International Journal of Pure and Applied Mathematics

Volume 48 No. 2 2008, 67-72

CODES SATISFYING THE CHAIN CONDITION OVER ROSENBLOOM-TSFASMAN SPACES

Luciano Panek[1] §, Emerson Lazzarotto[2], Fernando Mucio Bando[3]

[1,2,3]Department of Mathematics
UNIOESTE – Universia Brasil - Universidade Estadual do Oeste do Paraná
1300, Av. Tarquínio Joslin dos Santos
Foz do Iguaçu - PR, CEP 85870-650, BRAZIL
[1]e-mail: lucpanek@gmail.com

Abstract: Let $M_{n\times m}(\mathbb{F}_q)$ be the linear space of all $n \times m$ matrices over the finite field $\mathbb{F}_q$, equipped with the new weight introduced by Rosenbloom and Tsfasman. In this paper we extend the concept of generalized Wei weights for Rosenbloom-Tsfasman weights and show that all linear codes satisfy the chain condition in $M_{n\times 1}(\mathbb{F}_q)$.

AMS Subject Classification: 94B05, 94B65
Key Words: Rosenbloom-Tsfasman weight, generalized Hamming weights, chain condition

1. Introduction

Let $M_{n\times m}(\mathbb{F}_q)$ be the linear space of all $n \times m$ matrices over the finite field $\mathbb{F}_q$. In 1997 Rosenbloom and Tsfasman equipped the space $M_{n\times m}(\mathbb{F}_q)$ with new weight (see [1]), called *Rosenbloom-Tsfasman weight* w_ρ, defined as follows: if $(a_{ij}) \in M_{n\times m}(\mathbb{F}_q)$, then

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

assuming $\max \emptyset = 0$. Moreover, if $n = 1$ the Rosenbloom-Tsfasman weight w_ρ over space $M_{1\times m}(\mathbb{F}_q)$ are the Hamming weight w_H of classical coding theory. The Rosenbloom-Tsfasman weights constitute an important family of weights which can be applied to concrete communication systems (see [1], [2]).

Received: July 4, 2008

§Correspondence author

Motivated by several applications in cryptography, Victor Wei introduced in 1991 the concept of generalized Hamming weights (see [3]). We extend here the concept of generalized Wei weights to Rosenbloom-Tsfasman weights. If D is a linear subspace of the linear code C we write $D \leq C$. When D is a proper subspace of C we write $D < C$. The *generalized Rosenbloom-Tsfasman weight* $\|\cdot\|_\rho$, we write *generalized ρ weight*, of a r-dimensional subspace $D \leq M_{n\times m}(\mathbb{F}_q)$ is defined as

$$\|D\|_\rho = \sum_{j=1}^{m} \max\{i : a_{ij} \neq 0, a_{ij} \text{ element of the } j\text{-th column of } (a_{ij}) \in D\}.$$

The *r-th minimum ρ weight* of a k-dimensional code $C \leq M_{n\times m}(\mathbb{F}_q)$ is

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

A k-dimensional code C with *ρ weights hierarchy* $(d_1(C), \ldots, d_k(C))$ is called an $[n \cdot m; k; d_1(C), \ldots, d_k(C)]_q$*-code*. If $n = 1$, then the r-th minimum ρ weight is usual r-th minimum Hamming weight of $M_{1\times m}(\mathbb{F}_q) \simeq \mathbb{F}_q^m$.

As in [3], we have the monotonicity of the minimum ρ weights.

Proposition 1.1. *For any $[n \cdot m; k; d_1(C), \ldots, d_k(C)]_q$-code $C \leq M_{n\times m}(\mathbb{F}_q)$ we have that*

$$1 \leq d_1(C) < d_2(C) < \ldots < d_k(C) \leq n \cdot m.$$

Proof. We observed initially that $d_{r-1}(C) \leq d_r(C)$. In fact, let D_{r-1} and D_r be subcodes of C with dimensions $r-1$ and r respectively such that $\|D_{r-1}\|_\rho = d_{r-1}(C)$ and $\|D_r\|_\rho = d_r(C)$. If $\|D_{r-1}\|_\rho > \|D_r\|_\rho$, then for any subcode $D'_{r-1} < D_r$ of dimension $r-1$ we have that $\|D'_{r-1}\|_\rho \leq \|D_r\|_\rho < \|D_{r-1}\|_\rho = d_r(C)$. But this contradicts the minimality of $d_r(C)$. We claim that the inequality $d_{r-1}(C) \leq d_r(C)$ is strict. Let D be a subcode of C with dimension r such that $\|D\|_\rho = d_r(C)$. Then there exists s such that

$$\{i : a_{is} \neq 0, a_{is} \text{ element of the } s\text{-th column of } (a_{ij}) \in D\} \neq \emptyset.$$

If i' is the maximal element of the above set, then $D_{i'} := \{(x_{ij}) \in D : x_{i's} = 0\}$ is a subcode of C with dimension $r-1$ such that

$$d_{r-1}(C) \leq \|D_i\|_\rho \leq \|D\|_\rho - 1 = d_r(C) - 1. \qquad \square$$

Since $d_{r+1}(C) \geq d_r(C) + 1$ and $d_k(C) \leq n \cdot m$ we immediately get the generalized *Singleton bound.*

Corollary 1.1. *For an $[n \cdot m; k; d_1(C), \ldots, d_k(C)]_q$-code $C \leq M_{n\times m}(\mathbb{F}_q)$,*

$$r \leq d_r(C) \leq n \cdot m - k + r.$$

We investigated in this work the possibility of the existence of new codes satisfying the chain condition with the generalized ρ weights. A k-dimensional code $C \leq M_{n\times m}(\mathbb{F}_q)$ satisfies the *chain condition* if there exists a sequence of linear subspaces

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

with $\|D_r\|_\rho = d_r(C)$ and $\dim(D_r) = r$ for all $r \in \{1, 2, \ldots, k\}$. In the case that $n = 1$ ($w_\rho = w_H$) the Hamming codes, dual Hamming codes, Reed-Muller codes for all orders, maximum-separable-distance codes and Golay codes satisfy the chain condition (see [4]).

In this work we will show that any code C over the Rosenbloom-Tsfasman space $M_{n\times 1}(\mathbb{F}_q) \simeq \mathbb{F}_q^n$ satisfies the chain condition. Moreover, the sequence of linear subspaces $D_1 < D_2 < \ldots < D_{k-1} < D_k = C$ that achieve the minimum Rosenbloom-Tsfasman weights in $M_{n\times 1}(\mathbb{F}_q)$ is unique. It follows that if $\|D_r\|_\rho = d_r(C)$ for all $r \in \{1, 2, \ldots, k\}$, then $D_1 < D_2 < \ldots < D_{k-1} < D_k = C$.

2. Codes Satisfying the Chain Condition

Initially we give an example of a code satisfying the chain condition with ρ weight that does not satisfy the chain condition with the usual Hamming weight.

Example 2.1. The $[9; 3; 3, 6, 9]_2$-code

$$C = \text{span}\left\{ (111000000)^T \ , \ (000111100)^T \ , \ (000001111)^T \right\}$$

does not satisfy the chain condition with the generalized Hamming weights. Now with the ρ weight the $[9; 3, 3, 7, 9]_2$-code C satisfies the chain condition:

$$\text{span}\left\{ (111000000)^T \right\} \subset \text{span}\left\{ \begin{array}{l} (111000000)^T \\ (000111100)^T \end{array} \right\} \subset C.$$

Now we will show that every code C satisfies the chain condition in the Rosenbloom-Tsfasman space $M_{n\times 1}(\mathbb{F}_q)$.

Theorem 2.1. *Let C by a code in $M_{n\times 1}(\mathbb{F}_q) \simeq \mathbb{F}_q^n$, endowed with the ρ weight. Then C satisfies the chain condition.*

Proof. We observed that $1 \leq d_1(C) < d_2(C) < \ldots < d_k(C) \leq n$. Since

$$\|D\|_\rho = \max\{i : x_i \neq 0, (x_1, \ldots, x_m) \in D\},$$

so that for every $j \in \{1, 2, \ldots, k\}$ there is $v_j \in C$ such that $w_\rho(v_j) = d_j(C)$.

The set $\{v_1, v_2, \ldots, v_k\}$ is clearly linearly independent and consequently

$$\dim\left(\text{span}\left\{v_1, v_2, \ldots, v_j\right\}\right) = j$$

and

$$\text{span}\left\{v_1\right\} < \text{span}\left\{v_1, v_2\right\} < \ldots < \text{span}\left\{v_1, v_2, \ldots, v_k\right\} = C.$$

Since $\left\|\text{span}\left\{v_1, v_2, \ldots, v_j\right\}\right\|_\rho = d_j\left(C\right)$ for every $j \in \{1, 2, \ldots, k\}$, we find that C satisfies the chain condition. □

They are not many the sequences of subspaces that achieve the generalized minimum poset-weights, as display the next result.

Theorem 2.2. *If $C \leq M_{n\times 1}\left(\mathbb{F}_q\right) \simeq \mathbb{F}_q^n$ satisfies the chain condition, then there is a unique sequence of subspaces that achieve the generalized minimum ρ weights.*

Proof. Let $k = \dim\left(C\right)$, $\left(d_1\left(C\right), d_2\left(C\right), \ldots, d_k\left(C\right)\right)$ the ρ weights hierarchy of C and $\{e_1, e_2, \ldots, e_n\}$ the canonical base of $\mathbb{F}_q^n$. Let $D_1 \leq C$ an 1-dimensional subcode of C such that $\left\|D_1\right\|_\rho = d_1\left(C\right)$. We will prove that D_1 is unique. In fact, let $D_1' \leq C$ be an 1-dimensional subcode of C such that $\left\|D_1'\right\|_\rho = d_1\left(C\right)$ and $D_1' \cap D_1 = \{\mathbf{0}\}$. Then there are $u \in D_1$ and $v \in D_1'$ such that

$$u = \alpha_1 e_1 + \ldots + \alpha_{d_1(C)-1} e_{d_1(C)-1} + e_{d_1(C)},$$

$$v = \beta_1 e_1 + \ldots + \beta_{d_1(C)-1} e_{d_1(C)-1} + e_{d_1(C)},$$

with $\alpha_j \neq \beta_j$ for some $j \in \{1, 2, \ldots, d_1\left(C\right) - 1\}$. If

$$l = \max\left\{j \in \{1, 2, \ldots, d_1\left(C\right) - 1\} : \alpha_j \neq \beta_j\right\},$$

it follow that $u + (q-1)\, v$ is a non zero vector of C such that $\left\|u + (q-1)\, v\right\|_\rho = l < d_1\left(C\right)$. But this contradicts the minimality condition of the 1-th minimum Rosenbloom-Tsfasman weight of the code C. We conclude that D_1 is the unique subcode of C that achieve the 1-th minimum Rosenbloom-Tsfasman weight of C.

The result follows now by induction on $\dim\left(D_r\right) = r$. Let $D_1 < D_2 < \ldots < D_{t-1} < C$, with $t - 1 < k$, be the sequence of linear subspaces that achieve the r-th minimum Rosenbloom-Tsfasman weights of the code C with $r \in \{1, 2, \ldots, t-1\}$. Suppose that D_t and D_t' are t-dimensional subcodes of C containing D_{t-1} such that $D_t \neq D_t'$ and $\left\|D_t\right\|_\rho = \left\|D_t'\right\|_\rho = d_t\left(C\right)$. Then there exists $w \in D_t$ and $z \in D_t'$ such that

$$w = \gamma_1 e_1 + \ldots + \gamma_{d_t(C)-1} e_{d_t(C)-1} + e_{d_t(C)},$$

$$z = \eta_1 e_1 + \ldots + \eta_{d_t(C)-1} e_{d_t(C)-1} + e_{d_t(C)},$$

with $\gamma_j \neq \eta_j$ for some $j \in \{1, 2, \ldots, d_t(C) - 1\}$. If

$$m = \max\{j \in \{1, 2, \ldots, d_t(C) - 1\} : \gamma_j \neq \eta_j\},$$

then $x = w + (q-1)z$ is a non zero vector of C such that $\|x\|_\rho = m < d_t(C)$ and $x \notin D_{t-1}$. We denote by $\operatorname{span} X$ the linear subspace of $\mathbb{F}_q^n$ spanned by the set $X \subset \mathbb{F}_q^n$, and then, for every linearly independent subset $\{y_1, \ldots, y_{t-1}\} \subset D_{t-1}$, we find that $\operatorname{span}\{y_1, \ldots, y_{t-1}, x\}$ is a t-dimensional subspace of C such that $\|\operatorname{span}\{y_1, \ldots, y_{t-1}, x\}\|_\rho \leq d_t(C) - 1$, contradicting the minimality of $d_t(C)$.

By induction, the sequence of linear subspaces $D_1 < D_2 < \ldots < D_{k-1} < C$ that achieve the r-th minimum Rosenbloom-Tsfasman weights of code C is unique. □

For each subset $P' \subseteq \{(1,1), (2,1), \ldots, (n,m)\}$ we denoted by $[P']$ the subspace of $M_{n\times m}(\mathbb{F}_q)$ generated by the base $\{e_{rs}\}_{(r,s)\in P'}$, e_{rs} the canonical vector of $M_{n\times m}(\mathbb{F}_q)$. So, if $P_i = \{(1,i), (2,i), \ldots, (n,i)\}$ we have that $M_{n\times m}(\mathbb{F}_q)$ is a direct sum

$$[P_1] \oplus \ldots \oplus [P_m].$$

As $[P_i]$ is isometric to the $M_{n\times 1}(\mathbb{F}_q)$ for every $i \in \{1, 2, \ldots, m\}$, Theorems 2.1 and 2.2 assure that:

Corollary 2.1. *Let C be a linear code over the space $M_{n\times m}(\mathbb{F}_q)$, endowed with the ρ weight, such that $C \leq [P_i]$ for some $i \in \{1, 2, \ldots, m\}$. Then there exists only one sequence of linear subspaces $D_1 < D_2 < \ldots < D_{k-1} < C$ with the property that $\|D_r\|_\rho = d_r(C)$ for all $r \in \{1, 2, \ldots, k\}$. Consequently, if $D_1, D_2, \ldots D_{k-1}, D_k = C$ is a sequence of subspaces of C such that $\|D_j\|_\rho = d_j(C)$ and $\dim(D_j) = j$ for all $j \in \{1, 2, \ldots, k\}$, then $D_1 < D_2 < \ldots < D_{k-1} < C$.*

Now we present a lower bound for the number of codes satisfying the chain condition.

Proposition 2.1. *The number of codes satisfying the chain condition in the Rosenbloom-Tsfasman space $M_{n\times m}(\mathbb{F}_q)$ is larger that or equal to the*

$$\sum_{i=1}^{m}\sum_{j=1}^{n}\prod_{k=1}^{j}\frac{\left(q^n - q^{k-1}\right)}{\left(q^j - q^{k-1}\right)}.$$

Proof. If $P_i = \{(1,i), (2,i), \ldots, (n,i)\}$ we have that $M_{n\times m}(\mathbb{F}_q)$ is a direct sum

$$[P_1] \oplus \ldots \oplus [P_m],$$

where each $[P_i]$ is isometric to the $M_{n\times 1}(\mathbb{F}_q)$. Corollary 2.1 assures that all code

$C \leq [P_i]$ satisfies the chain condition. Therefore the number of j-dimensional codes of $[P_i]$ satisfying the chain condition equals

$$\prod_{k=1}^{j} \frac{\left(q^n - q^{k-1}\right)}{\left(q^j - q^{k-1}\right)}$$

for each $i \in \{1, 2, \ldots, m\}$. This completes the proof of the proposition. □

References

[1] M.Y. Rosenbloom, M.A. Tsfasman, Codes for the m-metric, *Probl. Inf. Transm.*, **33** (1997), 45-52.

[2] M.M. Skriganov, Coding theory and uniform distributions, *St. Petersburg Math. J.*, **13**, No. 2 (2002), 301-337.

[3] V.K. Wei, Generalized Hamming weights for linear code, *IEEE Trans. Inform. Theory*, **37**, No. 5 (1991), 1412-1418.

[4] V.K. Wei, K. Yang, On the generalized Hamming weights for product code, *IEEE Trans. Inform. Theory*, **39**, No. 5 (1993), 1709-1713.