Projective Systems and Extremal Non-Chain Codes

Hans Georg Schaathun

12th August 1999

Abstract

The weight hierarchy of a linear $[n,k;q]$ code $\mathcal{C}$ over $\mathsf{GF}(q)$ is the sequence $(d_1, d_2, \ldots, d_k)$ where d_r is the smallest support size of any r-dimensional subcode of $\mathcal{C}$. Codes may be classified according to whether there is a $[r, d_r]$ subcode $\mathcal{D}_1$ and an $[s, d_s]$ subcode $\mathcal{D}_2$, such that $\mathcal{D}_1 \subset \mathcal{D}_2$. The extreme cases are chained codes and extremal non-chain codes.

Projective systems are sets of projective points allowing repetitions, and these systems may be used to represent linear codes. Using this language we provide upper bounds on weight hierarchies of extremal non-chain codes.

Keywords

Weight hierarchy, chain condition, difference sequence, linear codes, value assignment

1 Introduction

1.1 Notations and definitions

Throughout this paper $\mathcal{C}$ will denote an $[n, k+1; q]$ code, i.e. a linear code of length n and dimension $k+1$ over the Galois field, $\mathsf{GF}(q)$, with q elements. Codes of dimension $k+1$ will be studied in a projective space, $\mathsf{PG}(k,q)$, of dimension k and order q.

For any code $\mathcal{C}$ we define the support size, $w_S(\mathcal{C})$, to be number of coordinate positions where some code word is non-zero. For $0 \leq r \leq k+1$ *the r-th generalised Hamming weight* of $\mathcal{C}$ is defined by:

$$d_r(\mathcal{C}) \stackrel{\text{def}}{=} \min\{w_S(\mathcal{D}) \mid \mathcal{D} \text{ is an } [n, r; q] \text{ subcode of } \mathcal{C}\}.$$

The sequence $(d_1, d_2, \ldots d_{k+1})$ is called the weight hierarchy of $\mathcal{C}$. We note that the minimum weight of the code is $d = d_1$. For completeness $d_0 = 0$.

We note that by adding a zero-position to $\mathcal{C}$, we get an $[n+1, k+1; q]$ code

$$\mathcal{C}' = \{(\mathbf{c}|0) \mid \mathbf{c} \in \mathcal{C}\},$$

which has the same weight hierarchy as $\mathcal{C}$. Therefore, without loss of generality, we can restrict our study to codes with no zero-position; that is, we assume that $d_{k+1} = n$. Such codes are called *nondegenerate*.

A projective system X in $\mathsf{PG}(k,q)$ is a set of points from $\mathsf{PG}(k,q)$, allowing repetitions. It is nondegenerate if it is not contained in a proper subspace of $\mathsf{PG}(k,q)$. We say that two projective systems are equivalent if one can be obtained from the other by a change of coordinates. Taking the points of X to be the columns, we get a generator matrix for a code. This correspondence is one-to-one between equivalence classes of nondegenerate codes and equivalence classes of nondegenerate projective systems, as proved in [TV95].

The weight hierarchy of a projective system X is defined to be the sequence $(d_1, \ldots d_{k+1})$, where

$$d_i = n - \max\{\#(X \cap \Pi) \mid \Pi \subseteq \mathsf{PG}(k,q), \dim \Pi = i\},$$

where n is the number of elements of X.

A projective subsystem of X is the intersection $\Pi \cap X$ where Π is a subspace of $\mathsf{PG}(k,q)$. It was also proved [TV95, HKY92] that a subsystem of codimension r corresponds to a subcode of dimension r. From this it follows that the correspondence between projective systems and linear codes preserves the weight hierarchy.

In this paper we describe a projective system, X, by giving the number of occurences of each projective point. This is a map

$$\nu : \mathsf{PG}(k,q) \longrightarrow \mathbb{N}_0 \stackrel{\text{def}}{=} \{0, 1, \ldots\},$$

which we call the *value assignment*. The *value* of a point $\mathbf{x}$ is the number $\nu(x)$. Value assignments have been treated in [CK97a] and [Sch99], and the correspondence between codes and value assignments was also showed without using the concept of projective systems.

We extend the definition of values to subsets of $\mathsf{PG}(k,q)$ to be

$$\nu(U) = \sum_{\mathbf{x} \in U} \nu(\mathbf{x}), \forall U \subseteq \mathsf{PG}(k,q).$$

The weight hierarchy of a value assignment is the weight hierarchy of the corresponding projective system.

The difference sequence (DS) of a code, value assignment or projective system is the sequence $(\delta_0, \delta_1, \ldots \delta_k)$, defined by

$$\delta_j \stackrel{\text{def}}{=} d_{k+1-j} - d_{k-j}, \quad j = 0, 1, \ldots k.$$

We note that the difference sequence is easily computed from the weight hierarchy and vice versa. We say that the difference sequence, $(\delta_0, \delta_1, \ldots \delta_k)$, has dimension $k+1$. Due to the strict monotonicity of the generalised Hamming weights, the elements of the difference sequence are positive.

1.2 Object

We will now study upper bounds on the difference sequence of value assignments, knowing that they are equivalent to upper bounds on the weight hierarcy of linear codes. In fact the existence of a code with weight hierarchy $(d_1, d_2, \ldots, d_{k+1})$ is equivalent to the existence of a value assignment ν, such that:

$$\max\{\nu(\Pi_m) \mid \Pi_m \in \mathsf{PG}^{(m)}(k,q)\} = \sum_{i=0}^{m} \delta_i, \quad m = 0, 1, \ldots k. \tag{1}$$

The set of m-spaces of maximum value is denoted by M_m:

$$M_m \stackrel{\text{def}}{=} \left\{ \Pi_m \mid \Pi_m \in \mathsf{PG}^{(m)}(k,q) \ \wedge \ \nu(\Pi_m) = \sum_{i=0}^{m} \delta_i \right\}.$$

The *chain condition* was introduced by Wei and Yang [WY93]. Using the language of value assignment, we define it as follows:

$$\forall i = 0, 1, \ldots k-1, \ \exists \ \alpha_i \in M_i, \quad \text{s.t. } \alpha_0 \subset \alpha_1 \subset \ldots \subset \alpha_{k-1}.$$

A code satisfying this condition is called a *chained code*.

We define a number of subconditions, which all are implications of the chain condition. For any i and j such that $1 \leq i \leq j \leq k-1$, we have the condition:

$$(\mathrm{C}i.j) : \exists \alpha \in M_{i-1}, \beta \in M_j, \quad \text{s.t. } \alpha \subset \beta.$$

The negations of these conditions, $(\mathrm{N}i.j) \stackrel{\text{def}}{=} \neg(\mathrm{C}i.j)$, will be called the *non-chain conditions*. The chain condition will be denoted by (C0). *Extremal non-chain codes* are codes satisfying all of the non-chain conditions. The difference sequence of an extremal non-chain code will be called an ENDS (*extremal non-chain difference sequence*).

Linear codes can be classified according to which of the conditions they satisfy. For chained codes we know a lot about possible weight hierarchies [EK94, CK98b]. Chen and Kløve [CK97a, CK98a, CK97b, CK99] have started the determination of possible weight hierarchies for the other classes in dimension four.

In this paper we look at extremal non-chain codes, to provide upper bounds on the difference sequence in arbitrary dimension. It has been proved that these are the best possible bounds in dimension 4 and 5.

2 Upper bounds

2.1 The main theorem

The main result of this work is the following theorem.

Theorem 1
If $(\delta_0, \delta_1, \ldots \delta_k)$ is an ENDS, $1 \leq m \leq k-1$, then

$$\delta_m \leq q^m \delta_0 - \sum_{i=0}^{m} q^i. \tag{2}$$

Definition 1
We say that an ENDS is m-optimal, *$1 \leq m \leq k-1$, if it satisfies the bound on δ_m from Theorem 1 with equality. An extremal non-chain code, $\mathcal{C}$, is* m-optimal *if its difference sequence is an m-optimal ENDS.*

Definition 2
Given a k-dimensional code, $\mathcal{C}$, we call the code defined by some $\Pi_{k-1} \in M_{k-1}$, a derived code, *$\mathcal{C}_{(1)}$, of $\mathcal{C}$. We form* a derived series of codes, *$\{\mathcal{C}_{(0)}, \mathcal{C}_{(1)}, \ldots \mathcal{C}_{(k)}\}$, where $\mathcal{C}_{(0)} \stackrel{\text{def}}{=} \mathcal{C}$, and $\mathcal{C}_{(i)}$ is a derived code of $\mathcal{C}_{(i-1)}$, for $i = 1, \ldots k$.*

It is noted that in general, the derived code and the derived series of codes are not unique. Also the derived codes are not subcodes. Just as it seems to be difficult to find relations between projective systems corresponding to dual codes [TV95], it seems to be difficult to find direct relations between the codes defined by a projective system and some subsystem of it.

To prove Theorem 1 we consider a subcode $\mathcal{D}$, defined by $\Pi \in M_m(\mathcal{C})$. Then we consider a derived series $\{\mathcal{D}_{(0)}, \dots \mathcal{D}_{(m)}\}$ of $\mathcal{D}$. Let $(\varepsilon_0^{(i)}, \varepsilon_1^{(i)}, \dots \varepsilon_{m-i}^{(i)})$ be the difference sequence of $\mathcal{D}_{(i)}$.

Quite clearly $\mathcal{D}_{(m)}$ is a one-dimensional code, whose non-zero words has weight $\varepsilon_0^{(m)} < \delta_0$. The following lemmas make it possible to bound $\varepsilon_i^{(m-i)}$ for each i.

Lemma 1
For any code with difference sequence, $(\delta_0, \delta_1, \dots \delta_k)$, we have $\delta_k \leq q\delta_{k-1}$.

Lemma 2
If $(\delta_0, \delta_1, \dots \delta_k)$ is the difference sequence of a code $\mathcal{D}$, and $(\delta_0^{(1)}, \dots \delta_{k-1}^{(1)})$ is the difference sequence of a derived code, $\mathcal{D}_{(1)}$, then $\delta_{k-1} \leq \delta_{k-1}^{(1)}$.

We assume that if the code meets the bound on δ_m, then it meets it with equality. Combining the above lemmas m times and applying the inductive hypothesis, we get that $\varepsilon_0^{(m)} \geq \lceil q^{-m}\varepsilon_m \rceil \geq \delta_0 - 1$. Hence $\varepsilon_0^{(m)} = \delta_0 - 1$.

This allows for another induction, where the inductive hypothesis is that $\varepsilon_j^{(m-j)} = q^j\delta_0 - (q^{j+1} - 1)/(q - 1)$, for any $j < i$. This induction carries out to prove that $\varepsilon_{m-1}^{(1)} = q^{m-1}\delta_0 - (q^m - 1)/(q - 1)$, and using the two lemmas again gives $\varepsilon_m^{(0)} \leq q^m\delta_0 - (q^{m+1} - 1)/(q - 1) + 1$. The following result finishes the proof.

Lemma 3
If $\mathcal{C}$ and $\mathcal{D}$ are defined as above, with the given difference sequences, then $\delta_m \leq \varepsilon_m - 1$.

The following theorem is another consequence of the proof of Theorem 1.

Theorem 2
Let $\mathcal{C}$ be an m-optimal for some m, such that $2 \leq m \leq k - 1$. Then $\mathcal{C}$ is also $(m-1)$-optimal, and the subcode $\mathcal{D}$ defined by $\Pi_m \in M_m$, is a chained code with difference sequence $(\delta_0 - 1, \delta_1, \delta_2, \dots, \delta_{k-1}, \delta_k + 1)$.

The following theorem has been a most useful tool to construct m-optimal, extremal non-chain codes.

Theorem 3
Let $\mathcal{C}$ be an m-optimal extremal non-chain code, and $\mathcal{D}$ the code defined by $\nu \mid_\Pi$ for some $\Pi \in M_m(\mathcal{C})$. Then there exists a collection S, of exactly one i-space in Π_m, for each $i = 1, \dots m$, such that $\nu(p) = \delta_0 - \#\{\Psi \in S \mid p \in \Psi\}$, for any $p \in \Pi$.

Corollary 1
If $(\delta_0, \delta_1, \dots \delta_k)$ is an ENDS where $k \geq 4$, then $\delta_0 \geq 3$.

2.2 Upper bounds on the total value

Theorem 4
If $(\delta_0, \delta_1, \ldots \delta_k)$*,* $k \geq 2$*, satisfies* $(\mathrm{N}m.m)$*, then*

$$\nu(\mathsf{PG}(k,q)) \leq \sum_{i=0}^{m-1} \delta_i + (\delta_m - 1) \sum_{i=0}^{k-m} q^i, \quad \forall 1 \leq m \leq k-1.$$

For an ENDS, several bounds may be derived from the above theorem. The bound in the following corollary is the best possible for $(k-1)$-optimal codes.

Corollary 2
For any $(\delta_0, \delta_1, \ldots \delta_k)$*,* $k \geq 2$*, if* $(\mathrm{N}1.1)$ *is satisfied, then*

$$\nu(\mathsf{PG}(k,q)) \leq \delta_0 + (\delta_1 - 1) \sum_{i=0}^{k-1} q^i \leq \left(\sum_{i=0}^{k} q^i \right) \delta_0 - (q+2) \sum_{i=0}^{k-1} q^i.$$

Theorem 5
There exists a non-binary, extremal non-chain code, which is $(k-1)$*-optimal and meets the bound of Corollary 2 with equality.*

By using the restrictions from Theorem 3, optimal five-dimensional codes can be found by trial and error in a few minutes, using a computer.

3 Binary codes

Theorem 6
If $(\delta_0, \delta_1, \ldots \delta_k)$*,* $k \geq 3$*, is a binary ENDS, then*

$$\delta_{k-1} \leq 2^{k-2}\delta_1 - 2 - 2^{k-2}.$$

This obviously implies that no binary, extremal non-chain code can be $(k-1)$-optimal. It also implies that Corollary 2 is no longer the best possible bound on δ_k. The following theorem is a better bound which is also a corollary of Theorem 4.

Theorem 7
If $(\delta_0, \delta_1, \ldots \delta_k)$*,* $k \geq 2$*, is a binary ENDS, then*

$$\delta_k \leq 2\delta_{k-1} - 3.$$

Theorem 8
There exists a five-dimensional binary, extremal non-chain code, which is $(k-2)$*-optimal and meets the bounds from Theorems 6 and 7 with equality.*

References

[CK97a] Wende Chen and Torleiv Kløve. Bounds on the weight hierarchies of extremal non-chain codes of dimension 4. *Applicable Algebra in Engineering, Communication and Computing*, 8:379–386, 1997.

[CK97b] Wende Chen and Torleiv Kløve. Bounds on the weight hierarchies of linear codes of dimension 4. *IEEE Trans. Inform. Theory*, 43:2047–2054, 1997.

[CK98a] Wende Chen and Torleiv Kløve. Classification of the weight hierarchies of binary linear codes of dimension 4. Technical Report 147, Department of Informatics, University of Bergen, March 1998.

[CK98b] Wende Chen and Torleiv Kløve. Weight hierarchies of linear codes satisfying the chain condition. *Designs, Codes and Cryptography*, 11, 1998.

[CK99] Wende Chen and Torleiv Kløve. Weight hierarchies of extremal non-chain binary codes of dimension 4. *IEEE Trans. Inform. Theory*, 45:276–289, 1999.

[EK94] Sylvia Encheva and Torleiv Kløve. Codes satisfying the chain condition. *IEEE Trans. Inform. Theory*, 40:175–180, 1994.

[HKY92] Tor Helleseth, Torleiv Kløve, and Øyvind Ytrehus. Generalized Hamming weights of linear codes. *IEEE Trans. Inform. Theory*, 38:1133–1140, 1992.

[Sch99] Hans Georg Schaathun. Upper bounds on weight hierarchies of extremal non-chain codes. Technical Report 171, Department of Informatics, University of Bergen, 1999. Also available at http://www.ii.uib.no/~georg/sci/inf/coding/public/.

[TV95] Michael A. Tsfasman and Serge G. Vlăduţ. Geometric approach to higher weights. *IEEE Trans. Inform. Theory*, 41(6, part 1):1564–1588, 1995. Special issue on algebraic geometry codes.

[WY93] Victor K. Wei and Kyeongcheol Yang. On the generalized Hamming weights of product codes. *IEEE Trans. Inform. Theory*, 39(5):1709–1713, 1993.