Klaidas taisantys kodai

Hamingo atstumas

$\mathcal{A}_q$ - abėcėlė sudaryta iš q simbolių. ($|\mathcal{A}_q| = q$)
$\mathcal{A}_q^n$ - abėcėlės $\mathcal{A}_q$ ilgio n žodžių aibė. ($|\mathcal{A}_q^n| = q^n$)
Hamingo atstumas tarp dviejų aibės $\mathcal{A}_q^n$ elementų
$\mathbf{x} = x_1 \dots x_n$ ir $\mathbf{y} = y_1 \dots y_n$ yra

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

Hamingo atstumas aibėje $\mathcal{A}_q^n$ tenkina visas metrikos savybes:

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

Kodas ir jo minimalus atstumas

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

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

vadinsime kodo $\mathbf{C}$ *koeficientu.*

Kodas ir jo minimalus atstumas

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

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

vadinsime kodo $\mathbf{C}$ *koeficientu.*

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

$$d(\mathbf{C}) = \min_{\substack{\mathbf{x},\mathbf{y} \in \mathbf{C} \\ \mathbf{x} \neq \mathbf{y}}} d_H(\mathbf{x}, \mathbf{y}) \, .$$

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

Hamingo kodai

Tegu $q = 2,\ \mathcal{A}_q = \{0, 1\}$. Kiekvienas 4 bitų pranešimas koduojamas prijungiant 3 kontrolinius bitus. Gaunamas binarinis kodas, kurio koeficientas $R = 4/7$, minimalus atstumas $d = 3$. Hamingo kodas yra $(7, 16, 3)$ kodas, taisantis vieną klaidą.
Pavyzdys. Koduojamas pranešimas 1011 rašomas 3, 5, 6 ir 7 bituose. 1, 2 ir 4 yra kontroliniai bitai.

Kodavimas							
	1	2	3	4	5	6	7
Tekstas			1		0	1	1
Kodas	0	1	1	0	0	1	1
Klaida			x				
Gauta	0	1	0	0	0	1	1

Dekodavimas
Kontrolinės sumos
(**1): $\varepsilon_1 + \varepsilon_3 + \varepsilon_5 + \varepsilon_7 =$1
(*1*): $\varepsilon_2 + \varepsilon_3 + \varepsilon_6 + \varepsilon_7 =$1
(1**): $\varepsilon_4 + \varepsilon_5 + \varepsilon_6 + \varepsilon_7 =$0
Klaidos adresas: 011=3

Analogiškai konstruojami Hamingo kodai $(n, 2^{n-r}, 3)$, kai $n = 2^r - 1,\ r \geq 2$.

Klaidų radimas

Klaidų paieškai ir jų taisymui naudojama minimalaus atstumo dekodavimo taisyklė.

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.*

Teorema. (n, N, d) *kodas* $\mathbf{C}$ *yra tiksliai* t *klaidų randantis kodas tada ir tik tada, kai* $d = t + 1$.

Klaidų taisymas

Apibrėžimas. *Kodą* $\mathbf{C}$ *vadinsime* t *klaidų taisančiu kodu, jei siunčiamame žodyje įvykus* $m, \ m \leq t$, *iškraipymų ir dekoduojant pagal minimalaus atstumo taisyklę, visada bus dekoduojama teisingai. Tokį kodą vadinsime tiksliai* t *klaidų taisančiu kodu, jeigu jis ne visada taiso* $t+1$ *klaidų.*

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*

$$\left[\frac{d-1}{2}\right]$$

klaidų.

Pavyzdys. Hamingo kodas visada taiso 1 klaidą. Todėl $d \geq 3$. Bet $d_H(0000000, 1000011) = 3$.
Taigi Hamingo kodo parametrai yra $(7, 16, 3)$.

Kodo geometrija

Apibrėžimas. *Žodžių aibės $\mathcal{A}_q^n$ spindulio $r \geq 0$ rutuliu su centru $\mathbf{x} \in \mathcal{A}_q^n$ vadinsime aibę*

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

Šios aibės elementų skaičių vadinsime rutulio tūriu.

Rutulio tūris nepriklauso nuo centro, bet priklauso nuo kodo ilgio:

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

Kodo geometrija

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

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

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

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 d susijęs taip: $r_p(\mathbf{C}) = [(d-1)/2]$.

Tobulieji kodai

Skirtumas $r_d(\mathbf{C}) - r_p(\mathbf{C})$ gali būti didelis. Pavyzdys: $(n, 2)$ kodui $\mathbf{C} = \{000\ldots00, 000\ldots11\}$ $r_p(\mathbf{C}) = 0, r_d(\mathbf{C}) = n - 1.$

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 $NV_q(n, t) = q^n$.*

Įrodymas. Jei (n, N, d) kodas $\mathbf{C}$ tobulas, tai $d(\mathbf{C}) = 2t + 1,\ r_p(\mathbf{C}) = t$. Kodas $\mathbf{C}$ tobulas tada ir tik tada, kai

$$\bigcup_{\mathbf{c}\in\mathbf{C}} B_q(\mathbf{c}, t) = \mathcal{A}_q^n\ .$$

Rutuliai $B_q(\mathbf{c}, t),\ \mathbf{c} \in \mathbf{C}$, nesikerta. Todėl pastarasis sąryšis ekvivalentus lygybei $NV_q(n, t) = q^n$.

$\square$

Trivialūs tobulieji kodai

- Kodas, sudarytas iš vieno aibės $\mathcal{A}_q^n$ žodžio.
- Kodas, sudarytas iš visų aibės $\mathcal{A}_q^n$ žodžių.
- Dvejetainis $(q = 2)$ pakartojimo kodas su nelyginio ilgio žodžiais: $\{00...0,\ 11...1\}$.

Netrivialūs tobulieji kodai

- Dvejetainis kodas $(q = 2)$ su parametrais $(23, 2^{12}, 7)$ būtų tobulas. Tokie kodai egzistuoja. Vienas jų - dvejetainis Golay kodas.
- Trejetainis kodas $(q = 3)$ su parametrais $(11, 3^6, 5)$ būtų tobulas. Pavyzdžiui - trejetainis Golay kodas.
- Kai q yra pirminio skaičiaus laipsnis, kodas su parametrais $(n, N, 3)$,

$$n = \frac{q^m - 1}{q - 1}, \quad N = q^{n-m}, \; m \geq 2,$$

būtų tobulas. Tokie kodai egzistuoja - tai Hamingo kodų šeima.

Pastaba. Kai q yra pirminio skaičiaus laipsnis, daugiau tobulų kodų nėra.

Maksimalūs kodai

$A_q(n,d) = \max\{N :$ egzistuoja (n,N,d) kodas $\mathbf{C} \subset \mathcal{A}_q^n\}$.
Kodus su parametrais $(n, A_q(n,d), d)$ vadinsime **maksimaliais**. Jie pasižymi tuo, kad nė vieno n ilgio žodžio negalima pridėti prie tokio kodo, nesumažinant minimalaus kodo atstumo.

Teorema. *Bet kokiems* $q \geq 1, n \geq 1, d \geq 1$ *teisingi sąryšiai*

1) $A_q(n,1) = q^n, \quad A_q(n,n) = q\,,$

2) $A_q(n,d) \leq A_q(n+1,d) \leq qA_q(n,d).$

Maksimalių kodų dydžio įverčiai

Tegu $q > 1, \ n \geq 1, \ 1 \leq d \leq n$.

Maksimalių kodų dydžio įverčiai

Tegu $q > 1,\ n \geq 1,\ 1 \leq d \leq n$.

1. Sigletono įvertis:

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

Maksimalių kodų dydžio įverčiai

Tegu $q > 1,\ n \geq 1,\ 1 \leq d \leq n$.

1. Sigletono įvertis:

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

2. Hamingo įvertis:

$$A_q(n, d) \leq q^n \left(\sum_{0 \leq k \leq t} \binom{n}{k} (q-1)^k \right)^{-1}, \ t = \left[\frac{d-1}{2} \right].$$

Maksimalių kodų dydžio įverčiai

Tegu $q > 1,\ n \geq 1,\ 1 \leq d \leq n$.

1. Sigletono įvertis:

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

2. Hamingo įvertis:

$$A_q(n,d) \leq q^n \left(\sum_{0 \leq k \leq t} \binom{n}{k} (q-1)^k \right)^{-1}, \ t = \left[\frac{d-1}{2} \right].$$

3. Gilberto-Varšamovo įvertis:

$$A_q(n,d) \geq q^n \left(\sum_{0 \leq k \leq d-1} \binom{n}{k} (q-1)^k \right)^{-1}.$$

Ekvivalentūs kodai

Tegu $\mathbf{C} \subset \mathcal{A}_q^n$ yra (n, N) kodas, o σ – n elementų perstata, t.y. injektyvus atvaizdis
$\sigma \ : \ \{1, 2, \ldots, n\} \ \to \ \{1, 2, \ldots, n\}.$
Jei $\mathbf{x} = x_1 \ldots x_n \in \mathcal{A}_q^n$, tai
$\sigma(\mathbf{x}) = x_{\sigma(1)} \ldots x_{\sigma(n)}, \quad \sigma(\mathbf{C}) = \{\sigma(\mathbf{c}) : \mathbf{c} \in \mathbf{C}\}.$
Tegu $\pi : \{1, 2, \ldots, q\} \to \{1, 2, \ldots, q\}$ yra kokia nors perstata.
Jei $\mathcal{A}_q = \{a_1, \ldots, a_q\}$, tai $\pi(a_i) = a_{\pi(i)}$ ir

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

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

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