# Reedo-Solomono ir BCH kodai

2010

## Reedo-Solomono kodai

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

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

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



## Apibendrintieji Reedo-Solomono kodai

**Apibrėžimas.** Tegu $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ yra žodis sudarytas tik iš nenulinių $\mathbb{F}_q$ elementų, o $\mathbf{a} = (\beta_1, \beta_2, \ldots, \beta_n)$ – būtinai iš skirtingų šio kūno elementų. Kodą, kurio generuojanti matrica yra

$$\begin{pmatrix} v_1 & v_2 & \ldots & v_n \\ v_1\beta_1 & v_2\beta_2 & \ldots & v_n\beta_n \\ v_1\beta_1^2 & v_2\beta_2^2 & \ldots & v_n\beta_n^2 \\ \ldots & \ldots & \ddots & \vdots \\ v_1\beta_1^{k-1} & v_2\beta_2^{k-1} & \ldots & v_n\beta_n^{k-1} \end{pmatrix}$$

vadinsime apibendrintuoju Reedo-Solomono kodu ir žymėsime $\mathbf{RS}_{n,k}(\mathbf{v}, \mathbf{a})$.



## Apibendrintieji Reedo-Solomono kodai

Jeigu $k_1 \leq k_2$, tai $\mathbf{RS}_{n,k_1}(\mathbf{v}, \mathbf{a}) \subset \mathbf{RS}_{n,k_2}(\mathbf{v}, \mathbf{a})$.

**Teorema.** Kodo $\mathbf{RS}_{n,k}(\mathbf{v}, \mathbf{a})$ $(1 \leq k \leq n)$ parametrai yra

$$[n, k, n-k+1].$$

## Atskiras atvejis

Pasirinkime skaičių $n$, kuris dalija $q-1$ ir kūne $\mathbb{F}_q$ pasirinkime elementą $\beta$, kurio eilė yra $n$.

Sudarykime rinkinį $\mathbf{a}$ taip:

$$\mathbf{a} = (1, \beta, \beta^2, \ldots, \beta^{n-1}).$$

ir imkime

$$\mathbf{v} = \mathbf{a}_0 = (1^0, \beta^0, (\beta^2)^0, \ldots, (\beta^{n-1})^0) = (1, 1, \ldots, 1).$$

Dabar galime sudaryti Reedo-Solomono kodą $\mathbf{RS}_{n,k}(\mathbf{a}_0, \mathbf{a})$.



## Ciklinis kodas

**Teorema.** Jeigu $\beta \in \mathbb{F}_q$ yra $n$-os eilės kūno elementas,

$$\mathbf{a} = (1, \beta, \beta^2, \ldots, \beta^{n-1}), \quad \mathbf{a}_0 = (1, 1, \ldots, 1),$$

tai kodas $\mathbf{RS}_{n,k}(\mathbf{a}_0, \mathbf{a})$ yra ciklinis, o vienas iš jo generuojančių daugianarių yra

$$g(x) = (x-\beta)(x-\beta^2)\ldots(x-\beta^{n-k})$$



## Bendresnis teiginys

Teoremą galima suformuluoti ir kiek bendriau. Jei pažymėsime

$$\mathbf{a}_m = (1^m, \beta^m, (\beta^2)^m, \ldots, (\beta^{n-1})^m),$$

tai $\mathbf{RS}_{n,k}(\mathbf{a}_m, \mathbf{a})$ kodas irgi bus ciklinis, o jo generatorius – daugianaris

$$g(x) = (x-\beta^{1-m})(x-\beta^{2-m})\ldots(x-\beta^{n-k-m}).$$

## Nauja idėja

Tarkime sukonstravome kokį nors tiesinį $[n, k, d]$ kodą $\mathbf{L} \subset \mathbb{F}_q^n$ $(q = p^m)$. Kadangi $\mathbb{F}_p^n \subset \mathbb{F}_q^n$, tai galime sudaryti sankirtą $\mathbf{L}^* = \mathbf{L} \cap \mathbb{F}_p^n$.

Aibė $\mathbf{L}^*$ netuščia (nulinis žodis jai tikrai priklauso), ji sudaro $\mathbb{F}_p^n$ tiesinį poerdvį.

Taigi $\mathbf{L}^*$ yra tiesinis kodas iš abėcėlės $\mathbb{F}_p$ žodžių.

Žinios apie jo parametrus: tai $[n, k^*, d^*]$ kodas, čia $k^* \leq k$, $d^* \geq d$.



## BCH kodai

**Apibrėžimas.** Tegu $n$ yra skaičiaus $q - 1$ $(q = p^m)$ daliklis, $\beta \in \mathbb{F}_q$ yra $n$-os eilės elementas, $1 \leq k \leq n$, $t = n - k + 1$,

$$\mathbf{a}_0 = (1, 1, \ldots, 1), \quad \mathbf{a}_1 = (1, \beta, \beta^2, \ldots, \beta^{n-1}),$$

Kodą $\mathbf{L} = \mathbb{F}_p^n \cap \mathbf{RS}_{n,k}(\mathbf{a}_0, \mathbf{a}_1)$ vadinsime BCH kodu su numatytuoju minimaliuoju atstumu $t$.



## Kaip BCH kodus nusakyti tiesiogiai?

Tegu $\mathbf{L} \subset \mathbb{F}_p^n$ yra BCH kodas, gautas iš kodo $\mathbf{RS}_{n,k}(\mathbf{a}_0, \mathbf{a}_1) \subset \mathbb{F}_q^n$. Tegu $\beta$ yra Reedo-Solomono kodui konstravimui panaudotas $n$-osios eilės elementas. Tada Reedo-Solomono kodo generatorius yra

$$g(x) = (x - \beta)(x - \beta^2) \ldots (x - \beta^{t-1}), \quad t = n - k + 1.$$

Visi Reedo-Solomono kodo žodžiai, interpretuojami kaip daugianariai, dalijasi iš $g(x)$, kitaip tariant – elementai $\beta, \beta^2, \ldots, \beta^{t-1}$ yra jų šaknys.

## Kaip BCH kodus nusakyti tiesiogiai?

Kodo $\mathbb{L}$ žodžius irgi galime interpretuoti kaip daugianarius, tačiau su koeficientais iš $\mathbb{F}_p$. Taigi tie patys elementai yra ir jų šaknys.

Jeigu elementas $\beta \in \mathbb{F}_q$ yra daugianario $f(x) \in \mathbb{F}_p[x]$ šaknis, tai $f(x)$ turi dalytis iš elemento $\beta$ minimalaus daugianario.

Taigi bet kuris BCH kodo žodis, interpretuojamas kaip daugianaris su koeficientais iš $\mathbb{F}_p$ dalijasi iš minimaliųjų daugianarių

$$m_\beta(x),\ m_{\beta^2}(x),\ \ldots,\ m_{\beta^{t-1}}(x).$$



## Kitas būdas apibrėžti BCH kodus

**Teorema.** BCH kodas $\mathbb{L} \subset \mathbb{F}_p^n$ su numatytuoju atstumu $t$ yra ciklinis kodas, kurio generatorius yra mažiausias bendras minimaliųjų daugianarių

$$m_\beta(x),\ m_{\beta^2}(x),\ \ldots,\ m_{\beta^{t-1}}(x)$$

kartotinis; čia $\beta$ yra $n$-os eilės elementas, kurį galime rasti plėtinyje $\mathbb{F}_{p^k}$, tokiame, kad $p^k - 1$ dalijasi iš $n$.



## Pavyzdys

Sukonstruokime BCH kodą $\mathbf{L} \subset \mathbb{F}_3^{13}$ su numatytuoju atstumu $t = 3$.

$n = 13$, kokiame kūne rasime $n$-os eilės elementą? Kadangi iš $13$ dalijasi $q - 1 = 3^3 - 1$, tai reiks plėtinio $\mathbb{F}_{3^3}$.

Geriausia jo konstrukcijai panaudoti primityvųjį trečios eilės daugianarį

$$f(x) = x^3 - x + 1.$$

Taigi galime laikyti, kad $\alpha$ yra primityvusis elementas ir skaičiuoti naudodamiesi sąryšiu $\alpha^3 = \alpha - 1$.

## Pavyzdys

Reikalingas $n$-osios eilės elementas bus tiesiog $\beta = \alpha^2$, o elementai, kurių minimaliuosius daugianarius teks skaičiuoti bus:

$$\beta_1 = \beta = \alpha^2, \quad \beta_2 = \beta^2 = \alpha^4 = \alpha^2 - \alpha.$$



## Pavyzdys

Apskaičiuosime minimalųjį daugianarį $m_{\beta_1}(x)$. Elemento $\beta_1$ eilė yra $13$, todėl reikia surasti mažiausiąjį $m$, kad $3^m \equiv 1 \pmod{13}$. Aišku, $m = 3$.

Galime užrašyti pirmojo elemento minimalųjį daugianarį:

$$m_{\beta_1}(x) = (x - \beta_1)(x - \beta_1^{3^1})(x - \beta_1^{3^2}) = (x - \alpha^2)(x - \alpha^6)(x - \alpha^{18}).$$



## Pavyzdys

Elemento $\beta_2$ eilė irgi tokia pati, taigi

$$m_{\beta_2}(x) = (x - \beta_2)(x - \beta_2^{3^1})(x - \beta_2^{3^2}) = (x - \alpha^4)(x - \alpha^{12})(x - \alpha^{36}),$$

$$\alpha^{36} = \alpha^{10}.$$



## Pavyzdys

Matome, kad bendrų daugiklių daugianariai neturi, taigi BCH kodo generuojantis daugianaris bus

$$g(x) = m_{\beta_1}(x) m_{\beta_2}(x).$$

Belieka sudauginti minimaliuosius daugianarius:

$$m_{\beta_1}(x) = x^3 + x^2 + x + 2, \quad m_{\beta_2}(x) = x^3 + x^2 + 2.$$

Taigi mūsų sukonstruoto kodo dimensija $k = n - \deg(g) = 7$.