P-Chain Codes

Beatriz Casulari da Motta Ribeiro

beatriz@ice.ufjf.br

Joint work with Pedro Esperidião and Allan Moura

Universidade Federal de Juiz de Fora

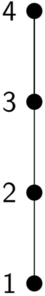
Posets

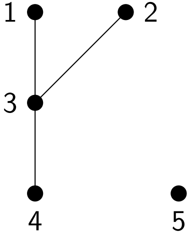
Fix $[n] := \{1, ..., n\}$, the set of ordered coordinate positions of $\mathbb{F}_q^n$.

Posets

Fix $[n] := \{1, \ldots, n\}$, the set of ordered coordinate positions of $\mathbb{F}_q^n$.

- A poset $P = ([n], \preceq_P)$ is a partial order on $[n]$.
- A linear poset (or chain) is a well ordered poset ($i \preceq_{\mathrm{P}} j$ or $j \preceq_{\mathrm{P}} i$ for every $i, j \in P$).
- A Hamming poset (or antichain) is a poset such that $i \preceq_{\mathrm{P}} j \Leftrightarrow i = j$.





Posets

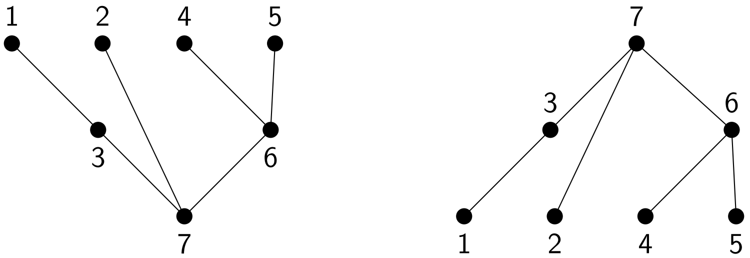
Let P be a poset on $[n]$, the opposite (dual) poset $\overline{P}$ is given by

$$i \preceq_{\overline{P}} j \Leftrightarrow j \preceq_P i$$

Posets

Let P be a poset on $[n]$, the opposite (dual) poset $\overline{P}$ is given by

$$i \preceq_{\overline{P}} j \Leftrightarrow j \preceq_P i$$



Ideals

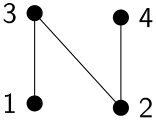
- A subset $I \subseteq P$ is called an ideal if

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

- Given a subset $A \subseteq P$, the ideal generated by A is the smallest ideal of P containing A, denoted by $\langle A \rangle_P$.

Ideals

- A subset $I \subseteq P$ is called an ideal if
$$i \in I \text{ and } j \preceq_P i \Rightarrow j \in I\,.$$
- Given a subset $A \subseteq P$, the ideal generated by A is the smallest ideal of P containing A, denoted by $\langle A \rangle_P$.

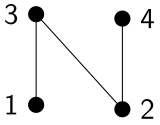


Ideals

- A subset $I \subseteq P$ is called an ideal if

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

- Given a subset $A \subseteq P$, the ideal generated by A is the smallest ideal of P containing A, denoted by $\langle A \rangle_P$.



In the poset to the left:

- $\{1, 2, 3\}$, $\{2, 4\}$ and $\{2\}$ are examples of ideals
- $\{2, 3\}$ is not an ideal: $1 \preceq 3$, but $1 \notin \{2, 3\}$.

P-metric

- If $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, we define the support of x by

$$\mathrm{supp}(x) = \{i; x_i \neq 0\}$$

and the $P-$weight of x by

$$w_P(x) = |\langle \mathrm{supp}(x) \rangle_P|$$

- If $x, y \in \mathbb{F}_q^n$, the $P-$distance between x and y is given by

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

- Note that the Hamming distance is the poset distance using the Hamming poset (that explains its name).

Example

- We consider the element $x = 1100$ in $\mathbb{F}_2^4$.
- We have

$$\langle \mathrm{supp}(x) \rangle_H = \mathrm{supp}(x) = \{1, 2\}$$

and

$$\langle \mathrm{supp}(x) \rangle_P = \langle \{1, 2\} \rangle = \{1, 2, 3\}$$

- Therefore $w_H(x) = 2$ and $w_P(x) = 3$.

Figura : The posets P and H.

P-Codes

- The pair $(\mathbb{F}_q^n, d_P)$ is a metric space.
- A $P-$linear code C is a vector subspace of $\mathbb{F}_q^n$ with this metric.
- If $\dim C = k$, we refer to it as an $[n, k]_q-$ $P-$code.
- The minimal distance (or weight) of C:

$$d_P(C) = \min\{w_P(x); 0 \neq x \in C\}$$

P-weight hierarchy

- The (generalized) P-weight of a subset $D \subset \mathbb{F}_q^n$:

$$w_P(D) = |\langle \mathrm{supp}(D) \rangle_P|$$

P-weight hierarchy

- The (generalized) P-weight of a subset $D \subset \mathbb{F}_q^n$:

$$w_P(D) = |\langle \mathrm{supp}(D) \rangle_P|$$

- The $r-$th minimal generalized $P-$weight of a $[n, k]_q-$ $P-$Code:

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

P-weight hierarchy

- The (generalized) P-weight of a subset $D \subset \mathbb{F}_q^n$:

$$w_P(D) = |\langle \mathrm{supp}(D) \rangle_P|$$

- The $r-$th minimal generalized $P-$weight of a $[n,k]_q-$ $P-$Code:

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

- Note that the first minimal weight is the minimal distance $d_P(C)$.

P-weight hierarchy

- The (generalized) P-weight of a subset $D \subset \mathbb{F}_q^n$:

$$w_P(D) = |\langle \mathrm{supp}(D) \rangle_P|$$

- The $r-$th minimal generalized $P-$weight of a $[n,k]_q-$ $P-$Code:

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

- Note that the first minimal weight is the minimal distance $d_P(C)$.
- The $P-$weight hierarchy of a $[n,k]_q$ P-code C is the set

$$\{d_1^P(C), d_2^P(C), d_3^P(C), \ldots, d_k^P(C)\}$$

- The hierarchy is strictly increasing and satisfies the generalized Singleton Bound:

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

Extension

Def. If P and Q are posets on $[n]$ such that $x \preceq_Q y \Rightarrow x \preceq_P y$ then we say that P is a extension of Q.

Extension

Def. If P and Q are posets on $[n]$ such that $x \preceq_Q y \Rightarrow x \preceq_P y$ then we say that P is a extension of Q.

- Every finite poset is an extension of the Hamming poset and can be extended to a linear poset (over the same $[n]$).

Extension

Def. If P and Q are posets on $[n]$ such that $x \preceq_Q y \Rightarrow x \preceq_P y$ then we say that P is a extension of Q.

- Every finite poset is an extension of the Hamming poset and can be extended to a linear poset (over the same $[n]$).
- If P is an extension of Q and C is a code, it follows that C: $d_r^Q(C) \leq d_r^P(C)$

Extension

Def. If P and Q are posets on $[n]$ such that $x \preceq_Q y \Rightarrow x \preceq_P y$ then we say that P is a extension of Q.

- Every finite poset is an extension of the Hamming poset and can be extended to a linear poset (over the same $[n]$).
- If P is an extension of Q and C is a code, it follows that C: $d_r^Q(C) \leq d_r^P(C)$
- Also: if C is a $r-$MDS code using the poset Q (that is, $d_r^Q(C) = n - k + r$), then it is also a $r-$MDS code using the poset P (that is, $d_r^P(C) = n - k + r$).

Extension

Def. If P and Q are posets on $[n]$ such that $x \preceq_Q y \Rightarrow x \preceq_P y$ then we say that P is a extension of Q.

- Every finite poset is an extension of the Hamming poset and can be extended to a linear poset (over the same $[n]$).
- If P is an extension of Q and C is a code, it follows that C: $d_r^Q(C) \leq d_r^P(C)$
- Also: if C is a $r-$MDS code using the poset Q (that is, $d_r^Q(C) = n - k + r$), then it is also a $r-$MDS code using the poset P (that is, $d_r^P(C) = n - k + r$).
- In particular, $d_r(C) \leq d_r^P(C)$, where $d_r(C)$ is the rth Hamming distance, and every $r-$MDS code in the Hamming metric is also a $r-$MDS code for every poset P over the same $[n]$.

P-chain code

A $[n, k]_q-$code is said to be a $P-$chain code if there is a sequence of linear subspaces D_i, $i = 1, 2, ..., k$ such that

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

where

$$w_P(D_i) = d_i^P(C)$$
$$\dim D_i = i$$

In this case, we say that C satisfies the P-chain condition.

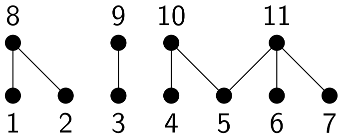
Example

For the Hamming poset:

- The following codes satisfy the chain condition:
  - Hamming codes
  - Dual Hamming codes
  - Reed-Muller codes for all orders
  - Maximum Separable Distance codes
  - Golay codes
- Moreover, every perfect code must satisfy the chain condition.

Example

Let P be the following poset.



Let $u_1, u_2, u_3 \in \mathbb{F}_2^{11}$ be as below and consider $D = [u_1, u_2, u_3]$.

$$u_1 = 00000000100, \;\; u_2 = 01000110001, \;\; u_3 = 01100000010$$

D satisfies the P-chain condition in different ways, both with hierarchy $\{2, 4, 9\}$:

$$\{0\} \subsetneq [u_1] \subsetneq [u_1, u_2] \subsetneq D$$

$$\{0\} \subsetneq [u_1] \subsetneq [u_1, u_3] \subsetneq D$$

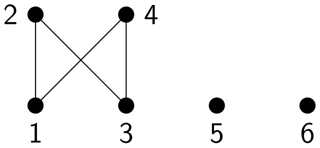
Some results

Lemma. Let P be a poset in $[n]$ and $1 \leq j_1 < j_2 < ... < j_k \leq n \in \mathbb{Z}$.

There is a sequence of codes $C_1 \subsetneq C_2 \subsetneq ... \subsetneq C_k = C$ such that $w_P(C_i) = j_i$.

Remark.
However it is not possible to assure that this sequence satisfies the $P-$chain condition.

Example



- Fix $v_1 = 110000$, $v_2 = 000100$ and $E = [v_1, v_2]$.

$$\begin{aligned} v_1 &= 110000 \\ v_2 &= 000110 \\ v_1 + v_2 &= 110110 \end{aligned} \quad \Longrightarrow \quad \begin{aligned} w_P(v_1) &= 3 \\ w_P(v_2) &= 3 \\ w_P(v_1+v_2) &= 4 \end{aligned}$$

- E satisfies the P-chain condition with sequence $\{3, 4\}$:

$$0 \subsetneq [v_1] \subsetneq E$$

Example

- Let P be the Hamming poset over $\mathbb{F}_2^6$. Let's look for a $P-$chain code C with hierarchy $\{3, 4\}$.
- We must have $w_H(C_1) = d_1^H(C) = 3$ and $\dim C_1 = 1$ (that is $C_1 = [v_1]$).
- WLG: let $v_1 = 111000 \in C_1 \subsetneq C_2 = C$.
- Now, we must have $4 = d_2^H(C) = w_P(C_2) = \#\mathrm{supp}[v_1, v_2]$.
- As $w_P(v_1) = 3$, we must have $\#(\mathrm{supp}[v_2] \setminus \mathrm{supp}[v_1]) = 1$.
- Then:

$$w_P(v_2) \geq 3 \Rightarrow d(v_1, v_2) \leq 2 \Rightarrow w_P(v_2 - v_1) \leq 2 < d_1(C) = 3$$

- Therefore, there is no code that satisfies the P-chain condition with weight sequence $\{3, 4\}$.

Some results

Thm. (Moura-Firer) If the support of a $P-$code C is a total ordered subset of P then C satisfies the $P-$chain condition.

Some results

Thm. (Moura-Firer) If the support of a $P-$code C is a total ordered subset of P then C satisfies the $P-$chain condition.

Cor. Every code over the linear poset (chain poset) satisfies the P-chain condition.

Some results

Thm. (Moura-Firer) If the support of a $P-$code C is a total ordered subset of P then C satisfies the $P-$chain condition.

Cor. Every code over the linear poset (chain poset) satisfies the P-chain condition.

Thm. (Moura-Firer) A code C satisfies the $P-$chain condition iff $C^{\perp}$ satisfies the $\overline{P}$-chain condition.

Some results

Thm. Let $J_1 \subsetneq J_2 \subsetneq \ldots \subsetneq J_k$ be ideals of a poset P such that

$$\# J_i \leq \# \langle J_{i+1} \backslash J_i \rangle_P \, .$$

Then there exists a code C that satisfies the $P-$chain condition in the following sense: there is a chain of codes

$$\{0\} = C_0 \subsetneq C_1 \subsetneq C_2 \subsetneq \ldots \subsetneq C_k = C$$

over $\mathbb{F}_q^n$ such that $d_i^P(C) = w_P(C_i) = \# J_i$ and $\dim(C_i) = i$.

Some results

Thm. Let $J_1 \subsetneq J_2 \subsetneq \dots \subsetneq J_k$ be ideals of a poset P such that

$$\#J_i \leq \#\langle J_{i+1} \backslash J_i \rangle_P \,.$$

Then there exists a code C that satisfies the $P-$chain condition in the following sense: there is a chain of codes

$$\{0\} = C_0 \subsetneq C_1 \subsetneq C_2 \subsetneq \dots \subsetneq C_k = C$$

over $\mathbb{F}_q^n$ such that $d_i^P(C) = w_P(C_i) = \#J_i$ and $\dim(C_i) = i$.

Thm. Let Q be a poset on $[n]$ and X be the set $\{d_1, d_2, \dots, d_k\} \subset [n]$.

Then there is an extension P of Q such that there exists a code C satisfying the P-chain condition with hierarchy X.

OBRIGADA!