International Journal of Pure and Applied Mathematics
Volume 85 No. 4 2013, 751-759
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v85i4.11

CODES SATISFYING THE CHAIN CONDITION WITH POSET WEIGHTS

Luciano Panek

Center of Exact Sciences and Engineering
State University of West Parana
85870-650, Foz do Iguaçu, PR, BRAZIL

Abstract: In this paper we extend the concept of generalized Hamming weights for poset-weight codes and show that any linear code C satisfies the chain condition if support of C is a totally ordered subposet.

AMS Subject Classification: 94B05, 06A06
Key Words: poset codes, generalized Hamming weights, chain condition, total order

1. Introduction

In 1995, Brualdi, Graves and Lawrence ([1]) extended the scope of metrics to be considered in coding theory, considering the notion of poset-codes, as we briefly introduce in the next paragraph.

Let $(P, \leq)$ be a partially ordered finite set, abbreviated as *poset*, and assume $P = \{1, 2, \ldots, n\}$. An *ideal* I of P is a subset of P with the property that $y \in I$ and $x \leq y$, implies that $x \in I$. Given $A \subset P$, we denote by $\langle A \rangle$ the smallest ideal of P containing A. Given $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, the *support* of x is the set

$$\operatorname{supp}(x) := \{i \in P : x_i \neq 0\}.$$

We define the *poset-weight* w_P of x (also called P-*weight*), as the cardinality of the smallest ideal containing $\operatorname{supp}(x)$, that is

Received: February 21, 2013

$$w_P(x) := |\langle \mathrm{supp}(x) \rangle| .$$

The P-weight w_P induces a metric in the vector space $\mathbb{F}_q^n$ defined by $d_P(x,y) = w_P(x-y)$ ([1, Lemma 1.1]). If P is *antilinear*, i.e., $x \leq y$ iff $x = y$, then the P-weight is the usual Hamming weight w_H. An important family of poset weights (non-Hamming weights) which can be applied to concrete communication systems are Rosenbloom-Tsfasman weights (see [6], [5]), and a particular case of interest is a *linear (or total)* order: $i_1 < i_2 < \ldots < i_n$.

Motivated by several applications in cryptography, Wei introduced in 1991 the concept of generalized Hamming weights ([7]). We extend here the concept of generalized Hamming weights to poset-weights. Let $P = \{1, 2, \ldots, n\}$ be a partially ordered set. 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 P-weight* $\|\cdot\|_P$ of a r-dimensional subspace $D \leq \mathbb{F}_q^n$ is defined as

$$\|D\|_P = \left| \bigcup_{x \in D} \langle \mathrm{supp}(x) \rangle \right| .$$

The *r-th P-weight* of a k-dimensional code $C \leq \mathbb{F}_q^n$ is

$$d_{(P,r)}(C) = \min \{ \|D\|_P : D \leq C, \dim(D) = r \} .$$

Since it will cause no ambiguity, we denote $d_{(P,r)}(c)$ simply by $d_r(C)$. A k-dimensional code $C \leq \mathbb{F}_q^n$ with P-weights hierarchy $(d_1(C), \ldots, d_k(C))$ is called an $[n; k; d_1(C), \ldots, d_k(C)]_q$*-code*.

Many new perfect codes have been found with such poset-metrics (see [2], for example). Motivated by this fact we investigated in this work the possibility of the existence of new codes satisfying the chain condition with the generalized P-weights. In the terminology of Wei and Yang ([8]), a k-dimensional code $C \leq \mathbb{F}_q^n$ satisfies the *chain condition* if there exists a sequence of nested linear subspaces (*maximal flag*)

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

with $\|D_r\|_P = d_r(C)$ and $\dim(D_r) = r$ for every $r \in \{1, 2, \ldots, k\}$. If P is antilinear ($w_P = w_H$) the Hamming codes, dual Hamming codes, Reed-Muller codes for all orders, maximum-separable-distance codes and Golay codes satisfy the chain condition (see [8]). Moreover, every perfect code must be a code satisfying the chain condition (see [3]).

In this work we will show that any poset-code $C \leq \mathbb{F}_q^n$ with support totally ordered satisfies the chain condition. Moreover, the sequence of linear subspaces $D_1 < D_2 < \ldots < D_{k-1} < D_k = C$ that achieve the P-weights is unique. It will follow that if $\|D_r\|_P = d_r(C)$ with $D_r \leq C$ for every $r \in \{1, 2, \ldots, k\}$, then $D_1 < D_2 < \ldots < D_{k-1} < D_k = C$.

2. Codes Satisfying the Chain Condition

Before we show that any poset-code with support totally ordered satisfies the chain condition, we give an example in the case that P is a weak order and shows the monotonicity of the minimum poset-weights.

We denote by $spanX$ the linear subspace of $\mathbb{F}_q^n$ spanned by the set $X \subset \mathbb{F}_q^n$.

Example 2.1. Let $P = n_1\mathbf{1} \oplus \ldots \oplus n_9\mathbf{1}$ be the *weak order* given by the ordinal sum of the antilinear subposets $n_1\mathbf{1}, \ldots, n_9\mathbf{1}$ with 3 elements. Explicitly, P is the poset whose underlying set is

$$\{1, 2, \ldots, 27\} = n_1\mathbf{1} \cup \ldots \cup n_9\mathbf{1},$$

with

$$n_1\mathbf{1} = \{1, 2, 3\}, n_2\mathbf{1} = \{4, 5, 6\}, \ldots, n_9\mathbf{1} = \{25, 26, 27\}$$

and order relation are given by $x < y$ if and only if $x \in n_i\mathbf{1}$, $y \in n_j\mathbf{1}$ for some i, j with $i < j$.

If $M_{9\times 3}(\mathbb{F}_2)$ is the linear space of all 9×3 matrices over the finite field $\mathbb{F}_2$, we defined the poset-weight w_P of

$$x = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \\ \vdots & \vdots & \vdots \\ a_{22} & a_{23} & a_{24} \\ a_{25} & a_{26} & a_{27} \end{pmatrix} \in M_{9\times 3}(\mathbb{F}_2)$$

as $w_W(x) = w_W(a_1, a_2, a_3, \ldots, a_{25}, a_{26}, a_{27})$.

Consider the $[27;3]_2$ code C spanned by $\{v_1, v_2, v_3\}$ where

$$v_1 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \; v_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \; v_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Considering the usual Hamming weight w_H, C is a $[27;3;3,6,9]_2$-code that does not satisfy the chain condition, since the weight hierarchy is achieved by the subspaces $span\{v_1\}$, $span\{v_2, v_3\}$, $span\{v_1, v_2, v_3\} = C$:

$$\begin{aligned} d_{(H,1)} &= 3 = \|span\{v_1\}\| \\ d_{(H,2)} &= 6 = \|span\{v_2, v_3\}\| \\ d_{(H,3)} &= 9 = \|C\| \end{aligned}$$

Now over the weak-metric space $M_{9\times 3}(\mathbb{F}_2)$, C is a $[27;3;7,19,25]_2$-code that satisfies the chain condition with

$$\begin{aligned} d_{(W,1)} &= 7 = \|span\{v_1\}\| \\ d_{(W,2)} &= 19 = \|span\{v_1, v_2\}\| \\ d_{(W,3)} &= 25 = \|C\|. \end{aligned}$$

We observe that

$$\operatorname{supp}(C) = \{1, 4, 7, 11, 14, 17, 21, 24, 27\}$$

is totally ordered in weak order W.

As in [7], we have the monotonicity of the minimum poset-weights.

Proposition 2.1. *For any $[n;k;d_1(C),\ldots,d_k(C)]_q$-code $C \leq \mathbb{F}_q^n$ we have that*

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

Proof. We first observe that $d_{r-1}(C) \leq d_r(C)$. Indeed, let D_{r-1} and D_r subcodes of C with dimensions $r-1$ and r respectively such that $\|D_{r-1}\|_P = d_{r-1}(C)$ and $\|D_r\|_P = d_r(C)$. If $\|D_{r-1}\|_P > \|D_r\|_P$, then for any subcode

$D'_{r-1} < D_r$ of dimension $r-1$ we have that $\left\|D'_{r-1}\right\|_P \leq \|D_r\|_P < \|D_{r-1}\|_P = d_r(C)$. 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 a subcode of C with dimension r such that $\|D\|_P = d_r(C)$. If i is a maximal element of $\operatorname{supp}(D)$, then $D_i := \{v \in D : v_i = 0\}$ is a subcode of C with dimension $r-1$ such that

$$d_{r-1}(C) \leq \|D_i\|_P \leq \|D\|_P - 1 = d_r(C) - 1.$$

□

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

Corollary 2.1. *For an $[n; k; d_1(C), \ldots, d_k(C)]_q$-code $C \leq \mathbb{F}_q^n$,*

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

Now we will show that any poset-code C with $\operatorname{supp}(C)$ totally ordered satisfies the chain condition.

Theorem 2.1. *Let C be a code in $\mathbb{F}_q^n$, endowed with a poset-weight w_P. If $\operatorname{supp}(C)$ is a totally ordered subposet of P then C satisfies the chain condition.*

Proof. Since $\operatorname{supp}(C)$ is totally ordered, for every $u, v \in C$ we have that either $\langle \operatorname{supp}(u) \rangle \subseteq \langle \operatorname{supp}(v) \rangle$ or $\langle \operatorname{supp}(v) \rangle \subseteq \langle \operatorname{supp}(u) \rangle$ and it follows that

$$\|D\|_P = \left| \bigcup_{u \in D} \langle \operatorname{supp}(u) \rangle \right| = \max \{ |\langle \operatorname{supp}(u) \rangle| : u \in D \},$$

so that for every $j \in \{1, 2, \ldots, k\}$ there is $v_j \in C$ such that $w_P(v_j) = d_j(C)$. The set $\{v_1, v_2, \ldots, v_k\}$ is linearly independent, since $w_P(v_1) < \ldots < w_P(v_k)$ (see Proposition 2.1) and $\operatorname{supp}(C)$ is totally ordered. Consequently

$$\dim(\mathit{span}\{v_1, v_2, \ldots, v_j\}) = j$$

and

$$\mathit{span}\{v_1\} < \mathit{span}\{v_1, v_2\} < \ldots < \mathit{span}\{v_1, v_2, \ldots, v_k\} = C.$$

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

Theorem 2.2. *Let $C \leq \mathbb{F}_q^n$ be a code of a space endowed with a P-weight and suppose that $\operatorname{supp}(C)$ is a totally ordered subposet of P. Then there is a unique maximal flag that achieves the generalized P-weights hierarchy.*

Proof. Let $k = \dim(C)$, $(d_1(C), d_2(C), \ldots, d_k(C))$ the P-weights hierarchy of C and $\{e_1, e_2, \ldots, e_n\}$ the canonical base of $\mathbb{F}_q^n$. We denote $\text{supp}(C) = \{i_1, i_2, \ldots, i_m\}$, assume it is ordered by $i_1 < i_2 < \ldots < i_m$ and let $D_1 \leq C$ an 1-dimensional subcode of C such that $\|D_1\|_P = d_1(C)$. We will prove that D_1 is unique. Indeed, let $D_1' \leq C$ be an 1-dimensional subcode of C such that $\|D_1'\|_P = d_1(C)$ and $D_1' \cap D_1 = \{\mathbf{0}\}$. Then there are $u \in D_1$ and $v \in D_1'$ such that

$$u = \alpha_1 e_{i_1} + \ldots + \alpha_{r-1} e_{i_{r-1}} + e_{i_r},$$

$$v = \beta_1 e_{i_1} + \ldots + \beta_{r-1} e_{i_{r-1}} + e_{i_r},$$

with $\alpha_j \neq \beta_j$ for some $j \in \{1, 2, \ldots, r-1\}$ and $w_P(u) = w_P(v) = w_P(e_{i_r}) = d_1(C)$. If

$$l = \max\{j \in \{1, 2, \ldots, r-1\} : \alpha_j \neq \beta_j\},$$

it follow that $u - v$ is a non zero vector of C such that

$$w_P(u - v) = w_P(e_{i_l}) < d_1(C),$$

since $l < r$. But this contradicts the minimality condition of the 1-th P-weight of the code C, since $u - v \in C$. We conclude that D_1 is the unique subcode of C that achieve the 1-th P-weight of C.

The result follows now by induction on $\dim(D_r) = r$. 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 Hamming P-weights of the code C with $r \in \{1, 2, \ldots, t-1\}$, assures by Theorem 2.1. 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 $\|D_t\|_P = \|D_t'\|_P = d_t(C)$. Then there exist $w \in D_t$ and $z \in D_t'$ such that

$$w = \gamma_1 e_{i_1} + \ldots + \gamma_{s-1} e_{i_{s-1}} + e_{i_s},$$

$$z = \eta_1 e_{i_1} + \ldots + \eta_s e_{i_{s-1}} + e_{i_s},$$

with $\gamma_j \neq \eta_j$ for some $j \in \{1, 2, \ldots, s-1\}$ and $w_P(w) = w_P(z) = w_P(e_{i_s}) = d_t(C)$. If

$$l = \max\{j \in \{1, 2, \ldots, s-1\} : \gamma_j \neq \eta_j\},$$

then $x = w - z$ is a non zero vector of C such that $w_P(x) = w_P(e_{i_l}) < d_t(C)$ and $x \notin D_{t-1}$. Then, for every linearly independent subset $\{y_1, \ldots, y_{t-1}\} \subset D_{t-1}$, we find that $span\{y_1, \ldots, y_{t-1}, x\}$ is a t-dimensional subspace of C such that $\|span\{y_1, \ldots, y_{t-1}, x\}\|_P \leq d_t(C) - 1$, 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 P-weights of code C is unique. □

The next corollary is an immediate consequence of the previous theorem.

Corollary 2.2. *Let C be a linear code in $\mathbb{F}_q^n$, endowed with a poset-weight w_P, such that $\mathrm{supp}(C)$ is totally ordered. If D_1,D_2,..., D_{k-1},$D_k = C$ is a sequence of subspaces of C such that $\|D_r\|_P = d_r(C)$ for all $r \in \{1, 2, \ldots, k\}$ and $\dim(D_j) = j$, then $D_1 < D_2 < \ldots < D_{k-1} < C$.*

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

Proposition 2.2. *Let $P = \{1, 2, \ldots, n\}$ be a poset and suppose that $P = P_1 \cup \ldots \cup P_r$ is a partition of P into r disjoint linear subposets. Then*

$$\sum_{i=1}^{r} \sum_{j=1}^{\nu_i} \prod_{k=1}^{j} \frac{\left(q^{\nu_i} - q^{k-1}\right)}{\left(q^j - q^{k-1}\right)}$$

is a lower bound for the number of codes satisfying the chain condition in the space $\left(\mathbb{F}_q^n, d_P\right)$, where $\nu_i = |P_i|$ with $i \in \{1, 2, \ldots, r\}$ and r is larger that or equal to the size of the largest antilinear subposet of P.

Proof. For each subset $P' \subseteq P$ we denoted by $[P']$ the subspace of $\mathbb{F}_q^n$ generated by the base $\{e_i\}_{i \in P'}$, e_i the canonical vector of $\mathbb{F}_q^n$. So, if $P = \bigcup_{i=1}^{r} P_j$ is a partition (disjoint union of sets) we have that $\mathbb{F}_q^n$ is a direct sum

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

As P_i is a linear subposet for every $i \in \{1, 2, \ldots, r\}$, Theorem 2.1 ensures that any code $C \leq [P_i]$ satisfies the chain condition. Therefore the number of j-dimensional codes of $[P_i]$ satisfying the chain condition equals

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

for each $i \in \{1, 2, \ldots, r\}$. This completes the proof of the Proposition. The Dilworth's Theorem (see [4]) assures that P can be partitioned into r chains if the largest antilinear in the poset P has size r. □

Let $\{e_1, e_2, \ldots, e_n\}$ be the canonical base of $\mathbb{F}_q^n$. The trivial code $C = span\{e_1, e_2, \ldots, e_n\}$ obviously satisfies the chain condition, independently of the poset structure on $\mathbb{F}_q^n$. This fact can be generalized in the following way: let

$$C = C_1 \oplus C_2 \oplus \ldots \oplus C_t$$

be a linear code in $\mathbb{F}_q^n$, endowed with a P-weight w_P, such that

$$\operatorname{supp}(C) = \operatorname{supp}(C_1) \cup \operatorname{supp}(C_2) \cup \ldots \cup \operatorname{supp}(C_t)$$

is a disjoint union of chains. Its follows from theorem 2.2 there is a unique chain

$$D_1^{(i)} \subset D_2^{(i)} \subset \ldots \subset D_{k_i}^{(i)} = C_i$$

such that $\left\| D_j^{(i)} \right\|_P = d_j(C_i)$ for every $j \in \{1, 2, \ldots, k_i\}$ for all $i \in \{1, 2, \ldots, t\}$. Suppose now that

$$\left\| D_{k_i}^{(i)} \right\|_P \leq \left\| D_1^{(i+1)} \right\|_P$$

for every $i \in \{1, 2, \ldots, t-1\}$. Then, using the same kind of reasoning used in the proof of Theorem 2.1, it is easy to see that C satisfies the chain condition. Moreover, there is a unique chain that realizes the hierarchy of the generalized P-weights, as in Theorem 2.2:

$$D_{(0,1)} \subset \ldots \subset D_{(0,k_1)} \subset \ldots \subset D_{(t-1,1)} \subset \ldots \subset D_{(t-1,k_t)}$$

with

$$D_{(i,j)} = D_j^{(i+1)} \oplus D_{k_i}^{(i)} \oplus D_{k_{i-1}}^{(i-1)} \oplus \ldots \oplus D_{k_0}^{(0)},$$

and $D_{r_0}^{(0)} = \{\mathbf{0}\}$.

References

[1] R. Brualdi, J. S. Graves, M. Lawrence, Codes with a poset metric, *Discrete Math.*, **147** (1995), 57-72, http://dx.doi.org/10.1016/0012-365X(94)00228-B.

[2] J. Y. Hyun, H. K. Kim, The poset structures admitting the extended binary Hamming code to be a perfect code, *Discrete Math.*, **288** (2004), 37-47, http://dx.doi.org/10.1016/j.disc.2004.07.010.

[3] F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland Mathematical Library (1997).

[4] B. S. W. Schroder, *Ordered Sets - An Introduction*, Birkhauser (2003).

[5] M. M. Skriganov, Coding theory and uniform distributions, *St. Petersburg Math. J.*, **13** (2002), 301-337.

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

[7] V. K. Wei, Generalized Hamming weights for linear code, *IEEE Trans. Inform. Theory*, **37** (1991), 1412-1418, http://dx.doi.org/10.1109/18.133259.

[8] V. K. Wei, K. Yang, On the generalized Hamming weights for product code, *IEEE Trans. Inform. Theory*, **39** (1993), 1709-1713, http://dx.doi.org/10.1109/18.259662.