Klaidas randantys ir taisantys kodai 1 / 20

2.1. Bendrosios sąvokos

$\mathcal{A}$ yra abėcėlė, $|\mathcal{A}| = q$. Žymėsime: $\mathcal{A} = \mathcal{A}_q,\ \mathcal{A}_q^n = \mathcal{A}_q \times \mathcal{A}_q \times \ldots \times \mathcal{A}_q$

Pagrindinis apibrėžimas

Apibrėžimas. (n, N) kodu iš abėcėlės $\mathcal{A}_q$ žodžių vadinamas bet koks poaibis $\mathbf{C} \subset \mathcal{A}_q^n$, čia $|\mathbf{C}| = N$.

2 / 20

Hammingo atstumas

Apibrėžimas. Tegu $\mathbf{x} = x_1 \ldots x_n,\ \mathbf{y} = y_1 \ldots y_n$ yra du aibės $\mathcal{A}_q^n$ žodžiai. Hamingo atstumu tarp $\mathbf{x}, \mathbf{y}$ vadinsime dydį

$$h(\mathbf{x}, \mathbf{y}) = \sum_{\substack{i=1,\ldots,n \\ x_i \neq y_i}} 1.$$

3 / 20

Hammingo atstumas yra atstumas

Teorema. Hamingo atstumas aibėje $\mathcal{A}_q^n$ turi šias savybes:

- $h(\mathbf{x}, \mathbf{x}) = 0,\ \mathbf{x} \in \mathcal{A}_q^n;$
- $h(\mathbf{x}, \mathbf{y}) = h(\mathbf{y}, \mathbf{x}),\ \mathbf{x}, \mathbf{y} \in \mathcal{A}_q^n;$
- $h(\mathbf{x}, \mathbf{y}) \leq h(\mathbf{x}, \mathbf{z}) + h(\mathbf{y}, \mathbf{z}),\ \mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathcal{A}_q^n.$

4 / 20

Minimalaus atstumo dekodavimo taisyklė

Apibrėžimas. Dekodavimo taisyklę $f : \mathcal{A}_q^n \to \mathbf{C}$ vadinsime minimalaus atstumo taisykle, jei su kiekvienu $\mathbf{d} \in \mathcal{A}_q^n$

$$h(\mathbf{d}, f(\mathbf{d})) = \min_{\mathbf{c} \in \mathbf{C}} h(\mathbf{d}, \mathbf{c}).$$

5 / 20

Minimalus kodo atstumas

Apibrėžimas. Kodo $\mathbf{C}$ minimaliu atstumu vadinsime dydį

$$d(\mathbf{C}) = \min_{\substack{\mathbf{c}, \mathbf{d} \in \mathbf{C} \\ \mathbf{c} \neq \mathbf{d}}} h(\mathbf{d}, \mathbf{c}).$$

Jei (n, N) kodo $\mathbf{C}$ minimalus atstumas yra d, tai kodą vadinsime (n, N, d) kodu.

6 / 20

Klaidas randantys kodai

Apibrėžimas. Kodą $\mathbf{C}$ vadinsime t klaidų randančiu kodu, jei bet kuriame kodo žodyje įvykus $m, m \leq t,$ iškraipymų, gautas rezultatas $\mathbf{d}$ jau nebėra kodo žodis, t. y. $\mathbf{d} \notin \mathbf{C}$.

Apibrėžimas. t klaidų randantį kodą vadinsime tiksliai t klaidų randančiu, jei jis nėra $t + 1$ klaidų randantis kodas.

7 / 20

Klaidas taisantys kodai

Apibrėžimas. Kodą $\mathbf{C}$ vadinsime t klaidų taisančiu kodu, jei siunčiamame žodyje įvykus $m, m \leq t$, iškraipymų ir dekoduojant pagal minimalaus atstumo taisyklę, dekoduojama bus visada teisingai.

Klaidų taisymas ir minimalus atstumas

Teorema. Kodas $\mathbf{C}$ yra tiksliai t klaidų taisantis kodas tada ir tik tada, kai $d(\mathbf{C}) = 2t + 1$ arba $d(\mathbf{C}) = 2t + 2$.

Išvada. *Bet koks* (n, N, d) *kodas taiso lygiai* $[(d-1)/2]$ *klaidų.*

Pavyzdžiai

1969 - 1973 NASA kosminis laivas Mariner 9 Marso fotografijoms siųsti naudojo Reedo–Mullerio kodą: žodžių ilgis 32 (6 informacijos bitai + 26 kontroliniai), 7 taisomos klaidos. Duomenų perdavimo greitis buvo 16,000 bitų per sekundę.

Kodai, naudojami įrašant CD taiso apie 4 tūkstančių klaidų pliūpsnius!

Kodo koeficientas

Apibrėžimas. Abėcėlės $\mathcal{A}_q$ (n, N) kodo $\mathbf{C}$ koeficientu vadinsime dydį

$$R(\mathbf{C}) = \frac{\log_q N}{n}.$$

Rutulys ir jo tūris

Jei $\mathbf{x} \in \mathcal{A}_q^n$, tai žymėsime

$$B_q(\mathbf{x}, r) = \{\mathbf{y} \in \mathcal{A}_q^n : h(\mathbf{x}, \mathbf{y}) \leq r\}.$$

Elementų skaičius rutulyje $B_q(\mathbf{x}, r)$ nepriklauso nuo jo centro $\mathbf{x}$, tad žymėsime

$$V_q(n, r) = |B_q(\mathbf{x}, r)|.$$

Teorema. Teisinga lygybė

$$V_q(n, r) = \sum_{0 \leq k \leq r} \binom{n}{k} (q-1)^k.$$

12 / 20

Kodo pakavimo spindulys

Apibrėžimas. Tegu $\mathbf{C}$ yra koks nors (n, N) kodas. Didžiausią sveikąjį skaičių t, kuriam

$$B_q(\mathbf{c}_1, t) \cap B_q(\mathbf{c}_2, t) = \emptyset, \quad jei \;\; \mathbf{c}_1, \mathbf{c}_2 \in \mathbf{C}, \quad \mathbf{c}_1 \neq \mathbf{c}_2,$$

vadinsime kodo $\mathbf{C}$ pakavimo spinduliu. Pakavimo spindulį žymėsime $r_p = r_p(\mathbf{C})$.

13 / 20

Kodo dengimo spindulys

Apibrėžimas. Mažiausią sveikąjį skaičių s, tenkinantį sąlygą

$$\mathcal{A}_q^n \subset \bigcup_{\mathbf{c} \in \mathbf{C}} B_q(\mathbf{c}, s),$$

vadinsime kodo dengimo spinduliu ir žymėsime
$r_d = r_d(\mathbf{C})$.

Teisinga nelygybė $r_p(\mathbf{C}) \leq r_d(\mathbf{C})$.
Pakavimo spindulys su minimaliu kodo atstumu susijęs taip:

$$r_p(\mathbf{C}) = [\frac{d-1}{2}]$$

14 / 20

Tobulieji kodai

Apibrėžimas. Kodą $\mathbf{C}$ vadinsime tobulu, jei

$$r_p(\mathbf{C}) = r_d(\mathbf{C}).$$

Teorema. (n, N, d) kodas $\mathbf{C}$ yra tobulas tada ir tik tada, kai $d = 2t + 1$ ir galioja lygybė

$$N \cdot V_q(n, t) = q^n.$$

15 / 20

Kokie tobulieji kodai egzistuoja?

Hammingo kodai
Tegu q yra pirminis skaičius. Egzistuoja abėcėlės $\mathcal{A}_q$ žodžių kodai su parametrais

$$\left(n, q^{n-r}, 3\right), \quad n = \frac{q^r - 1}{q - 1}, \quad r > 1,$$

ir jie yra tobuli.

16 / 20

Kokie tobulieji kodai egzistuoja?

Dvinariai Golay kodai
Egzistuoja abėcėlės $\mathcal{A}_2 = \{0, 1\}$ žodžių kodai su parametrais $(23, 2^{12}, 7)$ ir jie yra tobuli.

Trinariai Golay kodai
Egzistuoja abėcėlės $\mathcal{A}_3 = \{0, 1, 2\}$ žodžių kodai su parametrais $(11, 3^6, 5)$ ir jie yra tobuli.

Netrivialaus tobulo kodo parametrai sutampa arba su Hammingo kodo, arba su vieno iš Golay kodų parametrais.

17 / 20

Kodo pertvarkymai

Tegu $\mathbf{C}$ yra (n, N) kodas, o σ – n elementų perstata, t.y. injektyvus atvaizdis

$$\sigma \ : \ \{1, 2, \ldots, n\} \ \rightarrow \ \{1, 2, \ldots, n\}.$$

Juo apibrėšime injektyvų atvaizdį $\mathcal{A}_q^n \rightarrow \mathcal{A}_q^n$, kurį taip pat žymėsime σ. Jei $\mathbf{x} = x_1 \ldots x_n$, tai

$$\sigma(\mathbf{x}) = x_{\sigma(1)} \ldots x_{\sigma(n)}.$$

Iš kodo $\mathbf{C}$ šiuo atvaizdžiu gauname naują kodą

$$\sigma(\mathbf{C}) = \{\sigma(\mathbf{c}) : \mathbf{c} \in \mathbf{C}\}.$$

18 / 20

Kodo pertvarkymai

Tegu $\pi : \{1, 2, \ldots, q\} \to \{1, 2, \ldots, q\}$ yra kokia nors perstata, o abėcėlės $\mathcal{A}$ simboliai sunumeruoti:

$$\mathcal{A} = \{a_1, \ldots, a_q\}.$$

Galime π nagrinėti kaip atvaizdį $\mathcal{A} \to \mathcal{A}$, apibrėždami $\pi(a_i) = a_{\pi(i)}$.
Pasirinkime $i \leq n$, ir apibrėškime injektyvų atvaizdį $\langle \pi, i \rangle : \mathcal{A}_q^n \to \mathcal{A}_q^n$ šitaip:

$$\langle \pi, i \rangle (x_1 \ldots x_i \ldots x_n) = x_1 \ldots \pi(x_i) \ldots \ x_n.$$

Kodą, kurį gauname iš $\mathbf{C}$ imdami žodžius $\langle \pi, i \rangle (\mathbf{c})$, $\mathbf{c} \in \mathbf{C}$, žymėsime $\langle \pi, i \rangle (\mathbf{C})$.

19 / 20

Ekvivalentieji kodai

Apibrėžimas. Du (n, N) kodus $\mathbf{C}, \mathbf{C}'$ vadinsime ekvivalenčiais, jei egzistuoja n elementų perstata σ ir q elementų perstatos $\pi_1, \ldots, \pi_n$, kad

$$\mathbf{C}' = \langle \pi_1, 1 \rangle (\ldots (\langle \pi_n, n \rangle (\sigma(\mathbf{C}))) \ldots).$$

Apibrėžimas. Jei kodai $\mathbf{C}, \mathbf{C}'$ ekvivalentūs, tai $d(\mathbf{C}) = d(\mathbf{C}')$.

20 / 20