Canonical-Systematic Form of Hierarchical Codes

Luciano Viana Felix∗ and Marcelo Firer†

September 1, 2011

Abstract

In this work we present a canonical-systematic form of a code when considering in the ambient space $F_n^q$ a metric determined by a hierarchical poset, showing that up to a linear isometry of the ambient space any code is equivalent to the direct sum of codes with smaller dimensions. The canonical-systematic form enables to exhibit simple expressions for the generalized minimal weights (in the sense defined by Wei), the packing radius of the code and also syndrome decoding algorithm that has (in general) exponential gain when compared to usual syndrome decoding.

1 Introduction

Poset metrics were introduced by Brualdi, Graves and Lawrence in 1995 ([1]), generalizing both the usual Hamming metric of code theory and what is nowadays known as Niederreiter-Rosenbloom-Tsfasman metrics (see [7], [8] and [9]). Since then codes in spaces with such metrics have been studied in many different aspects, including one of the main problem of coding theory that is to determine the main parameters of a code, including the minimal distance and also the generalized Wei weights.

In a work published in 2010, Alves Panek and Firer ([2]) classified all codes in a space endowed with one of such poset metrics, the Niederreiter-Rosenbloom-Tsfasman metric (NRT-metric). This classification was based on a canonical form of the generating matrix, a form that is ”cleaner” than the usual systematic form of a generating matrix and is canonical in the sense it is determined by the generalized minimal weights (in the sense defined by Wei). The possibility of having

∗Universidade Federal Rural do Rio de Janeiro, BR467, km7, 23890-000 Seropédica - RJ, Brazil Email: luvifelix@yfrrj.br
†IMECC - UNICAMP, Rua Sérgio Buarque de Holanda, 651, CEP 13083-859, Campinas - SP, Brazil. Email: mffirer@ime.unicamp.br. Partially supported by FAPESP grant 2007/56052-8.
such canonical form is due to the fact that the isometry group of such a space being larger than in the usual Hamming case, as can be seen in [3].

NRT-metrics is a singular family, unique in a given dimension. A much larger family of poset is the family of what is called hierarchical posets: in any given dimension \( n \), there are essentially as many hierarchical poset metrics as are partitions of the integer \( n \). In this work we devote our attention for this kind of metrics and present a canonical-systematic form for the generating matrix of a code endowed with an hierarchical metric, and show that, despite the fact it does not classify the codes, it enables to calculate both the generalized minimal weights, including the minimal distance, to determine the packing radius and to describe syndrome decoding algorithm.

2 Poset codes

In this section we introduce basic concepts and definitions concerning posets and poset codes.

Consider a partial order on the set \([n] := \{1, 2, \ldots, n\}\), with order relation denoted by \( \preceq \). The pair \( P = ([n], \preceq) \) is called a partially ordered set (abbreviated as poset). An ideal in \( P \) is a subset \( I \subseteq P \) with the property that if \( i \in I \) and \( j \preceq i \), than \( j \in I \). Given a subset \( X \subset I \), we denote by \( \langle X \rangle \) the smallest ideal containing \( X \), called the ideal generated by \( X \).

Let \( \mathbb{F}_q \) be a finite field with \( q \) elements and \( \mathbb{F}_q^n \) the \( n \)-dimensional vector space of \( n \)-tuples over \( \mathbb{F}_q \). When no confusion may arise, we may denote \( \mathbb{F}_q \) just as \( V \).

Given \( x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n \), the support of \( x \) is the set \( \text{supp}(x) = \{i \in P| x_i \neq 0\} \).

The \( P \)-weight of \( \omega_P(x) \) of \( x \) is

\[
\omega_P(x) = |\langle \text{supp}(x) \rangle|
\]

where \(|\cdot|\) denotes the cardinality of the given set.

The function \( d_P : \mathbb{F}_q^n \times \mathbb{F}_q^n \rightarrow \mathbb{N} \), defined by \( d_P(x, y) = \omega_P(x - y) \) is a metric on \( \mathbb{F}_q^n \) called a poset-metric or \( P \)-metric and endowed with such a metric \( \mathbb{F}_q^n \) is called a poset space or more specifically, a \( P \)-space.

An \([n, k, \delta_P]_q \) poset code is a \( k \)-dimensional subspace \( C \subset \mathbb{F}_q^n \) where \( \mathbb{F}_q^n \) is endowed with a poset-metric \( d_P \) and \( \delta_P = \delta_P(C) = \min\{\omega_P(x)| 0 \neq x \in C\} \) is the minimal \( P \)-distance of the code \( C \). When the minimal \( P \)-distance does not play a relevant role, we will write just \([n, k]_q \).

An \([n, k, \delta_P]_q \) code \( C \subset (\mathbb{F}_q^n, d_P) \) and an \([n, k, \delta_{P'}]_q \) code \( C' \subset (\mathbb{F}_q^n, d_{P'}) \) are said to be equivalent if there is a linear isometry \( T : (\mathbb{F}_q^n, d_P) \rightarrow (\mathbb{F}_q^n, d_{P'}) \) such that \( T(C) = C' \). In particular we must have \( P \) and \( P' \) order-isomorphic.

2
Definition 1 We say a poset \( P = ([n], \preceq) \) is an hierarchical poset if there is a partition

\[ [n] = \bigcup_{l=1,\ldots,h} H_l \]

of \([n]\) such that \(i \preceq j\) if and only if \(i = j\) or \(i \in H_l, j \in H_l\) and \(l_i < l_j\). Each class \(H_i\) is called the \(i\)-level of \(P\) and \(h\) is the height of the poset.

Example 2 A chain poset is a hierarchical poset over \([n]\) with height \(n\) and a anti-chain poset is a hierarchical poset over \([n]\) with height 1. The chain and anti-chain posets give rise to the NRT-metric and the usual Hamming metric respectively.

![Figure 1: Examples of hierarchical posets: anti-chain, chain and "general" hierarchical poset](image)

We remark that the family of hierarchical posets, with which we are concerned in this work, is a large family of posets. Indeed, to define a hierarchical poset on \([n]\) is equivalent to define a positive partition of \(n\) and the number \(p(n)\) of such partitions behaves asymptotically as \(\frac{1}{4n}\sqrt{\pi} e^{2n/3}\) (see [6]).

We say that \(C \in \mathbb{F}_q^n\) is an hierarchical poset code when we consider on \(\mathbb{F}_q^n\) a metric determined by an hierarchical poset. In this work we are concerned only with hierarchical poset codes. We say \(P\) is an \((n; n_1, \cdots, n_h)\)-poset, where \(n_l = |H_l|\) is the cardinality of the level \(H_l\). To avoid summations in the indexes we denote by \(s_i = \sum_{j=1}^i n_j\) the cardinality of the poset up to level \(i\), with \(s_0 = 0\).

We should remark that up to order-isomorphism an hierarchical poset is determined by the values of \((n; n_1, \cdots, n_h)\). Hence, we may assume without loss of generality that \(H_i = \{s_{i-1} + 1, \cdots, s_{i-1} + n_i\}\), for every \(i \in \{1, 2, \cdots, h\}\), what is called the natural labeling of the poset.

It is worthwhile to give a explicit expression for the \(P\)-weight when \(P\) is a hierarchical poset. Given a \((n; n_1, \cdots, n_h)\) hierarchical poset \(P\), and \(x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n\),
then \( \omega_P(x) = s_l + \omega_{P,l+1}(x) \) where \( l + 1 \) is minimal with the property that \( x_i = 0 \) for \( i > s_{l+1} \) and \( \omega_{P,l+1}(x) := |\text{supp}(x) \cap H_{l+1}| \). The set \( \text{supp}(x) \cap H_{l+1} \) is maximal (in the poset order) elements in \( \text{supp}(x) \) is denoted by \( M(x) \).

### 3 Canonical-Systematic Form for the Generating Matrix

From here on we assume \( P \) is a \((n; n_1, \ldots, n_h)\) hierarchical poset and \( C \subset \mathbb{F}_q^n \) is a \([n,k]_q\) linear poset code.

The set \( \hat{C}_i = \{ v \in C | M(v) \subset H_i \} \) of codewords with support of maximal height at level \( i \) is not a vector subspace but \( C_i = \cup_{j=1}^{t_i} \hat{C}_j \) is so and clearly \( C_1 \subseteq C_2 \subseteq \cdots \subseteq C_h \) is a chain of subspaces. Let \( \Lambda(C) := \{ t_1, \ldots, t_h \} \) be the set of levels for which \( \hat{C}_{t_j} \neq \emptyset \).

We define \( d_j := \dim(C_{t_j}) - \dim(C_{t_j-1}) \) for \( j > 1 \) and \( d_1 = \dim(C_{t_1}) \) so that \( \dim(C_{t_j}) = d_1 + \cdots + d_j \). The following lemma is trivial, but will be stated since it will be used repeatedly.

**Lemma 3** If \( v \in C_{t_j} \) and \( v \notin C_{t_{j-1}} \), then \( v \in \hat{C}_{t_j} \).

**Proof:** Let \( v \in C_{t_j} \setminus C_{t_{j-1}} \). So \( v \in \cup_{l=t_{j-1}+1}^{t_j} \hat{C}_l = \hat{C}_{t_j} \), since \( \hat{C}_l = \emptyset \) for \( t_{j-1} + 1 \leq l \leq t_j - 1 \).

We denote by \( e_i = (0, \ldots, 0, 1_i, 0, \ldots, 0) \) the vector that has all entries nulls, except by the \( i \)–th that is 1, so that \( \{e_i | 1 \leq i \leq n\} \) is the usual base of \( \mathbb{F}_q^n \).

We start finding a generating matrix without considering codes equivalence.

**Theorem 4** Let \( P \) be a \((n; n_1, \ldots, n_h)\) hierarchical poset and \( C \subset \mathbb{F}_q^n \) a poset code. Then, \( C \) has a generating matrix \( G = (G_{k,j}) \) consisting of blocks \( G_{k,j} \) of size \( d_{t_k} \times n_j \) where \( G_{k,j} \) is the null matrix, for every \( j > t_k \), that is, \( C \) has as generating matrix of the form

\[
G = \begin{pmatrix}
G_{s,1} & \cdots & \cdots & \cdots & G_{s,t_s} & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
G_{2,1} & \cdots & \cdots & G_{2,t_2} & 0 & \cdots & 0 \\
G_{1,1} & \cdots & G_{1,t_1} & 0 & \cdots & 0
\end{pmatrix}
\]
Proof: We consider the first non-null level $t_1$ of $C$ and recall that $\dim(C_{t_1}) = d_1$. Let $\hat{\beta}_1 = \beta_1 = \{v_{11}, \ldots, v_{1d_1}\}$ be a base of $C_{t_1}$. As $v_{1j} \in \hat{C}_{t_1}$, we have $M(v_{1j}) \subseteq H_{t_1}$, hence

$$v_{1j} = \sum_{i=1}^{s_1} e_i a_i^{1j}, \quad a_i^{1j} \in F_q.$$  

We consider now the $(d_1 + \cdots + d_{r-1})$-dimensional subspace $C_{r-1}$ and assume $\beta_{r-1} = \hat{\beta}_1 \cup \cdots \cup \hat{\beta}_{r-1}$ is a base of $C_{r-1}$ where $\hat{\beta}_k = \{v_{k1}, \ldots, v_{kd_k}\}$ is such that

$$v_{kj} = \sum_{i=1}^{s_k} e_i a_i^{kj}, \quad a_i^{kj} \in F_q.$$  

We move now to the $r$-th level $C_r$ of $C$. We recall that $C_r$ is a $(d_1 + \cdots + d_r)$-dimensional space and $C_{r-1} \subseteq C_r$. Let $\beta_r$ be a base of $C_r$ such that $\beta_{r-1} \subseteq \beta_r$, i.e.,

$$\beta_r = \{v_{11}, \ldots, v_{1d_1}, \ldots, v_{(r-1)d_{r-1}}, v_{r1}, \ldots, v_{rd_r}\}.$$  

Since $\dim(C_{r-1}) < d_1 + \cdots + d_{r-1} + 1$, from Lemma 3 it follows that $v_{rj} \in C_r \setminus C_{r-1}$ and hence $v_{rj} = \sum_{i=1}^{s^*} e_i a_i^{rj}, \quad a_i^{rj} \in F_q$. 

Repeating this procedure until we reach the highest level $t_s$, we get an ordered base $\beta_s = \{v_{11}, \ldots, v_{1d_1}, \ldots, v_{s1}, \ldots, v_{sd_s}\}$ of $C_s = C$. The generator matrix of $C$ that has as rows the elements of $\beta_s$ ordered from the bottom to the top fulfills the conditions stated in the Theorem. 

Let $W = W_1 \oplus W_2 \oplus \cdots \oplus W_n$ be a decomposition of a vector space as direct sum of subspaces. Each $v \in W$, can be uniquely decomposed as $v = v_1 + v_2 + \cdots + v_n$, where $v_1 \in W_1$. We let $p_i(v) = v_i$ be the projection of $v$ into $W_i$ and denote $q_i(v) = v - v_i$. 

Assuming the natural labeling of the poset, we write $\mathbb{F}_q^n = V = V_1 \oplus V_2 \oplus \cdots \oplus V_n$, where $V_i = \mathbb{F}_q^{m_i}$, i.e., we decompose $\mathbb{F}_q^n$ by the levels of the poset. Observe that $C_i \subseteq V_1 \oplus V_2 \oplus \cdots \oplus V_i$. 

Lemma 5 Let $\beta_j = \{v_{11}, \ldots, v_{1d_1}, \ldots, v_{jd_j}\}$ be the base of $C_{t_j}$ determined in Theorem 4. Then $p_{t_j}(\hat{\beta}_j) = \{p_{t_j}(v_{j1}), \ldots, p_{t_j}(v_{jd_j})\}$ is linearly independent. 

Proof: Define $w_{jl} = p_{t_j}(v_{jl}), u_{jl} = v_{jl} - w_{jl}$ and suppose that $\sum_{i=1}^{d_j} a_i w_{ji} = 0$. It follows that

$$\sum_{i=1}^{d_j} a_i v_{ji} = \sum_{i=1}^{d_j} a_i w_{ji} + \sum_{i=1}^{d_j} a_i u_{ji} = \sum_{i=1}^{d_j} a_i u_{ji} = u,$$

so that $u \in \langle \hat{\beta}_j \rangle$ and $p_{t_j}(u) = 0$. It follows that $M(u) \not\subseteq H_{t_j}$, hence $u \not\in \hat{C}_{t_j}$ and by Lemma 3 we find that $u \in C_{t_j-1}$. Therewith, we have $u \in \langle \hat{\beta}_j \rangle \cap \langle \beta_{j-1} \rangle$. 

\begin{figure}[h]  

\end{figure}
and $\beta_j = \hat{\beta}_j \cup \hat{\beta}_j$ is a base of $C_{t_j}$, so $u = \sum_{i=1}^{d_j} a_i v_{ji} = 0$ and it follows that $a_i = 0, \forall i \in \{1, \cdots, d_j\}$ so that
\[ p_{t_j}(\hat{\beta}_j) = \{w_{jl} = p_{t_j}(v_{j1}), \cdots, w_{jd} = p_{t_j}(v_{jd})\} \]
is a linearly independent set. \(\Box\)

**Remark 6** We denote the usual base of $V_l$ by $\hat{\Gamma}_l$ and notice that $x \in V_1 \oplus \cdots \oplus V_{t_j}$ if and only if, $\text{supp}(x) \subset \bigcup_{l=1}^{t_j} H_l$.

We have now a sequence of three lemmas that will help in the description of the canonical-systematic form of a generating matrix for codes in spaces endowed with an hierarchical poset-metric.

**Lemma 7** Given an $[n,k]_q$ code $C$, for each $j = 1, \cdots, s$ there is a base $\alpha_j$ of $V_1 \oplus \cdots \oplus V_{t_j}$, such that $\alpha_j = \Gamma_j \cup \beta_j \cup \Delta_j$, where:

- $\beta_j$ is the base of $C_{t_j}$ determined in Theorem 4,
- $\Gamma_j = \left( \bigcup_{l=1}^{t_j} \hat{\Gamma}_l \right)_{l \notin \Lambda(C)}$
- $\Delta_j = \bigcup_{l=1}^{t_j} \hat{\Delta}_l$ is such that if $v \in \hat{\Delta}_l$, then $M(v) \subset H_i$ for some $i \leq t_j - 1$.

**Proof:** Let $\Gamma_1$ be the usual base of $V_1 \oplus \cdots \oplus V_{t_1-1}$. We observe that $\beta_1 \cup \Gamma_1$ is a linearly independent subset of $V_1 \oplus \cdots \oplus V_{t_1}$. Indeed, if $\sum_{i=1}^{d_1} a_i v_{1i} + \sum_{\gamma \in \Gamma_1} b_{i\gamma} = 0$ then the vector
\[ w := \sum_{i=1}^{d_1} a_i v_{1i} = - \sum_{\gamma \in \Gamma_1} b_{i\gamma} \in C \]
since $w \in \langle \beta_1 \rangle$ and $M(w) \subset H_i$ for some $i \leq t_1 - 1$, because $w \in \langle \Gamma_1 \rangle$. Therewith $w = 0$ since $t_1$ is the first level of the poset such that $M(x) \subset H_i$ for some $x \in C, x \neq 0$. But both $\Gamma_1$ and $\beta_1$ are linearly independent sets, and it follows that $a_i = b_{i\gamma} = 0$ for every $i \in \{1, \cdots, d_1\}$ and $\gamma \in \Gamma$.

So, there is a set $\Delta_1$ such that $\Gamma_1 \cup \beta_1 \cup \Delta_1$ is a base of $V_1 \oplus \cdots \oplus V_{t_1}$ and we need to show that $M(v) \subset H_1$ for every $v \in \Delta_1$.

Consider $v \in \Delta_1$ and suppose that $M(v) \notin H_1$. It will follow from Remark 6 that $\text{supp}(v) \subset \bigcup_{l=1}^{t_1-1} H_l$, i.e., $v \in V_1 \oplus \cdots \oplus V_{t_1-1}$. However, since $\Gamma_1$ is a base of
\( V_1 \oplus \cdots \oplus V_{t_j - 1} \), we have that \( v \in \langle \Gamma_1 \rangle \), where \( \langle A \rangle \) denotes the subspace spanned by \( A \). Since we also have that \( v \in \langle \Delta_1 \rangle \) we find that \( v = 0 \).

Consider now
\[
V_1 \oplus \cdots \oplus V_{t_j - 1} \oplus V_{t_j - 1} \oplus V_{t_j}
\]
and let \( \Gamma_{j - 1} \cup \beta_{j - 1} \cup \Delta_{j - 1} \) be a base of \( V_1 \oplus \cdots \oplus V_{t_j - 1} \). It is obvious that \( \Gamma_j \cup \beta_{j - 1} \cup \Delta_{j - 1} \) is a base of \( V_1 \oplus \cdots \oplus V_{t_j - 1} \oplus \cdots \oplus V_{t_j - 1} \).

Consider \( v_{jl} \in \hat{\beta}_j \subset \hat{C}_t \) such that \( M(v_{jl}) \subset H_t \) but \( M(v_{jl}) \nsubseteq H_{t_j - 1} \). It follows that
\[
v_{jl} \in V_1 \oplus \cdots \oplus V_{t_j} \setminus V_1 \oplus \cdots \oplus V_{t_j - 1}.
\]

We claim that
\[
\Gamma_j \cup \beta_{j - 1} \cup \Delta_{j - 1} \cup \hat{\beta}_j = \Gamma_j \cup \Delta_{j - 1} \cup \beta_j
\]
is a linearly independent subset of \( V_1 \oplus \cdots \oplus V_{t_j} \). Indeed, let us denote \( \hat{\beta}_j = \{ v_{j1}, \ldots, v_{jd_j} \} \) and suppose that
\[
\sum_{i=1}^{d_j} a_{ji} v_{ji} + \sum_{v \in \beta_{j - 1}} a_v v + \sum_{\gamma \in \Gamma_j} b_{\gamma} \gamma + \sum_{\delta \in \Delta_{j - 1}} c_{\delta} \delta = 0.
\]
Considering the projection on the level \( t_j \) we have that
\[
p_{t_j}(w) = p_{t_j}(\sum_{i=1}^{d_j} a_{ji} v_{ji})
\]
\[
= \sum_{i=1}^{d_j} a_{ji} p_{t_j}(v_{ji}) = 0
\]
and so, by Lemma 5, we have \( a_i = 0 \) for \( i = 1, \ldots, d_j \). It follows that
\[
\sum_{v \in \beta_{j - 1}} a_v v + \sum_{\gamma \in \Gamma_j} b_{\gamma} \gamma + \sum_{\delta \in \Delta_{j - 1}} c_{\delta} \delta = 0
\]
and since \( \beta_{j - 1} \cup \Gamma_j \cup \Delta_{j - 1} \) is a base of \( V_1 \oplus \cdots \oplus V_{t_j - 1} \oplus \cdots \oplus V_{t_j - 1} \), we have that
\[
a_v = b_\gamma = c_\delta = 0
\]
for every \( v \in \beta_{j - 1}, \gamma \in \Gamma_j \) and \( \delta \in \Delta_{j - 1} \) and it follows that \( \Gamma_j \cup \Delta_{j - 1} \cup \beta_j \) is a linearly independent subset of \( V_1 \oplus \cdots \oplus V_{t_j} \).

We let now \( \hat{\Delta}_j \) be a set such that \( \Gamma_j \cup \beta_j \cup \Delta_{j - 1} \cup \hat{\Delta}_j \) is a base of \( V_1 \oplus \cdots \oplus V_{t_j} \).

All is left is to show that \( M(v) \subset H_{t_j} \) for \( 0 \neq v \in \hat{\Delta}_j \) what is done in the same way.
as we did for the case \( t_j = t_1 \). □

In the previous Lemma we found a base for the subspace of \( V_1 \oplus \cdots \oplus V_{t_s} \subseteq \mathbb{F}_q^n \) that includes vectors with zero coordinates above \( t_s \), the highest level of the code \( C \). Considering the level decomposition above this level,

\[
V = V_1 \oplus \cdots \oplus V_{t_s} \oplus E_{s+1} \oplus \cdots \oplus E_n,
\]

where \( E_i = \langle e_i \rangle \), it is immediate to verify that

\[
\beta = \alpha_s \cup \left( \bigcup_{l=t_s+1}^h \hat{\Gamma}_l \right)
\]

\[
= \left( \bigcup_{l \in \Lambda(C)} \hat{\Gamma}_l \right) \cup \beta_s \cup \Delta_s
\]

is a base of \( V \).

Before we continue, we should establish some more notations. For \( i \in P \) we denote \( (i)^* = \langle i \rangle \setminus \{i\} \) and given \( X \subset [n] \) we define \( E_X := \{v \in V | \text{supp}(v) \subset X\} \).

Lemma 8 Let \( T : V \rightarrow V \) be the linear transformation that is defined upon the base \( \beta \) in the following way:

\[
T (v) = \begin{cases} 
  v & \text{for } v \in \bigcup_{l \in \Lambda(C)} \hat{\Gamma}_l \\
  p_{\beta_l} (v) & \text{for } v \in \cap \hat{\beta}_1 \cup \Delta_1
\end{cases}
\]

Then, for any \( i \in \{1, \ldots, n\} \) and any \( e \in E_i \), there are \( 0 \neq e' \in E_i \) and \( u \in E_{(i)^*} \), such that \( T(e) = e' + u \).

Proof: Let us consider \( e \in E_i \). If \( e \) is a base vector, that is, if \( e \in \hat{\Gamma}_i \), then we just take \( e' = e \) and \( u = 0 \).

Assume now that \( e \in E_k \subset V_{t_j} \) for some \( t_j \in \Lambda(C) \), i.e., there is \( k \in H_{t_j} \) so that \( (k)^* = \bigcup_{l=1}^{t_j} H_1 \) and hence \( E_{(k)^*} = V_1 \oplus \cdots \oplus V_{t_j-1} \). Since (by Lemma 7) \( \alpha_j = \Gamma_j \cup \beta_j \cup \Delta_j \) is a base of \( V_1 \oplus \cdots \oplus V_{t_j} \), we may decompose

\[
e = \gamma + \sum_{l=1}^j b_l + \sum_{l=1}^j \delta_l
\]

with \( \gamma \in \langle \Gamma_j \rangle \), \( b_l \in \langle \hat{\beta}_l \rangle \) and \( \delta_l \in \langle \hat{\Delta}_l \rangle \). It follows that
\[ T(e) = T(\gamma) + \sum_{l=1}^{j} T(b_l) + \sum_{l=1}^{j} T(\delta_l) \]

\[ = \gamma + \sum_{l=1}^{j} p_t(b_l) + \sum_{l=1}^{j} p_t(\delta_l) \]

\[ = \gamma + \sum_{l=1}^{j-1} p_t(b_l) + \sum_{l=1}^{j-1} p_t(\delta_l) + (p_t(b_j) + p_t(\delta_j)) \]

\[ = \gamma + \sum_{l=1}^{j-1} p_t(b_l + \delta_l) + p_t(b_j + \delta_j) \]

hence

\[ T(e) = \gamma + \sum_{l=1}^{j-1} p_t(b_l + \delta_l) + p_t(b_j + \delta_j) \]

with

\[ \gamma + \sum_{l=1}^{j-1} p_t(b_l + \delta_l) \in V_1 \oplus \cdots \oplus V_{t-1}. \]

We remark that

\[ e = p_t(e) = p_t(\gamma + \sum_{l=1}^{j-1} b_l + \sum_{l=1}^{j-1} \delta_l) \]

\[ = p_t(b_j + \delta_j) \]

so that \( p_t(b_j + \delta_j) \in E_k. \)

Thereby, taking \( e' = p_t(b_j + \delta_j) \) and \( u = \gamma + \sum_{l=1}^{j-1} p_t(b_l + \delta_l) \) we find that \( T \) satisfies the stated conditions. \( \square \)

We state without proving the following trivial lemma:

**Lemma 9** Let \( W = W_1 \oplus \cdots \oplus W_m \) be a decomposition of a vector space. If \( A_1, \cdots, A_m \) are linearly independent sets with \( A_i \subset W_i \) for each \( i = 1, \cdots, m \) then \( A_1 \cup \cdots \cup A_m \) is a linearly independent set.

Now, we finally will state the canonical-systematic form of an hierarchical posets code.
**Theorem 10 (Canonical-systematic form)** Let $C$ be a $[n, k]_q$ code. Then $C$ is equivalent to a code $\hat{C}$ that has a generating matrix $G' = (G'_{k,j})$ consisting of blocks $G'_{k,j}$ of size $d_{tk} \times n_j$ such that $G'_{k,j}$ is the null matrix for every $j \neq t_k$ and for $j = t_k$ it has the form $G'_{k,t_k} = [Id_{t_k} | A_{t_k}]$ where $Id_{t_k}$ is the identity matrix of size $t_k \times t_k$ and $A_{k,j}$ is a matrix of size $d_{tk} \times (n_j - t_k)$. In other words, $G'$ has the following form:

$$G' = \begin{pmatrix}
0_{s,1} & \ldots & 0_{s,t_1} & \ldots & 0_{s,t_2} & \ldots & [Id_{t_s} | A_{t_s}] & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0_{t_1} & \ldots & 0_{t_1,t_1} & \ldots & [Id_{t_1} | A_{t_1}] & 0 & \ldots & 0 \\
0_{0,1} & \ldots & 0_{0,t_1} & \ldots & [Id_{0} | A_{0}] & 0 & \ldots & 0
\end{pmatrix}$$

**Proof:** We may assume that $C$ has a generator matrix of the form presented in Theorem 4. Let us consider the linear transformation $T : V \rightarrow V$ defined as

$$T(v) = \begin{cases}
v & \text{for } v \in \bigcup_{\ell \notin \Lambda(C)} \hat{\Gamma}_\ell \\
p_{t_j}(v) & \text{for } v \in \cap_{\beta_1} \cap \Delta_1
\end{cases}$$

as stated in Lemma 8.

We will prove that $T$ is a linear isometry. Since $T$ is linear by definition, in order to prove it is an isomorphism, we need to show that

$$T(\beta) = \bigcup_{\ell \notin \Lambda(C)} T\left(\hat{\Gamma}_\ell\right) \bigcup_{t_i \in \Lambda(C)} T\left(\hat{\beta}_{t_i}\right) \bigcup_{t_i \in \Lambda(C)} T\left(\hat{\Delta}_{t_i}\right)$$

$$= \bigcup_{\ell \notin \Lambda(C)} \hat{\Gamma}_\ell \bigcup_{t_i \in \Lambda(C)} p_{t_j}\left(\hat{\beta}_{t_i}\right) \bigcup_{t_i \in \Lambda(C)} p_{t_j}\left(\hat{\Delta}_{t_i}\right)$$

is linearly independent.

By Lemma 9 it is enough to show that $p_{t_j}\left(\hat{\beta}_{\delta}\right) \cup p_{t_j}\left(\hat{\Delta}_{\delta}\right)$ is linearly independent for every $j = 1, \ldots, s$, remembering that $\Lambda(C) = \{t_1, \ldots, t_s\}$.

We restrict ourself to the level $t_j$. From the definition of the projection $p_i$ and $q_i$, we have that

$$\sum_{i=1}^{d_j} a_i v_{ji} + \sum_{\delta \in \Delta} b_{\delta} \delta = \sum_{i=1}^{d_j} a_i \left(p_{t_j}(v_{ji}) + q_{t_j}(v_{ji})\right) + \sum_{\delta \in \Delta} b_{\delta} \left(p_{t_j}(\delta) + q_{t_j}(\delta)\right)$$

10
and assuming that
\[
\sum_{i=1}^{d_j} a_i p_{t_j} (v_{ji}) + \sum_{\delta \in \Delta} b_{\delta} p_{t_j} (\delta) = 0
\]
we have that
\[
\sum_{i=1}^{d_j} a_i v_{ji} + \sum_{\delta \in \Delta} b_{\delta} = \sum_{i=1}^{d_j} a_i q_{t_j} (v_{ji}) + \sum_{\delta \in \Delta} b_{\delta} q_{t_j} (\delta)
\]
By definition of \( q_{t_j} \) we have that
\[
\sum_{i=1}^{d_j} a_i q_{t_j} (v_{ji}) + \sum_{\delta \in \Delta} b_{\delta} q_{t_j} (\delta) = \sum_{i=1}^{d_j} a_i v_{ji} + \sum_{\delta \in \Delta} b_{\delta} \delta = 0.
\]
It follows that
\[
a_1 = \cdots = a_{d_j} = 0 \text{ and } b_{\delta} = 0, \forall \delta \in \Delta
\]
hence \( p_{t_j} (\hat{\beta}_j) \cup p_{t_j} (\hat{\Delta}_j) \) is a linearly independent so that \( T \) is actually a linear isomorphism.

By Proposition 4.3 in [3] we find that \( T \) is actually an isometry, so that \( C \) and \( \hat{C} = T (C) \) are equivalent codes and the way we constructed \( T \) ensures that the generating matrix of \( \hat{C} \) consisting of the vectors of the ordered base \( T(\beta_s) \) as its rows (positioned from bottom to top) has the form
\[
B = \begin{pmatrix}
0_{s,1} & \cdots & \cdots & B_{s,t_s} & 0 \\
\vdots & \ddots & \vdots & \vdots & \vdots \\
0_{2,1} & \cdots & \cdots & B_{2,t_2} & 0 & \cdots & 0 \\
0_{1,1} & \cdots & B_{1,t_1} & 0 & \cdots & 0 \\
\end{pmatrix}
\]
where each block \( B_{k,t_k} \) has size \( d_{t_k} \times n_{t_k} \) and rank \( n_{t_k} \).
We remark that the space generated by each row
\[
\begin{pmatrix}
0_{j,1} & \cdots & \cdots & B_{j,t_j} & 0 & \cdots & 0 \\
\end{pmatrix}
\]
is contained in a subspace of $\mathbb{F}_q^n$ spanned by the coordinates corresponding to a unique level of the hierarchical poset $P$, so that the metric $d_P$ restricted to this subspace coincides with the Hamming metric. Inasmuch as we are concerned only with a unique level, we are in the usual setting of codes with Hamming metric and hence, we can replace each block $B_{k,t_k}$ by the standard form $G'_{k,t_k} = [Id_{t_k} | A_{k,t_k}]$ where $Id_{t_k}$ is the identity matrix of size $t_k \times t_k$ and $A_{k,t_k}$ is a matrix of size $d_{t_k} \times (n_j - t_k)$. □

**Remark 11** Theorem 10 means that, considering a hierarchical poset-metric, a $[n,k]_q$-code $C$ may be considered, up to equivalence, to be of the form

$$C = C_1 \oplus C_2 \oplus \cdots \oplus C_h$$

where $h$ is the height of the hierarchical poset $P$, supp $(C_i)$ is contained in the i-level $H_i$ and $\sum_{i=1}^{h} \dim(C_i) = k$.

**Remark 12** We call the generating matrix described in Theorem 10 a canonical-systematic form, meaning that it is canonical in the levels, in the sense that $\dim(C_i)$ is uniquely determined by the generalized weight hierarchy of $C$ as will be seen in Section 4. In particular, the levels that corresponds to blocks that are identically nulls along the columns of the matrix $G'$ or equivalently, the levels corresponding to codes $C_i$ in decomposition 11 with $\dim(C_i) = 0$ corresponds to the levels not contained in $\Lambda(C)$, that is, $\dim(C_i) = 0$ if $i \in [n]$.

### 4 Minimal Distance, Packing Radius and Syndrome Decoding

Considering the canonical-systematic form it is not difficult to describe important invariants of code theory, such as the minimal distance and the packing radius of a code, and also to describe syndrome decoding algorithm.

In this section we will assume that $P$ is a $(n;n_1,\cdots,n_h)$ hierarchical poset and that $C$ is an $[n,k]_q$ code in its canonical-systematic form established in Theorem 10. We let

$$C = C_1 \oplus C_2 \oplus \cdots \oplus C_h$$

be its decomposition as presented in Remark 11. We denote by $k_i$ the dimension of $C_i$ and let $\Omega(C) = \{i|k_i > 0\}$. Since we are considering codes in its canonical-systematic form, it is clear that $\Omega(C) = \Lambda(C)$, as defined in the beginning of Section 3. We remark that the restriction $d'_P$ of $d_P$ to $C_i$ is equivalent to the usual Hamming metric, since given $i,j \in \{s_{l-1} + 1,\cdots, s_l\}$ we have that $i \preceq_P j$ iff $i = j$ where $s_i = n_1 + \cdots + n_{i-1} + n_i$, as we have already defined.
Proposition 13 Under the conditions stated, the minimal distance of $\mathcal{C}$ is

$$
\delta_P = s_{t_1-1} + \delta_{t_1}
$$

where $t_1 = \min \Lambda (\mathcal{C})$ and $\delta_{t_1}$ is the minimal distance of $\mathcal{C}_{t_1}$ considered as a Hamming code.

Proof: Let $c_{t_1} \in \mathcal{C}_{t_1}$ be such that $d_{t_1} (c_{t_1}) = \delta_{t_1}$. Then $d_P (c_{t_1}) = s_{t_1-1} + \delta_{t_1}$, so that $\delta_P \geq n_1 + \cdots + n_{t_1-1} + \delta_{t_1}$. Clearly that can not be $c \in \mathcal{C}$ with $d_P (c) \leq n_1 + \cdots + n_{t-1} + \delta_{t_1}$ since this would imply that either $t_1 > \min \Lambda (\mathcal{C})$ or that the minimal distance of $\mathcal{C}_{t_1}$ is strictly smaller than $\delta_{t_1}$.

Generalizing the definition given by Wei in [10], the $i$-th $P$-weight of a code $\mathcal{C}$ (where $i$ runs from 1 to $k$) is

$$
\delta_{P,i} := \delta_{P,i} (\mathcal{C}) = \min |\langle \text{supp} (D) \rangle |
$$

where $D$ is an $i$-dimensional subspace of $\mathcal{C}$ and

$$
\text{supp} (D) = \{ i \in [n] | x_i \neq 0 \text{ for some } x \in D \}.
$$

We remark that $\delta_{P,1} = \delta_P$.

In a similar way it is possible to describe generalized weights of $\mathcal{C}$. Let us recall some notations established in the beginning of Section 3: $\Lambda (\mathcal{C}) = \{ t_1 < t_2 < \cdots < t_s \}$, $s = |\Lambda (\mathcal{C})|$ and $r_i = d_1 + d_2 + \cdots + d_i$, for $i = 1, 2, \cdots, h$ where $d_i = \dim (\mathcal{C}_i)$ and $d_0 = 0$.

With this notation we have the following result:

Proposition 14 Given $1 \leq i \leq k$, let $j$ be such that $r_{j-1} < i \leq r_j$. Then, the $i$-th $P$-weight $\delta_{P,i}$ of a code $\mathcal{C}$ is

$$
\delta_{P,i} = s_{t_j-1} + \delta_{(i-r_{j-1})} (\mathcal{C}_{t_j})
$$

where $\delta_{(i-r_{j-1})} (\mathcal{C}_{t_i})$ is the $(i-r_{j-1})$-th generalized weight of $\mathcal{C}_{t_j}$ considered as a Hamming code.

Proof: The proof follows in the same way as in Proposition 13. Let $\hat{\mathcal{D}}_{t_j} \subset \mathcal{C}_{t_j}$ be such that $|\text{supp} (\hat{\mathcal{D}}_{t_j})| = \delta_{(i-r_{j-1})} (\mathcal{C}_{t_j})$. Then $|\langle \text{supp} (\hat{\mathcal{D}}_{t_j}) \rangle | = s_{t_j-1} + \delta_{(i-r_{j-1})} (\mathcal{C}_{t_j})$. We consider the code

$$
\hat{\mathcal{D}} = \mathcal{C}_1 \oplus \cdots \mathcal{C}_{t_{j-1}} \oplus \hat{\mathcal{D}}_{t_j},
$$

13
Then it is clear that \( \dim(\hat{D}) = r_{j-1} + (i-r_{j-1}) = i \) and noticing that \( |\langle \text{supp}(\hat{D}) \rangle| = |\langle \text{supp}(\hat{D}_{t_j}) \rangle| = s_{t_j-1} + \delta_{(i-r_{j-1})} (C_{t_j}) \) it follows that \( \delta_{P,i} \leq s_{t_j-1} + \delta_{(i-r_{j-1})} (C_{t_j}) \).

We consider now a subcode of \( C \) that realizes the \( i \)-th weight: \( D \subset C \) is such that \( |\langle \text{supp}(D) \rangle| = s_{t_j} \). First of all we note that \( D \subset C_1 \oplus \cdots C_{t_j} \), since otherwise we would have

\[
|\langle \text{supp}(D) \rangle| > s_{t_j} > s_{t_j-1} + \delta_{(i-r_{j-1})} (C_{t_j}) = |\langle \text{supp}(\hat{D}) \rangle|.
\]

We can hence consider the decomposition

\[
D = D_1 \oplus \cdots \oplus D_{t_j},
\]

where \( D_l \subset C_l \) for \( l \in \{1, \cdots, t_j\} \). It is obvious that

\[
|\langle \text{supp}(D) \rangle| = |\langle \text{supp}(D_{t_j}) \rangle| = |\text{supp}(D_{t_j})| + s_{t_j-1}.
\]

By the minimality of \( \delta_{(i-r_{j-1})} (C_{t_j}) \) we find that

\[
|\text{supp}(D_{t_j})| + s_{t_j-1} \geq s_{t_j-1} + \delta_{(i-r_{j-1})} (C_{t_j})
\]

and since \( \delta_{P,i} = |\langle \text{supp}(D) \rangle| \) we have that \( \delta_{P,i} \geq s_{t_j-1} + \delta_{(i-r_{j-1})} (C_{t_j}) \).

It follows that \( \delta_{P,i} = s_{t_j-1} + \delta_{(i-r_{j-1})} (C_{t_j}) \). \( \square \)

We remark that, as a consequence of expression 1, \( \dim (C_i) \) is determined by the weight distribution of \( C \), what justifies calling the decomposition determined in Theorem 10 to be canonical.

Similar consideration leads us for finding the packing radius of \( C \), giving an explicit expression that depends solely on the minimal distance of \( C \) and the minimal distance of \( C_{t_j} \) viewed as a Hamming code.

First of all we recall that the packing radius of a code \( C \) relatively to the poset metric \( d_P \) is

\[
R_P(C) := \max \{ r \in \mathbb{N} | B_P(c, r) \cap B_P(c', r) = \emptyset \text{ for } c, c' \in C \text{ and } c \neq c' \},
\]

where \( B_P(c, r) = \{ x \in \mathbb{F}_q^n | d_P(x, c) \leq r \} \) is the usual closed metric ball.

**Proposition 15** Under the same conditions of Proposition 13,

\[
R := R_P(C) = s_{t_1-1} + \left\lfloor \frac{\delta_{t_1} - 1}{2} \right\rfloor
\]

where \( \lfloor x \rfloor \) is as usual the integer part of \( x \).
Proof: Since $C$ is a linear code, it is enough to prove that $B_P(0, R) \cap B_P(c, R) = \emptyset$ for every $c \in C$ and that $B_P(0, R + 1) \cap B_P(c, R + 1) \neq \emptyset$ for some $c \in C$.

We consider $C$ to be in the canonical-systematic form given in Theorem 10 and recall that $t_1 = \min \Lambda(C)$. Let $c \in C$ and suppose there is $x \in B_P(0, R) \cap B_P(c, R)$. We claim that $M(x) \subset H_{t_1}$. Indeed, if $M(x) \subset H_j$ with $j < t_1$ we would have

$$d_P(x, c) = \omega_P(c) \geq \delta_P = s_{t_1-1} + \delta_{t_1} > s_{t_1-1} + \left\lfloor \frac{\delta_{t_1} - 1}{2} \right\rfloor.$$ 

On the other hand, if we had $j > t_1$ we would have

$$d_P(x, 0) = \omega_P(x) \geq s_{j-1} + 1 > s_{t_1} > s_{t_1-1} + \left\lfloor \frac{\delta_{t_1} - 1}{2} \right\rfloor.$$ 

So that $j = t_1$. It follows that

$$\omega_P(x-c) = s_{t_1-1} + |M(x-c)| \leq s_{t_1-1} + \left\lfloor \frac{\delta_{t_1} - 1}{2} \right\rfloor,$$ 

hence

$$|M(x-c)| \leq \left\lfloor \frac{\delta_{t_1} - 1}{2} \right\rfloor < \frac{\delta_{t_1}}{2}.$$ 

But this implies that

$$|M(x) \cap M(c)| \geq \frac{\delta_{t_1}}{2} > \left\lfloor \frac{\delta_{t_1} - 1}{2} \right\rfloor$$ 

so that

$$\omega_P(x) = s_{t_1-1} + |M(x)| > s_{t_1-1} + \left\lfloor \frac{\delta_{t_1} - 1}{2} \right\rfloor = R$$ 

contradicting the assumption that $x \in B_P(0, R)$.

Now we need to prove that $B_P(0, R + 1) \cap B_P(c, R + 1) \neq \emptyset$ for some $c \in C$. Let $c \in C$ be a world of minimal length $s_{t_1-1} + \left\lfloor \frac{\delta_{t_1} - 1}{2} \right\rfloor$. Assuming the canonical-systematic form of Theorem 10 we can write

$$c = \sum_{i=1}^{n_{t_1}} c_i e_{s_{j-1}+i}$$ 

15
where \( \{e_1, e_2, ..., e_n\} \) is the usual base of \( \mathbb{F}_q^n \) with \( \text{supp}\left\{e_{s_{j-1}+1}, e_{s_{j-1}+2}, \cdots, e_{s_j}\right\} = H_j \). Defining \( A = \{i = 1, \cdots, n_t | c_i \neq 0\} \) we have that \( |A| = \delta_{t_1} \). Let \( B \subset A \) be a subset such that \( |B| = \left\lfloor \delta_{t_1} - \frac{1}{2} \right\rfloor + 1 \). Then, defining
\[
x = \sum_{i \in B} c_i e_{s_{j-1}+i}
\]
we find that
\[
d_P(x, 0) = s_{t_1-1} + \left\lfloor \frac{\delta_{t_1} - 1}{2} \right\rfloor + 1
\]
and
\[
d_P(x, 0) = s_{t_1-1} + |\{i \in A | i \notin B\}|
\]
and \( |\{i \in A | i \notin B\}| \) is either \( \left\lfloor \frac{\delta_{t_1} - 1}{2} \right\rfloor \) or \( \left\lfloor \frac{\delta_{t_1} - 1}{2} \right\rfloor + 1 \) depending on the parity of \( \delta_{t_1} \). In either case, we have that \( x \in B_P (0, R+1) \cap B_P (c, R+1) \).

\( \square \)

### 4.1 Syndrome Decoding

Considering the canonical-systematic form of Theorem 10, with
\[
\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2 \oplus \cdots \oplus \mathcal{C}_h,
\]
it is quite simple to realize how to perform syndrome decoding for a hierarchical poset. Given \( y \in \mathbb{F}_q^n \) let us consider the decomposition \( y = y_1 + y_2 + \cdots + y_h \) where \( \text{supp}(y_i) \subset H_i \), the \( i \)-level of the poset. Then we just perform usual syndrome decoding of each \( y_i \) relatively to the \( i \)-th component \( C_i \). We remark that whenever \( i \notin \Lambda \), then the usual syndrome decoding is just neglecting \( y_i \), that is, substituting \( y_i \) by the null vector. Hence, if we denote
\[
y_{\Lambda} = \sum_{i \in \Lambda} y_i \quad \text{and} \quad y_{\Lambda^\perp} = \sum_{i \notin \Lambda} y_i,
\]
when receiving a word \( y \) we neglect the component \( y_{\Lambda^\perp} \) and substitute \( y \) by \( y_{\Lambda} \) and then perform the non-trivial syndrome decoding of each \( y_i \) relative to \( C_i \), for \( i \in \Lambda \).

**Remark 16** Syndrome decoding complexity is determined mainly by the search of coset-leaders and given an \([n, k]_q\) code, the number of coset-leaders is \( q^{n-k} \). Given a hierarchical poset with height \( h \) and considering the code to be an hierarchical poset-code in its canonical-systematic form, we have that for each \( i \in [h] \setminus \Lambda \) decoding is just erasing up to \( n_i \) coordinates and for each \( i \in \Lambda \) we are actually making a
syndrome decoding of a \([n_i, k_i]_q\) code, having hence to perform \(n_i \times k_i\) operations for computing the syndrome and then perform a search among \(q^{n_i-k_i}\) coset-leaders. All together we have

\[
\sum_{i \in [h] \setminus \Lambda} n_i + \sum_{i \in \Lambda} \left( n_i \times k_i + q^{n_i-k_i} \right)
\]

operations. Considering a minimal hierarchical poset\(^1\), which induces the Hamming metric on \(\mathbb{F}_q^n\), we have \(h = 1\) so that \(\Lambda = \{1\}\), \(n_i = n\) and \(k_i = k\) so that the complexity of syndrome decoding is \(n \times k + q^{n-k}\), as it is well known. On the other hand, when considering a maximal poset we have that \(h = n\), \(|\Lambda| = k\), \([h] \setminus \Lambda| = n-k\) and \(k_i = n_i = 1\) for every \(i \in \Lambda\), hence we have a minimal complexity \(n - k\) as found in \([2]\). In the between cases, we have an algorithm with exponential gain when compared to the usual syndrome decoding of Hamming codes and exponential loss when compared to a NRT poset code.

Acknowledgment Significant part of this work was developed during the summer of 2011, when one of the authors (M. Firer) was at the Centre Interfacultaire Bernoulli at EPFL, Lausanne, Switzerland, supported by the Swiss National Science Foundation, to which he deeply thanks.

References


\(^1\)The set of hierarchical posets (considered with a natural labeling) is by itself a partially ordered set, having the trivial poset \((i \preceq j \text{ iff } i = j)\) as the minimal element and a NRT poset \((1 \preceq 2 \preceq \cdots \preceq n)\) as a maximal element.


