CLASSIFICAÇÃO DOS CÓDIGOS LINEARES EM ESPAÇOS DE BLOCOS DE ROSENBLOOM-TSFASMAN

Luciano Panek[1], **Marcelo Firer**[2], **Marcelo Muniz Silva Alves**[3]

1.- Centro de Engenharias e Ciências Exatas, UNIOESTE, Av. Tarquínio Joslin do Santos, 1300, CEP 85870-650, Foz do Iguaçu, PR, Brazil. Email: lucpanek@gmail.com **2.-** IMECC - UNICAMP, Caixa Postal 6065, CEP 13081-970, Campinas, SP, Brazil. Email: mfirer@ime.unicamp.br **3.-** Departamento de Matemática, Centro Politécnico, UFPR, Caixa Postal 019081, Jd. das Américas, CEP 81531-990, Curitiba, PR, Brazil. Email: marcelomsa@ufpr.br

Resumo- Métricas ponderadas por ordens parciais e métricas de blocos foram introduzidas nos últimos anos como métricas alternativas para o estudo de códigos corretores de erros. Códigos de blocos ponderados foram introduzidos em 2008, intercalando as métricas de blocos e as métricas ponderadas por ordens parciais. Neste trabalho estudamos uma família particular destas métricas, as chamadas métricas de blocos de Rosenbloom-Tsfasman. Neste contexto classificamos as classes de códigos equivalentes e desenvolvemos muitos dos resultados clássicos da teoria dos códigos, incluindo a determinação do raio de empacotamento, raio de cobertura, classificação dos códigos MDS, classificação dos códigos perfeitos, caracterização dos códigos quasi-perfeitos e propomos um algoritmo de decodificação via síndromes.

Palavras-chave: Pesos de Rosenbloom-Tsfasman, pesos de blocos, códigos ponderados, pesos generalizados, códigos corretores de erros.

Classification of Rosenbloom-Tsfasman Block Codes

Abstract- Poset and block metrics were introduced in recent years as alternative metrics to study error correcting codes. Poset-block codes were introduced in 2008, intervening both poset and block metrics. In this work we study a family of such metrics, the Rosenbloom-Tsfasman block metrics. In this context we classify the classes of equivalent codes, describe canonical representatives of each class and develop much of the classical theory of error correcting codes for Rosenbloom-Tsfasman block codes, including determination of packing radius and classification of MDS and perfect codes, determination of covering radius and characterization of quasi-perfect codes and propose an algorithm for syndrome decoding, including precise description of syndrome leaders.

KeyWord: Rosenbloom-Tsfasman weights, block weights, poset codes, generalized weights, error correcting codes.

1. INTRODUÇÃO

Insatisfeito com o funcionamento de seu computador nos Laboratórios Bell (Bell Telephone Laboratories), Richard Hamming desenvolve em 1947 o primeiro código corretor de erros, conhecido hoje como código binário de Hamming. As idéias de Hamming foram publicadas somente em 1950 (ver [4]). Um exemplo de dimensão baixa do código binário de Hamming apareceu em 1948 no célebre trabalho de Claude Shannon (ver [21]). Em [4] Hamming também estabelece os conceitos fundamentais da teoria dos códigos corretores de erros: métrica de Hamming, códigos equivalentes e o limitante de empacotamento de esferas. Os fundamentos teóricos sobre códigos lineares foram estabelecidos em 1956 por David Slepian (ver [22]): códigos de grupo, arranjo padrão, síndromes e algoritmo de decodificação por máxima verossimilhança via síndromes. Seguindo os passos de Hamming e Slepian, apresentamos neste trabalho os conceitos fundamentais em relação a uma nova família de métricas, as chamadas métricas de blocos de Rosenbloom-Tsfasman (descritas na próxima seção).

Iniciamos apresentando de forma sucinta os conceitos introduzidos por Hamming e Slepian em [4] e [22]. Estes

conceitos são clássicos e são encontrados em qualquer bom livro de teoria dos códigos corretores de erros (por exemplo, ver [5]). Seja $\mathbf{F}_q^N$ o espaço vetorial das N-uplas sobre o corpo finito $\mathbf{F}_q$ com q elementos. Um vetor $x \in \mathbf{F}_q^N$ será denotado por $x_1x_2\ldots x_N$, sendo x_i a i-ésima coordenada de x. Um subespaço k-dimensional $C \subseteq \mathbf{F}_q^N$ é chamado de $[N;k]$ **código linear**. Os vetores de um $[N;k]$ código linear são chamados de **palavras-código**. Se $\{g_1, g_2, \ldots, g_k\}$ é uma base de C então $G = (g_i)$ é a chamada **matriz geradora** de C:

$$C = \left\{x \cdot G : x \in \mathbf{F}_q^k\right\}. \tag{1}$$

O subespaço

$$C^{\perp} = \left\{y \in \mathbf{F}_q^N : c \cdot y = 0 \text{ para todo } c \in C\right\}, \tag{2}$$

onde $c \cdot y = c_1 \cdot y_1 + \ldots + c_N \cdot y_N$ é o **produto interno** em $\mathbf{F}_q^N$, é o chamado **código dual** de C. Uma matriz geradora H de $C^{\perp}$ é dita uma **matriz de paridade** de C: denotando o vetor nulo $00\ldots0$ por $\mathbf{0}$, $c \in C$ se, e somente se, $H \cdot c^T = \mathbf{0}$. Para cada $x \in \mathbf{F}_q^N$ seja $\text{supp}_H(x) = \{i : x_i \neq 0\}$ o **suporte de Hamming** de x. O número $w_H(x) = |\text{supp}_H(x)|$ é o **peso de Hamming** de x. A **distância de Hamming** $d_H(x,y)$ entre x e y é o número de coordenadas distintas entre x e y, ou seja, $d_H(x,y) = w_H(x-y)$. A distância de Hamming é uma métrica em $\mathbf{F}_q^N$ (d_H é positiva definida, simétrica e satisfaz a desigualdade triangular). O espaço métrico $\left(\mathbf{F}_q^N, d_H\right)$ é conhecido como **espaço de Hamming**. Associado a um código linear C temos a **distância mínima de Hamming** de C:

$$d_H(C) = \min\left\{d_H\left(c,c'\right) : c \neq c' \in C\right\}. \tag{3}$$

Vale que $d_H(C) = \min\{w_H(c) : \mathbf{0} \neq c \in C\}$. Dado r um inteiro positivo e $x \in \mathbf{F}_q^N$, o conjunto de todos os vetores $y \in \mathbf{F}_q^N$ tal que $d_H(x,y) \leq r$ é denotado por $B_H(x;r)$ e chamado de **bola** de centro x e raio r. O maior r tal que $B_H(c;r) \cap B_H(c';r) = \emptyset$ para todo $c \neq c' \in C$ é a chamada **capacidade de correção de erros** de C (ou o **raio de empacotamento** de C). Dado um código linear C, é bem conhecido na literatura que

$$t := \left\lfloor \frac{d_H(C) - 1}{2} \right\rfloor \tag{4}$$

é a capacidade de correção de erros de C. Se durante a transmissão de uma palavra código c ocorrerem no máximo t erros e recebermos a mensagem x ($x = c + e$ com $w_H(e) \leq t$), então c é a única palavra código mais próxima de x: a mensagem x é decodificada corretamente com sendo a palavra código c. O procedimento de decodificar uma mensagem x como sendo a palavra código mais próxima de x é conhecido como **decodificador por máxima verossimilhança**. Um algoritmo simples para decodificação é baseado nas síndromes dos vetores de $\mathbf{F}_q^N$. Dado um $[N;k]$ código linear C e uma matriz de paridade H de C, definimos a **síndrome** $S(x)$ de $x \in \mathbf{F}_q^N$ como sendo o vetor $H \cdot x^T$. Como S é uma aplicação linear sobrejetora de $\mathbf{F}_q^N$ em $\mathbf{F}_q^{N-k}$ e a síndrome de uma palavra código c é o vetor nulo $\mathbf{0}$, $S(c+e) = S(e)$. A síndrome restrita aos vetores $e \in \mathbf{F}_q^N$ tal que $w_H(e) \leq t$, denotada por $\widetilde{S}$, é uma aplicação injetora. Assim os procedimentos para o algoritmo de decodificação por síndromes são: seja x uma mensagem recebida; suponha que $x = c + e$ com $c \in C$ e $e \in \mathbf{F}_q^N$ o vetor erro; calcule $S(x)$ (lembre que $S(x) = S(e)$); se $S(x) \notin \text{Im}\left(\widetilde{S}\right)$, então x não pode ser decodificada; agora se $S(x) \in \text{Im}\left(\widetilde{S}\right)$, ou seja, $w_H(e) \leq t$, decodifique x como sendo o vetor $x - \widetilde{S}^{-1}(S(x)) = x - e$.

Códigos em espaços de Hamming mostram-se eficientes para a correção de erros aleatórios, correção de erros em rajada aleatórias (bursts errors) e correção de rasuras aleatórias (erasures) (por exemplo, ver [8] e [11]). Em 1997 Rosenbloom e Tsfasman ([20]) apresentaram uma nova família de métricas (as chamadas métricas de Rosenbloom-Tsfasman) eficientes para medir erros em rajadas localizadas (neste sentido podemos dizer que os erros são do tipo rasuras em rajadas). Já em 2004 Ozen e Siap ([15]) propuseram um esquema de decodificação por máxima verossimilhança para mensagens transmitidas em canais de comunicação onde os erros ocorrem em rajadas nas primeiras coordenadas e aleatóriamente nas últimas coordenadas, intercalando a métrica de Rosenbloom-Tsfasman com a métrica de Hamming. O decodificador de Ozen e Siap é construído a partir de uma forma padrão de matriz geradora para códigos em espaços de Rosenbloom-Tsfasman ([15], Theorem 1). Os códigos considerados em [15] são lineares sobre corpos finitos. Extensões dos resultados em [15] para anéis de Galois podem ser encontrados em [14] e [13]. Em [13], [14] e [15] não são determinados a capacidade de correção de erros (ou o raio de empacotamento) dos códigos em relação a métrica de Rosenbloom-Tsfasman. Também não são propostos algoritmos de decodificação.

Neste trabalho apresentamos uma nova família de métricas intercalando a métrica de blocos introduzida por Feng, Xu e Hickernell em [3] com a métrica de Rosenbloom-Tsfasman. Assim como Wei em [23] consideramos os pesos generalizados em relação a nova métrica. A partir dos pesos generalizados estendemos os resultados de Ozen e Siap: determinação de uma forma padrão de matriz geradora, limitante de Singleton generalizado, cálculo do espectro dos pesos generalizados, decodificação por máxima verossimilhança. Determinamos também o raio de empacotamento, o raio de cobertura (em função do último peso generalizado) e apresentamos uma classificação dos códigos perfeitos e quase-perfeitos. Uma proposta de algoritmo de decodificação via síndromes é apresentada. Ficam assim estabelecidos os conceitos fundamentais da teoria dos códigos corretores de erros em espaços de blocos de Rosenbloom-Tsfasman.

A métrica de blocos de Rosenbloom-Tsfasman é um caso particular de uma família de métricas introduzidas por Alves, Panek e Firer em [1]. Em [1] são caracterizados os grupos de simetrias lineares (em particular o grupo de simetrias lineares dos espaços de blocos de Rosenbloom-Tsfasman). As métricas em [1] são ex-

tensões das métricas introduzidas por Brualdi, Graves e Lawrence em [2] (estudadas em [6], [7], [9], [16]) e Feng, Xu e Hickernell em [3] (estudadas em [10]). A métrica de Hamming é um caso particular das métricas de Rosenbloom-Tsfasman (estudadas em [13], [14], [15], [17], [18], [19]) que são casos particulares das métricas em [2].

2. ESPAÇOS DE BLOCOS DE ROSENBLOOM-TSFASMAN

Seja N um inteiro positivo e $\pi = (\pi_1, \pi_2, \ldots, \pi_n)$ uma partição de N:

$$N = \pi_1 + \pi_2 + \ldots + \pi_n \tag{5}$$

com $\pi_1 \geq \pi_2 \geq \ldots \geq \pi_n \geq 1$. Para cada π_i, $1 \leq i \leq n$, seja V_i o espaço vetorial $\mathbf{F}_q^{\pi_i}$ sobre o corpo finito $\mathbf{F}_q$. Definimos o espaço vetorial V como sendo a soma direta

$$V = V_1 \oplus V_2 \oplus \ldots \oplus V_n. \tag{6}$$

Temos que V é isomorfo a $\mathbf{F}_q^N$. Cada vetor $x \in V$ pode ser escrito de forma única como

$$x = x_1 + x_2 + \ldots + x_n \tag{7}$$

com $x_i \in V_i$ para cada $1 \leq i \leq n$. Definimos o **peso de blocos de Rosenbloom-Tsfasman** w_π (ou o **π-peso**) de $x = x_1 + x_2 + \ldots + x_n \in V$ pondo

$$w_\pi(x) = \begin{cases} \max\{i : x_i \neq \mathbf{0}\} & \text{se} \quad x \neq \mathbf{0} \\ 0 & \text{se} \quad x = \mathbf{0} \end{cases}. \tag{8}$$

O π-peso induz uma métrica em V, chamada **métrica de blocos de Rosenbloom-Tsfasman** (ou **π-métrica**): se $x, y \in V$ então

$$d_\pi(x, y) = w_\pi(x - y). \tag{9}$$

Nestas condições diremos que (V, d_π) é o **π-espaço de Rosenbloom-Tsfasman**. A **π-distância mínima** de um código linear C é o número

$$d_\pi = d_\pi(C) = \min\left\{d_\pi\left(c, c'\right) : c \neq c' \in C\right\}. \tag{10}$$

Associado ao peso de blocos de Rosenbloom-Tsfasman temos o peso generalizado de blocos de Rosenbloom-Tsfasman: se $D \subseteq V$ é um subespaço vetorial, então

$$\|D\| = \max\{w_\pi(x) : x \in D\} \tag{11}$$

é o **peso generalizado de blocos de Rosenbloom-Tsfasman** (ou **π-peso generalizado**) de D e

$$d_r = d_r(C) = \min\{\|D\| : D \subseteq C, \dim(D) = r\} \tag{12}$$

é o **r-ésimo peso mínimo de blocos de Rosenbloom-Tsfasman** (ou **r-ésimo π-peso generalizado**) de um código linear $C \subseteq V$. Um código linear $C \subseteq V$ de dimensão k com **hierarquia** de π-pesos generalizados $(d_1, d_2, \ldots, d_k)$ é dito um $[N; k; d_1, \ldots, d_k]$ **código linear**. Como $d_\pi(C) = \min\{w_\pi(c) : \mathbf{0} \neq c \in C\}$ e $\|D\| = w_\pi(c)$ para todo $\mathbf{0} \neq c \in D$ sempre que D é 1-dimensional, então $d_1(C) = d_\pi(C)$.

A métrica de blocos de Rosenbloom-Tsfasman é um caso particular da (P, π)-métrica introduzida por Alves, Panek e Firer em [1], que corresponde a P totalmente ordenado. Quando a partição π de N satisfaz $\pi_i = 1$ para todo $1 \leq i \leq n$ a π-métrica coincide com a métrica de Rosenbloom-Tsfasman proposta em [20].

3. MATRIZ GERADORA

Começaremos enunciando a monotonicidade dos r-ésimos π-pesos generalizados.

Teorema 1 *Seja C um $[N; k; d_1, \ldots, d_k]$ código linear. Então*

$$0 \leq d_1 \leq d_2 \leq \ldots \leq d_k \leq n. \tag{13}$$

Observação 1 *Os números da hierarquia de π-pesos generalizados não são necessariamente distintos. Seja $\pi = (2, 1, 1)$ uma partição de $N = 4$ e considere o código binário $C = \{0000, 1000, 0100, 1100\}$. Neste caso*

$$d_1(C) = \tag{14}$$

$$d_2(C) = \min\{w_\pi(1000), w_\pi(0100), w_\pi(1100)\} = 1. \tag{15}$$

Seja (V, d_π) um π-espaço de Rosenbloom-Tsfasman. Para cada m-upla $(\pi_{t_1}, \ldots, \pi_{t_m})$, definimos a aplicação projeção

$$p_{(t_1, \ldots, t_m)} : V \to V \tag{16}$$

em relação aos blocos $V_{t_1}, \ldots, V_{t_m}$ da seguinte forma: dado $u = u_1 + \ldots + u_n \in V$,

$$p_{(t_1, \ldots, t_m)}(u) = u_{t_1} + \ldots + u_{t_m}. \tag{17}$$

Teorema 2 *Seja C um $[N; k; d_1, \ldots, d_k]$ código linear. Então C admite uma matriz geradora $G = (G_{st})$ onde G_{st} são submatrizes de ordem $s \times t$, com $s \leq t$, $G_{s_i \pi_j} = \mathbf{0}$ se $j > t_i$ e para cada $1 \leq i \leq m$ o posto de $G_{s_i \pi_{t_i}}$ é igual a s_i. Nestas condições $s_1 + s_2 + \ldots + s_m = k$.*

Definição 1 *A forma matricial no teorema 2 será dita do **tipo** $((s_1, t_1), \ldots, (s_m, t_m))$.*

Lema 1 *Seja G uma matriz do tipo $((s_1, t_1), \ldots, (s_m, t_m))$. Então G é a matriz geradora de um $\left[N; \sum_{i=1}^m s_i\right]$ código linear.*

Lema 2 *Seja C um código gerado por uma matriz G do tipo $((s_1, t_1), \ldots, (s_m, t_m))$. Se D é um subcódigo de C, então $\|D\| = t_j$ para algum $1 \leq j \leq m$.*

Teorema 3 *Seja G uma matriz do tipo $((s_1, t_1), \ldots, (s_m, t_m))$. Então G é uma matriz geradora de um $\left[N; \sum_{i=1}^m s_i\right]$ código linear C com hierarquia de π-pesos generalizados*

$$d_1 = \ldots = d_{s_1} = t_1 \tag{18}$$

$$d_{s_1+1} = \ldots = d_{s_1+s_2} = t_2 \tag{19}$$

$$\vdots \tag{20}$$

$$d_{s_1+\ldots+s_{m-1}+1} = \ldots = d_{s_1+\ldots+s_{m-1}+s_m} = t_m. \tag{21}$$

Definição 2 *Os códigos com matriz geradora do tipo* $((s_1,t_1),\ldots,(s_m,t_m))$ *serão chamados de* ***códigos do tipo*** $((s_1,t_1),\ldots,(s_m,t_m))$.

Corolário 1 *Seja* C *um código do tipo* $((s_1,t_1),\ldots,(s_m,t_m))$. *Então* C *é um* $\left[N;\sum_{i=1}^{m}s_i\right]$ *código linear com hierarquia de* π*-pesos generalizados*

$$d_1=\ldots=d_{s_1}=t_1 \tag{22}$$

$$d_{s_1+1}=\ldots=d_{s_1+s_2}=t_2 \tag{23}$$

$$\vdots \tag{24}$$

$$d_{s_1+\ldots+s_{m-1}+1}=\ldots=d_{s_1+\ldots+s_{m-1}+s_m}=t_m. \tag{25}$$

Corolário 2 *Seja* C *um código do tipo* $((s_1,t_1),\ldots,(s_m,t_m))$ *e* $D_1,\ldots,D_m$ *subcódigos de* C *tal que* $\|D_j\|=t_j$ *e* $\dim(D_j)=s_1+\ldots+s_j$ *para todo* $1\leq j\leq m$ *(note que* $D_m=C$*). Então*

$$D_1\subset D_2\subset\ldots\subset D_m. \tag{26}$$

Corolário 3 *Para um código do tipo* $((s_1,t_1),\ldots,(s_m,t_m))$,

$$d_1=\ldots=d_{s_1}\leq n-m+1, \tag{27}$$

$$d_{s_1+1}=\ldots=d_{s_1+s_2}\leq n-m+2, \tag{28}$$

$$\vdots \tag{29}$$

$$d_{s_1+\ldots+s_{m-1}+1}=\ldots=d_{s_1+\ldots+s_{m-1}+s_m}\leq n. \tag{30}$$

Corolário 4 (*Limitante de Singleton*) *Para um* $[N;k;d_1,\ldots,d_k]$ *código linear* C,

$$d_\pi(C)\leq n-m+1. \tag{31}$$

4. DECODIFICAÇÃO POR MÁXIMA VEROSSIMILHANÇA

Seja (V,d_π) um π-espaço de Rosenbloom-Tasfasman. Dados $x\in V$ e r um inteiro positivo, o conjunto de todos os vetores $y\in V$ tal que $d_\pi(x,y)\leq r$ é a chamada **bola** de centro x e raio r. A bola de centro x e raio r será denotado por $B_\pi(x;r)$.

Lema 3 *Se* $y\in B_\pi(x;r)$ *e* $w_\pi(x)>r$, *então* $w_\pi(y)=w_\pi(x)$.

O **raio de empacotamento** s de um código linear C de V é o maior inteiro positivo tal que as bolas centradas nas palavras códigos de C são duas a duas disjuntas.

Teorema 4 *O raio de empacotamento de um* $[N;k;d_1,\ldots,d_k]$ *código linear* C *é igual a*

$$s=d_\pi(C)-1. \tag{32}$$

O processo que associa cada mensagem x a uma palavra código c mais próxima de x (segundo a π-métrica) é chamado de **decodificação por máxima verossimilhança**. Segue do teorema 4 que se uma mensagem x contém no máximo s erros nas s primeiras coordenadas, então existe um única palavra código c mais próxima de x.

Observação 2 *A métrica de blocos de Rosenbloom-Tsfasman é uma* ***ultra-métrica****:*

$$d_\pi(x,y)\leq\max\{d_\pi(x,z),d_\pi(z,y)\} \tag{33}$$

para todo $z\in V$. *Em espaços ultra-métricos* (X,d) *todo triângulo é isósceles e consequêntemente (ver [12]), dados* $x\neq y\in X$,

$$B_d(x;r)\cap B_d(y;r)=\emptyset \tag{34}$$

se, e somente se, $r=d(x,y)-\varepsilon$ *com* $\varepsilon>0$. *Como a* π*-métrica é discreta, dado um código* $C\subseteq V$, *da não-arquimedianidade de* (V,d_π) *concluímos que* $r=d_\pi(C)-1$ *é máximo com a propriedade* (50) *se* $d_\pi(x,y)=d_\pi(C)$. *Daí que* $d_\pi(C)-1$ *é o raio de empacotamento de* C.

A π-distância mínima (e conseqüentemente o raio de empacotamento) de um código linear C de V pode ser facilmente calculada se conhecemos uma matriz de paridade de C.

Teorema 5 *Seja* (V,d_π) *um* π*-espaço de Rosenbloom-Tsfasman. Seja* $C\subseteq V$ *um* $[N;k]$ *código linear e* $H=(H_1,H_2,\ldots,H_n)$ *uma matriz de paridade de* C *com* H_i *submatriz de ordem* $(N-k)\times\pi_i$ *para cada* $1\leq i\leq n$. *A distância mínima de* C *é igual a* $l+1$ *se, e somente se,*

$$l=\max\{r:posto((H_1,H_2,\ldots,H_r))=r\}. \tag{35}$$

Corolário 5 *Seja* $C\subseteq V$ *um código linear e* $H=(H_1,H_2,\ldots,H_n)$ *uma matriz de paridade de* C *com* H_i *submatriz de ordem* $(N-k)\times\pi_i$ *para cada* $1\leq i\leq n$. *O raio de empacotamento de* C *é igual a* l *se, e somente se,*

$$l=\max\{r:posto((H_1,H_2,\ldots,H_r))=r\}. \tag{36}$$

Diremos que um código C é **π-perfeito** se a união das bolas de raio $s=d_\pi(C)-1$ centradas nos vetores de C é igual a V. Um código C que atinge o limitante de Singleton, ou seja, $d_\pi(C)=n-m+1$, é dito um **código MDS** (Maximum Separable Code).

Teorema 6 *Seja* (V,d_π) *o* π*-espaço de Rosenbloom-Tsfasman tal que* $\pi_i=1$ *para todo* $1\leq i\leq n$ *e seja* C *um* $[N;k]$ *código linear em* V. *Então* C *é MDS se, e somente se,* C *é* π*-perfeito.*

Teorema 7 (*ver [1], Proposition 3.1*) *Seja* (V,d_π) *um* π*-espaço de Rosenbloom-Tsfasman e* $C\subseteq V$ *um código*

linear. Então C is π-perfeito com raio de empacotamento r se, e somente se, existe uma transformação linear

$$L : V_{r+1} \oplus \ldots \oplus V_n \to V_1 \oplus \ldots \oplus V_r \tag{37}$$

tal que

$$C = \{(L(v), v) : v \in V_{r+1} \oplus \ldots \oplus V_n\}. \tag{38}$$

Como consequência dos teoremas 6 e 7 temos:

Corolário 6 *Seja π a partição de N tal que $\pi_i = 1$ para todo $1 \leq i \leq n$ e $C \subseteq V$ um $[N;k]$ código linear. Então C é MDS se, e somente se, existe uma transformação linear*

$$L : \mathbf{F}_q^k \to \mathbf{F}_q^{N-k} \tag{39}$$

tal que

$$C = \left\{(L(v), v) : v \in \mathbf{F}_q^k\right\}. \tag{40}$$

Seja C um $[N;k;d_1,\ldots,d_k]$ código linear e $s = d_\pi(C) - 1$. Definimos o **raio de cobertura** $\rho = \rho(C)$ como sendo o menor inteiro positivo l tal que V é a união das bolas de raio l centradas nos vetores de C. É claro que $l \leq \rho(C)$ e $l = \rho(C)$ se, e somente se, C é π-perfeito. Se o código não é π-perfeito, seu raio de cobertura é estritamente maior do que seu raio de empacotamento.

Teorema 8 *Seja C um $[N;k;d_1,\ldots,d_k]$ código linear, $p_{(r,r+1,\ldots,n)}(C)$ a projeção de C em relação ao espaço $V_r \oplus \ldots \oplus V_n$ e*

$$l = \begin{cases} n+1 \text{ se } p_n(C) \neq V_n \\ \min\left\{r : p_{(r,r+1,\ldots,n)}(C) = V_r \oplus \ldots \oplus V_n\right\} \text{ c.c.} \end{cases}. \tag{41}$$

Então

$$\rho(C) = l - 1. \tag{42}$$

Corolário 7 *Seja C um $[N;k;d_1,\ldots,d_k]$ código linear e l definido como no teorema 8. Então*

$$\rho(C) = \begin{cases} l-1 & se \quad d_k = n \\ n & se \quad d_k < n \end{cases}. \tag{43}$$

Seja (V, d_π) um π-espaço de Rosenbloom-Tsfasman. Se C é um código linear em V com raio de empacotamento s e raio de cobertura $s+1$, C é dito **quase-perfeito**. Apresentaremos agora uma caracterização dos códigos quase-perfeitos em espaços de blocos de Rosenbloom-Tsfasman. Para os espaços de Hamming o problema da classificação dos códigos quase-perfeitos permanece aberto.

Teorema 9 *Seja C um $[N;k;d_1,\ldots,d_k]$ código linear. Então C é quase-perfeito se, e somente se,*

$$p_{(d_1+1,\ldots,n)}(C) = V_{d_1+1} \oplus V_{d_1+2} \oplus \ldots \oplus V_n \tag{44}$$

e $p_{d_1}(C) \neq V_{d_1}$.

5. ALGORITMO DE DECODIFICAÇÃO

Se c é a palavra código transmitida e $y = c + e$ é a mensagem recebida, então diremos que e é o **vetor erro** (ou simplesmente o **erro**). Fixada uma métrica, o procedimento que determina a palavra código mais próxima de uma mensagem recebida é conhecido como **decodificador por máxima verossimilhança**. A capacidade do decodificador por máxima verossimilhança é determinada pelo raio de empacotamento do código.

Os decodificadores por máxima verossimilhança em espaços de Hamming são eficientes na correção de erros aleatórios. Já em espaços de blocos de Rosenbloom-Tsfasman os decodificadores por máxima verossimilhnaça são limitados a correções de erros em rajada nos primeiros blocos.

Teorema 10 *Seja C um código linear, $s = d_\pi(C) - 1$ e $t = \left\lfloor \frac{d_H(C)-1}{2} \right\rfloor$:*

(i) Se na transmissão de uma palavra código c ocorrem até t erros aleatórios e recebemos a mensagem y, então c é a única palavra código tal que

$$d_H(c, y) = \min\left\{d_H\left(c', y\right) : c' \in C\right\}; \tag{45}$$

(ii) Se na transmissão de uma palavra código c ocorrem até $\pi_1+\ldots+\pi_s$ erros nas primeiras $\pi_1+\ldots+\pi_s$ coordenadas e y é a mensagem recebida, então c é a única palavra código tal que

$$d_\pi(c, y) = \min\left\{d_\pi\left(c', y\right) : c' \in C\right\}. \tag{46}$$

Demonstração O item (ii) é consequência do teorema 4. O item (i) é conhecido na literatura clássica (ver [5]).

Exemplo 1 *Seja $C = \{00000, 11111\}$ um código binário. Em relação a métrica de Hamming, $d_H(C) = 5$ e $t = 2$. Isto implica que C corrige até dois erros aleatórios. Os erros do tipo $11110, 01110, 10110, 11010$ são corrigidos de forma incorreta. Agora suponha que $\pi_i = 1$ para todo i. Em relação a métrica de blocos de Rosenbloom-Tsfasman, $d_\rho(C) = 5$, $s = 4$ e qualquer erro do tipo $11110, 01110, 10110, 11010$ é corrigido corretamente. A desvantagem neste caso é que os erros do tipo $10001, 01001, 00101, 00011, 00001$ são corrigidos incorretamente.*

O exemplo acima ilustra duas situações: se num determinado canal de comunicação a ocorrência de erros é aleatória, então a performance do código a ser implementado devem ser avaliados segundo a métrica de Hamming; agora se a ocorrência de erros não é aleatória e ocorre em rajadas (restrita as primeiras coordenadas), então a performance do código a ser implementado deve ser avaliado segundo a métrica de Rosenbloom-Tsfasman.

Convencidos de que os códigos em espaços de Rosenbloom-Tsfasman são eficientes para corrigir longos erros em rajada nas primeiras coordenadas, passamos a descrever um algoritmo para o decodificador por máxima verossimilhança em relação a métrica de blocos de Rosenbloom-Tsfasman.

Os próximos fatos são bem conhecidos na literatura e não dependem da estrutura métrica adotada em V (ver [5]). Seja C um código linear e H uma matriz de verificação de paridade de C. Em relação a síndrome $S : V \to \mathbf{F}_q^{N-k}$, dada por $S(u) = H \cdot u^T$, valem as seguintes propriedades: $S(c) = S(c+e)$ para todo $c \in C$ e para todo $e \in V$; $S : V \to \mathbf{F}_q^{N-k}$ é sobrejetora; se $C_v = \{u \in V : S(u) = v\}$, então $C_u \cap C_v = \emptyset$ se $u \neq v$; $C_{\mathbf{0}} = C$; $V = \bigcup_{v \in \mathbf{F}^{N-k}} C_v$; $C_v = \{u + c : c \in C\}$; $|C_v|$ não depende de v.

Os vetores com π-peso mínimo em C_v serão chamados de π-*líderes* de C_v.

Teorema 11 *Seja (V, d_π) um π-espaço de Rosenbloom-Tsfasman e C um código linear em V. Se $s = d_\pi(C) - 1$ e $u \in V$ é um π-líder de C_v tal que $w_\pi(u) \leq s$, então u é o único π-líder de C_v.*

Sendo assim, se $\widehat{c}$ é a palavra recebida, sendo $v = S(\widehat{c})$ e u um π-líder de C_v, decodificamos $\widehat{c}$ como sendo o vetor

$$c = \widehat{c} - u. \tag{47}$$

Se o erro é ocorre nos primeiros s blocos, então o teorema acima assegura que o algoritmo está retornando de fato a palavra transmitida.

Exemplo 2 *Suponha que $\pi_i = 1$ para todo i. Seja $C = \{00000, 10100, 01010, 11110\}$ um código binário. Temos que C é um $[5; 2]$ código com $d_\pi(C) = 3$. Como*

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix} = (I_2 | A) \tag{48}$$

é uma matriz geradora de C, então

$$H = \left(A^T \middle| I_3\right) = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{49}$$

é uma matriz de verificação de paridade de C. Vamos listar agora os π-líderes e suas respectivas síndromes:

	Líder				*Síndrome*
C	00000	10100	01010	11110	000
	10000	00100	11010	01110	100
	01000	11100	00010	10110	010
	11000	01100	10010	00110	110
	00001	10101	01011	11111	001
	00011	10111	01001	11101	011
	10011	00111	11001	01101	111
	10001	00101	11011	01111	101

(50)

Suponha agora que em nosso canal de comunicação os erros mais comuns são do tipo $10000, 01000, 11000$. Se recebemos a mensagem $\widehat{c} = 10010$, como $S(\widehat{c}) = 110$, decodificamos a mesma como sendo a palavra-código

$$c = \widehat{c} - 11000 = 01010. \tag{51}$$

Por conta das características do canal de comunicação $c = 01010$ é de fato a palavra-código enviada (o que equivale a dizer que em C_{110} o π-líder é único).

O que acontece se recebemos a mensagem $\widehat{c} = 10011$? Como $s(\widehat{c}) = 111$ e como 10011 é o π-líder de C_{111}, decodificamos então $\widehat{c}$ como sendo a palavra-código

$$c = \widehat{c} - 10011 = 00000. \tag{52}$$

E se escolhêssemos 00111 como π-líder de C_{111}? Neste caso decodificaríamos $\widehat{c} = 10011$ como sendo a palavra-código

$$c = \widehat{c} - 00111 = 10100. \tag{53}$$

Esta situação desconfortável é gerada pelo fato de que em C_{111} existem muitos π-líderes (na verdade todos os elementos de C_{111} são π-líderes). Isto acontecerá com qualquer vetor situado nas últimas quatro linhas da tabela.

6. DECODIFICADOR DE OZEN-SIAP

Nesta seção descreveremos um método de decodificação para informações transmitidas em canais de comunicação onde os erros ocorrem em rajadas nos primeiros blocos e aleatoriamente nos últimos blocos. Nosso método é uma extensão natural do método de decodificação proposto por Ozen e Siap em [15].

Como já sabemos, a métrica de blocos de Rosenbloom-Tsfasman é eficiente para a correção de erros em rajadas nos primeiros blocos. Para a correção de erros em blocos aleatórios utilizaremos a métrica de blocos, introduzida recentemente por Feng, Xu e Hickernell em [3].

Seja $\pi = (\pi_1, \pi_2, \ldots, \pi_n)$ uma partição de um inteiro positivo N e $V = V_1 \oplus V_2 \oplus \ldots \oplus V_n$ a decomposição de $\mathbf{F}_q^N$ como soma direta dos espaços $V_i = \mathbf{F}_q^{\pi_i}$, $1 \leq i \leq n$ (como na definição da métrica de blocos de Rosenbloom-Tsfasman). Dado $x = x_1 + x_2 + \ldots + x_n$ em V, $x_i \in V_i$ para cada $1 \leq i \leq n$, o **peso de blocos** w_Π de x é o número de blocos x_i não nulos de x:

$$w_\Pi(x) = |\{i : x_i \neq \mathbf{0}\}|. \tag{54}$$

Associado ao peso de blocos temos a **distância de blocos** d_Π: dados $x, y \in V$,

$$d_\Pi(x, y) = w_\Pi(x - y). \tag{55}$$

A distância de blocos é um métrica em V. Assim como em espaços de Hamming, a capacidade de correção de erros de um código C em relação a métrica de blocos é dada em função da distância mínima (ver [3]): se

$$d_\Pi(C) = \min\left\{d_\Pi\left(c, c'\right) : c \neq c' \in C\right\} \tag{56}$$

é a **distância mínima de blocos** de C, então

$$\left\lfloor \frac{d_\Pi(C) - 1}{2} \right\rfloor \tag{57}$$

é a sua **capacidade de correção de erros** (o raio de empacotamento de C no espaço métrico (V, d_Π)). A métrica de blocos mostra-se eficiente para a correção de

erros em blocos aleatórios (simultâneos erros em rajadas localizados).

Estamos prontos para descrever o decodificador de Ozen-Siap, que intercala a métrica de blocos de Rosenbloom-Tsfasman com a métrica de blocos.

Teorema 12 *Seja C um $((s_1,t_1),\ldots,(s_m,t_m))$ código linear, $C_{t_1} = p_{(1,2,\ldots,t_1)}(C)$ e $r = d_\pi(C_{t_1})$. Se $\dim(C_{t_1}) = \sum s_i$, então C corrige até $r-1$ erros nos $r-1$ primeiros blocos e até $n-t_1$ erros nos últimos $n-t_1$ blocos. Se $\dim(C_{t_1}) < \sum s_i$, então existe uma matriz geradora de C da forma*

$$\begin{pmatrix} G_1 & G_2 \\ \mathbf{0} & G_3 \end{pmatrix} \tag{58}$$

com $posto(G_1) = \dim(C_{t_1})$ sendo G_2 e G_3 matrizes triangulares inferiores (em relação a diagonal secundária). Nestas condições, se G_3 gera um código com distância mínima de blocos igual a s, então C corrige até $r-1$ erros nos primeiros $r-1$ blocos e até $\left\lfloor \frac{s-1}{2} \right\rfloor$ erros nos últimos $n-t_1$ blocos.

8. ALGORITMO PARA O DECODIFICADOR DE OZEN-SIAP

Finalizamos descrevendo um algoritmo simples para o decodificador de Ozen-Siap. Para o restante do texto C denotará um $((s_1,t_1),\ldots,(s_m,t_m))$ código linear, $C_1 = p_{(1,2,\ldots,t_1)}(C)$ e $r = d_\pi\left(\widetilde{C}\right)$.

1o. Caso: $\dim\left(\widetilde{C}\right) = \sum s_i$

Seja $G = \begin{pmatrix} G_1' & G_2' \end{pmatrix}$ uma matriz geradora de C como na demonstração do teorema 12. Sejam $g_{1,i}$ e $g_{2,i}$ as linhas de G_1' e G_2' respectivamente. Para o algoritmo são requeridos: uma lista contendo um π-líder de cada classe lateral de C_1; uma matriz de paridade de C_1 (para o cálculo da síndrome S_1 em relação a C_1). Agora suponha que $\widehat{c} = \widehat{c}_1 + \widehat{c}_2$ é uma mensagem recebida onde $\widehat{c}_1 \in V_1 \oplus \ldots \oplus V_{t_1}$ e $\widehat{c}_2 \in V_{t_1+1} \oplus \ldots \oplus V_n$. Os procedimentos do algoritmo são:

(1) Calcule $S_1(\widehat{c}_1)$;
(2) Se $S_1(\widehat{c}_1) = \mathbf{0}$, faça $c_1 = \widehat{c}_1$;
(3) Se $S_1(\widehat{c}_1) = v \neq \mathbf{0}$, faça $c_1 = \widehat{c}_1 - e_v$ onde e_v é um π-líder de $(C_1)_v$;
(4) Então, como $c_1 = \sum \alpha_i g_{1,i}$, faça $c_2 = \sum \alpha_i g_{2,i}$;
(5) Daí $c = c_1 + c_2$ é a palavra transmitida e finalize o algoritmo.

2o. Caso: $\dim\left(\widetilde{C}\right) < \sum s_i$

Seja

$$G = \begin{pmatrix} G_1 & G_2 \\ \mathbf{0} & G_3 \end{pmatrix} \tag{59}$$

uma matriz geradora de C como no enunciado do teorema 12. Sejam $g_{1,i}$, $g_{2,i}$, $g_{3,i}$ as linhas de G_1, G_2 e G_3 respectivamente. Para o algoritmo são requeridos: uma lista contendo um π-líder de cada classe lateral de C_1; uma lista contendo um Π-líder de cada classe lateral do código C_3 gerado por G_3; uma matriz de paridade de C_1 (para o cálculo da síndrome S_1 em relção a C_1); uma matriz de paridade de C_3 (para o cálculo da síndrome S_3 em relação a C_3). Agora suponha que $\widehat{c} = \widehat{c}_1 + \widehat{c}_2 + \widehat{c}_3$ é uma mensagem recebida onde $\widehat{c}_1 \in V_1 \oplus \ldots \oplus V_{t_1}$ e $\widehat{c}_2, \widehat{c}_3 \in V_{t_1+1} \oplus \ldots \oplus V_n$. Os procedimentos do algoritmo são:

(1) Calcule $S_1(\widehat{c}_1)$;
(2) Se $S_1(\widehat{c}_1) = \mathbf{0}$, faça $c_1 = \widehat{c}_1$;
(3) Se $S_1(\widehat{c}_1) = v \neq \mathbf{0}$, faça $c_1 = \widehat{c}_1 - e_v$ onde e_v é um π-líder de $(C_1)_v$;
(4) Então, como $c_1 = \sum \alpha_i g_{1,i}$, faça $c_2 = \sum \alpha_i g_{i,2}$ e calcule $S_3(\widehat{c}_3)$;
(5) Se $S_3(\widehat{c}_3) = \mathbf{0}$, faça $c_3 = \widehat{c}_3$;
(6) Se $S_3(\widehat{c}_3) = u \neq \mathbf{0}$, faça $c_3 = \widehat{c}_3 - e_u$ onde e_u é um Π-líder de $(C_3)_u$;
(7) Daí $c = c_1 + c_2 + c_3$ é a palavra transmitida e finalize o algoritmo.

Referências

[1] M.M.S. Alves, L. Panek and M. Firer, **Error-block codes and poset metrics**, Advances in Mathematics of Communications 2 (2008) 95-111.

[2] R.A. Brualdi, J.S. Graves and K.M. Lawrence, **Codes with a poset metric**, Discrete Mathematics 147 (1995) 57-72.

[3] K. Feng, L. Xu and F.J. Hickernell, **Linear error-block codes**, Finite Fields and Their Applications 12 (2006) 638-652.

[4] R.W. Hamming, **Error Detecting and Error Correcting Codes**, Bell System Technical Journal 29 (1950) 147-160.

[5] W.C. Huffman and V. Pless, **Fundamentals of Error-Correcting Codes**, Cambridge University Press (2003).

[6] J.Y. Hyun and H.K. Kim, **Maximum distance separable poset codes**, Designs, Codes and Cryptography (2008), doi:10.1007/s10623-008-9204-8.

[7] J.Y. Hyun and H.K. Kim, **The poset strutures admitting the extended binary Hamming code to be a perfect code**, Discrete Mathematics 288 (2004) 37-47.

[8] O. Keren and Simon Litsyn, **A Class of Array Codes Correcting Multiple Column Erasures**, IEEE Transactions on Information Theory 43 (1997) 1843-1851.

[9] Y. Lee, **Projective systems and perfect codes with a poset metric**, Finite Fields and Their Applications 10 (2004) 105-112.

[10] S. Ling and F. Özbudak, **Constructions and bounds on linear error-block codes**, Designs, Codes and Cryptography (2007), doi:10.1007/s10623-007-9119-9.

[11] J.J. Metzner, **On Correcting Bursts (and Random Errors) in Vector Symbol (n,k) Cyclic Codes**, IEEE Transactions on Information Theory 54 (2008) 1795-1807.

[12] L. Narici, **Functional Analysis and Valuation Theory**, Marcel Dekker, Inc., New York (1971).

[13] M. Ozen and I. Siap, **Codes over Galois rings with respect to the Rosenbloom-Tsfasman metric**, Journal of the Franklin Institute 344 (2007) 790-799.

[14] M. Ozen and I. Siap, **Linear Codes Over $\mathbf{F}_q[u]/(u^s)$ with Respect to the Rosenbloom-Tsfasman Metric**, Designs, Codes and Cryptography 38 (2006) 17-29.

[15] M. Ozen and I. Siap, **On the estructure and decoding of linear codes with respect to Rosenbloom-Tsfasman metric**, Selçuk Journal of Applied Mathematics 5 (2) (2004) 25-31.

[16] L. Panek, M. Firer, H.K. Kim and J.Y. Hyun, **Groups of linear isometries on poset structures**, Discrete Mathematics 308 (2008) 4116-4123.

[17] L. Panek, M. Firer and M.M.S. Alves, **Symmetry groups of Rosenbloom-Tsfasman spaces**, Discrete Mathematics (2008), doi: 10.1016/j.disc.2008.01.013.

[18] J. Quistorff, **On Rosenbloom and Tsfasman's generalization of the Hamming space**, Discrete Mathematics (2007), doi: 10.1016/j.disc.2007.01.005.

[19] M.M. Skriganov, **On linear codes with large weights simultaneously for the Rosenbloom-Tsfasman and Hamming metrics**, Journal of Complexity (2007), doi: 10.1016/j.jco.2007.02.004.

[20] M. Yu Rosenbloom and M. A. Tsfasman, **Codes for the m-metric,** Problems of Information Transmission 33 (1997) 45-52.

[21] C. Shannon, **A mathematical theory of communication**, Bell System Technical Journal 27 (1948) 379-423 and 623-656.

[22] D. Slepian, **A Class of Binary Signaling Alphabet**, Bell System Technical Journal 35 (1956) 203-234.

[23] V.K. Wei, **Generalized Hamming Weights for Linear Codes**, IEEE Transactions on Information Theory 37 (1991) 1412-1418.