Duality for Poset Codes

Allan de Oliveira Moura and Marcelo Firer

August 21, 2009

Abstract

In this work we extend Wei's Duality Theorem, relating the generalized Hamming weight hierarchy of a code to the hierarchy of the dual code, to the scope of codes with poset metrics. As a consequence of this duality theorem we prove some results concerning discrepancy of codes and chain condition for generalized weights.

keywords: Poset codes, generalized weight, weight duality.

1 Introduction

Let $\mathbb{F}_q^n$ be an n-dimensional vectorial space over the finite field with q elements $\mathbb{F}_q$. Let P be a partially ordered set (simply called *poset*) on the set $[n] = \{1, 2, ..., n\}$, the set of ordered coordinate positions of $\mathbb{F}_q^n$. We denote the partial order P by $\preceq_P$. A subset $I \subseteq P$ is called an (order) *ideal* if $i \in I$ and $j \preceq_P i$ implies that $j \in I$. Given a subset $A \subset P$, we denote by $\langle A \rangle_P$ the smallest ideal of P containing A, called the *ideal generated by* A. The *support* of a vector $\boldsymbol{v} = (v_1, v_2, ..., v_n)$ in $\mathbb{F}_q^n$ is the set

$$supp\,(\boldsymbol{v}) = \{i : v_i \neq 0\}$$

of the non-zero coordinate positions of $\boldsymbol{v}$. The *P-weight w_P of v* is the cardinality of the ideal of P generated by the support of $\boldsymbol{v}$:

$$w_P\,(\boldsymbol{v}) = |\langle supp\,(\boldsymbol{v})\rangle_P|\,,$$

where $|X|$ denotes the cardinality of the set X. The *P-distance* d_P between two vectors $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_q^n$ is defined as

$$d_P\,(\boldsymbol{u}, \boldsymbol{v}) = w_P\,(\boldsymbol{v} - \boldsymbol{u})\,.$$

The pair $\left(\mathbb{F}_q^n, d_P\right)$ is a metric space [1, Lema 1.1], so we may refer to d_P also as a *P-metric* and the metric space is called a *poset space* or *P-space.* A *P-linear code* is a vector subspace of the P-space $C \subseteq \mathbb{F}_q^n$. If $\dim C = k$ we refer to it as an $[n,k]_q$ *P-code.* The *minimal distance* between different elements of C (or the minimal weight of non-zero vectors in C) is denoted by $d_P(C)$.

Motivated by applications in cryptography, Victor Wei [2], introduced the concept of generalized Hamming weights that we now present. Given a subspace $D \subseteq \mathbb{F}_q^n$, the union

$$suppD := \bigcup_{\boldsymbol{v} \in D} supp(\boldsymbol{v})$$

is called the *support of* D and the cardinality of this support is called the *generalized Hamming weight of* D :

$$w(D) := |suppD| .$$

Given an $[n,k]_q$ code C, its *r-th generalized minimal Hamming weight* (for $1 \leq r \leq k$) is

$$d_r(C) := \min\left\{w(D) : D \subseteq C \text{ and } \dim D = r\right\}.$$

The same kind of generalization in the context of P-spaces was introduced in [3], defining the *(generalized) P-weight* of a subspace $D \subseteq \mathbb{F}_q^n$ as the cardinality of the ideal generated by its support, that is,

$$w_P(D) := \left|\langle suppD \rangle_P\right|,$$

and the *r-th minimal (generalized) P-weight* $d_r^P(C)$ *of an* $[n,k]_q$ P-code C as

$$d_r^P(C) = \min\left\{w_P(D) : D \subseteq C \text{ and } \dim D = r\right\}.$$

We observe that the first minimal P-weight is just the usual minimal P-weight: $d_1^P(C) = d_P(C)$.

The set $wh_P(C) := \left\{d_1^P(C), d_2^P(C), ..., d_k^P(C)\right\}$ of minimal P-weight is called the *P-weight hierarchy* of the $[n,k]_q$ P-code C.

We observe that considering the *anti-chain* poset H, defined by the trivial relations $i \preceq_H j \Leftrightarrow i = j$, d_H is the usual Hamming metric, so we may refer to H as the *Hamming poset*.

We state without proofs the following simple but relevant propositions:

Proposition 1 (Monotonicity) *[3, Proposition 2.1] The P-weight hierarchy of an $[n,k]_q$ P-code C is strictly increasing,*

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

Proposition 2 (Singleton Bound) *[3, Corollary 2.1] Given an $[n,k]_q$ P-code C,*

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

Given a subset $V \subseteq \mathbb{F}_q^n$ we define the *dual set*

$$V^{\perp} = \left\{ \boldsymbol{u} \in \mathbb{F}_q^n : \boldsymbol{u} \centerdot \boldsymbol{v} = 0 \,, \forall\, \boldsymbol{v} \in V \right\},$$

where

$$\boldsymbol{u} \centerdot \boldsymbol{v} = \sum_{n=1}^{n} u_i v_i$$

is the (formal) inner product.

The *opposite poset* $\overline{P}$ of a poset P is a partial order on the same set adjacent to P, defined by

$$j \preceq_{\overline{P}} i \iff i \preceq_P j.$$

The main result in this work is the *Duality Theorem*, a generalization of Wei's Duality Theorem [2, Theorem 3], establishing the relation between the weight hierarchy of a code and its dual.

Duality Theorem: Let C be an $[n,k]_q$ P-code and $C^{\perp}$ the dual code. Then the sets

$$X = wh_P(C) = \left\{ d_1^P(C), d_2^P(C), ..., d_k^P(C) \right\}$$

and

$$Y = \left\{ n+1-d_1^{\overline{P}}\left(C^{\perp}\right), n+1-d_2^{\overline{P}}\left(C^{\perp}\right), ..., n+1-d_{n-k}^{\overline{P}}\left(C^{\perp}\right) \right\}$$

are disjoint and

$$X \cup Y = \{1, 2, ..., n\}.$$

This theorem is proved in Section 3. The proof uses techniques of multisets, so that basic definitions and results concerning multisets need to be introduced in advance, and we do so in Section 2. At last, in Section 4, we explore some consequences of the Duality Theorem, relating the discrepancy and chain property of a code with the ones of its dual.

2 Multisets

The explicit use of multiset's techniques in the context of linear codes appears in [4] and [5], considering the usual environment of Hamming metric. We present here only the basic definitions and results needed for this work.

Definition 1 *A* multiset *over a set S in an unordered collection of elements of S, not necessarily distinct. The* multiplicity *of a multiset S is the map*

$$\gamma : S \to \mathbb{N},$$

that associates to each $s \in S$ the number $\gamma(s)$ of occurrences of s in S.

We frequently identify the multiset and its multiplicity. Two multisets γ_0 and γ_1 over the same set S are *equivalent* if there is a bijection σ of S such that $\gamma_1 = \gamma_0 \circ \sigma$.

We are interested in multisets consisting of vectors or vector subspaces of a given vector space.

Example 1 *Let $C \subseteq \mathbb{F}_q^n$ be an n-dimensional code and $\boldsymbol{G}$ a generator matrix for C. We consider the multiset $\gamma = m_{\boldsymbol{G}}$ over $\mathbb{F}_q^k$ consisting of the columns of $\boldsymbol{G}$, that is, the multiplicity map*

$$\begin{array}{rcl} m_{\boldsymbol{G}} : \mathbb{F}_q^k & \to & \{0,1,2,...,n\} \\ \boldsymbol{v} & \mapsto & m_{\boldsymbol{G}}(\boldsymbol{v}), \end{array}$$

associates to each $\boldsymbol{v} \in \mathbb{F}_q^k$ the value $m_{\boldsymbol{G}}(\boldsymbol{v})$ that is the number of times it appears as a column of $\boldsymbol{G}$.

Given two different generating matrices $\boldsymbol{G}$ and $\boldsymbol{G}'$ of the code C, they differ by a invertible matrix $\boldsymbol{A}$: $\boldsymbol{G}' = \boldsymbol{A} \boldsymbol{.} \boldsymbol{G}$. The map $\sigma : \boldsymbol{v} \mapsto \boldsymbol{A} \boldsymbol{.} \boldsymbol{v}$ substitutes each column $\boldsymbol{g}_i$ of $\boldsymbol{G}$ by $\boldsymbol{A} \boldsymbol{.} \boldsymbol{g}_i$ and thus the multisets $m_{\boldsymbol{G}}$ and $m_{\boldsymbol{G}'}$ are equivalent. Since different generating matrices of a code C give rise to equivalent multisets, we may say that $m_{\boldsymbol{G}}$ is the multiset associated to C *and denote it by m_C.*

Given a subspace (or subset) $U \subseteq \mathbb{F}_q^k$ we define its multiplicity as

$$m_C(U) := \sum_{\boldsymbol{u} \in U} m_C(\boldsymbol{u}).$$

The following proposition is known from the literature, but we present the proof since it will help us to extend the proposition into the environment of P-metrics.

Proposition 3 *[6, Lemma 1] Let $C \subseteq \mathbb{F}_q^n$ be a code and w the Hamming weight on $\mathbb{F}_q^n$. Given an r-dimensional subspace $D \subseteq C$, there is a subspace $U \subseteq \mathbb{F}_q^k$ of codimension r such that*

$$m_C(U) = n - w(D).$$

Proof. A generator matrix $\boldsymbol{G}$ of the code C defines a linear isomorphism ϕ between $\mathbb{F}_q^k$ and the code,

$$\begin{array}{rccl} \phi: & \mathbb{F}_q^k & \to & C \subseteq \mathbb{F}_k^n \\ & v & \mapsto & v \centerdot \boldsymbol{G} = (v \centerdot g_1, ..., v \centerdot g_n). \end{array} \tag{1}$$

So, given a subcode $D \subseteq C$ there is a subspace $V \subseteq \mathbb{F}_q^k$ isomorphic to D and such that

$$i \in supp(D) \Leftrightarrow \boldsymbol{g}_i \notin V^{\perp},$$

where $\boldsymbol{g}_i$ is the i-th column of $\boldsymbol{G}$ and it follows that

$$\begin{aligned} w(D) &= \left|\left\{i : \boldsymbol{g}_i \notin V^{\perp}\right\}\right| \\ &= n - \left|\left\{i : \boldsymbol{g}_i \in V^{\perp}\right\}\right| \\ &= n - \left|\{\text{columns of } \boldsymbol{G}\} \cap V^{\perp}\right| \\ &= n - m_C\left(V^{\perp}\right). \end{aligned}$$

So, the desired subspace is just $U = V^{\perp}$. □

We now extend this proposition to poset codes.

Given a collection $\{A_1, ..., A_m\}$ of subsets of a given vector space, we denote by $[A_1, ..., A_m]$ the subspace generated by $\bigcup_{i=1}^{m} A_i$.

First of all we remark that given a P-code C, with generator matrix $\boldsymbol{G}$, and $\boldsymbol{v} \in \mathbb{F}_q^k$, the P-weight of $\boldsymbol{v} \centerdot \boldsymbol{G}$ is

$$\begin{aligned} w_P(\boldsymbol{v} \centerdot \boldsymbol{G}) &= \left|\{i : \exists j \in supp(\boldsymbol{v} \centerdot \boldsymbol{G}) \text{ with } i \preceq_P j\}\right| \\ &= \left|\left\{i : \exists j \text{ with } i \preceq_P j \text{ and } \boldsymbol{g}_j \not\perp \boldsymbol{v}\right\}\right| \\ &= n - \left|\left\{i : \forall j \succeq_P i \text{ with } \boldsymbol{g}_j \perp \boldsymbol{v}\right\}\right| \\ &= n - \left|\left\{i : \left[\left\{\boldsymbol{g}_j : j \succeq_P i\right\}\right] \subseteq \{\boldsymbol{v}\}^{\perp}\right\}\right|. \end{aligned}$$

With this in mind, we can define another multiset $m_{\boldsymbol{G}}^{P}$ on $\mathcal{P}\left(\mathbb{F}_q^k\right) := \left\{X : X \subseteq \mathbb{F}_q^k \text{ is a vector subspace}\right\}$. Given an $[n,k]_q$ P-code C, let $\boldsymbol{G}$ be a generator matrix of C and let $\{\boldsymbol{g}_i : i \in [n]\}$ be the set of its columns. The multiset $m_{\boldsymbol{G}}^{P}$ is the collection of subspaces $U_i = \left[\left\{\boldsymbol{g}_j : j \preceq_P i\right\}\right]$, for $i \in [n]$, and the map

$$\begin{array}{rcl} m_{\boldsymbol{G}}^{P} : \mathcal{P}\left(\mathbb{F}_q^k\right) & \rightarrow & \{0,1,2,...,n\} \\ V & \mapsto & m_{\boldsymbol{G}}^{P}(V), \end{array}$$

is the number $m_{\boldsymbol{G}}^{P}(V)$ of i's such that $U_i \subseteq V$. It is immediate to see that $m_{\boldsymbol{G}}^{H} = m_{\boldsymbol{G}}$ when considering the Hamming poset H. Also in this case, different generating matrices for C define equivalent multiset, so we may refer to it just as m_C^P when the generator matrix is not relevant.

Proposition 4 *Let C be an $[n,k]_q$ P-code and $D \subseteq C$ a subcode of dimension r. Then, there is a subspace $U \subseteq \mathbb{F}_q^k$ of codimension r such that*

$$w_{\overline{P}}(D) = n - m_C^P(U),$$

where $\overline{P}$ is the opposite poset of P.

Proof. Let $\boldsymbol{G}$ be a generator matrix of C, with column vectors $\{g_1, ..., g_n\}$. Let $\phi : \mathbb{F}_q^n \rightarrow C$ be the linear isomorphism determined by (1). Given a subcode $\phi(V) = D \subseteq C$ of dimension r, we have that

$$\begin{array}{rcl} w_{\overline{P}}(D) & = & \left|\left\{i : \exists j \text{ with } i \preceq_{\overline{P}} j \text{ and } \boldsymbol{g}_j \not\perp V\right\}\right| \\ & = & n - \left|\left\{i : \forall j \succeq_{\overline{P}} i \text{ with } \boldsymbol{g}_j \perp V\right\}\right| \\ & = & n - \left|\left\{i : \left[\left\{\boldsymbol{g}_j : j \preceq_P i\right\}\right] \subseteq V^{\perp}\right\}\right| \\ & = & n - \left|\left\{i : U_i \subseteq V^{\perp}\right\}\right| \\ & = & n - m_C^P\left(V^{\perp}\right). \end{array}$$

The proposition follows considering $U = V^{\perp}$. □

Let $\beta := \{\boldsymbol{e}_1, ..., \boldsymbol{e}_n\}$ be the canonical base of $\mathbb{F}_q^n$. Each $\boldsymbol{e}_i$ can be considered as linear forms on $\mathbb{F}_q^n$. There is a natural endomorphism $\mu_C : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n / C^{\perp}$, defined by $\mu_C(\boldsymbol{v}) := \boldsymbol{v} + C^{\perp}$. The elements of $\mathbb{F}_q^n / C^{\perp}$ can be considered as linear forms on C and

$$\mu_C(\boldsymbol{e}_i)(\boldsymbol{c}) = \left(\boldsymbol{e}_i + C^{\perp}\right) \cdot \boldsymbol{c} = c_i = \boldsymbol{g}_i \cdot \boldsymbol{v}$$

where $\boldsymbol{c} = \boldsymbol{v} \cdot \boldsymbol{G}$. In this way, identifying C with $\mathbb{F}_q^k$ through the generator matrix $\boldsymbol{G}$, a column $\boldsymbol{g}_i$ is associated to $\mu_C(\boldsymbol{e}_i)$, establishing an isomorphism $\mathbb{F}_q^n / C^{\perp} \to \mathbb{F}_q^k$. So, to a P-code $C \subseteq \mathbb{F}_q^n$ we associate an ordered collection of subspaces $B_{\overline{P}} = (V_1, V_2, ..., V_n)$, called the *orthogonal covering set*, with $V_i = [\{\boldsymbol{e}_j : j \in \langle i \rangle_{\overline{P}}\}]$ being determined by the multiset

$$m_C^{\overline{P}} := \mu_C(B_{\overline{P}}) = \{\mu_C(V_1), \mu_C(V_2), ..., \mu_C(V_n)\}$$

defined on $\mathbb{F}_q^n / C^{\perp} \cong \mathbb{F}_q^k$.

Definition 2 *A* submultiset $\gamma' \subseteq \gamma$ *is a multiset (over the same set S) such that $\gamma'(s) \leq \gamma(s)$ for every $s \in S$.*

Lemma 1 *Let C be an $[n,k]_q$ P-code, $J \subseteq \{1, 2, ..., n\}$ and consider $B_J := \{V_j : j \in J\}$ with $V_j = [\{\boldsymbol{e}_i : i \in \langle j \rangle_{\overline{P}}\}]$. Then $m_J := \mu_C(B_J)$ is a submultiset of $m_C^{\overline{P}}$ and moreover, every submultiset of $m_C^{\overline{P}}$ can be obtained in this way.*

Proof. The fact that m_J is a submultiset of $m_C^{\overline{P}}$ follows immediately from the definition of submultiset. A submultiset of

$$m_C^{\overline{P}} = \{\mu_C(V_1), \mu_C(V_2), ..., \mu_C(V_n)\}$$

is a collection of subsets of the kind

$$m = \{\mu_C(V_{i_1}), \mu_C(V_{i_2}), ..., \mu_C(V_{i_s})\}$$

with $V_{i_l} = [\{\boldsymbol{e}_j : j \in \langle i_l \rangle_{\overline{P}}\}]$, for $l = 1, 2, ..., s$. We let $J = \{i_1, i_2, ..., i_s\}$ and get that $m = m_J$. □

Remark 1 *It follows imediately from the proof of Proposition 4 that the P-weight of a sub-code $D \subseteq C$ is realized by a submultiset $m_J = \mu_C(B_J)$ where $J = \left\{i : \mu_C(V_i) \subseteq \left(\phi^{-1}(D)\right)^{\perp}\right\}$. We also remark that since*

$$\begin{aligned} J &= \left\{i : \mu_C(V_i) \subseteq \left(\phi^{-1}(D)\right)^{\perp}\right\} \\ &= \left\{i : \left[\left\{\boldsymbol{g}_j : i \preceq_{\overline{P}} j\right\}\right] \subseteq \left(\phi^{-1}(D)\right)^{\perp}\right\} \end{aligned}$$

is an ideal of $\overline{P}$.

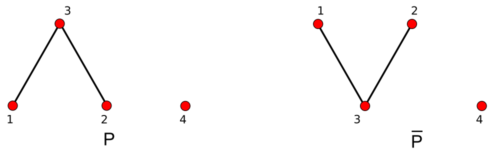

Figure 1: Hasse diagrams of an order P and its opposite $\overline{P}$

We may illustrate the preceding propositions with an example:

Example 2 *Let P and $\overline{P}$ be the posets illustrated by the Hasse diagrams in Fig. 1 bellow, each the opposite of the other.*

Let C be the P-code with generated matrix

$$\boldsymbol{G} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

and let

$$\boldsymbol{G}^{\perp} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

a matrix generated for the $\overline{P}$-code $C^{\perp}$.

The map $\mu_C : \mathbb{F}_2^4 \to \mathbb{F}_2^4 / C^{\perp} \approx \mathbb{F}_2^2$ is

$$\begin{aligned} \mu_C(1000) &= 1000 + C^{\perp} \longleftrightarrow 10 = \textit{Column 1}, \\ \mu_C(0100) &= 0100 + C^{\perp} \longleftrightarrow 11 = \textit{Column 2}, \\ \mu_C(0010) &= 0010 + C^{\perp} \longleftrightarrow 10 = \textit{Column 3}, \\ \mu_C(0001) &= 0001 + C^{\perp} \longleftrightarrow 01 = \textit{Column 4}. \end{aligned}$$

We remark that $1000 - 0010 = 1010 \in C^{\perp}$ so that 1000 and 0010 represent the same class in $\mathbb{F}_q^n / C^{\perp}$.

Now

$$\begin{aligned} & V_1 = [\{\boldsymbol{e}_1, \boldsymbol{e}_3\}], \; V_2 = [\{\boldsymbol{e}_2, \boldsymbol{e}_3\}], \\ & V_3 = [\{\boldsymbol{e}_3\}] \;\; \textit{and} \; V_4 = [\{\boldsymbol{e}_4\}] \end{aligned}$$

and the associated multiset is

$$\begin{aligned} \mu_C(B_{\overline{P}}) &= \{\mu_C(V_1), \mu_C(V_2), \mu_C(V_3), \mu_C(V_4)\} \\ &= \left\{[\{10\}], \mathbb{F}_2^2, [\{10\}], [\{01\}]\right\} = m_C^{\overline{P}}. \end{aligned}$$

with P-weight hierarchy

$$\begin{aligned} d_1^P(C) &= w_P(0101) \\ &= w_P(01 \boldsymbol{\cdot} \boldsymbol{G}) \\ &= 4 - m_C^{\overline{P}}\left([\{01\}]^{\perp}\right) \\ &= 4 - m_C^{\overline{P}}([\{10\}]) \\ &= 4 - m_J([\{10\}]) = 2, \end{aligned}$$

with $J = \langle 1, 3\rangle_{\overline{P}} = \{1, 3\}$.

$$\begin{aligned} d_2^P(C) &= w_P(C) \\ &= w_P\left(\mathbb{F}_2^2 \boldsymbol{\cdot} \boldsymbol{G}\right) \\ &= 4 - m_C^{\overline{P}}\left(\mathbb{F}_2^{2\perp}\right) \\ &= 4 - m_C^{\overline{P}}([\{00\}]) \\ &= 4 - m_I([\{00\}]) = 4, \end{aligned}$$

with $I = \emptyset$.

Recalling that B_J is defined as $\{V_j : j \in J\}$ we have the following:

Proposition 5 *$[B_J] = [\{\boldsymbol{e}_j : j \in \langle J\rangle_{\overline{P}}\}]$, for any $J \subseteq [n]$.*

Proof. Given $j \in \langle J\rangle_{\overline{P}}$ we have that $\boldsymbol{e}_j \in V_j = [\{\boldsymbol{e}_i : i \in \langle j\rangle_{\overline{P}}\}]$, so that $[\{\boldsymbol{e}_j : j \in \langle J\rangle_{\overline{P}}\}] \subseteq [B_J]$.

On the other hand, $V_i \subseteq [\{\boldsymbol{e}_j : j \in \langle J\rangle_{\overline{P}}\}]$ for every $V_i \in B_J$. It follows that $B_J \subseteq [\{\boldsymbol{e}_j : j \in \langle J\rangle_{\overline{P}}\}]$. □

Proposition 6 $\dim[B_J] \geq |B_J|$ *and equality holds iff J is an ideal of $\overline{P}$.*

Proof. In fact,

$$\begin{aligned} \dim[B_J] &= \dim[\{\boldsymbol{e}_j : j \in \langle J\rangle_{\overline{P}}\}] \\ &= |\langle J\rangle_{\overline{P}}| \\ &\geq |J| = |B_J|. \end{aligned}$$

So J is an ideal of $\overline{P}$ iff $\langle J\rangle_{\overline{P}} = J$. □

3 Duality

Given a poset P, a P-code C and a generator matrix $\boldsymbol{G}$ of C we may construct a multiset $m_C^{\overline{P}}$ as in Proposition 4. Also, to each P-code C we associate additional parameters $\left\{ d_1^{\overline{P}}\left(C^{\perp}\right), ..., d_{n-k}^{\overline{P}}\left(C^{\perp}\right) \right\}$, the $\overline{P}$-weight hierarchy of the code $C^{\perp}$ as done in Section 1. We will characterize those parameters using the multiset $m_C^{\overline{P}}$, hence generalizing [7, Theorem 4.1] and proving that, despite the fact that the multiset associated to a code depends on the choice of a generator matrix, the P-weight hierarchy can be determined from the multiset, indepedently of the chosen generator matrix.

Theorem 1 *Let P be a poset on $[n]$, C an $[n,k]_q$ P-code and $m_C^{\overline{P}}$ the multiset in $\mathcal{P}\left(\mathbb{F}_q^k\right)$ associated to C. Then*

$$d_r^{\overline{P}}\left(C^{\perp}\right) = \min\left\{ |B_J| : J \textit{ ideal of } \overline{P} \textit{ and } |B_J| - \dim[\mu_C(B_J)] \geq r \right\}. \tag{2}$$

Proof. Given a subspace $D \subseteq C^{\perp}$, we consider the $\overline{P}$-ideal $I = \langle supp\,(D) \rangle_{\overline{P}}$. By Proposition 5 we have that $[B_I] = [\{\boldsymbol{e}_i : i \in I\}]$. Since

$$D = [\{\boldsymbol{e}_i : i \in suppD\}] \cap C^{\perp} \subseteq [B_I] \cap C^{\perp}$$

for every $D \subseteq C^{\perp}$, it follows that D is contained in the kernel of $\mu_C|_{[B_I]}$, the restriction of μ_C to $[B_I]$, hence

$$\dim [B_I] - \dim [\mu_C (B_I)] = \dim Ker \left(\mu_C|_{[B_I]}\right) \geq \dim D.$$

Since I is an ideal, it follows that $\dim [B_I] = |B_I| = w_{\overline{P}}(D)$ and we have that

$$d_r^{\overline{P}}\left(C^{\perp}\right) \geq \text{ the right side of (2).}$$

To prove the other inequality, let J be an ideal of $\overline{P}$ for which the minimum in the right side of (2) is attained. Then $|B_J| - \dim [\mu_C (B_J)] \geq r$. If $D' := [B_J] \cap C^{\perp}$ we have that

$$\dim [\mu_C (B_J)] = \dim [B_J] - \dim D'.$$

Clearly $\dim [B_J] \geq w_{\overline{P}}(D')$. Since J is an ideal, $\dim [B_J] = |B_J|$, so that

$$\dim D' = |B_J| - \dim [\mu_C (B_J)] = r' \geq r$$

and

$$|B_J| \geq w_{\overline{P}}(D').$$

By the Monotonicity Proposition 1, $d_r^{(\overline{P})}\left(C^{\perp}\right) \leq d_{r'}^{(\overline{P})}\left(C^{\perp}\right)$ and it follows that

$$d_r^{\overline{P}}\left(C^{\perp}\right) \leq \text{ the right side of (2).}$$

□

We prove now the Duality Theorem for poset codes.

Theorem 2 (Duality) *Let C be an $[n,k]_q$ P-code and $C^{\perp}$ the dual code. Consider the sets*

$$X = \left\{d_1^P(C), d_2^P(C), ..., d_k^P(C)\right\}$$

and

$$Y = \left\{n+1-d_1^{\overline{P}}\left(C^{\perp}\right), n+1-d_2^{\overline{P}}\left(C^{\perp}\right), ..., n+1-d_{n-k}^{\overline{P}}\left(C^{\perp}\right)\right\}$$

Then X and Y are disjoint and

$$X \cup Y = \{1, 2, ..., n\}.$$

Proof. Since $X, Y \subset [n]$ and $|X| + |Y| = n$, it is sufficient to prove that $X \cap Y = \emptyset$. By Theorem 1, given r there is an ideal J in $\overline{P}$ such that

$$|B_J| = d_r^{\overline{P}}\left(C^{\perp}\right) \tag{3}$$

and

$$\dim\left[\mu_C(B_J)\right] \leq d_r^{\overline{P}}\left(C^{\perp}\right) - r.$$

Let $t := \operatorname{codim}\left[\mu_C(B_J)\right] \geq k - d_r^{\overline{P}}\left(C^{\perp}\right) + r$. By definition of generalized P-weights we have that

$$d_t^P(C) \leq w_P(D), \ \forall\, D \subseteq C \text{ with} \dim D = t.$$

But, Proposition 4 ensures the existence of a subcode $D \subseteq C$ with $\dim D = t$ such that

$$w_P(D) = n - |B_J| \overset{(3)}{=} n - d_r^{\overline{P}}\left(C^{\perp}\right),$$

so that

$$d_t^P(C) \leq n - d_r^{\overline{P}}\left(C^{\perp}\right).$$

We must now prove that $n+1-d_r^{\overline{P}}\left(C^\perp\right)$ is not contained in X. Supposing it is not the case, there would be an $l>0$ for which

$$d_{t+l}^P\left(C\right)=n+1-d_r^{\overline{P}}\left(C^\perp\right),$$

that is, there would be a subspace of codimension $t+l$ containing a subset $\mu_C\left(B_I\right)$, with

$$|B_I|=n-d_{t+l}^P\left(C\right)=d_r^{\overline{P}}\left(C^\perp\right)-1 \tag{4}$$

and

$$\dim\left[\mu_C\left(B_I\right)\right]\leq k-t-l\leq d_r^{\overline{P}}\left(C^\perp\right)-r-l.$$

This would imply that

$$|B_I|-\dim\left[\mu_C\left(B_I\right)\right]\geq r+l-1\geq r$$

and by Theorem 1 we would have $|B_I|\geq d_r^{\overline{P}}\left(C^\perp\right)$, a contradiction to (4). □

4 Consequences of duality

In this section we present some consequences of the Duality Theorem, relating the discrepancy of a given code to the one of its dual and also relating the chain property of a code and its dual.

4.1 P-MDS discrepancy

Discrepancy is a measure of how far is a code from being MDS: the *P-MDS discrepancy* of an $[n,k]_q$ P-code C, denoted by $\delta_P\left(C\right)$, is the smallest integer s such that $d_{s+1}^P\left(C\right)>n-k$. It is not surprising that the discrepancy of P-codes and $\overline{P}$-codes are related as follows:

Theorem 3 *Given an $[n,k]_q$ P-code C, then*

i) $\delta_P\left(C\right)=\left|\left\{1,2,...,n-k\right\}\cap\left\{d_r^P\left(C\right):1\leq r\leq k\right\}\right|,$

ii) $\delta_P\left(C\right)=\delta_{\overline{P}}\left(C^\perp\right).$

Proof. The first statement follows straight from Proposition 1 (Monotonicity). To prove the second statement we use the first statement of this Theorem (a), the Inclusion-Exclusion Principle (b), Theorem 2 (c), and basic sets equality (d) as follows:

$$\begin{aligned}
\delta_P(C) &\overset{a}{=} \left|[n-k] \cap \left\{d_r^P(C) : r \in [k]\right\}\right| \\
&\overset{b}{=} k - \left|([n] \setminus [n-k]) \cap \left\{d_r^P(C) : r \in [k]\right\}\right| \\
&\overset{c}{=} k - \left|([n] \setminus [n-k]) \cap \left\{[n] \setminus \left(n+1-d_r^{\overline{P}}\left(C^{\perp}\right) : r \in [n-k]\right)\right\}\right| \\
&\overset{d}{=} k - \left|[k] \cap \left([n] \setminus \left\{d_r^{\overline{P}}\left(C^{\perp}\right) : r \in [n-k]\right\}\right)\right| \\
&\overset{c}{=} \left|[k] \cap \left\{d_r^P\left(C^{\perp}\right) : r \in [n-k]\right\}\right| \\
&\overset{a}{=} \delta_{\overline{P}}\left(C^{\perp}\right),
\end{aligned}$$

recalling that $[k] = \{1, 2, \cdots, k\}$. □

4.2 Chain codes

We want now to study the chain-property of a code in view of the Duality Theorem. We start with the necessary definitions and notation.

Definition 3 *An $[n,k]_q$ P-code C is said to be a P-chain code if there is a sequence of linear subspaces*

$$\{0\} = D_0 \subseteq D_1 \subseteq D_2 \subseteq ... \subseteq D_k = C$$

such that $w_P(D_r) = d_r^P(C)$ and $\dim D_r = r$ for every $r \in \{1, 2, ..., k\}$. Under those circumstances, we say that C satisfies the P-chain condition.

Given a poset P we denote by $\mathcal{I}^r P$ the set of all ideals of cardinality r of P and, given an ideal $J \subseteq P$ we denote by $\mathcal{M}(J)$ the set of maximal elements in J. The following proposition, proved in [8, Proposition 1.1], will be used to prove the existence of codes satisfying the P-chain condition with any prescribed weight hierarchy.

Proposition 7 *Let P be a poset, then*

i) Given $0 \leq r \leq s \leq n$ and $I \in \mathcal{I}^r(P)$ there is $J \in \mathcal{I}^s P$ such that $I \subseteq J$.

ii) Given $0 \leq s \leq r \leq n$ and $I \in \mathcal{I}^r(P)$ there is $J \in \mathcal{I}^s P$ such that $J \subseteq I$.

Theorem 4 *Let P be a poset on $[n]$ and $1 \leq d_1 < d_2 < ... < d_k = n$ a sequence of integers. Then there is a code C satisfying the P-chain condition, with $d_r = d_r^P(C)$.*

Proof. By Proposition 7, there is a sequence of ideals $J_1 \subseteq ... \subseteq J_k$ of P such that $|J_i| = d_i$.

Let $\boldsymbol{v}_i = (x_1, x_2, ..., x_n)$ be such that

$$x_j = \begin{cases} 1 & \text{if } \; j \in \mathcal{M}(J_i), \\ 0 & \quad \text{otherwise,} \end{cases}$$

for $j = 1, 2, ..., n$. The set $\{\boldsymbol{v}_1, \boldsymbol{v}_2, ..., \boldsymbol{v}_k\}$ is linearly independent since given $i < l$ there is $r \in \mathcal{M}(J_l)$ such that $r \notin \mathcal{M}(J_i)$ and the code $C = [\boldsymbol{v}_1, ..., \boldsymbol{v}_k]$ satisfies, by construction, the P-chain condition, with $d_r = d_r^P(C)$. □

Remark 2 *We observe that the choices in the proof of the previous theorem are not unique. In fact, when defining the vectors $\mathbf{v}_i$ it is only required that coordinates corresponding to maximal elements of J_i should be nonzero, those corresponding to coordinates not in J_i should be zero and coordinates corresponding to non-maximal elements may assume any value in $\mathbb{F}_q$.*

If C satisfies the P-chain condition, it has a base $\{\boldsymbol{v}_1, ..., \boldsymbol{v}_k\}$ such that the first r vectors generate the r-th minimal subspace of C, that is,

$$d_r^P(C) = w_P(D_r)$$

with

$$D_r = [\boldsymbol{v}_1, \boldsymbol{v}_2, ..., \boldsymbol{v}_r].$$

Those vectors define a generator matrix $\boldsymbol{G}$ for C:

$$\boldsymbol{G} = \begin{pmatrix} \boldsymbol{v}_1 \\ \vdots \\ \boldsymbol{v}_k \end{pmatrix}.$$

Considering $J_r := \langle supp(D_r) \rangle_P$, we have that $J_r \subsetneq J_{r+1}$. We re-order the columns $(g_1, g_2, ..., g_n)$ of $\boldsymbol{G}$ by labelling first the columns corresponding to the ideal J_1, in such a way that columns corresponding to coordinates of smaller P-weight come before those corresponding to greater P-weight. Then we re-order in the same fashion the columns corresponding to coordinates in $J_2 \backslash J_1$ and so on, until we get to the columns of $\boldsymbol{G}$ corresponding to coordinates of $J_k \backslash J_{k-1}$.

This labelling process can be formally described as follows: for $i \in J_t$ and $j \in J_s$, we have that

- if $t \neq s$ then $\boldsymbol{g}_i$ appears before $\boldsymbol{g}_j$ iff $J_t \subsetneq J_s$,
- if $t = s$ then $\boldsymbol{g}_i$ appears before $\boldsymbol{g}_j$ iff $i \preceq_P j$.

With this labels we obtain a matrix

$$\boldsymbol{G}' = \left(\boldsymbol{g}_{i_1}, \boldsymbol{g}_{i_2}, ..., \boldsymbol{g}_{i_n}\right) = \begin{pmatrix} \boldsymbol{u}_1 \\ \boldsymbol{u}_2 \\ \vdots \\ \boldsymbol{u}_k \end{pmatrix}$$

such that the first r vectors generate an r-th minimal subspace $D'_r = [\boldsymbol{u}_1, .., \boldsymbol{u}_r]$ of a P-code C' and its r-th P-minimal weight is the cardinality of the ideal generated by the non-zero coordinates in the first $d_r^P(C)$ coordinates of $\boldsymbol{G}'$.

The labelling process we just described defines a map

$$\begin{aligned} \phi : \quad [n] &\rightarrow [n] \\ i_s &\mapsto s \end{aligned}$$

for $s \in [n]$ and this map induces an order P' on $[n]$, order-isomorphic to P: $s \preceq_{P'} r$ iff $i_s \preceq_P i_r$. Considering C as a P-code and C' as a P'-code, we claim those are isometric. Ineed, the map ϕ induces a map $T_\phi : \left(\mathbb{F}_q^n, d_P\right) \rightarrow \left(\mathbb{F}_q^n, d_{P'}\right)$ defined as

$$T_\phi\left(\sum_{i=1}^n \lambda_i \boldsymbol{e}_i\right) = \sum_{i=1}^n \lambda_i \boldsymbol{e}_{\phi(i)}$$

such that $T_\phi(C) = C'$. From [9, Corollary 1.1] it follows that T_ϕ is an isometry. So, without loss of generality, we may assume that a P-chain code is such that the ideal generated by the support of the first r rows is the first $d_r^P(C)$ coordinates.

Lemma 2 *Given posets P and Q and a poset isomorphism $\phi : [n]_P \to [n]_Q$, then $\phi : [n]_{\overline{P}} \to [n]_{\overline{Q}}$ is also a poset isomorphism.*

Proof. It is straightforward to prove that

$$j \preceq_{\overline{P}} i \Longleftrightarrow i \preceq_P j \Longleftrightarrow \phi(i) \preceq_Q \phi(j) \Longleftrightarrow \phi(j) \preceq_{\overline{Q}} \phi(i).$$

□

Remark 3 *Given $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$ and a poset isomorphism $\phi : [n]_P \to [n]_P$, writing $\boldsymbol{x} = \sum_{i=1}^{n} \alpha_i \boldsymbol{e}_i$ and $\boldsymbol{y} = \sum_{i=1}^{n} \beta_j \boldsymbol{e}_j$ $\quad (\{\boldsymbol{e}_1, ..., \boldsymbol{e}_n\}$ is the canonical base of $\mathbb{F}_q^n)$, we consider the P-isometry $T_\phi : \mathbb{F}_q^n \to \mathbb{F}_q^n$. Then $T_\phi(\boldsymbol{x}) = \sum_{i=1}^{n} \alpha_i \boldsymbol{e}_{\phi(i)}$ and $T_\phi(\boldsymbol{y}) = \sum_{i=1}^{n} \beta_j \boldsymbol{e}_{\phi(j)}$, and since*

$$\begin{aligned} T_\phi(\boldsymbol{x}) \cdot T_\phi(\boldsymbol{y}) &= \sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_i \beta_j \boldsymbol{e}_{\phi(i)} \cdot \boldsymbol{e}_{\phi(j)} \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_i \beta_j \delta_{\phi(i)\phi(j)} \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_i \beta_j \delta_{ij} \\ &= \boldsymbol{x} \cdot \boldsymbol{y} \end{aligned}$$

it follows that $T_\phi\left(C^\perp\right) = T_\phi(C)^\perp = C'^\perp$. But, from Lemma 2 we find that $\overline{\phi(P)} = \overline{P}$. Hence the $\overline{P}$-code $C^\perp$ is isometric (by T_ϕ) to the $\overline{\phi(P)}$-code $C'^\perp$.

The next theorem is the equivalent to the result proved in [10, Theorem 5] for usual Hamming weight and the proof follows the same line.

Theorem 5 *Given a poset P, a code C satisfies the P-chain condition iff $C^\perp$ satisfies the $\overline{P}$-chain condition.*

Proof. We may assume that the generator matrix $\boldsymbol{G}$ of C is such that the ideal generated by the support of the first r rows is the first $d_r^P(C)$ coordinates.

We claim there are linearly independent vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, ..., \boldsymbol{u}_{n-k}$ in $C^{\perp}$ such that the $\overline{P}$-ideal generated by the support of the first s of those vectors consists of the last $d_s^{\overline{P}}\left(C^{\perp}\right)$ coordinates. We prove this by induction on s.

The case $s = 0$ is trivial, so we assume there are L.I. vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, ..., \boldsymbol{u}_{s-1}$ in $C^{\perp}$ such that $\langle supp\,[\boldsymbol{u}_1, ..., \boldsymbol{u}_j]\rangle_{\overline{P}}$ consists of the last $d_j^{\overline{P}}\left(C^{\perp}\right)$ coordinates for every $1 \leq j \leq s-1$. We denote $a = d_s^{\overline{P}}\left(C^{\perp}\right)$ and let

$$D := \{(0, ..., 0, x_{n+1-a}, x_{n+2-a}, ..., x_n) : \exists\,(x_1, ..., x_n) \in C\}$$

and

$$D' := \left\{x = (0, ..., 0, x_{n+1-a}, ..., x_n) : \ x^{\,t} \cdot \ y \ = 0, \ \forall\, y \in D\right\}.$$

Then we have that

$$\dim D + \dim D' = a \ \text{ and } \ D' \subseteq C^{\perp}.$$

A generator matrix $\boldsymbol{G}_1$ for D can be obtained from $\boldsymbol{G}$ exchanging all first $n-a$ columns by zero columns. By duality ($d_t^P(C) \leq n-a$ for $t \geq k-(a-s)$) we find that

$$r\left|\left\{d_r^P(C) : 1 \leq r \leq k\right\} \cap \{n+1-a, n+2-a, ..., n\}\right| \leq a - s.$$

But this means that $\boldsymbol{G}_1$ has at most $a - s$ linearly independent vectors, hence $\dim D \leq a - s$ and $\dim D' \geq s$. It follows that the code D' contains $\boldsymbol{u}_1, \boldsymbol{u}_2, ..., \boldsymbol{u}_{s-1}$, another vector $\boldsymbol{u}_s$ can be chosen in $D' \backslash\, [\{\boldsymbol{u}_1, \boldsymbol{u}_2, ..., \boldsymbol{u}_{s-1}\}]$ and moreover, $\langle suppD'\rangle_{\overline{P}}$ consists of the last a coordinates. □

The following two results are immediate consequences of the previous theorem.

Corollary 1 *If the support of a P-code C is a totally ordered subset of P, then $C^{\perp}$ is a $\overline{P}$-chain code.*

Corollary 2 *Any $[n, n-1]_q$ or $[n, n-2]_q$ code is a $\overline{P}$-chain code for any order P on $[n]$.*

References

[1] R. A. Brualdi, J. S. Graves, and K. M. Lawrence, "Codes with a poset metric," Discrete Math., no. 147, pp.57-72, Dec. 1995.

[2] V. K. Wei, "Generalized Hamming weights for linear codes," IEEE Trans. Inform. Theory, vol. 37, no. 5, pp.1412-1418, Sep. 1991.

[3] L. Panek, and M. Firer, "Codes satisfying the chain condition with a poset weights," preprint.

[4] S. Dodunekov, and J. Simonis, "Codes and projective multisets," Electron. J. Combin., vol. 5, R37(electronic), 1998.

[5] H. G. Schaathun, "Duality and support weights distributions," IEEE Trans. Inform. Theory, vol. 50, no. 5, pp. 862-867, May 2004.

[6] T. Helleseth, T. Klove, and O. Ytrehus, "Generalized Hamming weight of linear codes," Trans. Inform. Theory, vol. 38, no. 3, pp. 1133-1140, May 1992.

[7] M. A. Tsfasman, and S. G. Vladut, "Geometric approach to higher weights," IEEE Trans. Inform. Theory, vol. 41, no. 6, pp.1564-1588, Nov. 1995.

[8] J. Y. Hyun, and H. K. Kim, "Maximum distance separable poset codes," Des. Codes Cryptogr., vol. 48, no. 3, pp. 247-261, Sep. 2008.

[9] L. Panek, M. Firer, H. K. Kim, and J. Y. Hyun, "Groups of linear isometries on poset structures," Discrete Math., vol. 308, no. 18, pp. 4116-4123, Sep. 2008.

[10] V. K. Wei, and K. Yang, "On the generalized Hamming weights of product codes," IEEE Trans. Inform. Theory, vol. 39, no. 5, pp. 1709-1713, Sep. 1993.