Duality for poset codes

Allan O. Moura Marcelo Firer

State University of Campinas

Fq9 - UCD, July 13-17 2009

Outline

Outline

Notation

- $[n] = \{1, 2, ..., n\}$
- $[\{A_1, A_2, ..., A_n\}]$ is subspace generated by $\bigcup_{i=1}^{n} A_i$

Poset

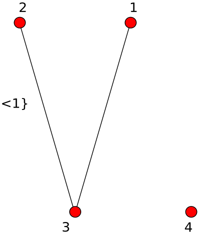
- A *poset* $P = (X, \preceq_P)$ is a partial order on a set X.
- $I \subseteq P$ is called an (order) *ideal* if

$$i \in I \text{ ,and } j \preceq_P i \text{ implies that } j \in I.$$

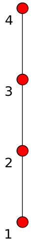
- $A \subseteq P$, we denote by $\langle A \rangle_P$ the smallest ideal of P containing A, called the *ideal generated by* A.
- We denote by $\overline{P}$ *the dual poset of* P: $i \preceq_{\overline{P}} j$ iff $j \preceq_P i$.

Hasse diagram.

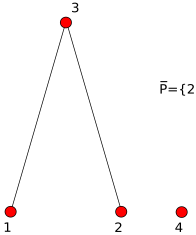
$P=\{3<2,3<1\}$



L=Poset Linear



$\bar{P}=\{2<3,1<3\}$



H=Poset Hamming

Poset Metric

- Over the vetor space $\mathbb{F}_q^n$, we introduce the *P-weight*

$$w_P(x) = |\langle supp(x) \rangle_P|,$$

where $supp(x) = \{i\,;\, x_i \neq 0\}$, $x = (x_1, x_2, ..., x_n)$ and $P = [n]$.

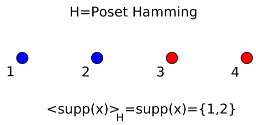
- The *P-Metric* is

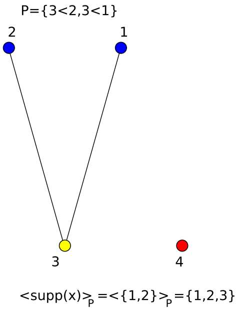
$$d_P(x, y) = w_P(y - x).$$

- The $[n, k]_q$ *P-Code* is a k-subspace of the metric space $(\mathbb{F}_q^n, d_P)$ with the P-metric (*P-Space*).

P-Metric Example

The element $x = 1100$ in $\mathbb{F}_2^4$ has H-weight 2 and P-weight 3:





Outline

Support of Subspaces

- The support of a subspace $D \subseteq \mathbb{F}_q^n$ is the set of non-zero coordinates of the subspace,

$$supp(D) = \bigcup_{x \in D} supp(x)$$

Example

Let $D \subseteq \mathbb{F}_2^5$ be a subspace generated by 10011 and 01010,

$$D = [\{10011, 01010\}] = \left\{ \begin{array}{c} 00000 \\ 10011 \\ 01010 \\ 11001 \end{array} \right\}$$

then

$$supp(D) = \{1, 2, 4, 5\}.$$

Generalized P-Weight

- The *generalized P-weight* of *a* subspace $D \subseteq \mathbb{F}_q^n$ is

$$w_P(D) := |\langle supp(D) \rangle_P|.$$

- The *r-th minimal (generalized)P-weight* $d_r^{(P)}(C)$ of an $[n,k]_q$ P-code $C \subseteq \mathbb{F}_q^n$ is

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

Outline

Wei's Theorem.

Wei's Duality Theorem

For H the Hamming poset. Let C be an $[n,k]_q$ H-code and $C^\perp$ the orthogonal code. Then the sets

$$X=\left\{d_1^{(H)}(C),d_2^{(H)}(C),\dots,d_k^{(H)}(C)\right\}(\text{called Hierarchy})$$

and

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

are disjoint and

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

Definition

- A *multiset* over a set S is 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.

Example

- Given an $[n,k]_q$ P-code C, let a be generating matrix G of C and let $\{g_i | i \in [n]\}$ be the set of its columns.
- The multiset m_C^P on $\mathscr{P}\left(\mathbb{F}_q^k\right) := \left\{X | X \subseteq \mathbb{F}_q^k\right\}$ is the collection of subspaces $U_i = [\{g_j ; j \preceq_P i\}]$, for $i \in [n]$, and the map

$$\begin{array}{rcl} m_C^P : \mathscr{P}\left(\mathbb{F}_q^k\right) & \longrightarrow & \{0,1,2,\ldots,n\} \\ V & \longmapsto & m_C^P(V) \end{array}$$

is the number $m_C^P(V)$ of i's such that $U_i \subseteq V$.

Example

- Let $C \subseteq \mathbb{F}_2^4$ be the $[4,2]_2$ P-code with generated matrix

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

- For the poset P we have the multiset m_C^P on $\mathscr{P}\left(\mathbb{F}_2^2\right)$

$$U_1 = [\{g_1, g_3\}] = [\{10\}], \; U_2 = [\{g_2, g_3\}] = \mathbb{F}_2^2,$$
$$U_3 = [\{g_3\}] = [\{10\}] \text{ and } U_4 = [\{g_4\}] = [\{01\}].$$

- Or just $m_C^P = \{[\{10\}], \mathbb{F}_2^2, [\{10\}], [\{01\}]\}$.

Lemma 1

Lemma 1

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 dual poset of P: $i \preceq_{\overline{P}} j$ iff $j \preceq_P i$.

Outline

Duality Theorem for P-Space.

Theorem

Let C be an $[n,k]_q$ P-code and $C^\perp$ the orthogonal code. Consider the sets

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

and

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

Then X and Y are disjoint and

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

Outline

Let $\beta := \{e_1, ..., e_n\}$ be the canonical base of $\mathbb{F}_q^n$. Let $\mu_C : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n / C^\perp$ be the natural projection.

- The elements of $\mathbb{F}_q^n / C^\perp$ may be considered as linear forms on C and
$$\mu_C(e_i)(c) = \left(e_i + C^\perp\right) . c = c_i = g_i . v$$
where $c = v . G$.
- If J is a ideal of P then $B_J := \{V_i; i \in J\}$ with $V_i = [\{e_l; l \in \langle i \rangle_P\}] . (\mu_C(V_i) = U_i)$

Lemma 2

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

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

Proof of the Theorem

- Since $X, Y \subset [n]$ it is sufficient to prove that $X \cap Y = \emptyset$.
- By lemma 2, given r there is an ideal J in $\overline{P}$ such that

1. $|B_J| = d_r^{(\overline{P})}(C^{\perp})$
2. $\dim[\mu_C(B_J)] \leq d_r^{(\overline{P})}(C^{\perp}) - r$

- Let $t = codim([\mu_C(B_J)]) \geq k - d_r^{(\overline{P})}(C^{\perp}) + r$. By lemma 1 we have

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

Proof of the Theorem

- We must 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

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

Proof of the Theorem

- By lemma 1, there would be a subspace of codimension $t + l$ containing a subset $\mu_C(B_l)$, with:

$$|B_l| = n - d_{t+l}^{(P)}(C) = d_r^{(\overline{P})}\left(C^{\perp}\right) - 1 \tag{2}$$

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

Proof of the Theorem

- This would imply that

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

- By lemma 2 we would have $|B_I| \geq d_r^{(\overline{P})}\left(C^{\perp}\right)$, a contradiction to 2.

Outline

MDS Discrepancy

- The *P-MDS discrepancy* of an $[n,k]_q$ P-code C, denoted by $\delta_P(C)$, is the smallest integer s such that $d_{s+1}^{(P)}(C) > n-k$.

Theorem

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

- $\delta_P(C) = \left| \{1,2,\ldots,n-k\} \cap \left\{ d_r^{(P)}(C); 1 \leq r \leq k \right\} \right|;$
- $\delta_P(C) = \delta_{\overline{P}}(C^{\perp}).$

P-Chain condition

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

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

such that $w_P(D_r) = d_r^{(P)}(C)$ and $\dim D_r = r$ for every $r \in \{1, 2, \ldots, k\}$.

- Under those circumstances, we may also say that *C satisfies the P-chain condition*.

Theorem

Let P be a poset. Then, a code C satisfies the P-chain condition iff $C^{\perp}$ satisfies the $\overline{P}$-chain condition.

References I

- Richard A. Brualdi, Janine Smolin Graves and K. Mark Lawrence; *Codes with a poset metric*; Discrete Math. 147:57-72, 1995.
- Victor K. Wei; *Generalized Hamming weights for linear codes*; IEEE Trans. Inform. Theory, 37 n.o. 5:1412-1418, 1991.
- Luciano Panek, Marcelo Firer, Hyun K. Kim and Jong Y. Hyun; *Groups of linear isometries on poset structures*; Discrete Math. 308:4116 – 4123, 2008.
- Hans Georg Schaathun; *Duality and support weights distribution*s; IEEE Trans. Inform. Theory 50 n.o: 5:862-867, 2004.