5 GRS a alternantní kódy

Ať F je komutativní těleso. Označme $\triangle(v_1, \ldots, v_n)$, kde $v_i \in F$, $1 \leq i \leq n$, diagonální matici $D = (d_{ij})$ řádu n, ve které $d_{ij} = 0$ pro $i \neq j$ a $d_{ii} = v_i$. Předpokládejme, že všechna v_i, $1 \leq i \leq n$, jsou nenulová. Je-li G generující matice kódu C nad $F = \mathbb{F}_q$ a H je jeho prověrková matice, budou GD a HD^{-1} generující a prověrková matice nějakého kódu C'. Všimněme si, že $u = (u_1, \ldots, u_n) \in C \Leftrightarrow (u_1 v_1, \ldots, u_n v_n) \in C'$.

Kódy se nazývají **monomiálně ekvivalentní**, pokud lze od jednoho k druhému přejít takovouto úpravou a (ještě navíc) permutací souřadnic.

Ať $n \leq q$ a ať $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ jsou po dvou různé. Uvažme matici

$$G = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix}.$$

S řádkem 1 asociujeme polynom $1 = x^0$, s řádkem 2 polynom x, s řádkem 3 polynom x^2 a s řádkem k polynom x^{k-1}. Odpovídající řádek můžeme tedy vždy chápat jako vyhodnocení polynomu x^i v bodech $\alpha_1, \ldots, \alpha_n$. Lineární obal řádků G jsou pak vyhodnocení všech polynomů f stupně menšího než k v bodech $\alpha_1, \ldots, \alpha_n$. Všechny polynomy stupně menšího než k tvoří vektorový prostor, řekněme V_k, který je dimenze k. Polynomy $x^0, \ldots, x^{k-1}$ jsou jeho bází. Zobrazení

$$f \mapsto (f(\alpha_1), \ldots, f(\alpha_n))$$

je lineární zobrazení $V_k \to \mathbb{F}_q^n$. Jeho jádrem jsou polynomy, které na $\alpha_1, \ldots, \alpha_n$ nabývají nulové hodnoty. Nenulový polynom s n nulovými body je stupně alespoň n. Pro $n \geq k$ se V_k skládá z polynomů stupně menšího než n. To znamená, že uvažované lineární zobrazení má v takovém případě triviální jádro. Je tedy prosté a převádí bázi na bázi. Proto je G pro $k \leq n$ hodnosti k.

Předpokládejme $n \geq k$ a uvažme, zda ke G, které chápeme jako generující matici, nelze nalézt prověrkovou matici tvaru HD, kde $D = \triangle(x_1, \ldots, x_n)$ a

$$H = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \cdots & \alpha_n^{n-k-1} \end{pmatrix}.$$

Bodový součin i-tého řádku G a j-tého řádku H je roven

$$\alpha_1^{i+j} + \alpha_2^{i+j} + \ldots + \alpha_n^{i+j},$$

takže vlastně chceme zjistit, zda bodový součin $\left(\alpha_1^{i+j}, \ldots, \alpha_n^{i+j}\right)$ s $(x_1, \ldots, x_n)$

je roven nule, pokud $0 \leq i+j \leq n-2$. Hledáme tedy řešení následující soustavy

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-2} & \alpha_2^{n-2} & \cdots & \alpha_n^{n-2} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

.

Takové řešení existuje, neboť zde vystupuje matice $(n-1)\times n$, která je hodnosti $n-1$. Ať $(x_1, \ldots, x_n)$ je nějaké netriviální řešení. Pokud by pro některé i, $1 \leq i \leq n$, platilo $x_i = 0$, tak vypuštěním hodnoty x_i a vypuštěním i-tého sloupce dostaneme součin $Ay^T = 0$, kde $y = (x_1, \ldots, x_{i-1}, x_{i+1}, x_n) \neq 0$ a A je čtvercová regulární matice řádu $n-1$. To není možné, a proto všechna x_i jsou nenulová. Tedy $H \cdot \triangle(x_1, \ldots, x_n)$ je prověrkovou maticí C.

Ať $v_1, \ldots, v_n \in \mathbb{F}_q^*$ a ať $1 \leq k \leq n$. Pokud $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q^*$ jsou po dvou různá, tak se kód s prověrkovou maticí $H\triangle(v_1, \ldots, v_n)$ nazývá **zobecněný Reed-Solomonův kód** (GRS kód) s **lokátory** $\alpha_1, \ldots, \alpha_n$ a **multiplikátory** $v_1, \ldots, v_n$.

Tvrzení 5.1. *Buďte $1 \leq k \leq n \leq q$. Ať C je GRS kód dimenze k s lokátory $\alpha_1, \ldots, \alpha_n$ a multiplikátory $v_1, \ldots, v_n$. Pak existují $v_i' \in \mathbb{F}_q^*$, $1 \leq i \leq n$, že $C^\perp$ je GRS kód s lokátory $\alpha_1, \ldots, \alpha_n$ a multiplikátory $v_1', \ldots, v_n'$. Kódy C i C' jsou MDS kódy.*

Důkaz. Tvrzení plyne z předchozích úvah. Je nutné si uvědomit, že každá $k \times k$ podmatice matice G je podle dokázaného hodnosti k, takže je regulární. GRS kódy jsou proto MDS. □

Součástí definice GRS kódu je předpoklad nenulovosti lokátorů α_i. Tento předpoklad jsme však v úvahách výše nijak nepoužili. Tvrzení 5.1 proto platí i tehdy, je-li některý lokátor nulový.

Některé GRS kódy mají zvláštní označení. Pokud $n = q-1$, nazýváme GRS kód **primitivní**. V takovém případě $\alpha_1, \ldots, \alpha_n$ procházejí celou množinu $\mathbb{F}_q^*$.

Normalizovaný GRS kód má všechny multiplikátory rovny jedné, takže k žádné úpravě základní matice nedochází.

O **GRS kódu v užším slova smyslu** hovoříme, pokud $v_j = \alpha_j$, $1 \leq j \leq n$. V takovém případě je prověrková matice tvaru

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-k} & \alpha_2^{n-k} & \cdots & \alpha_n^{n-k} \end{pmatrix}.$$

Konvenční (běžné) RS kódy (či pouze RS kódy) jsou určeny prvkem $\alpha \in \mathbb{F}_q^*$ řádu n, kde n dělí $q-1$. Předpokládá se, že $\alpha_j = \alpha^{j-1}$ a $v_j = \alpha^{b(j-1)}$, kde $b \geq 0$ je celé číslo.

Vidíme, že RS kódy mají prověrkovou matici

$$H = \begin{pmatrix} 1 & \alpha^b & \cdots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \cdots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{b+d-2} & \cdots & \alpha^{(n-1)(b+d-2)} \end{pmatrix},$$

kde se místo $n-k$ píše $d-1$ (připomeňme si, že se jedná o MDS kód). Případy $b=0$ a $b=1$ dávají matice

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha & \cdots & \alpha^{n-1} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{d-2} & \cdots & \alpha^{(d-2)(n-1)} \end{pmatrix} \text{ a } \begin{pmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{d-1} & \cdots & \alpha^{(d-1)(n-1)} \end{pmatrix}.$$

Kódy generované maticemi se v souladu s obecnou terminologií nazývají **RS kódy v normalizovaném tvaru** a RS kódy v užším slova smyslu.

Ať C' je nějaký $[n,k,D]$ kód nad $\mathbb{F}_{q^s}$. Kód C' je tedy lineární podprostor $(\mathbb{F}_{q^s})^n$. Víme, že $\mathbb{F}_{q^s}$ lze chápat jako vektorový prostor nad $\mathbb{F}_q \subseteq \mathbb{F}_{q^s}$, a to dimenze s. Při takovém pojetí se z $(\mathbb{F}_{q^s})^n$ stává vektorový prostor nad $\mathbb{F}_q$ dimenze sn. V tomto prostoru leží $(\mathbb{F}_q)^n$ jako podprostor. Z kódu C' můžeme odvodit q-ární kód $C = C' \cap (\mathbb{F}_q)^n$. Říkáme mu **reziduální** q-ární kód kódu C.

Reziduální kódy GRS kódu se nazývají **alternantní kódy**. Jejich podtřídou jsou BCH kódy, což jsou reziduální kódy RS kódu. Označení GRS kódu jako primitivního, normalizovaného nebo v užším slova smyslu se přenáší i na alternantní a BCH kódy.

Koncept reziduálního kódu přináší zejména odhad jeho minimální vzdálenosti. Okamžitě vidíme, že kód C je délky n, a že jeho minimální vzdálenost d je alespoň D. Pokud $k = \dim C$ je dostatečně velké, můžeme získat kód příznivých parametrů, jehož přímá konstrukce by byla obtížná.

Tentýž kód je obecně vzato možno získat jako reziduální kód více způsoby. Je-li z kontextu patrné, jakou reziduální konstrukcí jsme kód C získali, nazýváme D jeho **zaručenou vzdáleností** (nejde o přesný překlad anglického termínu *designed distance*, ale o volbu sousloví, které roli D co nejlépe vystihuje).

Jsou situace, kdy známe D, avšak zjištění $d \geq D$ je obtížné. Stejně tak není vždy snadné zjistit dimenzi k kódu C. Cílem samozřejmě je získat k co největší. Následující odhad dokážeme snadno, ovšem ten hodnotu k zpravidla značně podceňuje.

Lemma 5.2. *Ať C je $[n,k]_q$ alternantní kód zaručené vzdálenosti D, který je sestrojen jako reziduální z GRS kódu C' nad $\mathbb{F}_{q^s}$. Potom $k \geq n - s(D-1)$.*

Důkaz. Označme K dimenzi kódu C'. Víme, že C' je MDS kód parametrů $[n, K, D]$, takže $D = n - K + 1$. Nerovnost $k \geq n - s(n - K)$ zapíšeme jako $n - k \leq s(n - K)$. Protože $n - k$ je počet řádků prověrkové matice kódu C, tak k důkazu nerovnosti stačí nalézt takovou matici M rozměrů $(n - K)s \times n$, že $u \in C$ právě když $Mu^{\mathsf{T}} = 0$.

Zvolme nějakou bázi $(\beta_1, \ldots, \beta_s)$ tělesa $\mathbb{F}_{q^s}$ nad $\mathbb{F}_s$. Uvažme bodový součin $c \cdot u$ nějakých vektorů $c = (\gamma_1, \ldots, \gamma_n) \in \mathbb{F}_{q^2}^s$ a $u = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$. Ať $\gamma_j = \sum_{i=1}^{s} a_{ji}\beta_i$, kde $a_{ji} \in \mathbb{F}_q$, $1 \leq j \leq n$. Položme $a_i = (a_{1i}, \ldots, a_{ni})$. Pak $c \cdot u = \sum_{j=1}^{n} \sum_{i=1}^{s} c_j a_{ji} \beta_i = \sum_{i=1}^{s} (\sum_{j=1}^{n} c_j a_{ji}) \beta_j = \sum_{i=1}^{s} (c \cdot a_i)\beta_i$. Vidíme, že $c \cdot u = 0$ právě když $c \cdot a_i = 0$ pro všechna i, $1 \leq i \leq s$.

Buď nyní H prověrková matice kódu C' s řádky $c_1, \ldots, c_{n-K}$. Každý řádek $c_r = (\gamma_1, \ldots, \gamma_n)$ nahradíme s řádky $a_1, \ldots, a_s$ jakoby bylo $c = c_r$. Zkonstruovanou matici označíme M. Protože $u = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$ padne do C' právě když $Hu^{\mathsf{T}} = 0$, lze podle předchozího totéž ověřit vztahem $Mu^{\mathsf{T}} = 0$. □