

Códigos Satisfazendo a Condição de Cadeia sobre Espaços de Rosenbloom-Tsfasman e Edifícios de Tits

Luciano Panek

Depto de Matemática, Universidade Estadual de Maringá, UEM
87020-900, Maringá, PR
E-mail: lpanek@uem.br,

Marcelo Firer

IMECC-UNICAMP, Universidade Estadual de Campinas
Caixa Postal: 6065
13081-970, Campinas, SP
E-mail: mfirer@ime.unicamp.br

Seja $M_{n \times m}(\mathbf{F}_q)$ o espaço vetorial de todas as matrizes $n \times m$ sobre o corpo finito \mathbf{F}_q . Em 1997 Rosenbloom e Tsfasman muniram o espaço $M_{n \times m}(\mathbf{F}_q)$ com um novo peso ([2]), chamado *peso de Rosenbloom-Tsfasman* w_ρ , definido como segue: se $(a_{ij}) \in M_{n \times m}(\mathbf{F}_q)$, então

$$w_\rho((a_{ij})) = \sum_{j=1}^m \max \{i : a_{ij} \neq 0\},$$

assumindo que $\max \emptyset = 0$. Conseqüentemente, se $n = 1$ então o peso de Rosenbloom-Tsfasman w_ρ sobre o espaço $M_{1 \times m}(\mathbf{F}_q)$ coincide com o peso de Hamming w_H da clássica teoria dos códigos. Os pesos de Rosenbloom-Tsfasman constituem uma importante família de pesos com possíveis aplicações em sistemas de comunicação (ver [2]).

Em outra direção, motivado pelas aplicações em criptografia, Wei introduziu em 1991 o conceito de pesos generalizados de Hamming ([3]). Em nosso trabalho estendemos o conceito de pesos generalizados de Hamming para os pesos de Rosenbloom-Tsfasman. Se D é um subespaço vetorial de um código linear C escrevemos $D \leq C$. Quando D é um subespaço próprio de C escrevemos $D < C$. O *peso generalizado de Rosenbloom-Tsfasman*, e escrevemos ρ *peso generalizado* $\|\cdot\|_\rho$, de um subespaço $D \leq M_{n \times m}(\mathbf{F}_q)$ de dimensão r é definido por

$$\|D\|_\rho = \sum_{j=1}^m \max \{i : a_{ij} \neq 0, a_{ij} \text{ elemento da } j\text{-ésima coluna de } (a_{ij}) \in D\}.$$

O r -ésimo ρ *peso mínimo* de um código $C \leq M_{n \times m}(\mathbf{F}_q)$ de dimensão k é o número

$$d_r(C) = \min \left\{ \|D\|_\rho : D \leq C, \dim(D) = r \right\}.$$

A seqüência $(d_1(C), \dots, d_k(C))$ é chamada de *hierarquia de pesos* de C . Se $n = 1$, então o r -ésimo ρ *peso mínimo* é o usual r -ésimo peso mínimo de Hamming de $M_{1 \times m}(\mathbf{F}_q) \simeq \mathbf{F}_q^m$.

Em nosso trabalho investigamos a possibilidade da existência de novos códigos satisfazendo a condição de cadeia com os ρ pesos generalizados, e no caso particular em que $q = 2$ e $w_\rho = w_H$ estudamos os códigos de codimensão 1 via a estrutura de edifícios de Tits.

Um código $C \leq M_{n \times m}(\mathbf{F}_q)$ de dimensão k satisfaz a *condição de cadeia* se existe uma seqüência de subespaços encaixados

$$D_1 < D_2 < \dots < D_{k-1} < D_k = C$$

tal que $\|D_r\|_\rho = d_r(C)$ e $\dim(D_r) = r$ para todo $r \in \{1, 2, \dots, k\}$. No caso em que $n = 1$ ($w_\rho = w_H$) temos que os códigos de Hamming, dual de Hamming, Reed-Muller de todas as ordens, maximum-separable-distance e Golay satisfazem a condição de cadeia (ver [4]).

Os códigos lineares que satisfazem a condição de cadeia podem ser vistos como *bandeiras*, seqüências de subespaços que realizam os pesos do código dado e daí para tratarmos de edifícios de Tits é um passo natural: dado um espaço vetorial de dimensão n sobre um corpo \mathbf{F}_q , o conjunto de todos os códigos, com todos os seus possíveis subcódigos é um edifício de Tits ([1]).

Assim, fazendo uso da estrutura de edifícios de Tits das variedades bandeiras, estudamos o conjunto das bandeiras maximais

$$D_1 < D_2 < \dots < D_{n-1} < \mathbf{F}_q^n$$

sobre o corpo finito \mathbf{F}_q . No caso particular em que $q = 2$ e $w_\rho = w_H$, temos que os conjuntos

$$\Delta_2(2, 3, \dots, n) \text{ e } \Delta_2(1, 2, \dots, n-1)$$

das bandeiras maximais com hierarquia de pesos $(2, 3, \dots, n)$ e $(1, 2, \dots, n-1)$ são respectivamente conexas.

De maneira geral, a hierarquia de pesos de um código $C < \mathbb{F}_2^n$ de codimensão 1 é do tipo $(1, 2, \dots, \widehat{m+1}, \dots, n)$. Observamos agora que qualquer código $C < \mathbb{F}_2^n$ pode ser descrito como sendo o núcleo de um funcional linear $\phi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$:

$$\phi(v_1, \dots, v_n) = v_1 + \dots + \widehat{v_{i_1}} + \dots + \widehat{v_{i_m}} + \dots + v_n$$

(o que está abaixo do símbolo $\widehat{(\cdot)}$ deve ser omitido). Com isto passamos a caracterizar as componentes conexas do conjunto

$$\Delta_2(1, 2, \dots, \widehat{m+1}, \dots, n)$$

de todas as bandeiras maximais com hierarquia de pesos $(1, 2, \dots, \widehat{m+1}, \dots, n)$.

Denotando por $\Delta_2\{i_1, \dots, i_m\}$ o conjunto de todas as bandeiras maximais com hierarquia de pesos $(1, 2, \dots, \widehat{m+1}, \dots, n)$ que contém o código de codimensão 1 definido pelo núcleo do funcional acima, segue que:

O conjunto $\Delta_2(1, 2, \dots, \widehat{m+1}, \dots, n)$ é uma união disjunta das componentes J -conexas $\Delta_2 I$, com $I = \{i_1, \dots, i_m\}$ e $J = \{1, \dots, \widehat{m}, \dots, n-2\}$. Conseqüentemente o conjunto

$$\bigcup_{(d_1, \dots, d_{n-1})} \Delta_2(d_1, \dots, d_{n-1})$$

possui exatamente $2^n - n$ componetes conexas.

Podemos caracterizar o conjunto

$$\Delta_2(1, 2, \dots, \widehat{m+1}, \dots, n)$$

como sendo uma união de diversas cópias do produto

$$\Delta_2(1, 2, \dots, m-1) \times \Delta_2(2, 3, \dots, n-m)$$

utilizando a estrutura de coproduto. Seja $1 \leq r_1 < \dots < r_k \leq n$ uma seqüência de inteiros, $I = \{i_1, \dots, i_m\}$, $N = \{1, 2, \dots, n\}$, $I \subset N$ e $I^c = N \setminus I$. Denotamos por $\mathbb{F}_2^n(r_1, \dots, r_k)$ o conjunto de todas as bandeiras $D_{r_1} < \dots < D_{r_k}$ formadas por subespaços de \mathbb{F}_2^n tal que $\dim(D_{r_j}) = r_j$. Definimos as inclusões

$$i_I : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^n,$$

$$\widehat{i}_I : \mathbb{F}^m(1, \dots, m) \rightarrow \mathbb{F}^n(1, \dots, m)$$

e

$$\widehat{\widehat{i}}_I : \mathbb{F}^{n-m}(1, \dots, n-m-1) \rightarrow \mathbb{F}^n(m+1, \dots, n-1)$$

respectivamente por

$$i_I(x_1, \dots, x_m) = (0, \dots, 0, (x_1)_{i_1}, 0, \dots, 0, (x_m)_{i_m}, 0, \dots, 0),$$

$$\widehat{i}_I(D_1 < \dots < D_m) = i_I(D_1) < \dots < i_I(D_m)$$

e

$$\widehat{\widehat{i}}_I(D_1 < \dots < D_{n-m-1}) = i_{I^c}(D_1) \oplus i_I(\mathbb{F}_2^m) < \dots < i_{I^c}(D_{n-m-1}) \oplus i_I(\mathbb{F}_2^m).$$

Observamos que o produto direto

$$\widehat{i}_I(\Delta_2(1, 2, \dots, m-1)) \times \widehat{\widehat{i}}_I(\Delta_2(2, 3, \dots, n-m))$$

é isomorfo ao conjunto $\Delta_2 I$.

Assim, usando a notação $\Delta = \Delta_2(1, 2, \dots, m-1)$ e $\Delta' = \Delta_2(2, 3, \dots, n-m)$, temos o *coproduto*

$$\prod_{k=1}^{\binom{n}{m}} \Delta \times \Delta' = \bigcup_I \widehat{i}_I(\Delta) \times \widehat{\widehat{i}}_I(\Delta').$$

Daí segue que o conjunto $\Delta_2(1, 2, \dots, \widehat{m+1}, \dots, n)$ é isomorfo ao coproduto

$$\prod_{k=1}^{\binom{n}{m}} \Delta \times \Delta',$$

onde os códigos de dimensão m e $n-m-1$ de cada produto $\Delta \times \Delta'$ são identificados respectivamente com os códigos $\langle \{e_{i_j}\}_{j=1}^m \rangle$ e $\langle \{v_{j_2}^{j_1}\} \rangle$, $j_1, j_2 \in I^c$. Conseqüentemente temos que $\Delta_2(1, 2, \dots, \widehat{m+1}, \dots, n)$ possui exatamente $n!/2$ bandeiras.

No caso de um código C sobre o espaço de Rosenbloom-Tsfasman $M_{n \times 1}(\mathbf{F}_q) \simeq \mathbf{F}_q^n$, ou sobre $M_{2 \times 2}(\mathbf{F}_q)$, temos que todos os códigos satisfazem a condição de cadeia. Conseqüentemente a bandeira $D_1 < D_2 < \dots < D_{k-1} < D_k = C$ que realiza os pesos mínimos de Rosenbloom-Tsfasman em $M_{n \times 1}(\mathbf{F}_q)$ é única. Daí segue que se $\|D_r\|_\rho = d_r(C)$ para todo $r \in \{1, 2, \dots, k\}$, então

$$D_1 < D_2 < \dots < D_{k-1} < D_k = C.$$

Referências

- [1] M. Ronan, Lectures on Buildings, *Perspectives in Mathematics*, vol. 7, Academic Press, 1989.
- [2] M. Y. Rosenbloom, M. A. Tsfasman, Codes for the m -metric, *Probl. Inf. Transm.* 33 (1997) 45-52.
- [3] V. K. Wei, Generalized Hamming Weights for Linear Code, *IEEE Trans. Inform. Theory*, vol. 37, n. 5, pp. 1412-1418, September 1991.
- [4] V K. Wei, K. Yang, On the Generalized Hamming Weights for Product Code, *IEEE Trans. Inform. Theory*, vol. 39, n. 5, pp. 1709-1713, September 1993.