

Veiksmai su kodais

2010 m. ruduo

Kodo plėtinys	2
Kodo plėtinys	3
Sumažinimas ir sutrumpinimas	4
Kodo sumažinimas ir sutrumpinimas	5
Tiesioginė kodų suma	6
$u u + v$ konstrukcija	7
$u u + v$ konstrukcija	8
$u u + v$ konstrukcija	9
$u u + v$ konstrukcija ir Reedo-Mullerio kodai	10
Liekanų kodas	11
Liekanų kodo minimalus atstumas	12
Liekanų kodo minimalus atstumas	13
Liekanų kodo minimalus atstumas	14

Kodo plėtinys

Apibrėžimas. Tegu \mathbb{L} yra tiesinis kodas. Jo plėtiniu (*extended code*) vadinsime kodą

$$\mathbb{L}^* = \{c_1 \dots c_n c_{n+1} : c_1 \dots c_n \in \mathbb{L}, c_1 + c_2 + \dots + c_n + c_{n+1} = 0\}.$$

2 / 14

Kodo plėtinys

Jeigu tiesinio kodo \mathbb{L} kontrolinė matrica yra

$$H = \begin{pmatrix} h_{11} & h_{12} & h_{13} & \dots & h_{1n} \\ h_{21} & h_{22} & h_{23} & \dots & h_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{r1} & h_{r2} & h_{r3} & \dots & h_{rn} \end{pmatrix},$$

tai jo plėtinio \mathbb{L}^* kontrolinė matrica yra

$$H^* = \begin{pmatrix} h_{11} & h_{12} & h_{13} & \dots & h_{1n} & 0 \\ h_{21} & h_{22} & h_{23} & \dots & h_{2n} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ h_{r1} & h_{r2} & h_{r3} & \dots & h_{rn} & 0 \\ 1 & 1 & 1 & \dots & 1 & 1 \end{pmatrix}.$$

3 / 14

Sumažinimas ir sutrumpinimas

Apibrėžimas. Kodą, kuris gaunamas iš kodo C , išbraukiant visų jo žodžių i -ąjį simbolį, vadinsime sutrumpintu C kodu.

Kodą, kuris gaunamas iš C surinkus jo žodžius, turinčius tą patį i -ąjį simbolį ir jį išbraukus, vadinsime sumažintu C kodu.

4 / 14

Kodo sumažinimas ir sutrumpinimas

Teorema. Jeigu C yra tiesinis $[n, k, d]$ kodas tai ir sutrumpintas kodas yra tiesinis. Jeigu $d > 1$, tai sutrumpinto kodo parametrai yra $[n - 1, k, d^*]$, $d^* \geq d - 1$.

Teorema. Tegu C yra tiesinis kodas ir ne visų jo žodžių i -osios komponentės yra nulinės. Jeigu C sumažinamas surinkus visus kodo žodžius, turinčius nulinę i -ąją komponentę ir ją išbraukiant, tai sumažintas kodas yra tiesinis, o jo parametrai $[n - 1, k - 1, d^*]$, $d^* \geq d$.

5 / 14

Tiesioginė kodų suma

Jeigu jungtume kodų $\mathbb{L}_1, \mathbb{L}_2$ su parametrais $[n_1, k_1, d_1], [n_2, k_2, d_2]$ žodžius, gautume kodą su parametrais $[n_1 + n_2, k_1 + k_2, \min(d_1, d_2)]$.

6 / 14

$u|u + v$ konstrukcija

Apibrėžimas. Tegu $\mathbb{L}_1, \mathbb{L}_2$ yra du tiesiniai kodai iš tos pačios abėcėlės to paties ilgio žodžių. Kodu $\mathbb{L}_1|\mathbb{L}_2$ vadinsime tiesinį kodą

$$\mathbb{L}_1|\mathbb{L}_2 = \{\mathbf{x}|\mathbf{x} + \mathbf{y} : \mathbf{x} \in \mathbb{L}_1, \mathbf{y} \in \mathbb{L}_2\}.$$

7 / 14

$u|u + v$ konstrukcija

Teorema. Jei $\mathbb{L}_1, \mathbb{L}_2$ yra du tiesiniai kodai iš aibės \mathbb{F}_q^n žodžių, d_1, d_2 – jų minimalūs atstumai, tai kodo $\mathbb{L}_1|\mathbb{L}_2$ dimensija lygi kodų $\mathbb{L}_1, \mathbb{L}_2$ dimensijų sumai, o minimalus atstumas yra $d = \min(2d_1, d_2)$.

8 / 14

$u|u + v$ konstrukcija

Teorema. Tegu $\mathbb{L}_1, \mathbb{L}_2$ yra du tiesiniai kodai iš aibės \mathbb{F}_q^n žodžių, G_1, G_2 – jų generuojančios, H_1, H_2 – kontrolinės matricos. Tada kodo $\mathbb{L}_1|\mathbb{L}_2$ generuojanti ir kontrolinė matricos yra

$$G = \begin{pmatrix} G_1 & G_2 \\ O & G_2 \end{pmatrix}, \quad H = \begin{pmatrix} H_1 & O \\ -H_2 & H_2 \end{pmatrix},$$

čia O yra nulinė matrica.

9 / 14

$u|u + v$ konstrukcija ir Reedo-Mullerio kodai

Teorema. Reedo-Mullerio kodams teisingi sąryšiai

$$\mathbf{RM}(m+1, r) = \mathbf{RM}(m, r) | \mathbf{RM}(m, r-1).$$

10 / 14

Liekanų kodas

Apibrėžimas. Tegu \mathbb{L} yra dvinaris $[n, k, d]$ kodas, kurio generuojanti matrica yra

$$G = \left(\begin{array}{cccc|ccc} 1 & 1 & \dots & 1 & 0 & \dots & 0 \\ & & & G_1 & & & G_2 \end{array} \right),$$

čia pirmieji d pirmosios eilutės elementai lygūs vienetui. Tiesinis kodas $[n-d, k-1]$, kurio generuojanti matrica yra G_2 , vadinamas liekanų kodu (*residual code*).

11 / 14

Liekanų kodo minimalus atstumas

Teorema. Tegu \mathbb{L} yra dvinaris $[n, k, d]$ tiesinis kodas. Tada jo liekanų kodo minimalus atstumas d' tenkina nelygybę $d' \geq d/2$.

12 / 14

Liekanų kodo minimalus atstumas

Irodymas.

Tegu x yra liekanų kodo žodis, tada x yra tam tikra matricos G_2 eilučių tiesinė kombinacija. Jei y yra analogiška matricos G_1 eilučių kombinacija, tai $y|x \in \mathbb{L}$. Tada

$$y'|x = y|x + 11 \dots 1|00\dots 0 \in \mathbb{L}.$$

Taigi $y|x, y'|x \in \mathbb{L}$ ir

$$\begin{aligned} w(y|x) &= w(y) + w(x) \geq d, \\ w(y'|x) &= w(y') + w(x) \geq d. \end{aligned}$$

13 / 14

Liekanų kodo minimalus atstumas

Tačiau arba $w(y) \geq d/2$ arba $w(y') \geq d/2$. Iš bet kurios iš šių nelygybių išplaukia, kad kodo \mathbf{L}' žodžiui x teisinga nelygybė $w(x) \geq d/2$. Kadangi ši nelygybė teisinga bet kokiam kodo žodžiui, tai turi būti teisinga ir minimaliam atstumui $d' \geq d/2$.

14 / 14