf{RS}^*_{q+1,k}$. Jeigu q yra nelyginis pirminis arba jo laipsnis, o $k = \frac{q+1}{2}$, galima įrodyti, kad

$$\mathbf{RS}^*_{q+1,k}{}^{\perp} = \mathbf{RS}^*_{q+1,k}.$$

Taigi radome dar vieną savidualių kodų šeimą.