Kodavimo teorija

Vilius Stakėnas

2010 metų ruduo

Maksimalūs kodai

Apibrėžimas. Pažymėkime

$$A_q(n,d) = \max\{N : egzistuoja\ (n,N,d)\ kodas\ \mathbf{C} \subset \mathcal{A}_q^n\}.$$

Kodus su parametrais $(n, A_q(n,d), d)$ vadinsime maksimaliais.
Bet kokiems $q \geq 1, n \geq 1$,

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

3 / 14

Įverčiai

Teorema. Teisingos nelygybės

$$A_q(n,d) \leq A_q(n-1,d-1), \quad (n \geq 2, d \leq n),$$
$$A_q(n,d) \leq qA_q(n-1,d), \quad (n \geq 2,\ 1 \leq d \leq n-1).$$

Teisingos lygybės

$$A_2(n,2l-1) = A_2(n+1,2l), \quad A_2(n,2) = 2^{n-1}.$$

4 / 14

Hammingo įvertis

Teorema. Bet kokiems $n \geq 1,\ q > 1,\ n \geq d \geq 1$, teisingas įvertis

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

5 / 14

Gilberto įvertis

Teorema. Bet kokiam $n \geq 1,\ q > 1,\ d \geq 1,$

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

6 / 14

Singletono įvertis

Teorema. Bet kokiems $n \geq 1,\ q > 1,\ n \geq d \geq 1,$ teisingas įvertis

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

7 / 14

Kiek simbolių reikia pridėti, kad kodas taisytų t klaidų?

l – koduojamo žodžio ilgis
n – kodo žodžio ilgis
$r = n - l$ – pridedamų simbolių kiekis

$$\log_q V_q(n,t) \leq r \leq 1 + \log_q V_q(n,2t)$$

8 / 14

Klaidingo dekodavimo tikimybė

Jei kanalas yra skirtas dvejetainės abėcėlės simboliams siųsti, neturi atminties ir iškraipo simbolį su tikimybe p, tai iškraipytas dvejetainio kodo su parametrais $(n, N, 2t+1)$ žodis bus dekoduotas klaidingai su tikimybe

$$p_{klaidos} = 1 - \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}.$$

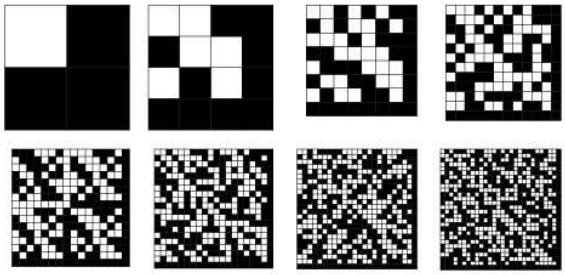
9 / 14

Hadamardo matricos

Apibrėžimas. n-tos eilės kvadratinė matrica $H_n = (h_{ij})$ vadinama Hadamardo matrica, jei

$$h_{ij} = \pm 1, \quad H_n \cdot H_n^\top = nI_n,$$

čia $H_n^\top$ žymi transponuotą matricą, I_n – vienetinę.



Kroneckerio sandauga

Apibrėžimas. Tegu $A = (a_{ij})$ yra $n \times n$, $B = (b_{ij})$, $m \times m$ matricos. Jų Kroneckerio sandauga vadinama $nm \times nm$ matrica

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1m}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{11}B & a_{12}B & \dots & a_{1m}B \end{pmatrix}$$

Teorema. Jei A, B yra Hadamardo matricos, tai $A \otimes B$ irgi Hadamardo matrica.

Normalinės Hadamardo matricos

Teorema. Sukeitus Hadamardo matricos dvi eilutes (stulpelius) vietomis gautoji matrica vėl yra Hadamardo matrica. Padauginus Hadamardo matricos eilutę (stulpelį) iš -1, gaunama Hadamardo matrica.

Apibrėžimas. n-tos eilės Hadamardo matrica $H_n = (h_{ij})$ vadinama normaline, jei visiems j teisinga lygybė

$$h_{1j} = h_{j1} = 1.$$

Teorema. Keičiant atitinkamas eilutes (stulpelius) vietomis bei dauginant eilutes (stulpelius) iš -1 kiekvieną Hadamardo matricą galima suvesti į normalinę matricą.

Hadamardo matricų egzistavimas

Teorema. Jei H_n yra Hadamardo matrica, tai $n = 1, 2$ arba n dalijasi iš 4.

Teorema. Jei q yra pirminis skaičius ir $q \equiv 3 \bmod 4$, tai egzistuoja $q + 1$-os eilės Hadamardo matrica.

Hadamardo kodas

Apibrėžimas. Tegu H_n yra Hadamardo matrica, M_n, M_n' - matricos, gautos iš H_n ir $-H_n$ pakeitus elementus -1 į 0. Hadamardo kodu $\mathcal{H}_n$ vadinsime dvejetainės abėcėlės kodą, kurį sudaro žodžiai, sudaryti iš M_n, M_n' eilučių.

Teorema. Hadamardo kodo $\mathcal{H}_n$ parametrai - $(n, 2n, n/2)$.