Support Weights in Linear Codes and Projective Multisets

Hans Georg Schaathun

Dissertation submitted in partial fullfillment of the requirements for the degree of Doctor Scientiarum.

Universitas Bergensis

Department of Informatics

DECEMBER 27TH 2001

To
the memory of
friends
who are no longer with
us.

Support Weights in Linear Codes and Projective Multisets

Hans Georg Schaathun
Institutt for Informatikk
Universitas Bergensis
Høyteknologisenteret
N-5020 Bergen, Norway
georg@ii.uib.no

December 27th 2001

Abstract

A linear code is a normed vector space, using the Hamming norm, where the norm of a codeword usually is called *the weight*. Weights of codewords is essential for the code's performance in many applications, and the minimum weight d and the weight enumerator A_i are well-known parameters.

In recent years, we have seen the weight concept being generalised to support weights of subcodes, and a number of new parameters have been introduced. In this thesis we will look at some of these parameters, namely the weight hierarchy, the support weight distribution, and the greedy weights, for certain classes of codes.

Projective multisets form an equivalent language describing linear codes, proving particularly useful for studying weight structure. Basically we take the columns of some generator matrix, counting multiplicities. All our results are described in this language.

Keywords

weight hierarchy, support weight distribution, greedy weights, projective multiset, product codes, dual code, chain condition

Støttevekter i lineære kodar og projektive multimengder

Samandrag

Ein lineær kode er eit normert vektorrom med hammingnormen. Normen til eit kodeord vert òg kalla *vekta* til kodeordet, og desse vektene er uvurderlege for å avgjera yteevna til koden. Minstevekta d og vektenumeratoren A_i er dei mest kjende måla.

Dei siste åra har me sett at vektomgrepet er utvida. Me kan tala om vekta til ein vilkårleg underkode, og slik har me fått ein rekkje nye og interessante parametrar. I avhandlingan skal me drøfta dei viktigaste av desse parametrane, nemleg vekthierarkiet (Wei 1991), støttevektfordelinga (Helleseth et al. 1977) og grådigvektene (Cohen et al. 1998).

Projektive multimengder dannar eit likeverdig språk for å skildra lineære kodar, og det har vist seg svært nyttig i arbeidet med høgare vektar og vert nytta gjennom heile avhandlinga. I utgangspunktet tek me søylene frå ein generatormatrise for å danna multimengda som svarer til ein gjeven kode. I ei multimengd kan eit og same element vera medlem fleire gonger.

Nykkelord

vekthierarki, støttevektfordeling, grådigvekter, projektive multimengder, produktkodar, duale kodar, kjedeføresetnaden

Acknowledgements

Many are the persons who deserve great thanks for their help and encouragement to my writing this thesis.

Firstly, I am grateful to my supervisor, prof. Torleiv Kløve. He proposed a great problem for my graduate thesis and gave me the leeway to wander where I wanted. He has read my drafts and given advice and encouragement whenever I asked. And he has proposed several problems which I have been allowed to give up on…

I am pleased to have had a second supervisor, prof. Trygve Johnsen, to guide me to algebraic geometry codes. I am grateful for all the interest he has taken in my work, and the help in understanding some algebraic and geometric concepts on which I have based my work.

It has been of great value be with such an active research group as ours. Some of my results could only be obtained because the group had the funding to send me to international conferences. The many discussions I have had with other people in the group have been a great source of inspiration. I have enjoyed many interesting talks with dr. Matthew Parker, and am very sorry that I never found the time to explore the connections between his field and the topics of the thesis.

I want to direct a special thanks to prof. Tor Helleseth, who takes such an enthusiastic interest in so many fields. I have discussed more topics with him than with any other person in the group, and like my supervisor, he has suggested me plenty of problems which I have not been equal to.

Dr. Wolfgang Willems from Magdeburg has coauthored one of the articles underlying my thesis, and I have learnt a lot from working with him. During the research on support weight distribution, I have found great help in corresponding with prof. Aaron Gulliver in Victoria.

A particularly interesting and valuable year of my studies was the eight-month research stay at Ecole Nationale Supérieure des Télécommunications in Paris. I want to express my warm thanks to prof. Gérard Cohen for inviting me, and to the Norwegian Research Council for funding the visit (project no. 138654/410). During this stay, thanks to prof. Cohen and dr. Sylvia Encheva from Haugesund, I was introduced to the topic of fingerprinting and watermarking.

My final thanks is to my family, who has always been there for me. I am ever grateful for their backing up almost anything I wanted, and also for discussing maths, at every level from before school and all the way to where I am.

Bergen, December 27th 2001
Hans Georg Schaathun

Contents

Acknowledgements **5**

Table of Contents **7**

1 Introduction **11**
1.1 Higher weights 11
1.2 Projective Multisets 12
1.3 Overview 13

2 Preliminaries **15**
2.1 Vectors, Codes, and Multisets 15
2.2 Weights 18
2.3 Projective geometry 20
2.4 Sub-multisets and Projection 20
2.5 Classes of Non-Chain Codes 22

3 Upper bounds on ENDS **23**
3.1 The main bound on ENDS 23
3.2 Structure of optimal codes 27
3.3 Upper bounds on the total value 37
3.4 Closing remarks 39

4 Optimal, 5-dimensional ENDS **41**
4.1 The projective multiset 41
4.2 Verifying the non-chain conditions 45

5 Optimal ENDS of dimension 6 **49**
5.1 Design 49
5.2 Analysis 52

6 Binary ENDS **59**
6.1 General bounds . . . 59
6.2 Construction requirements . . . 61
6.3 Lower bound on δ_0 . . . 62

7 Binary Construction **65**
7.1 The assignment . . . 65

8 Duality **71**

9 Sub-chains **73**
9.1 Duality relations . . . 73
9.2 A duality example . . . 75
9.3 Bounds on the Difference Sequences . . . 77

10 Greedy weights **79**
10.1 The Wire-Tap Channel of Type II . . . 79
10.2 Definitions . . . 81
10.3 Basic properties . . . 83
10.4 Duality . . . 85
10.5 Bounds on greedy weights . . . 87

11 Support weight distributions **89**
11.1 Definitions . . . 89
11.2 Previous results and motivation . . . 91
11.3 In the range $m_0 \leq r < m_1$ . . . 92
11.4 In the range $m_1 \leq r < m_2$ . . . 95
11.5 Discussion of future works . . . 101

12 Product codes **103**
12.1 Introduction . . . 103
12.2 The general result . . . 105
12.3 Some special cases . . . 113

13 Greedy weights of product codes **117**
13.1 The result . . . 117
13.2 Redefining the problem . . . 118
13.3 The proof . . . 120

14 Future research **127**
14.1 Product codes . . . 127
14.2 Cyclic codes . . . 128

14.3 Trellis complexity 129
14.4 Sub-chain conditions 129
14.5 Other problems 130

Bibliography **131**

1 Introduction

1.1 Higher weights

A linear code is a normed space and the weights (or norms) of codewords are crucial for the code's performance. In basic text books, we encounter two different parameters describing the weight structure of a code, the minimum weight and the weight enumerator.

The concept of weights can be generalised to subcodes or even arbitrary subsets of the code. This is often called higher weights, and the common name for classic and higher weights is support weights, support sizes, or just 'weights' for short. In recent years, we have seen an increased interest in higher weights. One of the key papers is [Wei91], where Wei defined the rth generalised Hamming weight to be the least weight of a r-dimensional subcode. After Wei's work, we have seen many attempts to determine the generalised Hamming weights for different classes of codes.

Weights are alpha and omega for codes. Yet we know very little about the weight structure of most useful codes. The generalised Hamming weights give some information, and several practical applications are known. Still they do not fully answer all our questions.

One practical application of the generalised Hamming weights is to determine the trellis complexity of the code. Fujiwara et al. [FKLT93] first found this relation. Forney [For94b] discussed the relation in more detail and introduced the ordered and the inverse ordered dimension/length profiles to determine the trellis complexity. It was evident that the generalised Hamming weights could only give lower bounds on this complexity in the general case. Recently, Chen and Coffey [CC01] used Forney's results to find optimal bit orderings of some self-dual codes.

Several other parameters describing weights of subcodes have been introduced, and they can perhaps contribute to understanding the structure of linear codes. The support weight distribution appeared as early as 1977 by [HKM77]. They found that the weight enumerator of certain infinite classes of irreducible cyclic codes could be computed from the support weight distribution of one code.

Other interesting parameters are related to chaining of subcodes with minimum weights. Codes satisfying the chain condition [WY93] appear to behave more nicely, at least with respect to weight hierarchies of product codes. The double chain condition from [For94a] was introduced in the research of trellis complexity. Chen and

Kløve have introduced certain sub-chain conditions, which they use to classify codes in a series of papers, e.g. [CK97a, CK96, CK99b]. Cohen, Encheva, and Zémor [CEZ99] have introduced a new set of parameters, which we will call CEZ weights, and they used them to prove that almost all codes violate the chain condition. Inspired by the CEZ weights, Chen and Kløve [CK01a, CK99a] have introduced the greedy weights.

1.2 Projective Multisets

We will Consider a linear $[n,k]$ code C. We usually define a linear code by giving the generator matrix G. The rows of G make a basis for C, and as such they are much studied. Many works consider the columns instead. This gives rise to the *projective multisets* [DS98]. The weight hierarchy is easily recognised in this representation [HKY92, TV95]. Other terms for projective multisets include projective systems [TV95] and value assignments [CK97a].

The relationship between projective multisets and linear codes was known as early as 1956, by Slepian [Sle56] using the term 'modular representation'. In the special case of projective codes, i.e. where no column of G is proportional to another column, the projective multiset becomes a regular set. Familiar configurations in combinatorial geometry turn out to correspond to certain special classes of codes. For instance, MDS codes correspond to arcs in the projective space. There are numerous papers on this and similar relations. A recent example is new, optimal binary and ternary codes found through caps in $\mathsf{PG}(8,2)$ and $\mathsf{PG}(8,3)$ [CS01].

The great advantage of projective multisets is that they do not depend on the coordinate system. Codes, on the other hand, depends heavily on the coordinate system, as the coordinates determine the weights. Therefore the projective multiset approach has proved very useful in the study of generalised Hamming weights. Problems which appear as hard in terms of linear codes may be easy in terms of projective multisets, e.g. determining the weight hierarchy of product codes [Sch00].

There are at least two ways to develope the correspondence between codes and multisets. Most coding theorists will probably just take the columns of some generator matrix (e.g. [HKY92, CK97a]). Some mathematicians (e.g. [DS98, TV95]) develope the projective multisets abstractly. They take the elements to be the coordinate forms on C

$$(c_1, c_2, \ldots, c_n) \mapsto c_i, \quad 1 \le i \le n,$$

and get a multiset on the dual space of C (this is *not* the dual code). Hence their argument does not depend on the (non-unique) generator matrix of C.

We will thoroughly attempt to develope both descriptions of the relation, and explain the connections between them.

1.3 Overview

This thesis is roughly composed of three projects: extremal non-chain codes, duality, and product codes, and it includes three published and three submitted papers, as well as five conference talks. Terminology and notation have changed between the published papers, following different practices from the literature. In the thesis, I attempt to make one unified and consistent discourse, causing virtually every part of the thesis to differ more or less from previous texts.

The first project, on extremal non-chain codes in Chapters 3 through 7, fits into a series of papers by my supervisor Torleiv Kløve and his coauthor Wende Chen [CK97a, CK96, CK99b], where they classify possible weight hierarchies in dimension 4 with respect to the subchain conditions. Extremal non-chain codes is one of the extreme classes in this classification, and we will discover general bounds on their weight hierarchies in arbitrary dimension. Moreover, we present optimal constructions for any characteristic in dimension 5, and odd characteristic in dimension 6.

The main results on extremal non-chain codes was presented at ISIT 2000 and have been published as full papers:

1. 'Upper bounds on weight hierarchies of extremal non-chain codes', [Sch01c], *Discrete Mathematics*, vol. 241 pp. 449–469 (Tverberg Anniversary volume) 2001.

2. ISIT 2000 in Sorrento, Italy: 'Projective Systems and Higher Weights', *Proc. IEEE Intern. Symp. Inform. Theory*, 2001 p. 255.

The six-dimensional construction in Chapter 5 is new and has never been published.

The second project, on duality, is concerned with a relation between a linear code and the projective multiset corresponding to its dual. From this starting point, three problems are attacked. Chapter 9, about subchain conditions and duality, has not been published. The results on greedy weights in Chapter 10 was presented at AAECC-14 in Melbourne, Australia 2001 and published as a full article in the proceedings. The third work, Chapter 11 on support weight distributions, has been submitted.

3. 'Duality and greedy weights for linear codes and projective multisets' [Sch01a], *Proceedings of AAECC-14*, Springer Lecture Notes in Computer Science vol. 2227 pp. 92–101, Springer-Verlag 2001.

4. 'Duality and support weight distributions'. Submitted to *IEEE Trans. Inform. Theory* 2001.

The third project is based on the relation between product codes and the Segre embedding of two projective multisets. The first result was a proof of the Wei-Yang conjecture [WY93], which was published in

5. ‘The weight hierarchy of product code’ [Sch00], *IEEE Trans. Inform. Theory* volume 46, Nov. 2001, pp. 2648–2651.

A second proof of this conjecture was found a little later by Conchita Martínez-Pérez and Wolfgang Willems, inspiring a joint project generalising the previous results. This work has lead to one paper and two conference talks:

6. with Conchita Martínez-Pérez and Wolfgang Willems: ‘On the weight hierarchies of product codes. The Wei-Yang Conjecture and more’. In Daniel Augot, editor, *Workshop on Coding and Cryptography*, January 2001, pp. 373–379. (Survey.)

7. with Wolfgang Willems: ‘A lower bound for the weight hierarchy of product codes and projective multisets’, *Proc. IEEE Intern. Symp. Inform. Theory*, 2001, p. 59, Washington DC, US. (Talk by Wolfgang Willems.)

8. with Wolfgang Willems: ‘A lower bound for the weight hierarchies of product codes’, Submitted to Discrete Applied Mathematics 2001 for a special issue for WCC 2001.

The original proof of the Wei-Yang Conjecture (from item no. 5) is omitted from the thesis. Instead we include the more general proof introduced in item no. 8. Chapter 12 thus comprise the preliminaries from item no. 5, the proof and improvements of the Wei-Yang Conjecture from item no. 8, and some special cases from item no. 5.

The last work under this third project (Chapter 13) concerns the greedy weights of product codes, presented at ISIT 2001 and submitted for publication:

9. ‘A lower bound on the greedy weights of product codes’, *Proc. IEEE Intern. Symp. Inform. Theory*, 2001 p. 120, Washington DC, US.

10. ‘A lower bound for the greedy weights of product codes’. Submitted to *Designs, Codes, and Cryptography*, 2001.

2 Preliminaries

This entire thesis will concern linear block codes. Whenever we talk about codes, we will always mean linear block codes. Basically, an $[n, k]$ code C is a k-dimensional subspace of some n-dimensional vector space V.

2.1 Vectors, Codes, and Multisets

A multiset is a collection of elements which are not necessarily distinct. More formally, we define a multiset γ on a set S as a map

$$\gamma : S \to \{0, 1, 2, \ldots\}.$$

The number $\gamma(s)$ is the number of occurrences of s in the collection γ. The map γ is always extended to the power set of S,

$$\gamma(S') = \sum_{s \in S'} \gamma(s), \quad \forall S' \subseteq S.$$

The number $\gamma(s)$, where $s \in S$ or $s \subseteq S$, is called the value of s. The size of γ is the value $\gamma(S)$. We will be concerned with multisets of vectors and multisets of projective points (projective multisets). We will always keep the informal view of γ as a collection in mind.

We consider a fixed finite field $\mathsf{GF}(q)$ with q elements. A message word is a k-tuple over $\mathsf{GF}(q)$, while a codeword is an n-tuple over $\mathsf{GF}(q)$. Let M be a vector space of dimension k (the message space), and V a vector space of dimension n (the channel space). The generator matrix G gives a linear, injective transformation $G : \mathsf{M} \to \mathsf{V}$, and the code C is simply the image under G.

As vector spaces, M and C are clearly isomorphic. For every message word $\mathbf{m}$, there is a unique codeword $\mathbf{c} = \mathbf{m}G$.

A codeword $(c_1, c_2, \ldots, c_n) = \mathbf{m}G$ is given by the value c_i in each coordinate position i. If we know $\mathbf{m}$, we obtain this value as the inner product of $\mathbf{m}$ and the ith column $\mathbf{g}_i$ of G, i.e.

$$c_i = \mathbf{g}_i \cdot \mathbf{m} = \sum_{j=1}^{k} m_j g_{i,j}, \tag{2.1}$$

where

$$\mathbf{g}_i = (g_{i,1}, g_{i,2}, \ldots, g_{i,k}),$$
$$\mathbf{m} = (m_1, m_2, \ldots, m_k).$$

The columns $\mathbf{g}_i$ are elements of M. These vectors are not necessarily distinct, so they make a multiset

$$\overline{\gamma}_C : \mathsf{M} \to \{0, 1, 2, \ldots\}.$$

Two codes are said to be permutation equivalent if one is obtained from the other by reordering the columns of the generator matrix. We note that $\overline{\gamma}_C$ defines C up to permutation equivalence.

Example 2.1
Let C be the $[7, 4]$ Hamming code. The message space M has dimension 4, while the channel space V has dimension 7. A generator matrix is

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

The corresponding vector multiset $\overline{\gamma}_C$ contains the vectors

$$(1000), (0100), (0010), (0001), (1101), (1011), (0111).$$

The first symbol of a codeword is determined by the first vector, (1000). For the message (0110), the first encoded symbol is $c_1 = (0110) \cdot (1000) = 0$. In fact, the corresponding codeword is $\mathbf{c} = (0110)G = (0110110)$.

A code C is said to be degenerate if there is an all-zero column in the generator matrix, otherwise it is non-degenerate. It is customary to assume that all codes are non-degenerate, and it is convenient because it allows us to pass from vector multisets to projective multisets. Still, all the results in the thesis are valid for degenerate codes as well.

There is a second type of equivalence for codes, described by replacing columns in the generator matrix by proportional columns. Thus we can consider the vectors of $\overline{\gamma}_C$ as projective points, to obtain a multiset γ_C on the projective space $\mathsf{P}(\mathsf{M})$, and γ_C also defines the code up to equivalence. Since there is no all-zero point in $\mathsf{P}(\mathsf{M})$, we assume that C in non-degenerate. We will alternately consider $\overline{\gamma}_C$ and γ_C, according to what is most convenient for the analysis.

A projective multiset γ on $\mathsf{PG}(k-1, q)$ is said to be degenerate if there is a hyperplane $\Pi \leqq \mathsf{PG}(k-1, q)$ such that $\gamma(\Pi) = \gamma(\mathsf{PG}(k-1, q))$. Otherwise it is non-degenerate. A degenerate projective multiset on $\mathsf{PG}(k-1, q)$ defines a code of dimension strictly less than k. Non-degenerate vector multisets are defined in a similar

way. In the sequel, we assume that all vector multisets and projective multisets are non-degenerate.

We say that two multisets $\overline{\gamma}$ and $\overline{\gamma}'$ on M are equivalent if $\overline{\gamma}' = \overline{\gamma} \circ \phi$ for some automorphism ϕ on M. Such an automorphism is given by $\phi : \mathbf{g} \mapsto \mathbf{g}A$ where A is a square matrix of full rank. Replacing all the $\mathbf{g}_i$ by $\mathbf{g}_i A$ in (2.1) is equivalent to replacing $\mathbf{m}$ by $A\mathbf{m}$. In other words, equivalent multisets give different encoding, but they give the same code. This equivalence concept carries over to the projective multiset γ_C in an obvious way. This is an important observation, because it implies that the coordinate systems on M and $\mathsf{P}(\mathsf{M})$ are not essential.

Now we seek a way to represent the elements of γ_C as vectors of V. Let $\mathbf{b}_i$ be the ith coordinate vector of V, that is the vector with 1 in position i and 0 in all other positions. The set of all coordinate vectors is denoted by

$$\mathcal{B} := \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}.$$

If we know the codeword $\mathbf{c}$ corresponding to $\mathbf{m}$, the ith coordinate position c_i is given as the inner product of $\mathbf{b}_i$ and $\mathbf{c}$.

$$c_i = \mathbf{b}_i \cdot \mathbf{c} = \sum_{j=1}^{n} c_j b_{i,j}, \tag{2.2}$$

where

$$\begin{aligned} \mathbf{b}_i &= (b_{i,1}, b_{i,2}, \ldots, b_{i,k}), \\ \mathbf{c} &= (c_1, c_2, \ldots, c_k). \end{aligned}$$

We note that $\mathbf{b}_i$ takes the role of $\mathbf{g}_i$, and $\mathbf{c}$ takes the role of $\mathbf{m}$ from (2.1).

However, $\mathbf{b}_i$ is not the only vector of V with this property. In fact, for any vector $\mathbf{c}' \in C^\perp$, we have $(\mathbf{b}_i + \mathbf{c}') \cdot \mathbf{c} = c_i$. Therefore, we can consider the vector $\mathbf{b}_i$ as the coset $\mathbf{b}_i + C^\perp$ of $C^\perp$. The set of such cosets is usually denoted $\mathsf{V}/C^\perp$, and it is a vector space of dimension

$$\dim \mathsf{V}/C^\perp = \dim \mathsf{V} - \dim C^\perp = n - (n-k) = k = \dim \mathsf{M}.$$

Hence $\mathsf{M} \cong \mathsf{V}/C^\perp$ as vector spaces. Obviously $\mathbf{b}_i + C^\perp$ corresponds to $\mathbf{g}_i$.

Example 2.1 (cont.)
We still consider the $[7,4]$ *Hamming code* C *and the codeword* $\mathbf{c} = (0110110)$. *The first coordinate is determined as*

$$\begin{aligned} c_1 &= (0110110) \cdot [(1000000) + C^\perp] \\ &= (0110110) \cdot (1000000) + (0110110) \cdot C^\perp = 0 + 0 = 0. \end{aligned}$$

We let μ denote the natural endomorphism,

$$\begin{aligned} \mu &: \mathsf{V} \to \mathsf{V}/C^{\perp}, \\ \mu &: \mathbf{g} \mapsto \mathbf{g} + C^{\perp}. \end{aligned} \tag{2.3}$$

This map is not injective, so if $S \subseteq \mathsf{V}$, it is reasonable to view the image $\mu(S)$ as a multiset. Our analysis gives this lemma.

Lemma 2.1
A code $C \subseteq \mathsf{V}$ is defined up to equivalence by the vector multiset $\gamma_C := \mu(\mathcal{B})$ on $\mathsf{V}/C^{\perp} \cong \mathsf{M}$.

Given a collection $\{s_1, s_2, \ldots, s_m\}$ of vectors and/or subsets of a vector space V, we write $\langle s_1, s_2, \ldots, s_m \rangle$ for its span. In other words $\langle s_1, s_2, \ldots, s_m \rangle$ is the intersection of all subspaces containing $s_1, s_2, \ldots, s_m$.

Also note that we write $A \subset B$ only if A is a proper subset of B. We write $A \subseteq B$ if A is an arbitrary subset of B, possibly equal to B. If U is a subspace of V, then we write $U \leqq V$.

2.2 Weights

We define the support $\chi(\mathbf{c})$ of $\mathbf{c} \in C$ to be the set of coordinate positions not equal to zero, that is

$$\chi(\mathbf{c}) := \{i \mid c_i \neq 0\}, \quad \text{where } \mathbf{c} = (c_1, c_2, \ldots, c_n).$$

The support of a subset $S \subseteq C$ is

$$\chi(S) = \bigcup_{\mathbf{c} \in S} \chi(\mathbf{c}).$$

The weight (or support size) $w(S)$ is the cardinality of $\chi(S)$. Observe that $w(\mathbf{c})$ is exactly the Hamming norm of $\mathbf{c}$. The ith minimum support weight (or generalised Hamming weight) $d_i(C)$ is the smallest weight of an i-dimensional subcode $D_i \subseteq C$. The subcode D_i will be called a minimum i-subcode. The weight hierarchy of C is $(d_1(C), d_2(C), \ldots, d_k(C))$, and was introduced by Wei [Wei91]. In Section 10.1, we will present the motivation for his introducing the weight hierarchy, as an introduction to the greedy weights.

Lemma 2.2 (Helleseth-Kløve-Ytrehus 1992)
There is a one-to-one correspondence between subcodes $D \subseteq C$ of dimension r and subspaces $U \subseteq \mathsf{M}$ of codimension r, such that $\overline{\gamma}_C(U) = n - w(D)$.

Proof: Since C and M are isomorphic, a subcode $D \subseteq C$ corresponds to a subspace $M \subseteq \mathsf{M}$. From (2.1) we can see that $i \in \chi(D)$ if and only if $\mathbf{g}_i$ is not orthogonal on M. Hence we get that

$$\gamma_C(M^\perp) = n - w(D), \tag{2.4}$$

where $M^\perp \subseteq \mathsf{M}$ is the subspace of vectors orthogonal on M. If $\dim D = r$, then $\dim M^\perp = k - r$. The lemma follows with $U = M^\perp$. □

Obviously, U in the lemma corresponds to a projective space $\Pi = \mathsf{P}(U) \leqq \mathsf{P}(\mathsf{M})$ of codimension r, which in turn also correspond to the subcode D.

Definition 2.1
Given a subcode $D \leqq C$, we write $D^* \leqq \mathsf{P}(\mathsf{M})$ for the corresponding projective subspace, and for a subspace $\Pi \leqq \mathsf{P}(\mathsf{M})$, we write $\Pi^* \leqq C$ for the corresponding subcode.

Consider a chain of subcodes

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

The proof of Lemma 2.2 implies that the corresponding subspaces of M form a chain

$$\mathsf{M} = U_0 \supset U_1 \supset U_2 \supset \ldots \supset U_k = \{0\},$$

where U_i corresponds to D_i.

We define $d_{k-1-r}(\gamma_C)$ such that $n - d_{k-1-r}(\gamma_C)$ is the largest value of an r-space $\Pi_r \leqq \mathsf{PG}(k-1, q)$. The following proposition follows directly from Lemma 2.2.

Proposition 2.1
If C is a linear code and γ_C is the corresponding multiset, then $d_i(\gamma_C) = d_i(C)$.

Definition 2.2 (Chain Condition)
We say that a code is chained if there is a chain $0 = D_0 \subseteq D_1 \subseteq \ldots \subseteq D_k = C$, where each D_i is a minimum i-subcode of C.

The chain condition was introduced in [WY93]. Many good codes satisfy the chain condition, such as the Hamming, Reed-Muller, MDS, and the extended Golay codes. Nevertheless, most codes do not satisfy this condition [CEZ99]. In terms of vector systems, the chain of subcodes corresponds to a chain of maximum value subspaces .

The difference sequence $(\delta_0, \delta_1, \ldots, \delta_{k-1})$ is defined by $\delta_i = d_{k-i} - d_{k-1-i}$, and is occasionally more convenient than the weight hierarchy. The maximum value of a projective r-space is

$$\Delta_r := \delta_0 + \delta_1 + \ldots + \delta_r = n - d_{k-1-r}.$$

Clearly, the maximum value of an r-dimensional vector space is Δ_{r-1}.

2.3 Projective geometry

Let $\mathsf{PG}(k-1,q) \cong \mathsf{P}(\mathsf{M})$ be the projective geometry of dimension $k-1$ over $\mathsf{GF}(q)$. The cardinality of $\mathsf{PG}(k-1,q)$ is $\theta(k-1)$, where

$$\theta(m) := \frac{q^{m+1}-1}{q-1} = \sum_{i=0}^{m} q^i.$$

An r-space of $\mathsf{PG}(k-1,q)$ is a subset which is itself a projective geometry of dimension r. We let $\mathsf{PG}^r(k-1,q)$ denote the set of r-spaces. The number of distinct r-spaces is

$$\#\mathsf{PG}^r(k-1,q) = \begin{bmatrix} k \\ r+1 \end{bmatrix} := \prod_{i=0}^{r} \frac{q^{k-i}-1}{q^{r+1-i}-1}.$$

The number of r-spaces containing a given m-space is given by

$$\begin{bmatrix} k-m-1 \\ r-m \end{bmatrix}.$$

Projective 0-, 1-, 2-, and 3-spaces are called points, lines, planes and solids, respectively. The only -1-space is the empty set, and a $(k-2)$-space is called a prime or a hyperplane.

It is a well known fact that the smallest subset of a projective space, intersecting any line in at least one point, is a prime. More generally we know that if $\mathcal{L}$ is a set of points in $\mathsf{PG}(k-1,q)$ such that, for any r-space Π_r, $\#(\mathcal{L} \cap \Pi_r) \geq \theta(s)$, then $\#\mathcal{L} \geq \theta(k-1-r+s)$. Also $\#\mathcal{L} = \theta(k-1-r+s)$ if and only if $\mathcal{L}$ is a $(k-1-r+s)$-space. (See [Hir98] pp. 87-88 for a proof.)

A subset meeting any t-space in at least one point, without containing any $(k-1-t)$-space is called a t-blocking set. Beutelspacher [Beu80] proved that if $\mathcal{L}$ is a t-blocking set in $\mathsf{PG}(k-1,q)$ where $k > t+1$, then

$$\#\mathcal{L} \geq \theta(t) + q^{t-1}\sqrt{q}.$$

2.4 Sub-multisets and Projection

Viewing the multiset γ as a collection, a sub-collection will be called a sub-multiset. The formal definition of a sub-multiset is this.

Definition 2.3 (Sub-multiset)
Let γ be a multiset on S. A sub-multiset $\gamma' \subseteq \gamma$ is a map

$$\gamma' : S \to \{0,1,2,\ldots\},$$

where $\gamma'(s) \leq \gamma(s)$ for all $s \in S$.

Note that passing from γ_C to a sub-multiset corresponds to puncturing the code C. The most interesting kind of sub-multisets for our purposes are cross-sections.

Definition 2.4 (Cross-sections)
Let γ be a multiset on a vector space V, and $U \subseteq \mathsf{V}$ a subspace. The cross-section $\gamma|_U$ is the sub-multiset given by

$$\gamma|_U(x) := \begin{cases} \gamma(x), & \text{if } x \in U, \\ 0, & \text{otherwise.} \end{cases}$$

If U has dimension r in the definition, then we call $\gamma|_U$ an r-dimensional cross-section. In some cases it is easier to deal with cross-sections and their sizes, than with subspaces and their values. In Lemma 2.2, we can consider the cross-section $\gamma_C|_U$ rather than the subspace U. In particular, we have that $n - d_{k-r}(\gamma_C)$ is the size of the largest r-dimensional cross-section of γ_C.

Definition 2.5 (Projections)
Consider an m-space $\Pi_m \leqq \mathsf{PG}(k-1,q)$. The projection map

$$\phi_{\Pi_m} : \mathsf{PG}(k-1,q) \backslash \Pi_m \to \mathsf{PG}(k-2-m,q)$$

takes every $(m+1)$-space containing Π_m to a distinct point of $\mathsf{PG}(k-2-m,q)$. Furthermore, three distinct points $x, y, z \in \mathsf{PG}(k-2-m,q)$ are collinear if and only if

$$\phi_{\Pi_m}^{-1}(x) \subseteq \langle \phi_{\Pi_m}^{-1}(y), \phi_{\Pi_m}^{-1}(z) \rangle.$$

Let C' be the code corresponding to $\gamma_{C'} := \gamma_C \circ \phi_{\Pi_m}^{-1}$. Then C' has parameters $[n - \gamma_C(\Pi_m), k-1-m]$. The following proposition is found in [DS98].

Proposition 2.2
The code C' defined by $\gamma_C \circ \phi_{\Pi_m}^{-1}$ is the subcode Π_m^*, and the cross-section $\gamma_C|_\Pi$ corresponds to the code obtained by puncturing C on $\chi(\Pi^*)$.

Proof: First consider the projective multiset $\gamma_C \circ \phi_{\Pi_m}^{-1}$. The relation to the subcode Π_m^* is best explained in terms of vector multisets, so let U be the $(m+1)$-dimensional subspace such that $\mathsf{P}(U) = \Pi_m$. Let $D = \Pi_m^*$ be the subcode corresponding to U. Remember that $D = U^\perp G$ and that $\overline{\gamma}_D = \mu'(\mathcal{B})$ where μ' is the natural endomorphism $\mathsf{V} \to \mathsf{V}/D^\perp$, but this map can be decomposed into maps

$$\mathsf{V} \to \mathsf{V}/C^\perp \cong \mathsf{M} \to \mathsf{M}/U,$$

the latter of which is exactly the projection map through U, which corresponds to ϕ_{Π_m} in the language of projective multisets. Thus we get the first result.

Finally consider puncturing C on $\chi(D)$ for some subcode $D \leqq C$. According to the proof of Lemma 2.2, this corresponds to removing the columns not contained in D^*, or in other words keeping the columns contained in D^*, to be left with the cross-section $\gamma|_{D^*}$. □

2.5 Classes of Non-Chain Codes

We define M_m to be the set of all projective m-spaces of maximum value, that is

$$M_m := \left\{ \Pi_m \;\middle|\; \Pi_m \in \mathsf{PG}^m \wedge \gamma(\Pi_m) = \Delta_m \right\}.$$

We define a number of subconditions, which all are implications of the chain condition. For any i and j such that $0 \leq i < j \leq k-2$, we have the condition:

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

The negations of these conditions, $(\mathrm{N}i.j) := \neg(\mathrm{C}i.j)$, will be called the *non-chain conditions*. The chain condition will be denoted by (C0).

The order of a condition $(\mathrm{C}i.j)$ or $(\mathrm{N}i.j)$ is the number $j-i$. For a code of dimension k, there are $k-2$ first-order sub-chain conditions defined. Of order t, $k-1-t$ conditions are defined. All together, there are $(k-1)(k-2)/2$ sub-chain conditions.

Codes may be classified according to which sub-chain conditions they satisfy [CK96, CK97a]. There are $2^{(k-1)(k-2)/2}$ different classes of codes of dimension k, not counting the class of chained codes. Extremal non-chain codes are codes satisfying all the non-chain conditions $(\mathrm{N}i.j)$. The difference sequence of an extremal non-chain code will be called an ENDS (*extremal non-chain difference sequence*).

The class of chained codes has been studied in arbitrary dimension [EK94, CK98b]. In dimension 4, there are eight classes plus the class of chained codes, and all the classes have been studied. Extremal non-chain codes were studied in [CK99b] (binary case) and [CK97a] (non-binary), while the other classes were studied in [CK97b] (non-binary) and [CK98a] (binary).

We shall study ENDS in Chapters 3 through 7. We will also get some results on the so-called Class B or B-codes, that is codes satisfying all the subchain conditions, but not the chain condition, in Chapter 9.

3 Upper bounds on ENDS

Our first result on ENDS is a general result bounding all differences but the last one. In Section 3.2, we will prove some necessary conditions for codes meeting the bounds with equality, and in Section 3.3, we will give a bound on the last difference. Finally, we will give some remarks on the existence of optimal codes in Section 3.4. In subsequent chapters, we will give optimal constructions and refinements for the binary case.

The bounds that we give in this chapter and in Chapter 6 are generalisations of the bounds from [CK97a, CK99b], and for $k = 4$ they coïncide with them.

3.1 The main bound on ENDS

Theorem 3.1
If $(\delta_0, \delta_1, \ldots, \delta_{k-1})$ is an ENDS and $1 \leq m \leq k-2$, then

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

If this bound holds with equality for $m = \bar{m} > 1$, then it also holds with equality for $m = \bar{m} - 1$.

The proof of this theorem is quite tedious, and we have to start with some auxiliary results.

Definition 3.1
*We say that an ENDS is m-*optimal, *$1 \leq m \leq k-2$, if it satisfies the bound on δ_m from Theorem 3.1 with equality. An extremal non-chain code C is m-*optimal *if its difference sequence is an m-optimal ENDS.*

Lemma 3.1
Given an arbitrary code with difference sequence $(\delta_0, \delta_1, \ldots, \delta_{k-1})$, we have $\delta_{k-1} \leq q\delta_{k-2}$.

Proof: Take some $\Pi_{k-3} \in M_{k-3}$. There are $q+1$ primes through Π_{k-3}, and for every such prime Π_{k-2} we have

$$\gamma(\Pi_{k-2} \backslash \Pi_{k-3}) \leq \delta_{k-2}.$$

The geometry is partitioned into $q+1$ disjoint subsets of the form $\Pi_{k-2}\backslash\Pi_{k-3}$, beside Π_{k-3}. Hence

$$\sum_{i=0}^{k-1}\delta_i \le (q+1)\delta_{k-2} + \sum_{i=0}^{k-3}\delta_i.$$

The lemma follows immediately. □

Lemma 3.2
Let $(\delta_0,\delta_1,\ldots,\delta_{k-1})$ be the difference sequence of some non-degenerate value assignment γ, and $(\delta'_0,\ldots,\delta'_{k-2})$ the difference sequence of $\gamma|_{\Pi_{k-2}}$ for some $\Pi_{k-2}\in M_{k-2}$. Then $\delta_{k-2}\le\delta'_{k-2}$.

Proof: We have $\Pi_{k-2}\in M_{k-2}(\gamma|_{\Pi_{k-2}})\subseteq M_{k-2}(\gamma)$. Let $\Pi_{k-3}\in M_{k-3}(\gamma)$ and $\Pi'_{k-3}\in M_{k-3}(\gamma|_{\Pi_{k-2}})$. Clearly $\gamma(\Pi'_{k-3})\le\gamma(\Pi_{k-3})$. Hence

$$\delta_{k-2}=\gamma(\Pi_{k-2})-\gamma(\Pi_{k-3})\le\gamma(\Pi_{k-2})-\gamma(\Pi'_{k-3})=\delta'_{k-2},$$

as required. □

Lemma 3.3
Let γ be the projective multiset of an extremal non-chain code with difference sequence $(\delta_0,\delta_1,\ldots,\delta_{k-1})$. If $\Pi_m\in M_m$ where $0\le m\le k-1$ and $\gamma|_{\Pi_m}$ has difference sequence $(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_m)$, then $\delta_m\le\varepsilon_m-1$.

Proof: This goes almost like the proof of Lemma 3.2, except that since the code is extremal non-chain, we get a stronger bound. We have $\Pi_m\in M_m(\gamma_{\Pi_m})\subseteq M_m(\gamma)$. Let $\Pi_{m-1}\in M_{m-1}(\gamma)$ and $\Pi'_{m-1}\in M_{m-1}(\gamma|_{\Pi_m})$. Since the code is extremal non-chain, we have $\gamma(\Pi'_m)<\gamma(\Pi_m)$. Hence

$$\delta_m=\gamma(\Pi_m)-\gamma(\Pi_{m-1})\le\gamma(\Pi_m)-(\gamma(\Pi'_{m-1})+1)=\varepsilon_m-1,$$

as required. □

Lemma 3.4
If $k\ge 3$ and $(\delta_0,\delta_1,\ldots,\delta_{k-1})$ satisfies (N0.1), *then $\delta_1\le q\delta_0-(q+1)$ and $\delta_0\ge 2$.*

Proof: A line consists of $q+1$ points, and by (N0.1), $\delta_1+\delta_0\le(q+1)(\delta_0-1)$. Hence $\delta_1\le q\delta_0-(q+1)$. Also if $\delta_0\le 1$, then $\delta_1\le -1$, which is absurd. □

Proof of Theorem 3.1: The proof goes by induction on m, so we assume that the theorem holds for every $m<\bar{m}$. Lemma 3.4 proves it for $m=1$. Now we consider an extremal non-chain code C such that

$$\delta_{\bar{m}}\ge q^{\bar{m}}\delta_0-\theta(\bar{m}) \tag{3.1}$$
$$\delta_m\le q^m\delta_0-\theta(m),\quad 1\le m\le\bar{m}-1. \tag{3.2}$$

Our aim is to prove that then we must have equality both in (3.1) and in (3.2).

Take an arbitrary $\Theta_{\bar{m}} \in M_{\bar{m}}(C)$, and let

$$\Theta_0 \subset \Theta_1 \subset \ldots \subset \Theta_{\bar{m}-1} \subset \Theta_{\bar{m}}$$

be a chain such that $\Theta_i \in M_i(\gamma|_{\Theta_{i+1}})$ for $0 \leq i \leq \bar{m}-1$. Let $(\varepsilon_0^{(i)}, \ldots, \varepsilon_i^{(i)})$ be the difference sequence of $\gamma|_{\Theta_i}$.

By Lemma 3.3 and (3.1), we get

$$\varepsilon_{\bar{m}}^{(\bar{m})} \geq \delta_{\bar{m}} + 1 \geq q^{\bar{m}}\delta_0 - \theta(\bar{m}) + 1. \tag{3.3}$$

Lemmata 3.2 and 3.1 give

$$\varepsilon_{\bar{m}-1}^{(\bar{m}-1)} \geq \varepsilon_{\bar{m}-1}^{(\bar{m})} \geq \left\lceil \frac{\varepsilon_{\bar{m}}^{(\bar{m})}}{q} \right\rceil. \tag{3.4}$$

Repeating this argument $\bar{m}$ times and substituting from (3.3), we obtain

$$\varepsilon_0^{(0)} \geq \left\lceil \frac{\varepsilon_{\bar{m}}^{(\bar{m})}}{q^{\bar{m}}} \right\rceil \geq \left\lceil \frac{q^{\bar{m}}\delta_0 - \theta(\bar{m}) + 1}{q^{\bar{m}}} \right\rceil = \delta_0 - 1.$$

Clearly $\varepsilon_0^{(0)}$ is the value of Θ_0, which is a point in $\Theta_{\bar{m}} \in M_{\bar{m}}(C)$. Since C is extremal non-chain, we have $\varepsilon_0^{(0)} \leq \delta_0 - 1$. We conclude that

$$\varepsilon_0^{(l)} = \gamma(\Theta_0) = \delta_0 - 1, \quad \forall l,\ 0 \leq l \leq \bar{m}. \tag{3.5}$$

We assume for induction on j that for all $j < i$ where $0 < i < \bar{m}$, we have

$$\varepsilon_j^{(l)} = \varepsilon_j^{(j)} = q^j\delta_0 - \theta(j), \quad \forall l, \text{s.t. } j \leq l \leq \bar{m}. \tag{3.6}$$

We will prove that this equation also holds for $j = i$, and in the process, we will find the value of δ_i.

Our first step will be to prove that $\varepsilon_i^{(i)} = q^i\delta_0 - \theta(i)$. Repeating the argument of (3.4) $\bar{m} - i$ times, we get

$$\varepsilon_i^{(i)} \geq \left\lceil \frac{\varepsilon_{\bar{m}}^{(\bar{m})}}{q^{\bar{m}-i}} \right\rceil \geq \left\lceil \frac{q^{\bar{m}}\delta_0 - \theta(\bar{m}) + 1}{q^{\bar{m}-i}} \right\rceil = q^i\delta_0 - \theta(i). \tag{3.7}$$

By definition, we have $\varepsilon_i^{(i)} = \gamma(\Theta_i) - \gamma(\Theta_{i-1})$. Since C is extremal non-chain, we get by (3.2) that

$$\gamma(\Theta_i) \leq \sum_{j=0}^{i} \delta_j - 1 \leq \sum_{j=0}^{i} [q^j\delta_0 - \theta(j)],$$

and according to the induction hypothesis (3.6), we have

$$\gamma(\Theta_{i-1}) = \sum_{j=0}^{i-1} \varepsilon_j^{(i-1)} = \sum_{j=0}^{i-1} \varepsilon_j^{(j)} = \sum_{j=0}^{i-1} [q^j \delta_0 - \theta(j)]. \tag{3.8}$$

Combining these two expressions, we get an upper bound on $\varepsilon_i^{(i)}$:

$$\begin{aligned} \varepsilon_i^{(i)} &= \gamma(\Theta_i) - \gamma(\Theta_{i-1}) \\ &\leq \sum_{j=0}^{i} [q^j \delta_0 - \theta(j)] - \sum_{j=0}^{i-1} [q^j \delta_0 - \theta(j)] = q^i \delta_0 - \theta(i). \end{aligned} \tag{3.9}$$

Combining the upper and lower bounds (3.7) and (3.9), we conclude that

$$\varepsilon_i^{(i)} = q^i \delta_0 - \theta(i). \tag{3.10}$$

It remains to show that $\varepsilon_i^{(l)} = \varepsilon_i^{(i)}$ for $l > i$, but first we will have a short look on δ_i.

From (3.8) and (3.2) we can see that

$$\sum_{j=0}^{i-1} \delta_j - 1 \geq \gamma(\Theta_{i-1}) = \sum_{j=0}^{i-1} [q^j \delta_0 - \theta(j)] \geq \sum_{j=0}^{i-1} \delta_j - 1,$$

Hence $\delta_{i-1} = q^{i-1}\delta_0 - \theta(i-1)$. Also

$$\gamma(\Theta_i) = \varepsilon_i^{(i)} + \gamma(\Theta_{i-1}) = q^i \delta_0 - \theta(i) + \gamma(\Theta_{i-1}) \leq \sum_{j=0}^{i} \delta_j - 1.$$

Hence $q^i \delta_0 - \theta(i) \leq \delta_i$, and combining with (3.2), we get $\delta_i = q^i \delta_0 - \theta(i)$.

It follows from above that

$$\gamma(\Theta_i) = \sum_{j=0}^{i} \delta_j - 1,$$

and this number happens to be an upper bound on the value of any element in $M_i(\Theta_l)$ for any $l \geq i$. Hence $\Theta_i \in M_i(\Theta_l)$. Likewise we have $\Theta_{i-1} \in M_{i-1}(\Theta_l)$. Thus we get $\varepsilon_i^{(l)} = \varepsilon_i^{(i)}$. It follows by induction that $\delta_i = q^i \delta_0 - \theta(i)$ for $i = 1, 2, \ldots, \bar{m} - 1$.

We have

$$\varepsilon_{\bar{m}}^{(\bar{m})} = \Theta_{\bar{m}} - \Theta_{\bar{m}-1} = \sum_{i=0}^{\bar{m}} \delta_i - \Big(\sum_{i=0}^{\bar{m}-1} \delta_i - 1 \Big) = \delta_{\bar{m}} + 1,$$

and by Lemmata 3.1 and 3.2 and (3.10), we get

$$\delta_{\bar{m}} + 1 = \varepsilon_{\bar{m}}^{(\bar{m})} \leq q\varepsilon_{\bar{m}-1}^{(\bar{m})} \leq q\varepsilon_{\bar{m}-1}^{(\bar{m}-1)} = q^{\bar{m}}\delta_0 - \theta(\bar{m}) + 1.$$

Combining with the lower bound from (3.1) we get

$$\delta_{\bar{m}} = \varepsilon_{\bar{m}}^{(\bar{m})} - 1 = q^{\bar{m}}\delta_0 - \theta(\bar{m}),$$

and the theorem follows by induction. □

Corollary 3.1
Let C be an m-optimal code with difference sequence $(\delta_0, \delta_1, \ldots, \delta_{k-1})$ for some m such that $1 \leq m \leq k-2$. For every $\Pi_m \in M_m$, $\gamma|_{\Pi_m}$ corresponds to a chained code with difference sequence $(\delta_0 - 1, \delta_1, \delta_2, \ldots, \delta_{m-1}, \delta_m + 1)$.

Proof: In the proof of Theorem 3.1 we proved that $\Theta_i \in M_i(\gamma|_{\Theta_{\bar{m}}})$, where $\Theta_{\bar{m}} \subseteq M_{\bar{m}}(\gamma)$ was arbitrarily chosen. We also found the difference sequence as given in the corollary. □

Remark 3.1
We know from Lemma 3.4 that $\delta_0 \geq 2$, so the difference sequence has only positive elements as expected. Writing

$$(\varepsilon_0 = \delta_0 - 1, \varepsilon_1 = \delta_1, \ldots, \varepsilon_{m-1} = \delta_{m-1}, \varepsilon_m = \delta_m + 1)$$

for the difference sequence of $\gamma|_{\Pi_m}$, we have $\varepsilon_i = q\varepsilon_{i-1} - 1$ for $i = 1, \ldots, m-1$ and $\varepsilon_m = q\varepsilon_{m-1}$.

3.2 Structure of optimal codes

In this section, we will find further requirements for an extremal non-chain code to be m-optimal. For instance, if $\mathcal{H} \in M_3$ is a solid of maximum value, then there are a line $\ell \subseteq \mathcal{H}$ and a plane $\mathcal{P} \subseteq \mathcal{H}$ such that $\gamma(p) = \delta_0 - 3$ if $p \in \ell \cap \mathcal{P}$, $\gamma(p) = \delta_0 - 2$ if either $p \in \ell$ or $p \in \mathcal{P}$, but not both; and $\gamma(p) = \delta_0 - 1$ otherwise. The general result will be stated in Theorem 3.2.

Lemma 3.5
Let $(\delta_0, \delta_1, \ldots, \delta_{k-1})$ be the difference sequence of an unrestricted linear code. If $\delta_i = q\delta_{i-1} - 1$ for $i = 1, \ldots, k-1$, then

$$\sum_{i=m}^{k-1} \delta_i = \theta(k-1-m)\delta_m - \sum_{i=0}^{k-m-2} \theta(i), \quad 0 \leq m \leq k-1.$$

Proof: Since $\delta_i = q\delta_{i-1} - 1$, we get

$$\delta_r = q^i \delta_{r-i} - \theta(i-1), \quad 0 \le i \le r \le k-1,$$

The equality follows by summation of this expression. □

Lemma 3.6
If $0 \le a \le q-1$, *then*

$$\theta(m) - a\sum_{i=0}^{m-1} \theta(i) \ge m+1, \quad 0 \le m \le k-1.$$

Proof: We write

$$\begin{aligned}\theta(m) - a\sum_{i=0}^{m-1} \theta(i) &= \theta(m) - \frac{a}{q-1}\sum_{i=0}^{m-1}(q^{i+1}-1) \\ &= \theta(m) - \frac{a}{q-1}(\theta(m)-1-m) \\ &= \frac{q-1-a}{q-1}\theta(m) + \frac{a}{q-1}(1+m).\end{aligned}$$

Note that $\theta(m) \ge m+1$, and thus the above expression is at least $m+1$, proving the lemma. □

Lemma 3.7
Let γ *be a projective multiset with difference sequence* $(\delta_0, \delta_1, \ldots, \delta_{k-1})$ *where* $\delta_i = q\delta_{i-1} - 1$ *for* $i = 1, \ldots, k-2$. *If* $\Pi_m \in M_m$, *then* $\gamma|_{\Pi_m}$ *has difference sequence* $(\delta_0, \delta_1, \ldots, \delta_m)$.

Proof: The proof is trivial for $m = k-1$, so assume $m < k-1$. Let

$$\emptyset = \Theta_{-1} \subset \Theta_0 \subset \Theta_1 \subset \ldots \subset \Theta_m = \Pi_m$$

be a chain of subspaces such that Θ_i has the greatest value among the i-spaces containing Θ_{i-1}. Define $\delta'_i = \gamma(\Theta_i) - \gamma(\Theta_{i-1})$.

Let $(\delta''_0, \delta''_1, \ldots, \delta''_m)$ be the difference sequence of $\gamma|_{\Pi_m}$. It is sufficient to prove that $\delta'_i = \delta_i$ for all i, because

$$\sum_{i=0}^{j} \delta'_i \le \sum_{i=0}^{j} \delta''_i \le \sum_{i=0}^{j} \delta_i, \quad 0 \le j \le m. \tag{3.11}$$

Suppose for contradiction that there is an i such that $\delta_i \ne \delta'_i$. Let l be the smallest such i. Note that $\delta'_l < \delta_l$ by (3.11).

Since there are only $\theta(m-l)$ distinct l-spaces containing Θ_{l-1} in Π_m, we get

$$\gamma(\Pi_m) \leq \theta(m-l)\delta'_l + \sum_{i=0}^{l-1} \delta'_i \leq \theta(m-l)(\delta_l - 1) + \sum_{i=0}^{l-1} \delta_i.$$

Also note that by Lemma 3.5,

$$\gamma(\Pi_m) = \theta(m-l)\delta_l - \sum_{j=0}^{m-l-1} \theta(j) + \sum_{i=0}^{l-1} \delta_i.$$

Combine the two lines to get

$$\theta(m-l)\delta_l - \sum_{j=0}^{m-l-1} \theta(j) + \sum_{i=0}^{l-1} \delta_i \leq \theta(m-l)(\delta_l - 1) + \sum_{i=0}^{l-1} \delta_i,$$

which is equivalent to

$$\theta(m-l) - \sum_{j=0}^{m-l-1} \theta(j) \leq 0,$$

contradicting Lemma 3.6. □

Corollary 3.2
Any code with difference sequence $(\delta_0, \delta_1, \ldots, \delta_{k-1})$ *such that* $\delta_i = q\delta_{i-1} - 1$ *for* $i = 1, \ldots, k-2$ *satisfies the chain condition.*

Lemma 3.8
Let γ *be a projective multiset with difference sequence* $(\delta_0, \delta_1, \ldots, \delta_{k-1})$ *such that* $\delta_{k-1} = q\delta_{k-2}$. *For every prime* $\Pi_{k-2} \supset \Pi_{k-3} \in \boldsymbol{M}_{k-3}$, *we have* $\Pi_{k-2} \in \boldsymbol{M}_{k-2}$.

Proof: Consider $\Pi_{k-3} \in \boldsymbol{M}_{k-3}$. Let $\boldsymbol{B}_0, \ldots, \boldsymbol{B}_q$ be the primes such that $\Pi_{k-3} \subset \boldsymbol{B}_j$, $j = 0, \ldots, q$. We get

$$\gamma(\mathsf{PG}(k-1,q)) = \sum_{j=0}^{q} \gamma(\boldsymbol{B}_j \backslash \Pi_{k-3}) + \gamma(\Pi_{k-3}) = \sum_{j=0}^{k-1} \delta_j.$$

Since $\delta_{k-1} = q\delta_{k-2}$, we get that

$$(q+1)\delta_{k-2} = \sum_{j=0}^{q} \gamma(\boldsymbol{B}_j \backslash \Pi_{k-3}).$$

Comparing this with the fact that $\gamma(\boldsymbol{B}_j \backslash \Pi_{k-3}) \leq \delta_{k-2}$ for all j, we get that $\boldsymbol{B}_j \in \boldsymbol{M}_{k-2}$, as required. □

Lemma 3.9
Let γ be a be a projective multiset on $\mathsf{PG}(k-1,q)$ with difference sequence $(\delta_0,\delta_1,\ldots,\delta_{k-1})$ such that $\delta_i = q\delta_{i-1}-1$, $1 \le i \le k-1$. For every $\Pi_{m-1} \in M_{m-1}$, $0 \le m \le k-1$,

a. the number of distinct m-spaces of maximum value through Π_{m-1} is at least

$$\theta(k-1-m) - \sum_{j=0}^{k-2-m} \theta(j).$$

b. for $m = k-2$ there is a unique m-space $\Pi_m \notin M_m$ such that $\Pi_{m-1} \subset \Pi_m$, and

$$\gamma(\Pi_m) = \sum_{j=0}^{m} \delta_j - 1.$$

Proof: There are $\theta(k-1-m)$ m-spaces $\Theta_i \supset \Pi_{m-1}$. We get that

$$\gamma(\mathsf{PG}(k-1,q)) = \sum_{j=1}^{\theta(k-1-m)} \gamma(\Theta_j \backslash \Pi_{m-1}) + \gamma(\Pi_{m-1}) = \sum_{j=0}^{k-1} \delta_j. \tag{3.12}$$

and by Lemma 3.5,

$$\sum_{j=1}^{\theta(k-1-m)} \gamma(\Theta_j \backslash \Pi_{m-1}) = \sum_{j=m}^{k-1} \delta_j = \theta(k-1-m)\delta_m - \sum_{j=0}^{k-2-m} \theta(j). \tag{3.13}$$

Clearly

$$\gamma(\Theta_j \backslash \Pi_{m-1}) \le \delta_m, \quad 1 \le j \le \theta(k-1-m). \tag{3.14}$$

Comparing the last two equations, we note that at least

$$\theta(k-1-m) - \sum_{j=0}^{k-2-m} \theta(j)$$

of the Θ_i give equality in (3.14). If $m \le k-2$, then at least one gives inequality. The case where $m = k-2$, is just a special case where q of the Θ_i gives equality and one gives inequality. The exact value of the one with inequality is easily computed. □

Lemma 3.10
Let C be a code with difference sequence $(\delta_0,\delta_1,\ldots,\delta_{k-1})$. If $\delta_i = q\delta_{i-1}-1$ for $i = 1,\ldots,k-1$, then there exists at most one point which is not contained in any element of M_{k-2}.

Proof: Suppose there are two distinct points $P, Q \in \mathsf{PG}(k-1,q)$ which are not contained in any element of M_{k-2}. Consider a chain

$$\Pi_0 \subset \Pi_1 \subset \ldots \subset \Pi_{k-2} \subset \mathsf{PG}(k-1,q),$$

such that $\Pi_i \in M_i$ for each $i = 0, \ldots, k-2$. Let $\ell := \langle P, Q \rangle$. Obviously there is a point $S \in \ell \cap \Pi_{k-2}$. By assumption $P, Q \notin \Pi_{k-2}$, so $S \neq P$ and $S \neq Q$.

We claim that we can assume that $S \notin \Pi_{k-3}$. By Lemma 3.9b, there are q points in Π_1 which are elements of M_0, so if $S \in \Pi_0$, then we can replace Π_0 by some other point which is in Π_1 and in M_0. For all i such that $1 \leq i \leq k-3$, there are q i-spaces in M_i containing Π_{i-1} in Π_{i+1}. Thus if $S \in \Pi_i \backslash \Pi_{i-1}$, we can replace Π_i with some other i-space, maintaining the chain. By induction we can assume that $S \notin \Pi_{k-3}$, as required.

There are $q+1$ distinct primes spanned by Π_{k-3} and a point on ℓ, and only one of these is not an element of M_{k-2} by Lemma 3.9b. Since $\langle P \rangle \Pi_{k-3}$ and $\langle Q \rangle \Pi_{k-3}$ are two distinct primes, either P or Q is contained in some element of M_{k-2}. The lemma follows by contradiction. □

Lemma 3.11
Assume that $k \leq 3$ and let let γ be a projective multiset with difference sequence $(\delta_0, \delta_1, \ldots, \delta_{k-1})$ such that $\delta_i = q\delta_{i-1} - 1$ for $i = 1, \ldots, k-1$. Then there exists a collection S containing exactly one i-space for each $i = 0, \ldots, k-2$ such that

$$\gamma(p) = \delta_0 - \#\{\Pi \in S \mid p \in \Pi\}, \quad \forall p \in \mathsf{PG}(k-1,q).$$

Proof: For $k = 1$ the result is trivial.

For $k = 2$ there are $q+1$ points. By Lemma 3.9b there is one point P of value $\delta_0 - 1$ and q points of value δ_0. Hence $S = \{P\}$ forms the required collection.

Consider $k = 3$. There is a point $\wp \in M_0$. Let $\ell_0, \ldots, \ell_q$ be the distinct lines such that $\wp \subset \ell_i$ for all i. One of these lines, say ℓ_0, has value $\delta_1 + \delta_0 - 1$, while the remaining q lines have value $\delta_0 + \delta_1$ by Lemma 3.9b. This means that for $1 \leq i \leq q$, there is exactly one point, $\alpha_i \in \ell_i$, such that $\gamma(\alpha_i) = \delta_0 - 1$. There are at most two points in ℓ_0 with value $\delta_0 - 1$ or less. The remaining points have value δ_0. Obviously, every line in $\mathsf{PG}(2,q)$ has value at most $\delta_0 + \delta_1$, and hence has at least one point of value $\delta_0 - 1$ or less. A set of $q+2$ points cannot meet every line in a plane unless it contains a line [Beu80, Hir98]. It follows that there must be a line Π_1 such that $\gamma(p) \leq \delta_0 - 1$ for all $p \in \Pi_1$. Since $\gamma(\ell_0) = \delta_1 + \delta_0 - 1$, there is either one point $\Pi_0 = \Pi_1 \cap \ell_0$ which has value $\delta_0 - 2$ or two distinct points Π_0 and $\Pi_1 \cap \ell_0$ of value $\delta_0 - 1$. In either case $\{\Pi_0, \Pi_1\}$ forms the required collection S. □

Lemma 3.12
Assume that $q \geq 3$ and let γ be the projective multiset on $\mathsf{PG}(k-1,q)$ corresponding to a chained code C with difference sequence $(\delta_0, \delta_1, \ldots, \delta_{k-1})$ such that $\delta_i = q\delta_{i-1} - 1$

for $i = 1, \ldots, k-1$. Then there exists a collection S containing exactly one i-space for each $i = 0, \ldots, k-2$ such that

$$\gamma(p) = \delta_0 - \#\{\Pi \in S \mid p \in \Pi\}, \quad \forall p \in \mathsf{PG}(k-1, q).$$

Proof: Lemma 3.11 proves it for $k < 4$. Now assume that the lemma holds for $k < n$, and consider

$$\gamma : \mathsf{PG}(n, q) \to \mathsf{N}_0, \quad n \geq 4 \wedge q \geq 3.$$

For $\Pi_l \in M_l(C)$, $l < n$, let $S(\Pi_l)$ be the collection S corresponding $\gamma|_{\Pi_l}$. By the induction hypothesis, $S(\Pi_l)$ exists and has the property given in the lemma. We also define $\sigma_i(\Pi_l)$ to be the i-space in $S(\Pi_l)$.

First we make a general observation. Let $\Theta_1 \in M_{n-2}(C)$ and $\Theta_2 \in M_{n-1}(C)$ such that $\Theta_1 \subset \Theta_2$. We can use either $S(\Theta_1)$ or $S(\Theta_2)$ to express the value of a point $p \in \Theta_1$. Hence

$$\#\{\Pi \in S(\Theta_1) \mid p \in \Pi\} = \#\{\Pi \in S(\Theta_2) \mid p \in \Pi\}. \tag{3.15}$$

For all $i \geq 0$, $\sigma'_{i-1} := \sigma_i(\Theta_2) \cap \Theta_1$ is either an i-space if $\sigma_i \subseteq \Theta_1$, or else an $(i-1)$-space. Equation (3.15) can only be satisfied if $\dim \sigma'_i = i$, and then we can let σ'_i for $i \geq 0$ be the elements of $S(\Theta_1)$. Thus

$$S(\Theta_1) = \{\Pi \cap \Theta_1 \mid \Pi \in S(\Theta_2)\}.$$

Claim I
If $1 \leq i \leq n-2$, then there is an $(i+1)$-space σ'_{i+1} such that $\sigma_i(\mathcal{A}) \subset \sigma'_{i+1}$ for all $\mathcal{A} \in M_{n-1}$.

Consider $P \in M_{n-3}(C)$, $\alpha_0 \in M_{n-2}(C)$, $\mathcal{A}_1, \ldots, \mathcal{A}_q \in M_{n-1}(C)$, and $\mathcal{A}_0 \notin M_{n-1}(C)$ such that $P \subset \alpha_0 \subset \mathcal{A}_j$ for $0 \leq j \leq q$. Since $q \geq 3$, there are at least two distinct $(n-2)$-spaces $\alpha_1, \alpha_2 \in M_{n-2}(C)$ such that $P \subset \alpha_j \subset \mathcal{A}_1$ and $\alpha_0 \neq \alpha_j$ for $j = 1, 2$. There are also at least two distinct $(n-2)$-spaces $\beta_1, \beta_2 \in M_{n-2}(C)$ such that $P \subset \beta_j \subset \mathcal{A}_2$ and $\alpha_0 \neq \beta_j$ for $j = 1, 2$. Define $\sigma'_{i+1} := \sigma_i(\mathcal{A}_1)\sigma_i(\mathcal{A}_2)$. We have $\mathcal{A}_1 \cap \mathcal{A}_2 = \alpha_0 \in M_{n-2}(C)$, so

$$\sigma_{i-1}(\alpha_0) = \sigma_i(\mathcal{A}_1) \cap \alpha_0 = \sigma_i(\mathcal{A}_2) \cap \alpha_0 = \sigma_i(\mathcal{A}_1) \cap \sigma_i(\mathcal{A}_2).$$

Since $\dim \sigma_{i-1}(\alpha_0) = i-1$, we get $\dim \sigma'_{i+1} = i+1$. It remains to prove that

$$M_{n-1} = \mathfrak{S} := \{\mathcal{A} \in M_{n-1} \mid \sigma_i(\mathcal{A}) \subset \sigma'_{i+1}, 1 \leq i \leq n-2\}.$$

Consider the spaces $\alpha_1\beta_1$ and $\alpha_2\beta_1$. At least one of them is a space in $M_{n-1}(C)$, denote it $\mathcal{B}_1$. Similarly, let $\mathcal{B}_2$ be either $\alpha_1\beta_2$ or $\alpha_2\beta_2$ such that $\mathcal{B}_2 \in M_{n-1}(C)$. We

have the following

$$\begin{aligned}
&\mathcal{B}_1 \cap \mathcal{A}_1 = \alpha_j \in M_{n-2}(C), \quad j = 1 \vee j = 2,\\
&\mathcal{B}_1 \cap \mathcal{A}_2 = \beta_1 \in M_{n-2}(C),\\
&\mathcal{B}_2 \cap \mathcal{A}_1 = \alpha_j \in M_{n-2}(C), \quad j = 1 \vee j = 2,\\
&\mathcal{B}_2 \cap \mathcal{A}_2 = \beta_2 \in M_{n-2}(C).
\end{aligned}$$

It follows that $\sigma_i(\mathcal{B}_1) \cap \sigma_i(\mathcal{A}_1) = \sigma_{i-1}(\alpha_j)$ for $j = 1$ or $j = 2$, and $\sigma_i(\mathcal{B}_1) \cap \sigma_i(\mathcal{A}_2) = \sigma_{i-1}(\beta_1)$ are distinct $(i-1)$-spaces contained in σ'_{i+1}. Consequently $\sigma_i(\mathcal{B}_1) \subset \sigma'_{i+1}$. The same argument holds for $\mathcal{B}_2$, and hence $\sigma_i(\mathcal{B}_2) \subset \sigma'_{i+1}$.

At least one of the $(n-2)$-spaces $\mathcal{A}_3 \cap \mathcal{B}_1$ or $\mathcal{A}_3 \cap \mathcal{B}_2$ is an element $\alpha' \in M_{n-2}(C)$, because $P = \mathcal{A}_3 \cap \mathcal{B}_1 \cap \mathcal{B}_2 \in M_{n-3}$. It follows that $\sigma_i(\mathcal{A}_3)$ meets σ'_{i+1} in at least two distinct $(i-1)$-spaces, $\sigma_{i-1}(\alpha')$ and $\sigma_{i-1}(\alpha_0)$. We conclude that $\sigma_i(\mathcal{A}_3) \subset \sigma'_{i+1}$, and thus we have shown that

$$\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{B}_1, \mathcal{B}_2 \in \mathfrak{S}.$$

First we note that if there are two distinct elements $\mathcal{E}_1, \mathcal{E}_2 \in \mathfrak{S}$, and $\mathcal{A} \in M_{n-1}$ such that $\gamma_j := \mathcal{E}_j \cap \mathcal{A} \in M_{n-2}$ for $j = 1, 2$, then $\sigma_i(\mathcal{A})$ meets σ'_{i+1} in two distinct $(i-1)$-spaces $\sigma_{i-1}(\gamma_j)$. Hence $\mathcal{A} \in \mathfrak{S}$.

If there are three distinct elements $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3 \in \mathfrak{S}$ and $\mathcal{A} \in M_{n-3}$ such that

$$\bigcap_{j=1}^{3} \mathcal{E}_j \in M_{n-2} \quad \bigwedge \quad \mathcal{A} \cap \bigcap_{j=1}^{3} \mathcal{E}_j \in M_{n-3},$$

then at least two of the $\mathcal{E}_j$ meets $\mathcal{A}$ in an element of M_{n-2}, and $\mathcal{A} \in \mathfrak{S}$.

An element $\mathcal{A} \in M_{n-1}$ such that

$$P \subset \mathcal{A} \notin \{\mathcal{B}_1, \mathcal{B}_2, \mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3\}$$

meets either $\mathcal{A}_1$, $\mathcal{A}_2$, and $\mathcal{A}_3$ or $\mathcal{A}_1$, $\mathcal{B}_1$, and $\mathcal{B}_2$ in three distinct $(n-2)$-spaces and hence every such $\mathcal{A}$ is an element of $\mathfrak{S}$.

If $\mathcal{A} \in M_{n-1}(C)$ such that $\overline{P} := P \cap \mathcal{A} \in M_{n-4}$, then there is $\xi \in M_{n-2}$ such that $P \subset \xi$ and $S := \xi \cap \mathcal{A} \in M_{n-3}$. This is obvious from the fact that there are at least $q^2 - 1$ $(n-2)$-spaces of maximum value through P by Lemma 3.9, and at most $q+2$ $(n-3)$-spaces through $\overline{P}$ in $\mathcal{A}$ that are not elements of M_{n-3}. There are at least $q^2 - q - 3 \geq 3$ subspaces $\mathcal{E}_j \in M_{n-1}$, $j = 1, 2, 3$, through ξ, and

$$\mathcal{A} \cap \bigcap_{j=1}^{3} \mathcal{E}_j = S \in M_{n-3}.$$

Hence $\mathcal{A} \in \mathfrak{S}$.

Suppose for induction that if there is $R \subseteq \bar{P} := P \cap \mathcal{A}$ such that $R \in M_{j+1}$ and $\mathcal{A} \in M_{n-1}$, then $\mathcal{A} \in \mathfrak{S}$. This was proved for $j = n-5$ in the last paragraph. It even holds for $n = 3$, because if $j = -2$, then $R = \emptyset \in M_{-1}$.

Consider $\mathcal{A} \in M_{n-1}(C)$ such that there is $\bar{R} \in M_j$ such that $\bar{R} \subset \bar{P}$, but there is no $\bar{R}' \in M_{j+1}$ such that $\bar{R}' \subseteq \bar{P}$. Let $R \in M_{j+1}$ be such that $\bar{R} \subset R \subset P$. We shall prove that there is $\xi \in M_{n-2}$ such that $R \subset \xi$ and $\xi \cap \mathcal{A} \in M_{n-3}$. This is sufficient because then there are $q \geq 3$ elements of $\mathfrak{S}$ containing ξ by the induction hypothesis, and at least two of them meet $\mathcal{A}$ in elements of M_{n-2}.

We prove the existence of ξ by induction on m. Assume that

$$\exists R_m \in M_m, \text{ s.t. } R_m \cap \mathcal{A} \in M_{m-1}, \quad j+1 \leq m \leq n-3. \tag{3.16}$$

Let $R_{j+1} = R$. By Lemma 3.9, there are at least

$$\theta(n-(m+1)) - \sum_{l=0}^{n-(m+1)-1} \theta(l)$$

$(m+1)$-spaces of maximum value through R_m. Of these at most

$$\sum_{l=0}^{n-1-m-1} \theta(l)$$

meets $\mathcal{A}$ in an m-space which does not have maximum value. Hence at least

$$\theta(n-m-1) - 2 \sum_{l=0}^{n-m-2} \theta(l) \geq 1$$

$(m+1)$-spaces satisfies (3.16) by Lemma 3.6. By induction $\xi := R_{n-2}$ exists, and hence $\mathfrak{S} = M_{n-1}$. This proves the claim.

Claim II
For all $\mathcal{A} \in M_{n-1}$, $1 \leq i \leq n-2$, $\sigma_i(\mathcal{A}) = \sigma'_{i+1} \cap \mathcal{A}$.

Assume for contradiction that the claim fails for some i, and let m be the largest such i. Let $\mathcal{A} \in M_{n-1}$ be such that $\sigma'_{m+1} \subseteq \mathcal{A}$. Let $\mathcal{B} \in M_{n-1}$ such that $\sigma_m(\mathcal{A}) \neq \sigma_m(\mathcal{B})$. By Claim I we get that $\sigma_m(\mathcal{B}) \subset \sigma'_{i+1} \subseteq \mathcal{A}$. Note that

$$\begin{aligned} \#\sigma_m(\mathcal{B}) &= \theta(m) \\ \#(\sigma_m(\mathcal{A}) \cap \sigma_m(\mathcal{B})) &\leq \theta(m-1) \\ \#\bigcup_{j=0}^{m-1} \sigma_j(\mathcal{A}) &\leq \sum_{j=0}^{m-1} \theta(j). \end{aligned}$$

Hence

$$\#\Big(\sigma_m(\mathcal{B})\setminus\bigcup_{i=0}^{m}\sigma_i(\mathcal{A})\Big)\geq q^m-\sum_{j=0}^{m-1}\theta(j)\geq 1,$$

since $q\geq 3$. It follows that there exists

$$P\in\sigma_m(\mathcal{B})\setminus\bigcup_{i=0}^{m}\sigma_i(\mathcal{A}).$$

By the induction hypothesis

$$\begin{aligned}\gamma(P)&=\delta_0-\#\{i\mid P\in\sigma_i(\mathcal{B})\ \wedge\ 0\leq i\leq k-1\}\\&\leq\delta_0-1-\#\{i\mid P\in\sigma'_{i+1}\ \wedge\ m+1\leq i\leq k-1\}\\\gamma(P)&=\delta_0-\#\{i\mid P\in\sigma_i(\mathcal{A})\ \wedge\ 0\leq i\leq k-1\}\\&=\delta_0-\#\{i\mid P\in\sigma'_{i+1}\ \wedge\ m+1\leq i\leq k-1\},\end{aligned}$$

and these two equations contradict each-other, proving Claim II.

We write

$$U:=\{\sigma_0(\mathcal{A})\mid\mathcal{A}\in M_{n-1}(C)\}.$$

Lemma 3.10 says that at most one point is not contained in any element of $M_{n-1}(C)$. This means that we can form the set

$$S'=U\cup\{\sigma'_i\mid i=2,\ldots,n-1\},$$

giving the value of all points but at most one by the formula

$$\gamma(p)=\delta_0-\#\{\Pi\in S'\mid p\in\Pi\}.$$

Claim III
There is a line σ'_1 such that $\sigma_0(\mathcal{A})\subset\sigma'_1$ for all $\mathcal{A}\in M_{n-1}(C)$.

Take a point $F\in M_0(C)$ such that

$$F=\Pi_0\subset\Pi_1\subset\ldots\subset\Pi_{n-3}=P$$

is a chain of subspaces of maximum value. Let ϕ_F be the projection map through F and define $\gamma_F:=\gamma\circ\phi_F^{-1}$. Then γ_F defines an $(n-1)$-dimensional subcode code with length d_{n-1} and difference sequence $(\delta_1,\ldots,\delta_n)$. Hence by the induction hypothesis, there is a collection $S(\mathsf{PG}(n-1,q))$ of i-spaces $\sigma_i(\mathsf{PG}(n-1,q))$ for $i=0,\ldots,n-2$ such that

$$\gamma_F(p)=\delta_1-\#\{\Pi\in S(\mathsf{PG}(n-1,q))\mid p\in\Pi\}.$$

Clearly $F \not\subseteq \Pi$ for any $\Pi \in S'$. Hence $\phi_F(\sigma'_i)$ is an i-space. We get the following formula for the values of every point but at most one in $\mathsf{PG}(n-1,q)$:

$$\begin{aligned}\gamma_F(p) &= q\delta_0 - \#\{\Pi \in S' \mid p \in \phi_F(\Pi)\} \\ &= \delta_1 - \#\{\Pi \in S' \setminus \{\sigma'_{n-1}\} \mid p \in \phi_F(\Pi)\}.\end{aligned}$$

It follows that

$$\begin{aligned}\sigma_i(\mathsf{PG}(n-1,q)) = \phi_F(\sigma'_i), \quad 2 \le i \le n-2 \\ \phi_F(U) \subseteq \sigma_1(\mathsf{PG}(n-1,q)) \cup \sigma_0(\mathsf{PG}(n-1,q)).\end{aligned}$$

We have $U \cap \alpha_0 = \emptyset$ for otherwise the points of U would become elements of $S(\alpha_0)$. It follows that $\sigma_0(\mathcal{A}_i)$ for $i = 1,\ldots,q$ are q distinct elements of U. Let $U' \subset U$ be the set of these q points.

Now consider $V = \sigma_1(\mathsf{PG}(n-1,q)) \cup \sigma_0(\mathsf{PG}(n-1,q))$, the inverse image of which must consist of points in U and points not contained in any element of $M_{n-1}(C)$. In fact $\phi_F(U') \subset \sigma_1(\mathsf{PG}(n-1,q))$ because $\sigma_1(\mathsf{PG}(n-1,q))$ must contain the images of one point from each of the hyperplanes $\mathcal{A}_i$. Hence U' are coplanar points.

There are more chains

$$F \neq F' = \Pi'_0 \subset \Pi'_1 \subset \ldots \subset \Pi'_{n-3} = P$$

of subspaces of maximum value. By projecting through such a point F', we can show that U' is also contained in a plane which is not equal to the first. Hence U' is contained in a line, which we denote σ'_1, and $\phi_F(\sigma'_1) = \sigma_1(\mathsf{PG}(n-1,q))$

We shall prove that $U \cap \mathcal{A}_0 \subset \sigma'_1$, and consequently that $U \subseteq \sigma'_1$. Consider an arbitrary point $R \in U \cap A_0$. By the definition of U, there is $\mathcal{G} \in M_{n-1}(C)$ such that $R \in \mathcal{G}$. By Lemma 3.7 there is a subspace $\rho \subset \mathcal{G}$ such that $\rho \in M_{n-2}(C)$. By the argument used to prove Lemma 3.10, we can choose ρ such that $R \notin \rho$. Projecting through a couple of distinct points contained in $M_0(C)$ and in ρ, as we did in the previous paragraph, will show that $R \in \sigma'_1$, as required. This proves Claim III.

Claim IV

There is a point σ'_0 which is not contained in any element of $M_{n-1}(C)$, and $S := \{\sigma'_i \mid i = 0,\ldots,n-1\}$ forms the required collection such that

$$\gamma(p) = \delta_0 - \#\{\Pi \in S \mid p \in \Pi\}, \quad \forall p \in \Pi_n.$$

We have proved that this holds for all points except possibly for σ'_0. If it does fail for σ'_0, it must give us a wrong value for $\gamma(\mathsf{PG}(n,q))$, but

$$\gamma(\mathsf{PG}(n,q)) = \theta(n)\delta_0 - \sum_{\Pi \in S} \#\Pi = \theta(n)\delta_0 - \sum_{i=0}^{n-1} \theta(i) = \sum_{i=0}^{n} \delta_i,$$

by Lemma 3.5, and that is correct. If σ'_0 did not exist, we would have no point in S, and the total value would not be correct. This completes the proof of Claim IV and the lemma. □

Theorem 3.2
Let C be a chained, non-binary code with difference sequence $(\delta_0, \delta_1, \ldots, \delta_m)$. If

$$\begin{aligned} \delta_i &= q\delta_{i-1} - 1, \quad i = 1, \ldots, m-1, \\ \delta_m &= q\delta_{m-1}, \end{aligned}$$

then there exists a collection S of exactly one i-space in $\mathsf{PG}(m,q)$ for each $i = 1, \ldots, m-1$, such that

$$\gamma(p) = \delta_0 - \#\{\Pi \in S \mid p \in \Pi\}, \forall p \in \mathsf{PG}(m,q).$$

Proof: Lemma 3.12 says that for each $\Pi_{m-1} \in M_{m-1}(C)$, there is a set $S(\Pi_{m-1})$ such that $\gamma(p) = \delta_0 - \#\{\Pi \in S(\Pi_{m-1}) \mid p \in \Pi\}$ for all $p \in \Pi_{m-1}$. Let σ_i denote the i-space in S. If $m \geq 3$ we use the same argument as in the proof of Lemma 3.12, to show that

$$\sigma_i = \bigcup_{\Pi \in M_{m-1}} \sigma_{i-1}(\Pi), i = 1, 2, \ldots, m-1.$$

Because every point is contained in some $\Pi_{m-1} \in M_{m-1}(C)$, there is no point in S.

The cases for $m \leq 2$ are just as simple as the proof of Lemma 3.11. □

This theorem will of course apply to every subspace $\Pi_m \in M_m(C)$ for an m-optimal, extremal non-chain code C, and this fact has been most useful to limit the search for m-optimal constructions (see Chapter 4).

Corollary 3.3
If $(\delta_0, \delta_1, \ldots, \delta_{k-1})$ is an optimal ENDS where $k \geq 5$ and $q \geq 3$, then $\delta_0 \geq 3$.

Proof: Consider the theorem with $m = 3$, and note that there is a point, $P \in \Pi_3 \in M_3$ of value $\gamma(P) = \delta_0 - 3$. □

3.3 Upper bounds on the total value

We have established bounds for all differences but the last. The following is an extension of Theorem 3 in [CK97a].

Theorem 3.3
If $(\delta_0, \delta_1, \ldots, \delta_{k-1})$, $k \geq 3$, satisfies $(\mathrm{N}m-1.m)$ where $1 \leq m \leq k-2$, then

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

Proof: Let $\alpha \in M_{m-1}$. In $\mathsf{PG}(k-1,q)$, there are $\theta(k-1-m)$ m-spaces containing α, and for any such m-space, $\beta \supset \alpha$, we know by condition (N$m-1.m$) that

$$\gamma(\beta \backslash \alpha) \leq \delta_m - 1.$$

Thus $\gamma(\mathsf{PG}(k-1,q)\backslash\alpha) \leq (\delta_m - 1)\theta(k-1-m)$. By the definition of α, we know that

$$\gamma(\alpha) = \sum_{i=0}^{m-1} \delta_i,$$

and the theorem follows. □

For an ENDS, several bounds may be derived from the above theorem. The bound in the following corollary is tight for the code constructed in Chapter 4. When we take up the study of binary codes, we will derive another bound from the theorem.

Corollary 3.4
For any $(\delta_0, \delta_1, \ldots, \delta_{k-1})$, $k \geq 3$, *if* (N0.1) *is satisfied, then*

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

The bound holds with equality if and only if every line through $X \in M_0$ *has value* $(q+1)\delta_0 - (q+2)$.

Definition 3.2
An ENDS $(\delta_0, \delta_1, \ldots, \delta_{k-1})$ *is said to be* optimal *if it is* $(k-2)$*-optimal, and*

$$\gamma(\mathsf{PG}(k-1,q)) = \theta(k-1)\delta_0 - (q+2)\theta(k-2). \tag{3.17}$$

An extremal non-chain code is optimal *if its difference sequence is an optimal ENDS.*

Remark 3.2
We note that an ENDS satisfying (3.17) is not necessarily $(k-1)$*-optimal. In fact there is a ternary, five-dimensional code with difference sequence* $(3, 5, 14, 40, 101)$.

Lemma 3.13
If $(\delta_0, \delta_1, \ldots, \delta_{k-1})$ *is an optimal ENDS and* $\wp \in M_0$, *then for every line* $\ell \supset \wp$, *we have* $\gamma(\ell) = \delta_0 + \delta_1 - 1$.

Proof: This is obvious from the proof of Theorem 3.3, where $\alpha = \wp$ and $\beta = \ell$. □

3.4 Closing remarks

Theorem 3.4
There exists an optimal ENDS if one of the following holds:

$$\begin{array}{lllllll}
k=3 & \wedge & q=2 & \wedge & \delta_0 \geq 3 & \vee \\
k=3 & \wedge & q\geq 3 & \wedge & \delta_0 \geq 2 & \vee \\
k=4 & \wedge & q=3 & \wedge & \delta_0 \geq 3 & \vee \\
k=4 & \wedge & q\geq 4 & \wedge & \delta_0 \geq 2 & \vee \\
k=5 & \wedge & q\geq 3 & \wedge & \delta_0 \geq 3 & \vee \\
k=6 & \wedge & 2 \not| q & \wedge & \delta_0 \geq 3. &
\end{array}$$

Three-dimensional constructions are presented in the example below. A four-dimensional construction was first found by Chen and Kløve [CK97a], and this will be called the C-K construction. Five- and six-dimensional constructions will be presented in subsequent chapters.

We will also see that no optimal, binary ENDS exists if $k \geq 4$. It is not known if non-binary ENDS exists for $k \geq 7$ nor for $k = 6$ and $2|q$. Of course it would be interesting to find an infinite family of optimal, extremal non-chain codes for arbitrarily large k.

Example 3.1
An optimal ENDS in $\mathsf{PG}(2,q)$ *is easily obtained as follows. Let* ℓ *be a line, and* $X \notin \ell$ *a point. Let* $\gamma(X) = \delta_0$*. Consider each line* $\alpha \ni X$*. If* $q \geq 3$*, we choose two points in* $\alpha \backslash (\{X\} \cup \ell)$ *to have value* $\delta_0 - 2$*. All remaining points have value* $\delta_0 - 1$*. Note that* $\delta_0 \geq 2$*.*

If $q = 2$*, there is only one point in* $\alpha \backslash (\{X\} \cup \ell)$*, so that point must have value* $\delta_0 - 3$*, thus* $\delta_0 \geq 3$*.*

We have found several non-equivalent optimal constructions in dimension five, but only one will be presented in this thesis. We have looked for ways to generalise the constructions to arbitrary dimension, with no success, yet. Still, we feel like sharing some general observations relevant to future research for such generalisations.

The C-K construction contains a cross-section equivalent to the three-dimensional construction from Example 3.1. However, the C-K construction cannot be embedded in any optimal construction in dimension five. If the C-K construction were embedded, it would form a prime meeting some prime of maximum value in a plane, but there is no plane which can be both in the C-K construction and in a solid meeting the requirements of Theorem 3.2.

The construction given in Chapter 4 does contain a three-dimensional cross-section defining an optimal ENDS, which obviously cannot be equivalent to the C-K construction. The following remark outlines the procedure to verify this observation.

Remark 3.3
If $\Pi_m \in M_m$ and $\Pi_0 \in M_0$, such that $\gamma|_{\langle \Pi_m, \Pi_0 \rangle}$ defines an ENDS of dimension $m+2$, then it is optimal. This is the case if and only if for each $i = 1, \ldots m-i$, there is $\Pi_i \in M_i$ such that $\Pi_i \subset \langle \Pi_m, \Pi_0 \rangle$.

It is also possible to construct an optimal ENDS in $\mathsf{PG}(4,3)$, for which there do not exist $\Pi_m \in M_m$ and $\Pi_0 \in M_0$ such that $\gamma|_{\langle \Pi_m, \Pi_0 \rangle}$ defines an ENDS.

One sufficient criterion to determine that two constructions with the same ENDS are non-equivalent, is that the cardinalities of the sets M_i differ. For instance there are at least three ENDS constructions in $\mathsf{PG}(4,3)$, which do contain hyperplanes defining optimal ENDS, but which differ in the cardinalities of M_1 and M_2.

4 Optimal, 5-dimensional ENDS

In this chapter we simply present a projective multiset γ on $\mathsf{PG}(4,q)$ defining a five-dimensional code as promised by Theorem 3.4.

4.1 The projective multiset

As reference points, we chose five points, A, B, C, D and E, spanning $\mathsf{PG}(4,q)$. Consider the line $\langle D, E\rangle$. It has $q+1$ points, which we name $\rho_0 = D, \rho_1 = E, \rho_2, \rho_3, \ldots, \rho_q$. These points define $q+1$ hyperplanes with $\langle A, B, C\rangle$ as a subspace, and we call them $\mathcal{G}_i := \langle A, B, C, \rho_i\rangle$ for $i = 0, 1, \ldots, q$. We define $F := \rho_2$ and $G := \rho_3$. We also establish names for the affine spaces we get by removing $\langle A, B, C\rangle$ from $\mathcal{G}_i$:

$$\mathcal{A}_i := \mathcal{G}_i \setminus \langle A, B, C\rangle, \quad i = 0, 1, \ldots, q.$$

During the construction we will pay special attention to the points in $\mathcal{G}_0$, $\mathcal{G}_1$, $\mathcal{G}_2$ and $\mathcal{G}_3$. The remaining hyperplanes $\mathcal{G}_i$ will be similar to $\mathcal{G}_0$ in the sense that $\gamma|_{\mathcal{G}_i}$ is isomorphic to $\gamma|_{\mathcal{G}_0}$.

4.1.1 Defining subspaces of maximum values

First we decide that $\mathcal{G}_0$ be in M_3, and assign values satisfying the requirements from Theorem 3.2:

$$\begin{aligned}
\gamma(p) &= \delta_0 - 3, \quad \forall p \in \langle A, B\rangle \\
\gamma(p) &= \delta_0 - 2, \quad \forall p \in \langle A, B, C\rangle \setminus \langle A, B\rangle \\
\gamma(p) &= \delta_0 - 1, \quad \forall p \in \langle A, B, C, D\rangle \setminus \langle A, B, C\rangle
\end{aligned}$$

We go on by constructing a plane in M_2. For this, we choose $\mathcal{P} := \langle C, D, G\rangle$ and assign values such that it satisfies the requirements from Theorem 3.2:

$$\begin{aligned}
\gamma(p) &= \delta_0 - 2, \quad \forall p \in \langle C, G\rangle \\
\gamma(p) &= \delta_0 - 1, \quad \forall p \in \langle C, D, G\rangle \setminus \langle C, G\rangle
\end{aligned}$$

We note that $\mathcal{P}$ has but one point, C, in common with $\langle A, B, C\rangle$, which also means that it intersects each of the affine spaces, $\mathcal{A}_i$, in q points.

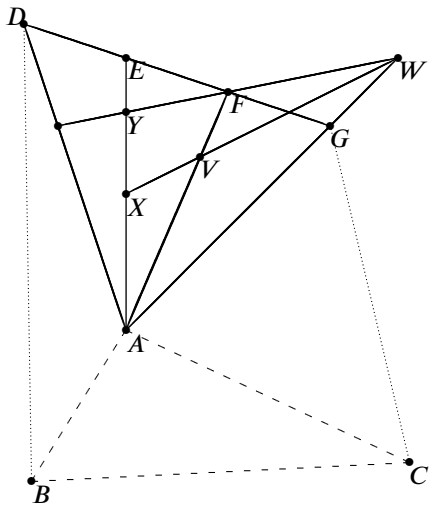


Figure 4.1: Parts of our optimal construction in $\mathsf{PG}(4,q)$, $q \geq 3$. Black lines are in $\langle A, D, G\rangle$, dotted and dashed lines are not.

Now we choose a point for M_0. We want to place it in $\mathcal{G}_1$, particularly on the line $\langle A, E\rangle$. We will have to refer to two distinct points on this line, so let:

$$X, Y \in \langle A, E\rangle \setminus \{A, E\}, \quad X \neq Y$$

Let $\wp := \{X\} \in M_0$ and assign $\gamma(X) = \delta_0$. It remains to choose a line, ℓ, for M_1, so let $\ell := \langle F, Y\rangle$. We know that each point on ℓ must have value $\delta_0 - 1$.

Having established members of the sets M_0, M_1, M_2, M_3, we turn to the problem of giving the remaining points values just low enough to satisfy the non-chain conditions. The point X will be the only point in M_0, so the remaining points will get value at most $\delta_0 - 1$.

4.1.2 Lines through X

For every line $\alpha \ni X$, we must have

$$\gamma(\alpha) \leq (q+1)(\delta_0 - 1) - 1 = \delta_0 + q(\delta_0 - 1) - 2,$$

because the DS is an ENDS. Hence α must have a point of value $\delta_0 - 3$ or less, or at least two points of value $\delta_0 - 2$.

First consider the lines through X, that does not intersect $\langle A, B, C\rangle$. We can handle a lot of these lines by assigning the value $\delta_0 - 3$ to all points in $\mathcal{A}_3$ that have not got any value yet:

$$\gamma(p) = \delta_0 - 3, \quad \forall p \in \mathcal{A}_3 \setminus (\mathcal{P} \cup \ell).$$

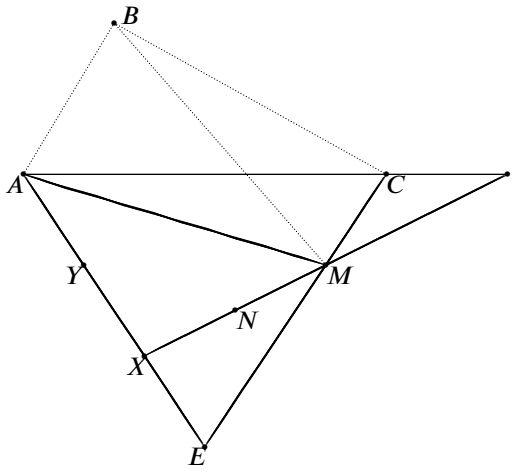


Figure 4.2: The hyperplane $\mathcal{G}_1$ in our optimal construction for $\mathsf{PG}(4,q)$. Black lines are in the plane $\langle A, C, E\rangle$, dotted lines are not.

Let α_i for $i = 1, 2, \ldots, q$ be the (distinct) lines through X meeting $\mathcal{A}_3$ in a point of value $\delta_0 - 2$, i.e. meeting $\langle C, G\rangle \setminus \{C\}$. The lines, α_i, meet $\mathcal{A}_2$ in distinct points. Let $\mathcal{T}$ be the set of these points:

$$\mathcal{T} := \bigcup_{i=1}^{q} (\alpha_i \cap \mathcal{A}_2) = \mathcal{A}_2 \cap \langle X, C, G\rangle.$$

Let $\mathcal{S} \subset \mathcal{A}_2$ be the set of points in $\mathcal{A}_2$, to which we have already assigned values. Thus

$$\mathcal{S} := \mathcal{A}_2 \cap (\mathcal{P} \cup \ell) = \mathcal{A}_2 \cap \langle C, D, G\rangle.$$

Obviously the plane $\langle X, C, G\rangle$ does not meet $\mathcal{S}$, and consequently $\mathcal{T}$ does not meet $\mathcal{S}$. We assign the value $\delta_0 - 2$ to each point in $\mathcal{T}$:

$$\gamma(p) = \delta_0 - 2, \quad \forall p \in \mathcal{A}_2 \cap \langle X, C, G\rangle.$$

Now $\gamma(\alpha_i) < \gamma(\ell)$ for all i.

There is one point of value $\delta_0 - 1$ in $\mathcal{A}_3$, namely the point on ℓ. We call this point W, and let V be the point where the line $\langle W, X\rangle$ intersects $\mathcal{A}_2$. We refer to Figure 4.1, and note that $V \in \langle A, F\rangle \setminus \{F\}$, and consequently $V \notin \mathcal{T} \cup \mathcal{S}$. Hence V has no value,

and we can assign a value of $\delta_0 - 3$, so that $\gamma(\langle W, X\rangle) < \gamma(\ell)$:

$$\begin{aligned} W &\in \ell \cap \mathcal{G}_3 \\ V &\in \langle W, X\rangle \cap \mathcal{G}_2 \\ \gamma(V) &= \delta_0 - 3. \end{aligned}$$

This concludes the study of lines through X, that does not intersect $\langle A, B, C\rangle$. Now we turn to lines through X that does intersect $\langle A, B, C\rangle$. In other words, we are to consider the values of points in $\mathcal{A}_1$.

Let $M \neq E$ be a point in $\mathcal{A}_1 \cap \mathcal{P}$.

$$M \in \mathcal{P} \cap \mathcal{A}_1 \setminus \{E\}.$$

Define $\psi := \langle A, B, M\rangle$. We have assigned values to $\{X, Y\} \subset \langle A, E\rangle$ and to $\langle C, E\rangle \subset \mathcal{P}$. The remaining points in $\mathcal{A}_1$ have no value yet. We note that $\langle A, E\rangle \cap \psi = \{A\}$ and $\langle C, E\rangle \cap \psi = \{M\}$. Hence the only points in ψ with assigned values are M and the points on $\langle A, B\rangle$. We assign the value $\delta_0 - 2$ to the remaining points in ψ:

$$\gamma(p) = \delta_0 - 2, \quad \forall p \in \langle A, B, M\rangle \setminus (\langle A, B\rangle \cup \{M\}).$$

Finally consider the line $\langle M, X\rangle$. We have assigned values to M and X, and also to $\langle M, X\rangle \cap \langle A, B, C\rangle$. The remaining points on $\langle M, X\rangle$ have no value, hence there is at least one point $N \in \langle M, X\rangle$ with no value yet. We give it the value $\delta_0 - 2$:

$$\begin{aligned} N &\in \langle M, X\rangle \setminus (\{M, X\} \cup \langle A, B, C\rangle) \\ \gamma(N) &= \delta_0 - 2 \end{aligned}$$

Now consider a line α, such that $X \in \alpha \subset \mathcal{G}_1$. If α meets $\langle A, B\rangle$, it has a point of value $\delta_0 - 3$, and so $\gamma(\alpha) < \gamma(\ell)$. Otherwise α meets $\langle A, B, C\rangle$ in a point of value $\delta_0 - 2$, but then it also meets $\langle A, B, M\rangle$ in some distinct point, ρ. Either $\gamma(\rho) = \delta_0 - 2$, or $\rho = M$, and $N \in \alpha$. In either case α has at least two points of value $\delta_0 - 2$, and consequently $\gamma(\alpha) < \gamma(\ell)$.

The preceding argument proves that for every line, $\alpha \ni X$, $\gamma(\alpha) < \gamma(\ell)$.

4.1.3 Finishing touches

All remaining points get the value $\delta_0 - 1$. We summarise the assignment in Table 4.1. The total value is easily verified by summing the values in the table.

value of p	p in	number of new points
δ_0	$\{X\}$	1
δ_0-3	$\langle A,B\rangle$	$q+1$
δ_0-2	$\langle A,B,C\rangle\backslash\langle A,B\rangle$	q^2
δ_0-1	$\mathcal{A}_0$	q^3
	$\cup_{i\geq 4}\mathcal{A}_i$	$(q-3)q^3$
	$\langle C,D,G\rangle\backslash\langle C,G\rangle$	$2q$
	$\langle F,Y\rangle$	2
	$\mathcal{A}_2\backslash(\{V\}\cup\langle X,C,G\rangle)$	q^3-2q-1
	$\mathcal{A}_1\backslash(\{N\}\cup\langle A,B,M\rangle$	q^3-q^2-q-1
δ_0-2	$\mathcal{A}_2\cap\langle X,C,G\rangle$	q
	$\langle C,G\rangle$	q
	$\langle A,B,M\rangle\backslash(\langle A,B\rangle\cup\{M\})$	q^2-1
	$\{N\}$	1
δ_0-3	$\mathcal{A}_3\backslash(\mathcal{P}\cup\mathcal{\ell})$	q^3-q-1
	$\{V\}$	1

Table 4.1: A projective multiset on $\mathsf{PG}(4,q)$, $q\geq 3$, $\delta_0\geq 3$.

4.2 Verifying the non-chain conditions

4.2.1 The point

The only point of value δ_0 or more is X, so

$$M_0=\{\{X\}\}.$$

4.2.2 Lines

We know that $\gamma(\mathcal{\ell})=(q+1)(\delta_0-1)$. Any line, $\alpha'\not\ni X$, consists of $q+1$ points of value at most δ_0-1, so $\gamma(\alpha')\leq(q+1)(\delta_0-1)=\gamma(\mathcal{\ell})$, with equality if and only if every point on α' has value δ_0-1. In Section 4.1.2, we proved that every line α, containing X have value $\gamma(\alpha)<\gamma(\mathcal{\ell})$. This proves that $\mathcal{\ell}\in M_1$, and (N1.1) follows.

We observe that every line $\mathcal{\ell}'\in M_1$, does not meet $\langle A,B,C\rangle$, because no point in $\langle A,B,C\rangle$ has value δ_0-1. This implies that $\mathcal{\ell}'\not\subset\mathcal{G}_i$ for all i.

There may be several lines of value $\delta_1+\delta_0$, and we don't give any expression for the number of such lines, except that at least one such line exists.

4.2.3 Planes

The study of planes is quite tedious. We will go as far as to prove that $\mathcal{P}$ is the only plane of maximum value. We suppose for a contradiction that $\mathcal{R} \neq \mathcal{P}$ is a plane, such that $\gamma(\mathcal{R}) \geq \gamma(\mathcal{P})$.

First assume that $X \in \mathcal{R}$. We have shown that every line through X, has value at most $(q+1)\delta_0 - q - 2$; and there are $q+1$ such lines in $\mathcal{R}$. Hence

$$\begin{aligned}\gamma(\mathcal{R}) &\leq (q+1)[(q+1)\delta_0 - q - 2 - \delta_0] + \delta_0 \\ &\leq (q^2+q+1)\delta_0 - q^2 - 3q - 2 < \gamma(\mathcal{P}),\end{aligned}$$

contrary to assumption; hence $X \notin \mathcal{R}$. Condition (N1.2) follows immediately.

Suppose that $\mathcal{R} \subset \mathcal{G}_i$ for some i. The intersection $\mathcal{R} \cap \langle A, B, C\rangle$ is a line with one point of value $\delta_0 - 3$, and q points of value at most $\delta_0 - 2$. The remaining q^2 points have value at most $\delta_0 - 1$, since $X \notin \mathcal{R}$. Hence the total value is

$$\gamma(\mathcal{R}) \leq (q^2+q+1)\delta_0 - q^2 - 2q - 3 < \gamma(\mathcal{P}),$$

contrary to assumption. We conclude that $\mathcal{R} \not\subset \mathcal{G}_i$ for all i.

Consider the possibility that $\langle C, G\rangle \subset \mathcal{R}$. All points on $\langle C, G\rangle$ have value $\delta_0 - 2$, so $\gamma(\langle C, G\rangle) = (q+1)\delta_0 - 2q - 2$. There is a point of intersection in $\mathcal{R} \cap \langle A, B, M\rangle$. If $\mathcal{R}$ should meet $\langle A, B\rangle$, $\mathcal{R}$ would be in $\mathcal{G}_3$, which it is not. If $M \in \mathcal{R}$, then $\mathcal{R} = \mathcal{P}$, contrary to assumption. Thus $\mathcal{R}$ meets $\langle A, B, M\rangle$ in a point of value $\delta_0 - 2$. There are $q^2 - 1$ more points in $\mathcal{R} \setminus \langle C, G\rangle$, and since $X \notin \mathcal{R}$, no point has value greater than $\delta_0 - 1$. This gives a total value of $\gamma(\mathcal{R}) \leq (q^2+q+1)\delta_0 - 2q - 3 < \gamma(\mathcal{P})$, which is impossible.

As $\langle C, G\rangle \not\subset \mathcal{R}$, the intersection $\mathcal{R} \cap \mathcal{A}_3$ has at most two points of value $\delta_0 - 2$ or more. One of them may be W, with value $\delta_0 - 1$; and the other may be on the line $\langle C, G\rangle$ and have value $\delta_0 - 2$. Hence

$$\gamma(\mathcal{R} \cap \mathcal{A}_3) \leq q\delta_0 - 3q + 3, \tag{4.1}$$

with equality if and only if $W \in \mathcal{R}$, and $\mathcal{R}$ meets $\langle C, G\rangle$ in a point different from C.

Each of the other affine spaces, $\mathcal{A}_i$ for $i \neq 1$, meet $\mathcal{R}$ in q points of value at most $\delta_0 - 1$. Hence

$$\gamma(\mathcal{R} \cap \mathcal{A}_i) \leq q\delta_0 - q, \quad \forall i \neq 3, \tag{4.2}$$

with equality if and only if every point in $\mathcal{R} \cap \mathcal{A}_i$ has value $\delta_0 - 1$.

Finally $\mathcal{R}$ meets $\langle A, B, C\rangle$ in a point, Ψ, of value at most $\delta_0 - 2$. Thus the total value

$$\gamma(\mathcal{R}) \leq (q^2+q+1)\delta_0 - q^2 - 3q + 1. \tag{4.3}$$

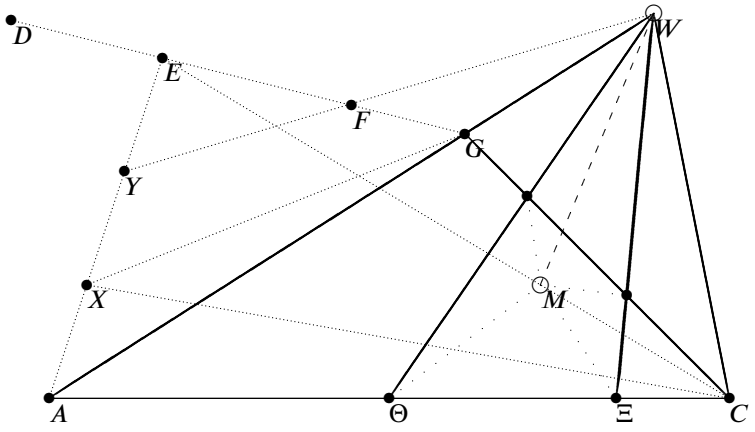


Figure 4.3: There are two choices for $\mathcal{R}$: $\langle M, W, \Xi \rangle$ and $\langle M, W, \Theta \rangle$. The planes $\langle C, G, X \rangle$ and $\mathcal{R}$ meet in a line.

For $q = 3$ this is exactly the value of $\mathcal{P}$, so equality is necessary. For $q \geq 4$, $\gamma(\mathcal{R}) < \gamma(\mathcal{P})$, contrary to assumption. Thus $\mathcal{R}$ can only exist if $q = 3$.

To get equality in (4.3), $\gamma(\Psi) = \delta_0 - 2$, so $\mathcal{R}$ cannot meet $\langle A, B \rangle$. Also all points in $\mathcal{R} \backslash \mathcal{G}_3$ must have value $\delta_0 - 1$, thus the intersection of $\mathcal{R}$ and $\langle A, B, M \rangle$ is M. We also need equality in (4.1), so $W \in \mathcal{R}$, and $\mathcal{R}$ meets $\langle C, G \rangle \backslash \{C\}$. This shows that

$$\langle W, M \rangle \subset \mathcal{R} \subset \langle W, M, C, G \rangle = \langle C, D, G, X \rangle.$$

Let $\Pi_3 := \langle C, D, G, X \rangle$, which is a three-space (see figure 4.3).

We know that $\langle C, G, X \rangle \cap \mathcal{G}_2$ is a line, β, of points of value $\delta_0 - 2$. Both β and $\mathcal{R}$ are in Π_3, so they meet in some point of value $\delta_0 - 2$. However $C \notin \mathcal{R}$, and all points in $\mathcal{R} \cap \mathcal{A}_2$ have value $\delta_0 - 1$, and thus we have a contradiction.

This shows that no other plane has as high value as $\mathcal{P}$, so $M_2 = \{\mathcal{P}\}$. Any line in $\mathcal{P}$ contains a point of value $\delta_0 - 2$, so (N2.2) is satisfied.

4.2.4 Hyperplanes

We have assigned the value $\delta_0 - 1$ to every point in $\mathcal{A}_0$ and in $\mathcal{A}_i$ for $i > 3$. As stated, $\mathcal{G}_0$ has the desired maximum value and so have $\mathcal{G}_i$ for $i > 3$. Each of $\mathcal{A}_1$, $\mathcal{A}_2$, and $\mathcal{A}_3$, have several points of value less than $\delta_0 - 1$ and at most one, namely X, of value higher than $\delta_0 - 1$. Hence $\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3 \notin M_3$.

We will prove that the hyperplanes of maximum values are exactly $\mathcal{G}_0$ and $\mathcal{G}_i$ for $i > 3$. Suppose for a contradiction that there is a hyperplane, $\aleph \neq \mathcal{G}_i$ for any i, such

that $\gamma(\aleph) \geq \gamma(\mathcal{G}_0)$.

First we assume that $X \in \aleph$. We have proved that every line through X has value at most $(q+1)(\delta_0-1)-1$, and $\aleph$ contains q^2+q+1 such lines, and has the value

$$\begin{aligned}\gamma(\aleph) &\leq (q^3+q^2+q)(\delta_0-1)-2(q^2+q+1)+\delta_0\\ &= (q^3+q^2+q+1)\delta_0-(q^3+3q^2+3q+3) < \gamma(\mathcal{G}_0),\end{aligned}$$

contrary to assumption. Thus we conclude that $X \notin \aleph$. Condition (N1.3) follows immediately.

Now $\aleph \cap \mathcal{G}_3$ is a plane, $\alpha \neq \langle A, B, C\rangle$, which intersects $\langle A, B, C\rangle$ in a line with one point of value δ_0-3 and q points of value at most δ_0-2, which gives

$$\gamma(\aleph \cap \langle A, B, C\rangle) \leq (q+1)\delta_0-2q-3. \tag{4.4}$$

Now consider values of points in $\mathcal{A}_3$. Most of the points in $\mathcal{A}_3$ have value δ_0-3. Exceptions are the q points in $(\langle C, G\rangle \setminus \{C\}) \subset \mathcal{P}$ with value δ_0-2, and the point $W \in \ell$ which has value δ_0-1. Thus the intersection $\alpha \cap \mathcal{A}_3$ has at most $q+1$ points of value greater than or equal to δ_0-2, out of which one, W, can have value δ_0-1 and the remaining q points can have value δ_0-2. This gives

$$\gamma(\aleph \cap \mathcal{A}_3) \leq q^2\delta_0-3q^2+q+2. \tag{4.5}$$

There are q^3 points in $\aleph \setminus \mathcal{G}_3$, and since $X \notin \aleph$, all these points have value δ_0-1 or less. Hence

$$\gamma(\aleph \setminus \mathcal{G}_3) \leq q^3(\delta_0-1). \tag{4.6}$$

We sum up equations (4.4), (4.5), and (4.6), to get

$$\gamma(\aleph) \leq \theta(3)\delta_0-q^3-3q^2-q-1 \leq \theta(3)\delta_0-q^3-2q^2-3q-4 < \gamma(\mathcal{G}_0),$$

contrary to assumption.

We conclude that

$$M_3 = \{\mathcal{G}_0, \mathcal{G}_i \mid i > 3\}.$$

We showed in Section 4.2.2, that for every $\ell' \in M_1$, $\ell' \not\subset \mathcal{G}_i$ for all i; hence (N2.3) follows. Obviously $\mathcal{P} \not\subset \mathcal{G}_i$ for all i, and there is no other plane in M_2; this proves (N3.3).

We have proved that all the non-chain conditions hold, so the construction is an ENDS.

5 Optimal ENDS of dimension 6

We recall the upper bounds on δ_1 through δ_4 given by Theorem 3.1, and the bound on $\gamma(\mathsf{PG}(5,q))$ from Corollary 3.4. In this chapter we will give a construction proving the following theorem.

Theorem 5.1
If q is an odd prime power and $\delta_0 \geq 3$, there exists a six-dimensional, q-ary, extremal non-chain code with optimal difference sequence.

Let $(\delta_0, \delta_1, \ldots, \delta_5)$ be the target difference sequence which meets the bounds from Theorem 3.1 and Corollary 3.4 with equality.

5.1 Design

As reference points, we chose six points, A, B, C, D, E, and F, spanning $\mathsf{PG}(5,q)$. Let $G, H \in \langle E, F\rangle$, such that E, F, G, and H are four distinct points. Let $\mathcal{G}_i$, $0 \leq i \leq q$, be the $q+1$ distinct hyperplanes containing $\mathcal{B} := \langle A, B, C, D\rangle$, such that $E \in \mathcal{G}_0$, $F \in \mathcal{G}_1$, $G \in \mathcal{G}_2$, and $H \in \mathcal{G}_3$.

First consider the plane $\langle D, E, F\rangle$ (cf. Figure 5.1), and name the following points therein:

$$
\begin{aligned}
X &\in \langle D, E\rangle \setminus \{D, E\} \\
L &\in \langle D, F\rangle \cap \langle G, X\rangle \\
M &\in \langle D, G\rangle \cap \langle E, L\rangle \\
N &\in \langle D, E\rangle \cap \langle F, M\rangle \\
Q &\in \langle D, G\rangle \cap \langle F, X\rangle.
\end{aligned}
$$

We claim that the named points $D, E, F, G, X, L, M, N, Q$ are all distinct. From the definition it is obvious that the seven first points are distinct, and that $N \neq M$ and $Q \neq X, N$. We also note that Q and M coïncide if and only if N and X do. If this is the case, then there is an embedding $\mathsf{PG}(2,2) \to \langle D, E, F\rangle$ whose image is the seven points $\{D, E, F, G, L, M = Q, N = X\}$. Such an embedding exists if and only if q is a power of 2, which it is not. Hence holds the claim.

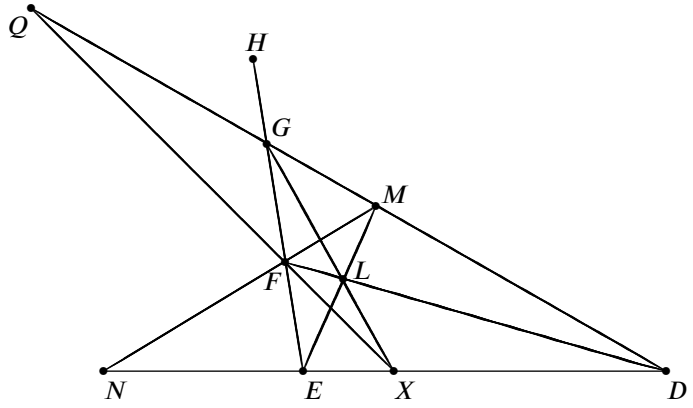


Figure 5.1: The $\langle D, E, F \rangle$ plane.

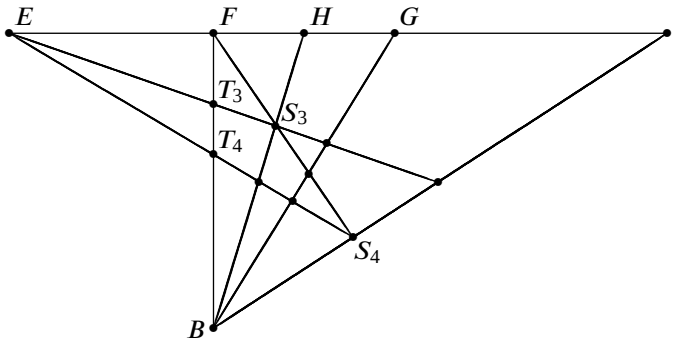


Figure 5.2: The $\langle B, E, F \rangle$ plane. We have $\langle B, S_4 \rangle = \mathcal{G}_4 \cap \langle B, E, F \rangle$. The intersections with $\mathcal{G}_i$ for $i \geq 5$ are not drawn.

Then consider the plane $\langle B, E, F\rangle$ (cf. Figure 5.2). Let

$$\begin{aligned} &T_3 \in \langle B, F\rangle \setminus \{B, F\} \\ &S_3 \in \langle B, H\rangle \cap \langle E, T_3\rangle \\ &S_i \in \langle F, S_3\rangle \cap \mathcal{G}_i, \qquad i = 3, 4, \ldots, q, \\ &T_i \in \langle E, S_i\rangle \cap \langle B, F\rangle, \quad i = 3, 4, \ldots, q. \end{aligned}$$

Finally let

$$K \in \langle A, D\rangle \setminus \{A, D\}.$$

Criterion 1 *We have $\gamma(X) = \delta_0$ and $\gamma(p) \leq \delta_0 - 1$ for all points $p \neq X$.*

Criterion 2 *For all $i \geq 3$, $\mathcal{G}_i$ meets the requirements of Theorem 3.2.*

Corollary 5.1
For all $i \geq 3$, $\gamma(\mathcal{G}_i) = \Delta_4$, and if $\xi \subset \mathcal{G}_i$ is a m-space with $m \leq 3$, then $\gamma(\xi) < \Delta_m$.

We make the following assignments to meet the above criteria:

$$\begin{aligned} &\gamma(X) = \delta_0 \\ &\gamma(p) = \delta_0 - 3, \quad \forall p \in \langle A, B, C\rangle \cup \{D\} \\ &\gamma(p) = \delta_0 - 2, \quad \forall p \in \Big(\langle A, B, C, D\rangle \cup \bigcup_{i=3}^{q} \langle D, S_i\rangle\Big) \setminus (\langle A, B, C\rangle \cup \{D\}) \\ &\gamma(p) = \delta_0 - 1, \quad \forall p \in \bigcup_{i=3}^{q} \mathcal{A}_i \setminus \langle D, S_i\rangle. \end{aligned}$$

Criterion 3 *All lines through X in $\mathcal{G}_0$ have value $(q+1)(\delta_0 - 1) - 1$.*

We assign the following values to meet the above design criterion:

$$\begin{aligned} &\gamma(E) = \delta_0 - 1 \\ &\gamma(p) = \delta_0 - 2, \quad \forall p \in \langle A, B, C, E\rangle \setminus (\langle A, B, C\rangle \cup \{E\}). \\ &\gamma(p) = \delta_0 - 1, \quad \forall p \in \mathcal{G}_0 \setminus (\langle A, B, C, D\rangle \cup \langle A, B, C, E\rangle \cup \{X\}). \end{aligned}$$

Finally assign

$$\begin{aligned}
\gamma(p) &= \delta_0 - 2, \quad \forall p \in \bigcup_{i=3}^{q} \langle D, T_i \rangle \setminus \{D\} \subset \mathcal{A}_1 \\
\gamma(p) &= \delta_0 - 2, \quad \forall p \in \langle K, L \rangle \cup \langle K, G \rangle \subset \mathcal{G}_1 \cup \mathcal{G}_2 \\
\gamma(Q) &= \delta_0 - 3, \quad Q \in \mathcal{A}_2, \\
\gamma(p) &= \delta_0 - 1, \quad \forall p \in \mathcal{A}_2 \setminus (\{Q\} \cup \langle K, G \rangle) \\
\gamma(F) &= \delta_0 - 1, \quad F \in \mathcal{A}_1, \\
\gamma(p) &= \delta_0 - 3, \quad \forall p \in \mathcal{A}_1 \setminus \Big(\langle K, L \rangle \cup \{F\} \cup \bigcup_{i=3}^{q} \langle D, T_i \rangle \Big).
\end{aligned}$$

5.2 Analysis

Lemma 5.1
We have

$$\begin{aligned}
\langle K, L, G \rangle \cap \langle D, S_i, T_i \rangle &= \{X\}, \quad \forall i, s.t.\ 3 \leq i \leq q. \\
\langle K, L, M \rangle \cap \langle D, S_i, T_i \rangle &= \{E\}, \quad \forall i, s.t.\ 3 \leq i \leq q.
\end{aligned}$$

Proof: First we prove that $\langle K, L \rangle \cap \langle D, S_i, T_i \rangle = \emptyset$, which is equivalent to

$$\dim \langle K, L, D, S_i, T_i \rangle = 4.$$

We can see from the definitions that

$$\langle K, L, D, S_i, T_i \rangle = \langle A, D, E, F, T_i \rangle = \langle A, D, E, F, B \rangle.$$

Since A, B, D, E, F are independent by definition, we get the result we want. It follows that the intersections in the lemma are at most one point each.

It is easily seen from Figures 5.1 and 5.2, that $\langle D, S_i, T_i \rangle = \langle D, E, T_i \rangle = \langle X, E, T_i \rangle$. Also $X \in \langle L, G \rangle$ and $E \in \langle L, M \rangle$, and the lemma follows. □

Lemma 5.2
Every line through X has value $(q+1)(\delta_0 - 1) - 1$.

Proof: Consider a line $\ell \ni X$. We have the following possibilities:

1. $\ell \subset \mathcal{G}_0$ in which case the result follows from Criterion 3. Note that

$$\langle K, X \rangle, \langle D, X \rangle \subset \mathcal{G}_0.$$

2. $\ell \subset \langle K, L, G\rangle$ (but $\ell \not\subseteq \mathcal{G}_0$) in which case there are two points $\ell \cap \langle K, L\rangle$ and $\ell \cap \langle K, G\rangle$ of value $\delta_0 - 2$. The remaining points except X have value $\delta_0 - 1$.

3. $\ell \subset \langle D, S_i, T_i\rangle$ for some i (but $\ell \not\subseteq \mathcal{G}_0$), in which case there are two points $\ell \cap \langle D, S_i\rangle$ and $\ell \cap \langle D, T_i\rangle$ of value $\delta_0 - 2$. The remaining points except X have value $\delta_0 - 1$.

4. $\ell = \langle F, Q\rangle$, where $\gamma(Q) = \delta_0 - 3$ and $\gamma(X) = \delta_0$, while the remaining points have value $\delta_0 - 1$.

5. otherwise $\gamma(\ell \cap \mathcal{A}_1) = \delta_0 - 3$, while the remaining points except X has value $\delta_0 - 1$.

□

Proposition 5.1 (Total Value)
We have $\gamma(\mathsf{PG}(k, q)) = \Delta_5$.

Proof: This follows directly from Corollary 3.4 and the above lemma. □

Lemma 5.3
If α *is an* i*-space containing* X *with* $i \geq 1$*, then* $\gamma(\alpha) < \Delta_i$.

Proof: Lemma 5.2 implies that if $\beta \ni X$ is an i-space, then

$$\begin{aligned}\gamma(\beta) &= \theta(i-1)[q\delta_0 - (q+2)] + \delta_0 \\ &= \theta(i)\delta_0 - \theta(i) - 2\theta(i-1) + 1 \\ &< \theta(i)\delta_0 - \sum_{j=1}^{i} \theta(j) = \Delta_i,\end{aligned}$$

as required. □

Lemma 5.4
If for some i, $\alpha \subseteq \mathcal{G}_i$ *is a line, then* $\gamma(\alpha) < \Delta_1$.

Proof: Suppose for a contradiction that $\gamma(\alpha) \geq \Delta_1$. By Lemma 5.3, $X \notin \alpha$. Hence all points in α have value $\delta_0 - 1$ or less. There is at least one point of value $\delta_0 - 2$ in $\alpha \cap \mathcal{B}$, so $\gamma(\alpha) \leq \Delta_1 - 1$. □

Lemma 5.5
If ℓ *is a line, then* $\gamma(\ell) \leq \Delta_1$*, and if* $F \notin \ell$*, then* $\gamma(\ell) < \Delta_1$*. Also* $\gamma(\langle F, N\rangle) = \Delta_1$.

Proof: Let ℓ be a line. If $X \in \ell$, then $\gamma(\ell) < \Delta_i$ by Lemma 5.2. If $X \notin \ell$, all points on ℓ have value at most $\delta_0 - 1$. Hence $\gamma(\ell) \leq \Delta_1$.

Suppose that $\gamma(\ell) = \Delta_1$. Then all points on ℓ has value $\delta_0 - 1$. By Lemma 5.4, we get that $\ell \not\subseteq \mathcal{G}_i$. Hence ℓ meets each of the sets $\mathcal{A}_i$ in one point of value $\delta_0 - 1$. The only such point in $\mathcal{A}_1$ is F, hence $F \in \ell$.

We know that $\langle F, N\rangle \cap \bigcup_{i=0}^{2} \mathcal{G}_i = \{N, F, M\}$, which are points of value $\delta_0 - 1$. It remains to prove that $\langle F, N\rangle$ does not meet $\langle D, S_i\rangle$ for any $i \geq 3$, but $F \in \langle F, N\rangle \cap \langle D, S_3, S_4\rangle$, and N is not in this intersection. Hence $\langle F, N\rangle \cap \langle D, S_3, S_4\rangle = \{F\}$, and $\langle F, N\rangle$ does not meet $\langle D, S_i\rangle$ for any $i \geq 3$. Consequently $\gamma(\langle F, N\rangle) = \Delta_1$. □

Proposition 5.2 (Lines)
The construction satisfies (N0.1), *and δ_0 and δ_1 are the two first elements of its difference sequence.*

Proof: By Criterion 1, δ_0 is the first element of the difference sequence, and by Lemma 5.5, δ_1 is the second one. Condition (N0.1) follows from Lemma 5.3. □

Lemma 5.6
If for some i, $\beta \subseteq \mathcal{G}_i$ is a plane, then $\gamma(\beta) < \Delta_2$.

Proof: Suppose for a contradiction that $\gamma(\beta) \geq \Delta_2$. By Lemma 5.3, $X \notin \beta$. Hence all points in β have value $\delta_0 - 1$ or less.

The intersection $\beta \cap \mathcal{B}$ is at least 1 point of value $\delta_0 - 3$ and at least q points of value $\delta_0 - 2$ or less. Hence

$$\gamma(\beta) \leq q^2(\delta_0 - 1) + q(\delta_0 - 2) + (\delta_0 - 3) = \Delta_2 - 1,$$

as required. □

Lemma 5.7
If β is a plane containing F, then $\gamma(\beta) < \Delta_2$.

Proof: Assume that $\beta \ni F$ is a plane of value $\gamma(\beta) \geq \Delta_2$. We know from previous observations that $X \notin \beta$ and $\beta \not\subseteq \mathcal{G}_i$ for any i. Hence all points on β have value $\delta_0 - 1$ or less, and β meets each of the $\mathcal{A}_i$ in q points. The only point in $\mathcal{G}_1$ of value $\delta_0 - 1$ or more is F, so $\beta \cap \mathcal{G}_1$ contains at least q points of value $\delta_0 - 2$ or less. Because $\gamma(\beta) \geq \Delta_2$, there can be at most one point of value $\delta_0 - 3$ in $\beta \cap \mathcal{G}_1$ or one point of value $\delta_0 - 2$ in $\beta \setminus \mathcal{G}_1$, but not both.

Consider the intersection $\lambda := \beta \cap \mathcal{A}_1$ which contains F. We know that most points in $\mathcal{A}_1$ have value $\delta_0 - 3$, so we consider the exceptions, namely $\langle D, T_i\rangle$, $\langle K, L\rangle$, and F. If λ meets $\langle D, T_i\rangle$ for some i, then it meets $\langle D, T_i\rangle$ for all i, but it does not meet $\langle K, L\rangle$, and thus there is one point of value $\delta_0 - 3$ in λ. If λ meets $\langle K, L\rangle \setminus \{K\}$, there is at least $q - 2 \geq 1$ points of value $\delta_0 - 3$ in λ. If λ meets neither $\langle K, L\rangle \setminus \{K\}$ nor

$\langle D, T_i\rangle$, then it has at least $q-1 \geq 2$ points of value $\delta_0 - 3$. We conclude that $\beta \cap \mathcal{A}_1$ contains a point of value $\delta_0 - 3$.

It follows from above that $\beta \cap \mathcal{A}_1$ meets either $\langle D, T_i\rangle$ or $\langle K, L\rangle \backslash \{K\}$, and that it does not meet D nor $\langle A, B, C\rangle$. Furthermore, all points in $\beta \backslash \mathcal{G}_1$ have value $\delta_0 - 1$.

If $E \notin \beta$, then β meets $\langle A, B, C, E\rangle$ in a point of value $\delta_0 - 2$. Hence $\langle E, F\rangle \subset \beta$. Now, if β meets $\langle D, T_i\rangle$, it also meets $\langle D, S_i\rangle$; and if it meets $\langle K, L\rangle \backslash \{K\}$, it also meets $\langle K, G\rangle \backslash \{K\}$. In either case we have at least one point of value $\delta_0 - 2$ in $\beta \backslash \mathcal{G}_1$, proving the lemma by contradiction. □

Lemma 5.8
If β is a plane, then $\gamma(\beta) \leq \Delta_2$. Also $\gamma(\langle K, L, M\rangle) = \Delta_2$.

Proof: The points on $\langle K, L\rangle$ have value $\delta_0 - 2$. By Lemma 5.1, $\langle K, L, M\rangle \cap \langle D, S_i, T_i\rangle = \langle E\rangle$ for all i; and $\langle K, G\rangle \cap \langle K, L, M\rangle = \{K\}$. We have $\gamma(E) = \delta_0 - 1$. Hence the points in $\langle K, L, M\rangle \backslash \langle K, L\rangle$ have value $\delta_0 - 1$, and $\gamma(\langle K, L, M\rangle) = \Delta_2$.

Suppose $\gamma(\beta) > \Delta_2$. By Lemma 5.3, all points in β have value $\delta_0 - 1$ or less. Also β can have at most q points of value $\delta_0 - 2$ or less, and consequently there is a line $\alpha \subseteq \beta$ with $q+1$ points of value $\delta_0 - 1$. By Lemma 5.5, $F \in \alpha$, but by Lemma 5.7, $F \notin \beta$, which is absurd. □

Proposition 5.3 (Planes)
The construction satisfies (N0.2) *and* (N1.2)*, and the second element of the difference sequence is δ_2.*

Proof: From Proposition 5.2 and Lemma 5.8, we get that δ_2 is the second difference. Lemma 5.3 implies (N0.2), and (N1.2) follows from Lemmata 5.5 and 5.7. □

Lemma 5.9
For a solid $\beta \not\subset \mathcal{G}_i$ for any i, we have $\gamma(\beta) < \Delta_3$.

Proof: We know that the lemma holds if $X \in \beta$, so assume $X \notin \beta$. The intersection $\beta \cap \mathcal{B}$ is a line including one point of value $\delta_0 - 3$ and q points of value $\delta_0 - 2$ or less.

The intersection $\beta \cap \mathcal{A}_1$ contains q^2 points. In $\mathcal{A}_1$ there is one point, F, of value $\delta_0 - 1$. There are $q(q-1)$ points of value $\delta_0 - 2$, they are on $\langle D, T_i\rangle$ for $i \geq 3$ and on $\langle K, G\rangle$. Since $\dim\langle D, T_3, T_4, K, G\rangle = 4$, β cannot contain both $\langle K, G\rangle$ and $\langle D, T_i\rangle$ for all $i \geq 3$. Hence $\beta \cap \mathcal{A}_1$ contains at most $q(q-2)+2$ points of value $\delta_0 - 2$ or more.

It follows that $\beta \cap \mathcal{A}_1$ contains at least $2q-2$ points of value $\delta_0 - 3$, at most one of value $\delta_0 - 1$, and $q^2 - 2q + 1$ of value $\delta_0 - 2$ or less. This gives

$$\begin{aligned} \gamma(\beta \cap \mathcal{A}_1) &\leq q^2\delta_0 - 2q^2 + 4q - 2 - 1 - 6q + 6 \\ &= q^2\delta_0 - 2q^2 - 2q + 3, \end{aligned} \tag{5.1}$$

$$\gamma(\beta \cap \mathcal{B}) \leq (q+1)\delta_0 - 2(q+1) - 1, \tag{5.2}$$

$$\gamma(\beta \backslash \mathcal{G}_1) \leq q^3(\delta_0 - 1). \tag{5.3}$$

We will now prove that we cannot have equality in both (5.2) and (5.3). We know that $\Theta := \langle A, B, C, E\rangle \cap \beta$ is a a line or a plane. If $\Theta \subset \langle A, B, C\rangle$, it gives more than one point of value $\delta_0 - 3$ in $\beta \cap \mathcal{B}$, and equality fails in (5.2). Otherwise $\Theta \cap \mathcal{A}_0$ contains some of the points of value $\delta_0 - 2$ from $\langle A, B, C, E\rangle$, and equality fails in (5.3).

By adding (5.1), (5.2), and (5.3), we get

$$\begin{aligned}\gamma(\beta) &< \theta(3)\delta_0 - q^3 - 2q^2 - 4q \\ &= \theta(3)\delta_0 - \theta(3) + 1 - \theta(2) + 1 - \theta(1) + 1 - q \\ &\leq \Delta_3,\end{aligned}$$

as required. □

Lemma 5.10
If β is a solid, then $\gamma(\beta) \leq \Delta_3$. If $\gamma(\beta) = \Delta_3$, then $\beta \subseteq \mathcal{G}_2$. We have $\gamma(\langle B, C, K, M\rangle) = \Delta_3$.

Proof: First consider some solid β such that $\gamma(\beta) \geq \Delta_3$. By Lemma 5.3, $X \notin \beta$. By Lemma 5.9, $\beta \subset \mathcal{G}_i$ for some i, and by Criterion 2, $i \leq 2$. Since $\gamma(\mathcal{B}) < \Delta_3$, $\beta \cap \mathcal{B}$ is a plane. The highest possible value is obtained if $\beta \backslash \mathcal{B}$ consists of q^3 points of value $\delta_0 - 1$, and $\beta \cap \mathcal{B}$ contains a line of $q+1$ points of value $\delta_0 - 3$ and q^2 points of value $\delta_0 - 2$. This gives exactly the value of Δ_3, so by the assumption this maximum must be attained and $\gamma(\beta) = \Delta_3$.

Thus $\beta \cap \mathcal{B}$ contains q^2 points of value $\delta_0 - 2$. If $i = 0$, then β meets $\langle A, B, C, E\rangle \backslash \mathcal{B}$ in some point of value $\delta_0 - 2$, which is impossible. Also, if $i = 1$, then $\beta \backslash \mathcal{B}$ must contain a point of value $\delta_0 - 3$, and that is impossible as well. Hence $\beta \subset \mathcal{G}_2$.

Now we prove that $\langle B, C, K, M\rangle \subseteq \mathcal{G}_2$ has value Δ_3. The plane $\langle B, C, K\rangle$ is a line $\langle B, C\rangle$ of points of value $\delta_0 - 3$ and q^2 points of value $\delta_0 - 2$. The remaining points are in $\mathcal{A}_2$, and the only points of value $\delta_0 - 2$ or less in $\mathcal{A}_2$ are in $\langle K, G\rangle \cup \{Q\}$. Note that $G, Q \in \langle D, M\rangle$, $M \in \langle B, C, K, M\rangle$, and $D \notin \langle B, C, K, M\rangle$, hence $G, Q \notin \langle B, C, K, M\rangle$. Also $K \in \langle B, C, K, M\rangle$, so $\langle K, G\rangle \cap \langle B, C, K, M\rangle = \{K\}$. Hence the points in $\langle B, C, K, M\rangle \backslash \mathcal{B}$ have value $\delta_0 - 1$ as required. □

Proposition 5.4 (Solids)
The construction satisfies (N0.3), (N1.3), *and* (N2.3)*; and the third element of the difference sequence is δ_3.*

Proof: The third element of the difference sequence follows from Proposition 5.3 and Lemma 5.10. Condition (N0.3) follows from Lemma 5.3. Conditions (N1.3) and (N2.3) follow from the fact that lines and planes of maximum values are not contained in $\mathcal{G}_i$ for any i, while solids of maximum value are. □

Lemma 5.11
Let ξ be a hyperplane such that $\xi \neq \mathcal{G}_i$ for any $i \geq 3$. Then $\gamma(\xi) < \Delta_4$.

Proof: Suppose $\gamma(\xi) \geq \Delta_4$. Due to Lemma 5.3, $X \notin \xi$. All the $\mathcal{G}_i$ contain $\mathcal{B}$, so to prove that $\gamma(\mathcal{G}_i) < \gamma(\mathcal{G}_3)$ for $i = 1, 2$ it suffices to prove $\gamma(\mathcal{A}_i) < \gamma(\mathcal{A}_3)$. However, $\mathcal{A}_3$ contains q points of value $\delta_0 - 2$, while the remaining points have value $\delta_0 - 1$. The set $\mathcal{A}_2$ contains q points of value $\delta_0 - 2$ and one point of value $\delta_0 - 3$, and $\mathcal{A}_1$ contains $q-1$ points of value $\delta_0 - 2$ and one of value $\delta_0 - 1$, while the remaining have value $\delta_0 - 3$. Hence $\xi \neq \mathcal{G}_i$ for any i.

We get that $\xi \cap \mathcal{G}_1$ is a solid Θ. First note that

$$\begin{aligned} \gamma(\Theta \cap \mathcal{B}) &\leq \theta(2)\delta_0 - 2\theta(2) - \theta(1), \\ \gamma(\xi \backslash \Theta) &\leq q^4(\delta_0 - 1). \end{aligned}$$

Thus

$$\gamma(\xi \backslash \mathcal{A}_1) \leq (q^4 + \theta(2))\delta_0 - q^4 - 2\theta(2) - \theta(1).$$

Among the remaining q^3 points, there are at most 1 of value $\delta_0 - 1$ and $q(q-1)$ of value $\delta_0 - 2$. The other points have value $\delta_0 - 3$. Hence

$$\gamma(\xi \cap \mathcal{A}_1) \leq q^3\delta_0 - 3q^3 + q^2 - q + 2.$$

We add the two inequalities to get

$$\begin{aligned} \gamma(\xi) &\leq \theta(4)\delta_0 - \theta(4) - \theta(3) - q^3 + q^2 - 2q + 1 \\ &\leq \theta(4)\delta_0 - \theta(4) - \theta(3) - \theta(2) - \theta(1) - 2q < \Delta_4. \end{aligned}$$

The lemma follows by contradiction. □

Combining this lemma with Corollary 5.1 and the maximum values of points, lines, and planes, we get the following:

Proposition 5.5 (Hyperplanes)
The construction satisfies (N0.4), (N1.4), (N2.4), *and* (N3.4), *and* δ_4 *is the fourth element in the difference sequence.*

Propositions 5.1 through 5.5 state that the construction correspond to an extremal non-chain code with the claimed difference sequence. Theorem 5.1 follows, q.e.d.

6 Binary ENDS

We remember from Chapter 3, several bounds on the differences of extremal non-chain codes. We know from the work of Chen and Kløve [CK99b], that binary, four-dimensional codes must meet stronger bounds. In this chapter we will prove such upper bounds for arbitrary dimension. A five-dimensional code meeting the bounds with equality will be provided in the next chapter.

We start with the general bounds. In Section 6.2 we will prove some special properties for codes meeting the bounds with equality. Finally we establish a lower bound on δ_0 in Section 6.3.

6.1 General bounds

The following is a generalisation of Lemma 1 part ii) from [CK99b], and it gives a stronger bound for the second to the last difference, δ_{k-2}.

Theorem 6.1
If $(\delta_0, \delta_1, \ldots, \delta_{k-1})$, $k \geq 4$, *is a binary ENDS, then*

$$\delta_{k-2} \leq 2^{k-3}\delta_1 - 2 - 2^{k-3}.$$

Proof: Take $\Pi_{k-2} \in M_{k-2}$ and $\Pi_{k-3} \in M_{k-3}$, and let $\Pi_{k-4} := \Pi_{k-2} \cap \Pi_{k-3}$. Because the code is extremal non-chain, Π_{k-4} is a $(k-4)$-space. Also let $\{P\} \in M_0$.

Define

$$\mathcal{S} \stackrel{\text{def}}{=} \Pi_{k-3} \backslash \Pi_{k-4} = \{S_i \mid i = 1, 2, \ldots, 2^{k-3}\},$$
$$\ell_i \stackrel{\text{def}}{=} \langle P, S_i \rangle = \{P, S_i, T_i\}, \quad i = 1, 2, \ldots, 2^{k-3}.$$

Any line through P meets Π_{k-2}, so the points T_i are in Π_{k-2}. Define the set

$$\mathcal{T} \stackrel{\text{def}}{=} \{T_i \mid i = 1, 2, \ldots, 2^{k-3}\}.$$

Because the code is an ENDS, $\gamma(\ell_i) \leq \delta_0 + \delta_1 - 1$, for all i; hence

$$\gamma(T_i) \leq \delta_1 - \gamma(S_i) - 1, \quad i = 1, 2, \ldots 2^{k-3},$$

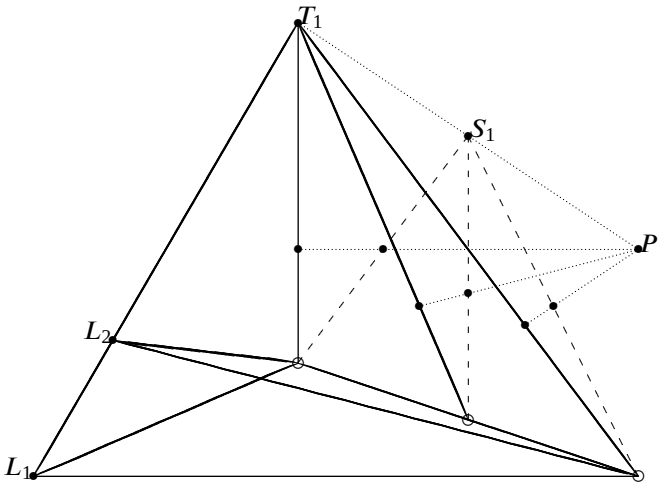


Figure 6.1: Representation of $\mathsf{PG}(4,2)$ for Theorem 6.1. Black lines are in Π_3, dashed lines in Π_2, and dotted lines are in neither. White points are in Π_1. The line Π_1 and L_1 span $\mathcal{L}_1$, and Π_1 and L_2 span $\mathcal{L}_2$.

and

$$\gamma(\mathcal{T}) \leq 2^{k-3}\delta_1 - \gamma(\mathcal{S}) - 2^{k-3}. \tag{6.1}$$

We know that

$$\gamma(\Pi_{k-3}) = \gamma(\mathcal{S}) + \gamma(\Pi_{k-4}) = \sum_{i=0}^{k-3} \delta_i, \tag{6.2}$$

so

$$\gamma(\mathcal{T}) - \gamma(\Pi_{k-4}) \leq 2^{k-3}\delta_1 - 2^{k-3} - \sum_{i=0}^{k-3} \delta_i. \tag{6.3}$$

The join of $\{P\}$ and Π_{k-3} is a prime, intersecting Π_{k-2} in a $(k-3)$-space, namely $\mathcal{T} \cup \Pi_{k-4}$. Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be the other two (distinct) $(k-3)$-spaces, such that $\Pi_{k-4} \subset \mathcal{L}_i \subset \Pi_{k-2}$, for $i = 1, 2$.

Now we have

$$\begin{aligned}\sum_{i=0}^{k-2} \delta_i = \gamma(\Pi_{k-2}) &= \gamma(\mathcal{L}_1) + \gamma(\mathcal{L}_2) - \gamma(\Pi_{k-4}) + \gamma(\mathcal{T}) \\ &\leq 2\left(\sum_{i=0}^{k-3} \delta_i - 1\right) + 2^{k-3}\delta_1 - 2^{k-3} - \sum_{i=0}^{k-3} \delta_i.\end{aligned}$$

This is simplified to

$$\delta_{k-2} \leq 2^{k-3}\delta_1 - 2^{k-3} - 2,$$

and the theorem is proved. □

For the last difference, δ_{k-1}, we use Theorem 3.3, to get a bound expressed in terms of δ_{k-2}. This bound coincides with the one given given for $k = 4$ in [CK99b].

Theorem 6.2
If $(\delta_0, \delta_1, \ldots, \delta_{k-1})$, $k \geq 3$, is a binary ENDS, then

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

Proof: From Theorem 3.3, we have for $m = k-2$,

$$\sum_{i=0}^{k-1} \delta_i \leq \sum_{i=0}^{k-3} \delta_i + \delta_{k-2}(q+1) - (q+1) = \sum_{i=0}^{k-2} \delta_i + 2\delta_{k-2} - 3,$$

and the lemma follows immediately. □

When $k = 5$, we get from Theorems 3.1, 6.1, and 6.2 the following bounds.

$$\begin{aligned}
\delta_1 &\leq 2\delta_0 - 3 \\
\delta_2 &\leq 4\delta_0 - 7 \\
\delta_3 &\leq 4\delta_1 - 6 \\
\delta_4 &\leq 2\delta_3 - 3.
\end{aligned}$$

In the next chapter, we will construct a code meeting all these four bounds with equality.

6.2 Construction requirements

Lemma 6.1
If $(\delta_0, \delta_1, \delta_2, \delta_3, \delta_4)$ is a binary ENDS, and $\delta_1 = 2\delta_0 - 3$ and $\delta_2 = 4\delta_0 - 7$, then for any $\wp \in M_0$, any $\ell \in M_1$, and any $\mathcal{P} \in M_2$, we have:

$$\ell \cap \mathcal{P} = (\ell\wp) \cap \mathcal{P} = \{X\} \in \mathsf{PG}^{(0)}(4,2).$$

Proof: Consider the plane $\ell\wp$. It consists of seven points, one of which has value δ_0 and three of which are on ℓ and hence have value $\delta_0 - 1$. The remaining three points have value at most $\delta_0 - 3$. Any point in $\mathcal{P}$ has value $\delta_0 - 1$ or $\delta_0 - 2$. It follows that $(\ell\wp) \cap \mathcal{P} \subseteq \ell \cap \mathcal{P}$. Since two planes always meet in $\mathsf{PG}(4,2)$, the left hand side is at least one point. The left hand side is at most one point from the non-chain condition, and the lemma follows. □

6.3 Lower bound on δ_0

In practice, our construction of a binary, five-dimensional ENDS requires $\delta_0 \geq 4$, so it is interesting to know if any smaller value for δ_0 is possible. We remember that Chen and Kløve [CK99b] showed that $\delta_0 \geq 5$ for four-dimensional codes, and they did so by first proving lower bounds on the other differences. A complete study of lower bounds is beyond the scope of this thesis, but we introduce two lemmata which will be used to prove that $\delta_0 \geq 4$ for any binary, five-dimensional ENDS.

Lemma 6.2
If $(\delta_0, \delta_1, \delta_2, \delta_3, \delta_4)$ is a binary ENDS, and

$$\lambda = \min\{\gamma(p) \mid p \in \ell\},$$

for some $\ell \in M_1$, then

$$\delta_4 \geq \delta_2 + \delta_0 + 1 + \lambda.$$

Proof: Let $\wp \in M_0$, $\ell \in M_1$, $\mathcal{P} \in M_2$, and $\mathcal{H} \in M_3$ be subspaces of maximum value. We know that $\mathcal{H}$ has value $\delta_0 + \delta_1 + \delta_2 + \delta_3$, and its complement, $\mathcal{H}^{\mathrm{C}}$, has value δ_4.

The intersection $\mathcal{P} \cap \mathcal{H}$ is a line of value at most $\delta_1 + \delta_0 - 1$, so $\gamma(\mathcal{P} \cap \mathcal{H}^{\mathrm{C}}) \geq \delta_2 + 1$. We know that ℓ has two points in $\mathcal{H}^{\mathrm{C}}$, at most one of which may coincide with a point in $\mathcal{P}$, and the other has value at least λ. Finally $\wp \subset \mathcal{H}^{\mathrm{C}}$, so $\delta_4 \geq \delta_2 + \delta_0 + 1 + \lambda$, as required. □

Lemma 6.3
If $(\delta_0, \delta_1, \ldots, \delta_{k-1})$, $k \geq 4$, is a binary ENDS, then

$$\delta_1 \geq 2 \tag{6.4}$$

$$\delta_2 \geq \delta_0 + 1. \tag{6.5}$$

Proof: Assume $\delta_1 = 1$. Let $\wp \in M_0$ be a point of maximum value. Obviously $\wp$ cannot be the only point of positive value, so let $\rho \neq \wp$ be another such point. The line $\wp\rho$ has value at least $\delta_0 + 1 = \delta_1 + \delta_0$, so it is a line of maximum value, and the code is no ENDS. We conclude that $\delta_1 \geq 2$.

Let $\ell \in M_1$ and $\wp \in M_0$ be a line and a point of maximum value. If $\delta_2 \leq \delta_0$, then

$$\gamma(\ell\wp) \geq 2\delta_0 + \delta_1 \geq \delta_2 + \delta_1 + \delta_0,$$

and the code is no ENDS, contrary to assumption. We conclude that $\delta_2 \geq \delta_0 + 1$. □

Theorem 6.3
If $(\delta_0, \delta_1, \delta_2, \delta_3, \delta_4)$ is a binary ENDS, then $\delta_0 \geq 4$.

Proof: We let ℓ and λ be defined as in Lemma 6.2. We have from Theorem 6.2 that

$$\delta_4 \leq 16\delta_0 - 39,$$

and from Lemma 6.2 that

$$\delta_4 \geq \delta_2 + \delta_0 + 1 + \lambda.$$

Combining these inequalities, we have

$$15\delta_0 \geq 40 + \delta_2 + \lambda.$$

This gives

$$\delta_0 \geq 2 + \frac{10 + \delta_2 + \lambda}{15}.$$

So either $\delta_0 \geq 4$, or $\delta_0 = 3$ and $\delta_2 + \lambda \leq 5$.

We consider $\delta_0 = 3$. Then $\delta_2 \geq \delta_0 + 1 = 4$, so that $\lambda \leq 1$. We have upper and lower bounds for the value of ℓ:

$$5 \leq \delta_0 + \delta_1 = \gamma(\ell) \leq 2(\delta_0 - 1) + \lambda = 4 + \lambda \leq 5.$$

It follows that $\delta_1 = 2$ and $\lambda = 1$, and $4 \leq \delta_2 \leq 5 - \lambda = 4$, so $\delta_2 = 4$.

If $\mathcal{P} \in M_2$ is a plane of maximum value, then $\gamma(\mathcal{P}) = \delta_2 + \delta_1 + \delta_0 = 4 + 2 + 3 = 9$. There are seven points in $\mathcal{P}$, so at least one point has value at least $\lceil 9/7 \rceil = 2$, and no point has value more that $\delta_0 - 1 = 2$. We let $P \in \mathcal{P}$ be a point of value 2. There are three lines through P in $\mathcal{P}$, each of which has value at most 4, or otherwise it would be in M_1. Thus the value of $\mathcal{P}$ is at most $3 \cdot 2 + 2 = 8$, which is impossible. Hence $\delta_0 \geq 4$, as required. □

7 Binary Construction

In this chapter we construct a value assignment for a five-dimensional, binary code, with the difference sequence $(4, 5, 9, 14, 25)$, which meets the bounds from Chapter 6 with equality. It is easily verified that by uniformly increasing the values of all points, we can get any value for $\delta_0 \geq 4$, and still meet the bounds with equality.

7.1 The assignment

There are 31 points in $\mathsf{PG}(4, 2)$, and we name them

$$A, B, C, \ldots, Y, Z, \Gamma, \Delta, \Theta, \Lambda, \Xi.$$

The geometry is defined by the list of lines in Table 7.1. All points are shown in Figure 7.1. Figure 7.2 is a simplified version, showing the points treated specially in the text. We note that the five points A, C, G, K and W span $\mathsf{PG}(4, 2)$.

We arbitrarily choose $\mathcal{H} := \langle A, C, G, W \rangle$ as a hyperplane of maximum value, and $\mathcal{P} := \langle A, C, K \rangle$ as a plane of maximum value. We define the hyperplanes $\mathcal{G} := \langle A, C, G, K \rangle$ and $\mathcal{I} := \langle A, C, G, \Delta \rangle$. Thus $\mathcal{P} \subset \mathcal{G}$ and the intersection of the three hyperplanes $\mathcal{G}$, $\mathcal{H}$, and $\mathcal{I}$, is the plane $\langle A, C, G \rangle$.

We let the line of maximum value, ℓ, intersect each of the hyperplanes $\mathcal{G}$, $\mathcal{H}$, and $\mathcal{I}$ in one point. We make sure that it intersects $\mathcal{P}$, and let $\ell := \ell_{95} = \{H, T, \Delta\}$. As a point of maximum value, we choose X which is in $\mathcal{I}$.

Now we assign the following values:

$$\begin{aligned} \gamma(X) &= 4 \\ \gamma(p) &= 3, \quad \forall p \in \ell \\ \gamma(p) &= 2, \quad \forall p \in \langle C, I \rangle \\ \gamma(p) &= 3, \quad \forall p \in \mathcal{P} \setminus \langle C, I \rangle \end{aligned}$$

This gives us sufficient information to limit our search, so that it may feasibly be done by trial and error on a computer. It can be verified that it is extremal non-chain, and that its difference sequence is indeed $(4, 5, 9, 14, 25)$. We summarise the result in the following theorem:

ℓ_i	$\gamma(\ell_i)$	the points
ℓ_0	8	$A(3), B(3), C(2)$
ℓ_1	7	$A(3), D(1), E(3)$
ℓ_2	8	$A(3), F(3), G(2)$
ℓ_3	8	$A(3), H(3), I(2)$
ℓ_4	8	$A(3), J(2), K(3)$
ℓ_5	5	$A(3), L(1), M(1)$
ℓ_6	5	$A(3), N(1), O(1)$
ℓ_7	6	$A(3), P(1), Q(2)$
ℓ_8	6	$A(3), R(2), S(1)$
ℓ_9	8	$A(3), T(3), U(2)$
ℓ_{10}	7	$A(3), V(2), W(2)$
ℓ_{11}	8	$A(3), X(4), Y(1)$
ℓ_{12}	5	$A(3), Z(1), \Gamma(1)$
ℓ_{13}	7	$A(3), \Delta(3), \Theta(1)$
ℓ_{14}	3	$A(3), \Lambda(0), \Xi(0)$
ℓ_{15}	7	$B(3), D(1), F(3)$
ℓ_{16}	8	$B(3), E(3), G(2)$
ℓ_{17}	8	$B(3), H(3), J(2)$
ℓ_{18}	8	$B(3), I(2), K(3)$
ℓ_{19}	5	$B(3), L(1), N(1)$
ℓ_{20}	5	$B(3), M(1), O(1)$
ℓ_{21}	6	$B(3), P(1), R(2)$
ℓ_{22}	6	$B(3), Q(2), S(1)$
ℓ_{23}	8	$B(3), T(3), V(2)$
ℓ_{24}	7	$B(3), U(2), W(2)$
ℓ_{25}	8	$B(3), X(4), Z(1)$
ℓ_{26}	5	$B(3), Y(1), \Gamma(1)$
ℓ_{27}	6	$B(3), \Delta(3), \Lambda(0)$
ℓ_{28}	4	$B(3), \Theta(1), \Xi(0)$
ℓ_{29}	5	$C(2), D(1), G(2)$
ℓ_{30}	8	$C(2), E(3), F(3)$
ℓ_{31}	8	$C(2), H(3), K(3)$
ℓ_{32}	6	$C(2), I(2), J(2)$
ℓ_{33}	4	$C(2), L(1), O(1)$
ℓ_{34}	4	$C(2), M(1), N(1)$
ℓ_{35}	4	$C(2), P(1), S(1)$
ℓ_{36}	6	$C(2), Q(2), R(2)$
ℓ_{37}	7	$C(2), T(3), W(2)$
ℓ_{38}	6	$C(2), U(2), V(2)$

ℓ_i	$\gamma(\ell_i)$	the points
ℓ_{39}	7	$C(2), X(4), \Gamma(1)$
ℓ_{40}	4	$C(2), Y(1), Z(1)$
ℓ_{41}	5	$C(2), \Delta(3), \Xi(0)$
ℓ_{42}	3	$C(2), \Theta(1), \Lambda(0)$
ℓ_{43}	5	$D(1), H(3), L(1)$
ℓ_{44}	4	$D(1), I(2), M(1)$
ℓ_{45}	4	$D(1), J(2), N(1)$
ℓ_{46}	5	$D(1), K(3), O(1)$
ℓ_{47}	5	$D(1), P(1), T(3)$
ℓ_{48}	5	$D(1), Q(2), U(2)$
ℓ_{49}	5	$D(1), R(2), V(2)$
ℓ_{50}	4	$D(1), S(1), W(2)$
ℓ_{51}	8	$D(1), X(4), \Delta(3)$
ℓ_{52}	3	$D(1), Y(1), \Theta(1)$
ℓ_{53}	2	$D(1), Z(1), \Lambda(0)$
ℓ_{54}	2	$D(1), \Gamma(1), \Xi(0)$
ℓ_{55}	7	$E(3), H(3), M(1)$
ℓ_{56}	6	$E(3), I(2), L(1)$
ℓ_{57}	6	$E(3), J(2), O(1)$
ℓ_{58}	7	$E(3), K(3), N(1)$
ℓ_{59}	6	$E(3), P(1), U(2)$
ℓ_{60}	8	$E(3), Q(2), T(3)$
ℓ_{61}	7	$E(3), R(2), W(2)$
ℓ_{62}	6	$E(3), S(1), V(2)$
ℓ_{63}	8	$E(3), X(4), \Theta(1)$
ℓ_{64}	7	$E(3), Y(1), \Delta(3)$
ℓ_{65}	4	$E(3), Z(1), \Xi(0)$
ℓ_{66}	4	$E(3), \Gamma(1), \Lambda(0)$
ℓ_{67}	7	$F(3), H(3), N(1)$
ℓ_{68}	6	$F(3), I(2), O(1)$
ℓ_{69}	6	$F(3), J(2), L(1)$
ℓ_{70}	7	$F(3), K(3), M(1)$
ℓ_{71}	6	$F(3), P(1), V(2)$
ℓ_{72}	7	$F(3), Q(2), W(2)$
ℓ_{73}	8	$F(3), R(2), T(3)$
ℓ_{74}	6	$F(3), S(1), U(2)$
ℓ_{75}	7	$F(3), X(4), \Lambda(0)$
ℓ_{76}	4	$F(3), Y(1), \Xi(0)$
ℓ_{77}	7	$F(3), Z(1), \Delta(3)$

ℓ_i	$\gamma(\ell_i)$	the points
ℓ_{78}	5	$F(3), \Gamma(1), \Theta(1)$
ℓ_{79}	6	$G(2), H(3), O(1)$
ℓ_{80}	5	$G(2), I(2), N(1)$
ℓ_{81}	5	$G(2), J(2), M(1)$
ℓ_{82}	6	$G(2), K(3), L(1)$
ℓ_{83}	5	$G(2), P(1), W(2)$
ℓ_{84}	6	$G(2), Q(2), V(2)$
ℓ_{85}	6	$G(2), R(2), U(2)$
ℓ_{86}	6	$G(2), S(1), T(3)$
ℓ_{87}	6	$G(2), X(4), \Xi(0)$
ℓ_{88}	3	$G(2), Y(1), \Lambda(0)$
ℓ_{89}	4	$G(2), Z(1), \Theta(1)$
ℓ_{90}	6	$G(2), \Gamma(1), \Delta(3)$
ℓ_{91}	8	$H(3), P(1), X(4)$
ℓ_{92}	6	$H(3), Q(2), Y(1)$
ℓ_{93}	6	$H(3), R(2), Z(1)$
ℓ_{94}	5	$H(3), S(1), \Gamma(1)$
ℓ_{95}	9	$H(3), T(3), \Delta(3)$
ℓ_{96}	6	$H(3), U(2), \Theta(1)$
ℓ_{97}	5	$H(3), V(2), \Lambda(0)$
ℓ_{98}	5	$H(3), W(2), \Xi(0)$
ℓ_{99}	4	$I(2), P(1), Y(1)$
ℓ_{100}	8	$I(2), Q(2), X(4)$
ℓ_{101}	5	$I(2), R(2), \Gamma(1)$
ℓ_{102}	4	$I(2), S(1), Z(1)$
ℓ_{103}	6	$I(2), T(3), \Theta(1)$
ℓ_{104}	7	$I(2), U(2), \Delta(3)$
ℓ_{105}	4	$I(2), V(2), \Xi(0)$
ℓ_{106}	4	$I(2), W(2), \Lambda(0)$
ℓ_{107}	4	$J(2), P(1), Z(1)$
ℓ_{108}	5	$J(2), Q(2), \Gamma(1)$
ℓ_{109}	8	$J(2), R(2), X(4)$
ℓ_{110}	4	$J(2), S(1), Y(1)$
ℓ_{111}	5	$J(2), T(3), \Lambda(0)$
ℓ_{112}	4	$J(2), U(2), \Xi(0)$
ℓ_{113}	7	$J(2), V(2), \Delta(3)$
ℓ_{114}	5	$J(2), W(2), \Theta(1)$
ℓ_{115}	5	$K(3), P(1), \Gamma(1)$
ℓ_{116}	6	$K(3), Q(2), Z(1)$

ℓ_i	$\gamma(\ell_i)$	the points
ℓ_{117}	6	$K(3), R(2), Y(1)$
ℓ_{118}	8	$K(3), S(1), X(4)$
ℓ_{119}	6	$K(3), T(3), \Xi(0)$
ℓ_{120}	5	$K(3), U(2), \Lambda(0)$
ℓ_{121}	6	$K(3), V(2), \Theta(1)$
ℓ_{122}	8	$K(3), W(2), \Delta(3)$
ℓ_{123}	5	$L(1), P(1), \Delta(3)$
ℓ_{124}	4	$L(1), Q(2), \Theta(1)$
ℓ_{125}	3	$L(1), R(2), \Lambda(0)$
ℓ_{126}	2	$L(1), S(1), \Xi(0)$
ℓ_{127}	8	$L(1), T(3), X(4)$
ℓ_{128}	4	$L(1), U(2), Y(1)$
ℓ_{129}	4	$L(1), V(2), Z(1)$
ℓ_{130}	4	$L(1), W(2), \Gamma(1)$
ℓ_{131}	3	$M(1), P(1), \Theta(1)$
ℓ_{132}	6	$M(1), Q(2), \Delta(3)$
ℓ_{133}	3	$M(1), R(2), \Xi(0)$
ℓ_{134}	2	$M(1), S(1), \Lambda(0)$
ℓ_{135}	5	$M(1), T(3), Y(1)$
ℓ_{136}	7	$M(1), U(2), X(4)$
ℓ_{137}	4	$M(1), V(2), \Gamma(1)$
ℓ_{138}	4	$M(1), W(2), Z(1)$
ℓ_{139}	2	$N(1), P(1), \Lambda(0)$
ℓ_{140}	3	$N(1), Q(2), \Xi(0)$
ℓ_{141}	6	$N(1), R(2), \Delta(3)$
ℓ_{142}	3	$N(1), S(1), \Theta(1)$
ℓ_{143}	5	$N(1), T(3), Z(1)$
ℓ_{144}	4	$N(1), U(2), \Gamma(1)$
ℓ_{145}	7	$N(1), V(2), X(4)$
ℓ_{146}	4	$N(1), W(2), Y(1)$
ℓ_{147}	2	$O(1), P(1), \Xi(0)$
ℓ_{148}	3	$O(1), Q(2), \Lambda(0)$
ℓ_{149}	4	$O(1), R(2), \Theta(1)$
ℓ_{150}	5	$O(1), S(1), \Delta(3)$
ℓ_{151}	5	$O(1), T(3), \Gamma(1)$
ℓ_{152}	4	$O(1), U(2), Z(1)$
ℓ_{153}	4	$O(1), V(2), Y(1)$
ℓ_{154}	7	$O(1), W(2), X(4)$

Table 7.1: The lines in $\mathsf{PG}(4,2)$, with the value of each point in parenthesis after the point.

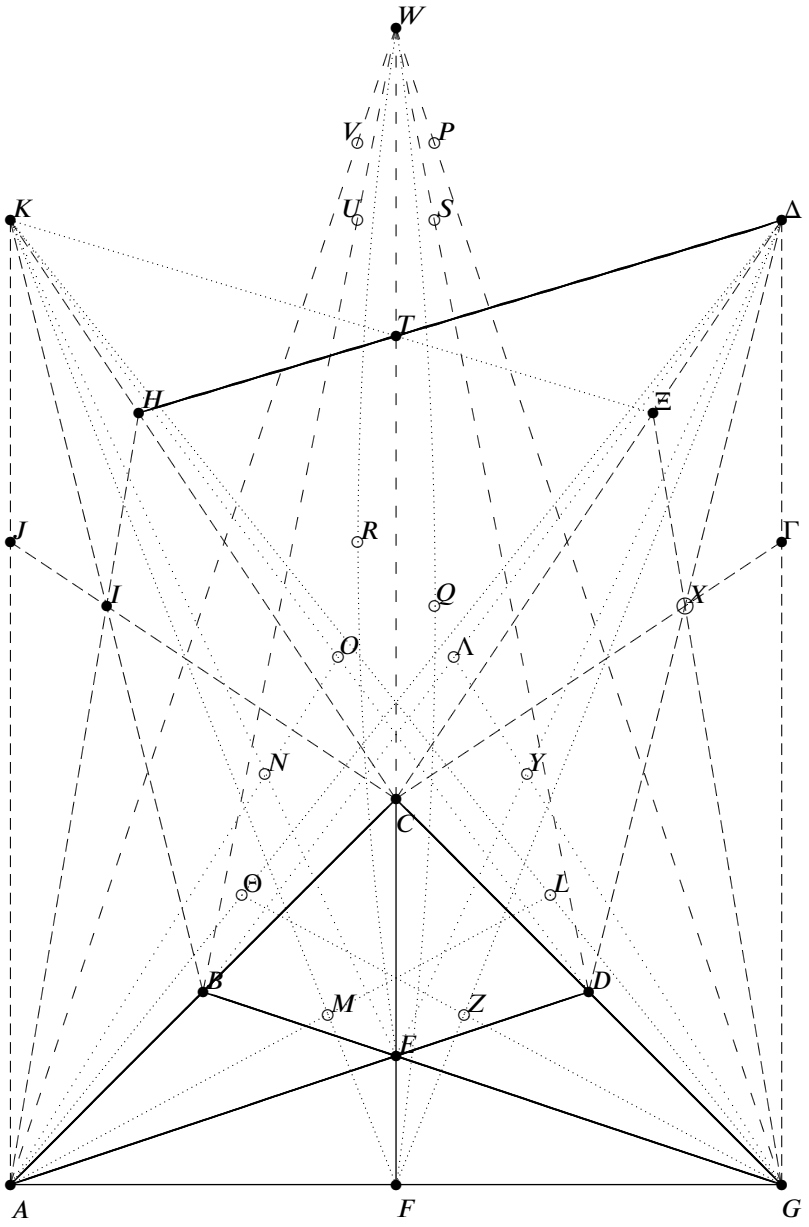


Figure 7.1: Representation of $\mathsf{PG}(4,2)$ for construction.

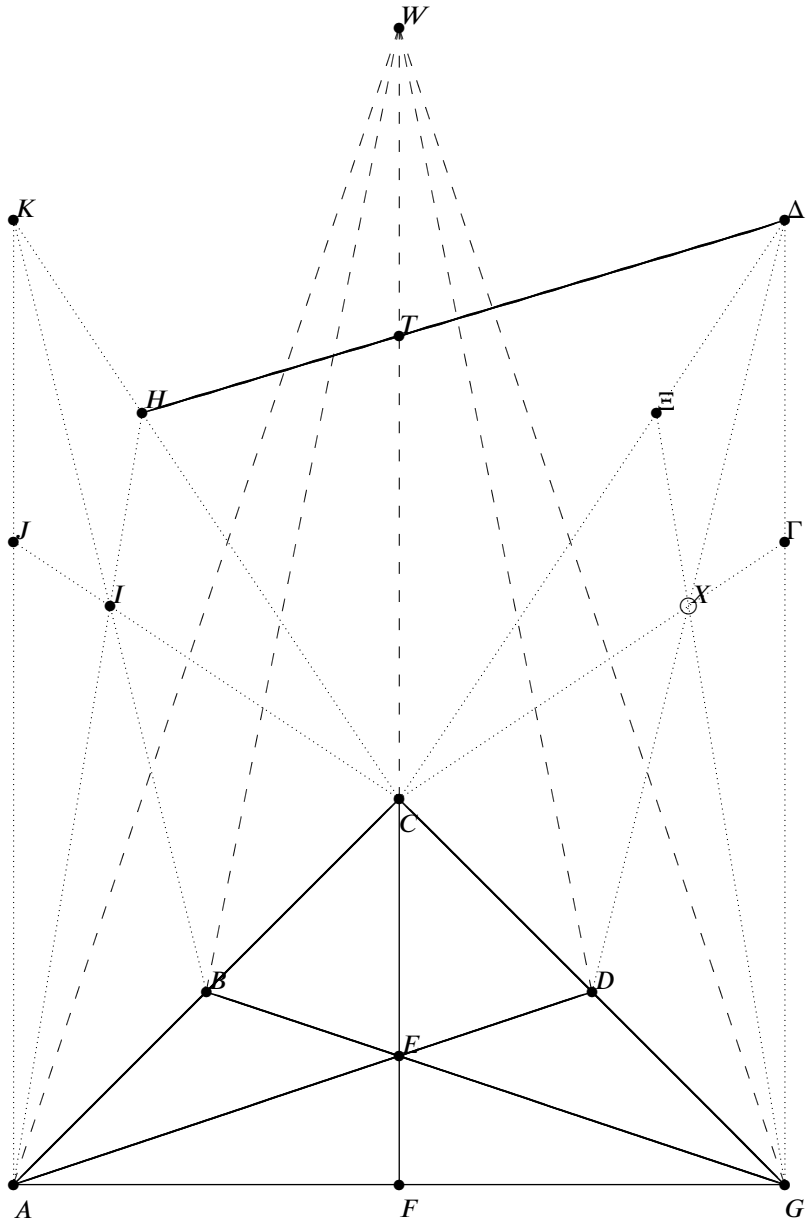


Figure 7.2: Simplified sketch of $\mathsf{PG}(4,2)$ for construction.

$\gamma(A) = 3$	$\gamma(B) = 3$	$\gamma(C) = 2$	$\gamma(D) = 1$	$\gamma(E) = 3$	$\gamma(F) = 3$
$\gamma(G) = 2$	$\gamma(H) = 3$	$\gamma(I) = 2$	$\gamma(J) = 2$	$\gamma(K) = 3$	$\gamma(L) = 1$
$\gamma(M) = 1$	$\gamma(N) = 1$	$\gamma(O) = 1$	$\gamma(P) = 1$	$\gamma(Q) = 2$	$\gamma(R) = 2$
$\gamma(S) = 1$	$\gamma(T) = 3$	$\gamma(U) = 2$	$\gamma(V) = 2$	$\gamma(W) = 2$	$\gamma(X) = 4$
$\gamma(Y) = 1$	$\gamma(Z) = 1$	$\gamma(\Gamma) = 1$	$\gamma(\Delta) = 3$	$\gamma(\Theta) = 1$	$\gamma(\Lambda) = 0$
$\gamma(\Xi) = 0$					

Table 7.2: A value assignment in $\mathsf{PG}(4, 2)$.

Theorem 7.1
If $\delta_0 \geq 4$, there exists a binary, five-dimensional, extremal non-chain code with the difference sequence:

$$\begin{aligned}\delta_1 &= 2\delta_0 - 3\\ \delta_2 &= 4\delta_0 - 7\\ \delta_3 &= 4\delta_1 - 6\\ \delta_4 &= 2\delta_3 - 3.\end{aligned}$$

8 Duality

Consider a code $C \subseteq \mathsf{V}$ and its orthogonal code $C^\perp \subseteq \mathsf{V}$. We write $(d_1, \ldots, d_k)$ for the weight hierarchy of C, and $(d_1^\perp, \ldots, d_{n-k}^\perp)$ for the weight hierarchy of $C^\perp$. Let $\mathcal{B}$ be the set of coordinate vectors for V, and let μ be the natural endomorphism as defined in (2.3). According to Lemma 2.1, the vector multiset corresponding to C, is $\overline{\gamma}_C := \mu(\mathcal{B})$. The topic of this chapter is the relation between $\overline{\gamma}_C$ and $C^\perp$.

Let $B \subseteq \mathcal{B}$. Then $\mu(B)$ is a sub-multiset of $\overline{\gamma}_C$. Every sub-multiset of $\overline{\gamma}_C$ is obtained this way. Obviously $\dim\langle B\rangle = \#B$. Let $D := \langle B\rangle \cap C^\perp$ be the largest subcode of $C^\perp$ contained in $\langle B\rangle$. Then D is the kernel of $\mu|_{\langle B\rangle}$, the restriction of μ to $\langle B\rangle$. Hence

$$\dim\langle \mu(B)\rangle = \dim\langle B\rangle - \dim D. \tag{8.1}$$

Clearly $\#B \geq w(D)$.

With regard to the problem of support weights, we are not interested in arbitrary sub-multisets of $\overline{\gamma}_C$. We are only interested in cross-sections. Therefore, we ask when $\mu(B)$ is a cross-section of $\mu(\mathcal{B})$. This is of course the case if and only if $\mu(B)$ equals the cross-section $\mu(\mathcal{B})|_{\langle\mu(B)\rangle}$.

Let $U \leqq \mathsf{V}/C^\perp$ be a subspace. We have $\mu(\mathcal{B})|_U = \mu(B)$, where $B = \{\mathbf{b} \in \mathcal{B} \mid \mu(\mathbf{b}) \in U\}$. Hence we have $\mu(B) = \mu(\mathcal{B})|_{\langle\mu(B)\rangle}$ if and only if there exists no point $\mathbf{b} \in \mathcal{B}\backslash B$ such that $\mu(\mathbf{b}) \in \langle\mu(B)\rangle$.

It follows from (8.1) that a large cross-section $\mu(B)$ of a given dimension, must be such that $\langle B\rangle$ contains a large subcode of $C^\perp$ of sufficiently small weight.

Define for any subcode $D \subseteq C^\perp$,

$$\beta(D) := \{\mathbf{b}_x \mid x \in \chi(D)\} \subseteq \mathcal{B}. \tag{8.2}$$

Obviously $\beta(D)$ is the smallest subset of $\mathcal{B}$ such that D is contained in its span. It follows from the above argument that if D is a minimum subcode and $\mu(\beta(D))$ is a cross-section, then $\mu(\beta(D))$ is a maximum cross-section for C. Thus we are lead to the following two lemmas.

Lemma 8.1
If $n - d_r = d_i^\perp$, $B \subseteq \mathcal{B}$, and $\#B = n - d_r$, then $\mu(B)$ is a cross-section of maximum size and codimension r if and only $B = \beta(D_i)$ for some minimum i-subcode $D_i \subseteq C^\perp$.

Lemma 8.2
Let r be an arbitrary number, $0 < r \leq n-k$. Let i be such that $d_i^\perp \leq n - d_r < d_{i+1}^\perp$, and let $D_i \subseteq C^\perp$ be a minimum i-subcode. Then $\mu(\langle B \rangle)$ is a maximum r-subspace for any $B \subseteq \mathcal{B}$ such that $D_i \subseteq \langle B \rangle$ and $\#B = n - d_r$.

As an example of our technique, we include two old results from [Wei91, WY93], with new proofs based on the argument above.

Proposition 8.1 (Wei 1991)
The weight sets

$$\{d_1, d_2, \ldots, d_k\} \quad \text{and} \quad \{n+1-d_1^\perp, n+1-d_2^\perp, \ldots, n+1-d_{n-k}^\perp\}$$

are disjoint, and their union is $\{1, 2, \ldots, n\}$.

Proof: Suppose for a contradiction that $d_i = n - s$ and $d_j^\perp = s+1$ for some i, j, and s. Let $D_j \subseteq C^\perp$ be a minimum j-subcode. Let $B_i \subseteq \mathcal{B}$ such that $\mu(B_i)$ is a maximum cross-section of codimension i. We have $\#\beta(D_j) = \#B_i + 1$ and thus $\dim\langle B_i \rangle \cap C^\perp < j$. Hence $\dim \mu(B_i) \geq \dim \mu(\beta(D_j))$. Thus $\mu(B_i)$ cannot be maximum cross-section, contrary to assumption. □

Proposition 8.2 (Wei and Yang 1993)
If a C is a chained code, then so is $C^\perp$, and vice versa.

Proof: Suppose $C^\perp$ is a chained code. We prove that then C is a chained code. The converse follows by duality.

Let

$$\{0\} = D_0 \subset D_1 \subset \ldots \subset D_k = C^\perp$$

be a chain of subcodes of minimum weight. Choose a coordinate ordering, such that

$$\chi(D_i) = \{1, 2, \ldots, d_i^\perp\}, \quad \forall i.$$

For each $r = 1, 2, \ldots, n$, let $B_r \subseteq \mathcal{B}$ be the set of the r first coordinate vectors. By our argument, $\mu(B_r)$ is a cross-section of maximum size except if $d_i^\perp = r+1$ for some i; in which case there is no cross-section of maximum size and r elements. Obviously $\mu(B_r) \subseteq \mu(B_{r+1})$ for all r. □

9 Sub-chains

We have seen that if C is chained, then so is $C^\perp$. In Section 2.5, we saw that the chained codes form but one of numerous classes of codes with respect to the subchain conditions. We also defined B-codes to be codes satisfying all the subchain conditions but not the chain condition. In this chapter we will prove that if C is a B-code, then so is $C^\perp$.

We shall also see that for some i and j we can determine if $C^\perp$ satisfies (C$i.j$) by studying C, but we do not succeed for all i and j.

9.1 Duality relations

Lemma 9.1
If $d_{s-1} = d_s - 1$, then (C$k-1-s.k-s$) *holds. In fact, for any minimum s-subcode D, and any subcode $D' \subset D$ of weight $w(D') \leq d_s - 1$, we can find a minimum $(s-1)$-subcode D'', such that $D' \subseteq D'' \subset D$.*

Proof: Let D and D' be as described. Arbitrarily choose $i \in \chi(D) \backslash \chi(D')$, and define $D'' := \{\mathbf{x} \in D \mid x_i = 0\}$. Clearly $\dim D'' = s-1$, $D' \subseteq D'' \subset D$, and $w(D'') \leq d_s - 1$, which is also the least possible weight. Hence D'' is a minimum $(s-1)$-subcode. □

Corollary 9.1
If $d_{s-i} = d_s - i$ for some s and $i > 1$, then (C$k-1-s.k-1+i-s$) *holds.*

Lemma 9.2
If $d_{k-1-r} = d_k - 1 - r$ where $0 \leq r \leq k-3$, then (C$r.s$) *holds for all s.*

Proof: First observe that $d_{k-1-r'} = d_k - 1 - r'$ for all $r' \leq r$. Let $D_{k-1-s} \subseteq C$ be a minimum $(k-1-s)$-subcode. By Lemma 9.1, we can form a chain

$$D_{k-1-s} \subset D_{k-1-r} \subset D_{k-r} \subset \ldots \subset D_k = C$$

of minimum subcodes, proving the lemma. □

Lemma 9.3
Suppose $C^\perp$ satisfies (N$n-k-1-j.n-k-1-i$) *where $i < j$, $d^\perp_{i+1} > d^\perp_i + 1$, and $d^\perp_{j+1} > d^\perp_j + 1$. Then C satisfies* (N$k-1-r.k-1-s$) *where $d^\perp_i = n - d_r$ and $d^\perp_j = n - d_s$.*

By biduality, the lemma is equivalent to the following remark for which the proof will look a little cleaner.

Remark 9.1
Suppose C satisfies $(\mathrm{N}k-1-j.k-1-i)$ *where* $i<j$, $d_{i+1}>d_i+1$, *and* $d_{j+1}>d_j+1$. *Then* $C^\perp$ *satisfies* $(\mathrm{N}n-k-1-r.n-k-1-s)$ *where* $d_i=n-d_r^\perp$ *and* $d_j=n-d_s^\perp$.

Proof: Since the lemma follows from the remark, we will prove the remark. Because $d_{i+1}>d_i+1$ and $d_{j+1}>d_j+1$, there are r and s such that $d_i=n-d_r^\perp$ and $d_j=n-d_s^\perp$.

Suppose for a contradiction that $C^\perp$ satisfies $(\mathrm{C}n-k-1-r.n-k-1-s)$. Let $D_s\subset D_r\subseteq C^\perp$ be minimum s- and r-subcodes. By Lemma 8.1, $\mu(\beta(D_r))$ and $\mu(\beta(D_s))$ are maximum cross-sections of codimensions i and j respectively, but $\mu(\beta(D_r))\subset\mu(\beta(D_s))$; thus the lemma follows by contradiction. □

Lemma 9.4
If $d_i^\perp=n-d_r$, *then* $r=k+i-d_i^\perp$.

Proof: By Proposition 8.1, we have that

$$\{d_1,\ldots,d_r,n+1-d_{n-k}^\perp,\ldots,n+1-d_i^\perp\}=\{1,2,\ldots,n+1-d_i^\perp\}.$$

Clearly $r+n-k-i+1$ is the cardinality on the left hand side, while $n+1-d_i^\perp$ is the cardinality on the right hand side. Hence $r+n-k-i+1=n+1-d_i^\perp$, and the lemma is proved. □

Proposition 9.1
If $d_{i+1}^\perp>d_i^\perp+1$ *and* $d_{j+1}^\perp>d_j^\perp+1$, *then* $C^\perp$ *satisfies* $(\mathrm{C}n-k-1-j.n-k-1-i)$ *if and only if* C *satisfies* $(\mathrm{C}d_i^\perp-i-1.d_j^\perp-j-1)$.

Proof: The only-if-part follows directly from Lemmata 9.3 and 9.4. The if-part follows by duality. □

Lemma 9.5
Suppose C *satisfies* $(\mathrm{N}k-1-r.k-1-s)$ *for some* r *and* s. *Let* $r''\geq r$ *be the least integer such that* $d_{r''+1}>d_{r''}+1$, *and let* $s''\geq s$ *be the least integer such that* $d_{s''+1}>d_{s''}+1$. *Then* C *also satisfies* $(\mathrm{N}k-1-r'.k-1-s')$ *for all* s' *and* r' *such that* $r\leq r'\leq r''$ *and* $s\leq s'\leq s''$.

Note that by Lemma 9.2, there must exist such an $r''<k$, and by Corollary 9.1 there exists such an $s''<r''$.

Proof: First consider the case where $d_{s+1}=d_s+1$. Suppose for a contradiction that $(\mathrm{C}k-1-r.k-2-s)$ holds. Then there is a minimum r-subcode D and a minimum $(s+1)$-subcode $D'\subset D$. By Lemma 9.1, there is a minimum s-subcode $D''\subset D'\subset D$. Hence $(\mathrm{N}k-1-r.k-2-s)$ holds by contradiction. By iterating the argument, we find that $(\mathrm{N}k-1-r.k-1-s')$ holds for $s'=s,s+1,\ldots,s''$.

Then consider the case where $d_{r+1} = d_r + 1$. Suppose for a contradiction that (C$k-2-r.k-1-s$) holds. Then there is a minimum s-subcode D and a minimum $(r+1)$-subcode $D' \supset D$. By Lemma 9.1, there is a minimum r-subcode D'' such that $D \subset D'' \subset D'$, contradicting (N$k-1-r.k-1-s$). Hence (N$k-2-r.k-1-s$) holds. By iterating the argument we prove (N$k-1-r'.k-1-s$) for $r' = r, r+1, \ldots, r''$.

By combining the two first results, we get that C satisfies (N$k-1-r'.k-1-s'$). □

Corollary 9.2
If C satisfies (C$k-1-r.k-1-s$) *for some r and s. Let $r'' \leq r$ be the greatest integer such that $d_{r''-1} < d_{r''} - 1$, and let $s'' \leq s$ be the greatest integer such that $d_{s''-1} < d_{s''} - 1$. Then C also satisfies* (C$k-1-r'.k-1-s'$) *for all r' and s' such that $r'' \leq r' \leq r$ and $s'' \leq s' \leq s$.*

Theorem 9.1
If C satisfies all the sub-chain conditions, then so does $C^\perp$.

Proof: Suppose for a contradiction that C satisfies all sub-chain conditions, while $C^\perp$ satisfies (N$n-k-1-j.n-k-1-i$) for some i and j. By Lemma 9.5, $C^\perp$ satisfies (N$n-k-1-j'.n-k-1-i'$), where $d^\perp_{i'+1} > d^\perp_{i'} + 1$ and $d^\perp_{j'+1} > d^\perp_{j'} + 1$. By Lemma 9.3, C satisfies (N$k-1-r.k-1-s$) where $d^\perp_{i'} = n - d_r$ and $d^\perp_{j'} = n - d_s$. The lemma follows by contradiction. □

Corollary 9.3
If C is a B-code, then so is $C^\perp$.

9.2 A duality example

In Chapter 7, we learnt that an optimal, binary, extremal non-chain code C has difference sequence $(4, 5, 9, 14, 25)$. This gives a weight hierarchy of $(25, 39, 48, 53, 57)$. The orthogonal code $C^\perp$ has weight hierarchy

$$(2, 3, 4, 6, 7, \ldots, 9, 11, 12, \ldots, 18, 20, 21, \ldots, 32, 34, 35, \ldots, 57),$$

by Proposition 8.1, and its dimension is 52. We will determine the non-chain conditions satisfied by $C^\perp$, cf. Table 9.1.

We observe that $d^\perp_{i+1} > d^\perp_i + 1$ if and only if

$$i \in \{i_0 = 0, i_1 = 3, i_2 = 7, i_3 = 15, i_4 = 28\}.$$

Note that $i_{j+1} = i_j + \delta_j - 1$. We also see that $d^\perp_0 = 0$, $d^\perp_3 = 4$, $d^\perp_7 = 9$, $d^\perp_{15} = 18$, and $d^\perp_{28} = 32$.

i	[0,22]	23	[24,35]	36	[37,43]	44	[45,47]	48	[49,50]	51
d_{k-1-i}	[56,34]	32	[31,20]	18	[17,11]	9	[8,6]	4	[3,2]	0
j										
$[0,22]$	(Y^2)	-	-	-	-	-	-	-	-	-
23	Y^3	-	-	-	-	-	-	-	-	-
$[24,35]$	Y^3	Y^2	(Y^2)	-	-	-	-	-	-	-
36	Y^3	N^1	Y^5	-	-	-	-	-	-	-
$[37,43]$	Y^3		Y^5	Y^2	(Y^2)	-	-	-	-	-
44	Y^3	N^1		N^1		-	-	-	-	-
$[45,47]$	Y^3			Y^4	Y^4	Y^2	(Y^2)	-	-	-
48	Y^3	N^1		N^1		N^1		-	-	-
$[49,50]$	Y^3			Y^4	Y^4	Y^4	Y^4	Y^2	(Y^2)	-
51	-	-	-	-	-	-	-	-	-	-

Table 9.1: The sub-chain conditions satisfied for $C^\perp$. The entry is Y if (C$i.j$) is satisfied. Entry - means that he sub-chain condition is not defined, while an entry in parenthesis means that the sub-chain condition is undefined for some values of i and j.

By Proposition 9.1 we get,

$$
\begin{aligned}
&C^\perp \text{ satisfies } (\mathrm{N}51-i_2.51-i_1) = (\mathrm{N}44.48)\\
&\Longleftarrow C \text{ satisfies } (\mathrm{N}4-3-1.9-7-1) = (\mathrm{N}0.1).\\
&C^\perp \text{ satisfies } (\mathrm{N}51-i_3.51-i_1) = (\mathrm{N}36.48)\\
&\Longleftarrow C \text{ satisfies } (\mathrm{N}4-3-1.18-15-1) = (\mathrm{N}0.2).\\
&C^\perp \text{ satisfies } (\mathrm{N}51-i_4.51-i_1) = (\mathrm{N}23.48)\\
&\Longleftarrow C \text{ satisfies } (\mathrm{N}4-3-1.32-28-1) = (\mathrm{N}0.3).
\end{aligned}
$$

And similarly, $C^\perp$ satisfies (N36.44), (N23.44), and (N23.36). This gives us the entries marked with superscript 1 in Table 9.1.

Now consider an arbitrary pair (r,s) where $0 \le s < r < n-k-1 = 51$ and ask, does $C^\perp$ satisfy (C$51-r.51-s$)?

Define $i_5 := n-k = 52$ for convenience. If $i_j < s < r \le i_{j+1}$, for some $j = 0,1,2,3,4$, then $d^\perp_s - d^\perp_r = s-r$, so (C$51-r.51-s$) holds by Corollary 9.1. In the table, the Y-s marked with a superscript '2' follow. From Lemma 9.2, we get the sub-chain conditions with Y^3 in the table.

To find further entries, we need more knowledge about C. It was found in Corollary 3.1 that any maximum cross-section of dimension 2 has difference sequence $(\delta_0-1,\delta_1,\delta_2+1)$, and a maximum cross-section of dimension 1 has difference sequence (δ_0-1,δ_1+1). Hence if D_2 and D_3 are minimum 2- and 3-subcodes of C,

there are subcodes

$$E_3 \supset D_2, \dim E_3 = 3, w(E_3) = d_3 + 1,$$
$$E_4 \supset D_2, \dim E_4 = 4, w(E_4) = d_4 + 1,$$
$$E'_4 \supset D_3, \dim E'_4 = 4, w(E'_4) = d_4 + 1.$$

Let $\mu^\perp : \mathsf{V} \to \mathsf{V}/C$ be the natural endomorphism, and let β be defined for any subcode $D \subseteq C$ as follows

$$\beta(D) := \{\mathbf{b}_x \mid x \in \chi(D)\} \subseteq \mathcal{B}.$$

(This a straight-forward extension of (8.2).) The cross-sections $\mu^\perp(\beta(D_2)) \subset \mu^\perp(\beta(E_3))$ gives us (C36.45). Similarly, we get (C36.49) and (C44.49). From Corollary 9.2, we get all the Y-s marked with superscript '4'.

Finally consider Theorem 3.3. A 2-space Π_2 of maximum value must be contained in a 3-space Π_3 with value $\delta_0 + \delta_1 + \delta_2 + \delta_3 - 1$. Hence a minimum 2-subcode $D_2 \subset C$ contains a 1-subcode of weight $d_1 + 1$, and for $C^\perp$, we get (C24.36). From Corollary 9.2, we get the Y-s marked with a superscript '5'.

This is as far as we get with the results we have found. Since there are several non-equivalent optimal extremal non-chain codes, the remaining sub-chain conditions may depend on the actual choice of C.

9.3 Bounds on the Difference Sequences

Chen and Kløve have treated the difference sequences of B-codes in several papers. The following proposition is from [CK97b]. Possibly, Corollary 9.3 may be of use in the continuation of their work, but it is difficult since no good bounds have yet been found for dimension $k \geq 5$.

Proposition 9.2 (Chen and Kløve 1997)
Let $(\delta_0, \delta_1, \delta_2, \delta_3)$ be a Case B difference sequence. Then

$$\delta_3 \leq q\delta_2 - (q+1)$$
$$\delta_2 \leq q\delta_1 - (q+1)$$
$$\delta_1 \leq q\delta_0 - (q+1).$$

Lemma 9.6
If $(\delta_0, \ldots, \delta_{k-1})$ is a Case B difference sequence, then $\delta_i \leq q\delta_{i-1}$ for all i.

Proof: Let Π_i be a minimum i-space and Π_{i-2} a minimum $(i-2)$-space such that $\Pi_{i-2} \subset \Pi_i$, where $1 \leq i \leq k-1$. There are $q+1$ $(i-1)$-spaces containing Π_{i-2} in Π_i. Hence

$$\gamma(\Pi_i) \leq (q+1)\delta_{i-1} + \delta_{i-2} + \delta_{i-3} + \ldots + \delta_0, \tag{9.1}$$

and the lemma follows. □

We note that these bounds are considerably weaker than the bounds for $k = 4$ in the proposition. The reason is that for $k = 4$, $\gamma(\Pi_{i-1}) < \delta_0 + \ldots + \delta_{i-1}$, lest the chain condition is satisfied. This holds for $k = 4$ only. If a code satisfies the bounds in Lemma 9.6 with equality for all i, then it is a simplex code and hence satisfies the chain condition.

10 Greedy weights

Cohen, Encheva, and Zémor [CEZ99] have introduced a new set of parameters, which we will call CEZ weights $(g_1, \ldots, g_k)$. The greedy weights $(e_1, \ldots, e_k)$ were introduced by Chen and Kløve [CK99a, CK01a] inspired by the CEZ weights. The second greedy weight coïncides with the second CEZ weight, and it has been studied in detail. Only a little is known about the higher greedy weights.

10.1 The Wire-Tap Channel of Type II

When Wei introduced the weight hierarchy, the prime motivation was the analysis of an application of linear codes to the Wire-Tap Channel of Type II [OW84]. This motivation is useful for presenting the greedy weights as well, even though the impatient reader may go directly to the formal definitions in the next section.

The Wire-Tap Channel of Type II is depicted in Figure 10.1. Alice has k information bits which she wants to send to Bob. She is allowed to use n bits on an error-free channel, but Eve can eavesdrop s bits of her choosing. How can Alice and Bob minimise the information Eve gets from her s channel bits?

Wei [Wei91] analysed one scheme due to Ozarow and Wyner [OW84]. Let C be an $[n, k]$ code. The scheme uses its dual $C^\perp$, which has q^k cosets corresponding to the q^k possible messages. Alice finds the coset corresponding to her message and transmits a random vector from this coset. Bob who reads the entire transmitted message may

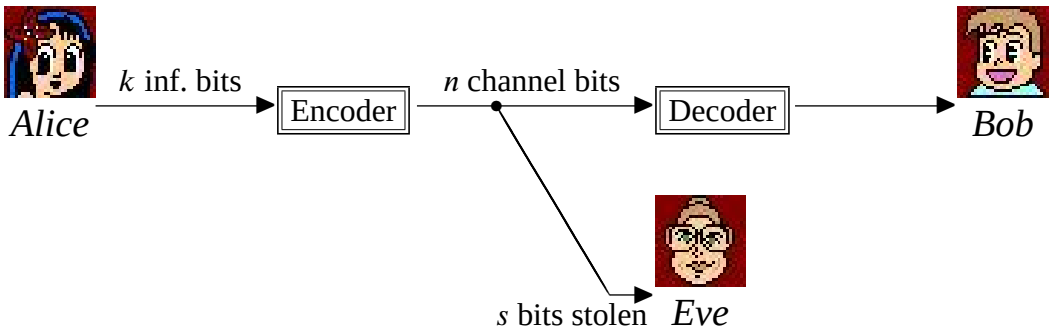


Figure 10.1: The Wire-Tape Channel of Type II.

00	01	10	11
00000	10000	00100	00001
11000	01000	11100	11001
00011	10011	00111	00010
10101	00101	10001	10100
01101	11101	01001	01100
01110	11110	01010	01111
10110	00110	10010	10111
11011	01011	11111	11010

Table 10.1: The four cosets of $C^\perp$ corresponding to four two-bit messages in Example 10.1.

decode. Eve who gets but s bits of the transmitted message gets only part of the information. Wei showed that she could get r bits of information if and only if $d_r(C) \leq s$.

Example 10.1
Let C be defined by the generator matrix

$$G = \begin{bmatrix} 11100 \\ 00111 \end{bmatrix}. \tag{10.1}$$

The $C^\perp$ has generator matrix

$$G^\perp = \begin{bmatrix} 11000 \\ 00011 \\ 10101 \end{bmatrix}. \tag{10.2}$$

The cosets of $C^\perp$ are given in Table 10.1. The weight hierarchy of C is $(3, 5)$. Suppose Alice wants to send the message '01', and randomly chooses the third vector from the coset (Table 10.1) '10011'. If $s = 2$ and Eve reads the first two message bits, she sees '10'. It is easily checked that '10' occurs twice in every coset as the two first bits. Hence Eve gets no information.

Suppose $s = 3$. Then Eve is, according to Wei, able to get one bit of information. This can be achieved by reading the three first bits, containing '100', and then Eve can observe that only '10' and '01' are possible messages, giving her one bit of information as expected.

If however, Eve opts to read the first, second, and fourth bits, then she gets no information at all. These bits read '101' which may correspond to the third vector corresponding to '01' or to the seventh vector corresponding to '00', '10', or '11'.

The fact that these three bits contain no information can also be seen from the fact that there exists no codeword $\mathbf{c} \in C$ *such that* $\chi(\mathbf{c}) \subseteq \{1,2,4\}$.

No matter if we consider the Wire-Tap Channel II to be a useful communication model or not, the analysis of it does teach us something about codes. The entropy in some set S of bits in C corresponds in a way to the maximum size of a subcode of $C^\perp$ with support contained in C. This is the correspondence exploited in the analysis of trellis complexity [FKLT93, For94b]. A formalised description in terms of entropy appears in [RB98, RB99], which considered trellis complexity in the non-linear case.

The greedy weights as defined by Chen and Kløve arise from the analysis of a greedy adversary. Suppose it takes a significant amount of time for Eve to eavesdrop each bit, and that her prime concern is to get at least one bit as soon as possible. Then she will first read some $d_1(C)$ bits required to get one bit of information. Then she will look how she can get a second bit of information. It is not certain that she can get this bit by eavesdropping only $d_2(C) - d_1(C)$ bits. If C satisfies the chain condition, then $d_2(C) - d_1(C)$ bits will suffice, otherwise more bits may be required.

The r-th greedy weight $e_r(C)$ can be defined as the number of bits required to get r bits of information by a greedy adversary. We give an equivalent and more abstract definition of greedy weights in the next section.

10.2 Definitions

Definition 10.1 (Greedy r-subcode)
A (bottom-up) greedy 1*-subcode is a minimum 1-subcode. A (bottom-up) greedy* r*-subcode,* $r \geq 2$*, is any* r*-dimensional subcode containing a (bottom-up) greedy* $(r-1)$*-subcode, such that no other such code has lower weight.*

Definition 10.2 (Greedy subspace)
Given a vector multiset $\overline{\gamma}$*, a (bottom-up) greedy hyperplane is a hyperplane of maximum value. A (bottom-up) greedy space of codimension* r*,* $r \geq 1$*, is a subspace of codimension* r *contained in a (bottom-up) greedy space of codimension* $r-1$*, such that no other such subspace has higher value.*

A greedy r-subcode corresponds to a greedy subspace of codimension r, and the r-th greedy weight may be defined from either, as follows.

Definition 10.3 (Greedy weights)
The r*th (bottom-up) greedy weight* e_r *is the weight of a (bottom-up) greedy* r*-subcode. For a vector multiset,* $n - e_r$ *is the value of a (bottom-up) greedy space of codimension* r*.*

The definition of greedy weights are inspired by the CEZ weights g_r defined in [CEZ99].

Definition 10.4 (CEZ r-subcode)
A CEZ r-subcode, $r \geq 1$, is an r-dimensional subcode containing a minimum $(r-1)$-subcode, such that no other such code has lower weight.

Definition 10.5 (CEZ weights)
The rth CEZ weight, g_r, is the weight of a CEZ r-subcode.

Remark 10.1
We have obviously that $d_1 = g_1 = e_1$, $g_2 = e_2$ and $d_k = g_k = e_k$, for any k-dimensional code. For most codes $e_2 = g_2 > d_2$ [CEZ99]. The chain condition is satisfied if and only if $e_r = d_r$ for all r.

The only paper we have found on CEZ weights is [CEZ99], and only the second weight $g_2 = e_2$ was studied. The main result of [CEZ99] was the proof that almost all codes are non-chain, a fact which was obtained by proving a Gilbert-Varshamov type bound on g_2 and showing that it differs from a similar bound on d_2.

We introduce a third set of parameters, the top-down greedy weights. It is in a sense the dual of the greedy weights, and we will see later that top-down greedy weights can be computed from the greedy weights of the orthogonal code, and vice versa.

Definition 10.6 (Top-Down Greedy Subspace)
A top-down greedy 0-space of a vector multiset is $\{0\}$. A top-down greedy r-space is an r-space containing a top-down greedy $(r-1)$-subspace such that no other such subspace has higher value.

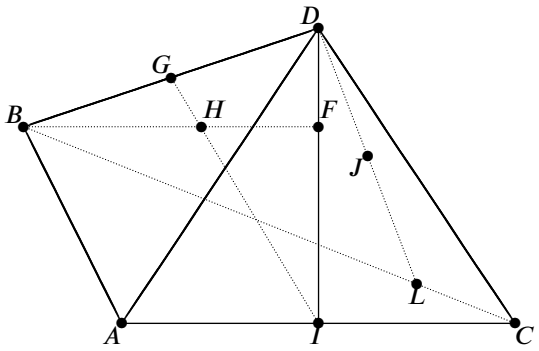
Definition 10.7 (Top-Down Greedy Weights)
The r-th top-down greedy weight $\tilde{e}_r$ is $n - \overline{\gamma}_C(\Pi)$, where Π is a top-down greedy subspace of codimension r.

We will occasionally speak of (top-down) greedy cross-sections, which is just $\overline{\gamma}_C|_U$ for some (top-down) greedy space U.

Remark 10.2
The top-down greedy weights share many properties with the (bottom-up) greedy weights. For all codes $\tilde{e}_r \geq d_r$. The chain condition holds if and only if $\tilde{e}_r = d_r$ for all r.

Example 10.2
We take an example of a B-code from [CK97b]. The projective multiset is presented in Figure 10.2. A chain of greedy subspaces is

$$\emptyset \subset \langle A \rangle \subset \langle A, L \rangle \subset \langle A, B, C \rangle \subset \mathsf{PG}(4, q),$$



$\gamma(p) =$	for
0	$p \in \langle A, B, C\rangle \setminus \{A, D\}$, $p \in \{F, H, I, J\}$
1	$p \in \langle B, F\rangle \setminus \{B, F, H\}$, $p \in \langle G, I\rangle \setminus \{G, H, I\}$, $p = D$
3	$p = C$
2	otherwise

Figure 10.2: Case B, Construction 1 in $\mathsf{PG}(3, q)$ from [CK97b].

and a chain of top-down greedy subspaces is

$$\emptyset \subset \langle C\rangle \subset \langle C, D\rangle \subset \langle A, C, D\rangle \subset \mathsf{PG}(4, q).$$

In the binary case, we get greedy weights $(4, 6, 9, 12)$*, and top-down greedy weights* $(3, 6, 10, 12)$*. The weight hierarchy is* $(3, 6, 9, 12)$.

10.3 Basic properties

Theorem 10.1 (Monotonicity)
If $(e_1, e_2, \ldots, e_k)$ *are greedy weights for some code* C*, then* $0 = e_0 < e_1 < e_2 < \ldots < e_k$*. Similarly, if* $(\tilde{e}_1, \tilde{e}_2, \ldots, \tilde{e}_k)$ *are top-down greedy weights for some code* C*, then* $0 = \tilde{e}_0 < \tilde{e}_1 < \tilde{e}_2 < \ldots < \tilde{e}_k$.

Proof: Let

$$\{0\} = \Pi_0 \subset \Pi_1 \subset \ldots \subset \Pi_k = \mathsf{M},$$

be a chain of greedy subspaces. We are going to show that $\overline{\gamma}_C|_{\Pi_i}$ contains more points than $\overline{\gamma}_C|_{\Pi_{i-1}}$ for all i. It is sufficient to show that $\overline{\gamma}_C|_{\Pi_i}$ contains a set of points spanning Π_i.

Since $\overline{\gamma}_C$ is non-degenerate, it contains a set of points spanning Π_k. Suppose for a contradiction that $\overline{\gamma}_C|_{\Pi_{i-1}}$ is degenerate for some i, and let r be the largest such i. Then $\overline{\gamma}_C|_{\Pi_r}$ contains a set of points spanning Π_r, and there is a point $x \in \overline{\gamma}_C|_{\Pi_r} - \overline{\gamma}_C|_{\Pi_{r-1}}$. Hence we can replace Π_{r-1} by $\langle \overline{\gamma}_C|_{\Pi_{r-1}}, x\rangle$ and get a subspace $\Pi'_{r-1} \subset \Pi_r$ with larger value. This contradicts the assumption that Π_{r-1} is a greedy subspace.

We can replace the Π_i with a chain of top-down greedy subspaces, and repeat the proof to prove the second statement of the lemma. □

Monotonicity also holds for the weight hierarchy by a similar argument [Wei91], but in general it does not hold for the CEZ weights.

Example 10.3
Consider the $[16, 4; 5]_2$ *code defined by the following generator matrix*

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

The weight hierarchy of the code is $(5, 9, 11, 16)$, *the greedy weights are* $(5, 11, 14, 16)$, *and the top-down greedy weights are* $(6, 9, 11, 16)$.

We can see that the fourth row generates a minimum one-subcode of weight 5. The first three rows generates a chained code with weight hierarchy $(6, 9, 11)$, *and this is also a CEZ 3-subcode. A CEZ 2-subcode is generated by the fourth and first rows, and has weight 11. Hence* $g_2 = g_3 = 11$.

In general the rth CEZ weight may be less than, equal to, or greater than the rth greedy weight. For a chained code $e_r = g_r$. For a B-code, $d_r = g_r$ for all r, but $e_r > g_r = d_r$ for some r. In the following example, $g_3 > e_3$.

Example 10.4
A binary code with $g_3 > e_3$ *is given by the generator matrix*

$$G = \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix},$$

where

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix},$$

$$G_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

The code given by G_1 *satisfies the chain condition and has weight hierarchy* $(6, 12, 16)$, *while* G_2 *gives a chained code with* $(7, 11, 17)$ *as a weight hierarchy.*

The code given by G *has weight hierarchy* $(6, 11, 16, 23, 27, 33)$. *The greedy weights differs from the weight hierarchy only in* $e_2 = 12$, *and the CEZ weights differs from the greedy weights only in* $g_3 = 17 > e_3 = d_3 = 16$.

10.4 Duality

By using the approach presented in Chapter 8, we will find duality results on the greedy weights. Let C be a code with top down greedy weights $(\tilde{e}_1, \ldots, \tilde{e}_{n-k})$, and let $(e_1^\perp, \ldots, e_k^\perp)$ be the bottom-up greedy weights of the dual code $C^\perp$. We start by making a top-down greedy analogue of Lemma 8.1.

Lemma 10.1
If $\tilde{e}_{s+1} > \tilde{e}_s + 1$ where $0 \leq s \leq k-1$ and $s = k + i - e_i^\perp$, then

1. *U is a top-down greedy subspace of codimension s of γ_C if and only if $U = \mu(\beta(D_i))$ for some greedy i-subcode $D_i \subseteq C^\perp$.*
2. *$\tilde{e}_s = n - e_i^\perp$.*

Proof: Let $\bar{s}$ be the largest value of $s \leq k-1$ such that $\tilde{e}_{s+1} > \tilde{e}_s + 1$. Then $\delta_j = 1$ for $0 \leq j \leq k-2-\bar{s}$. It follows that any subset B_j of $j \leq k-1-\bar{s}$ elements, gives rise to a top-down greedy cross-section $\mu(B_j)$ of dimension j (and size j). The codimension of such a $\mu(B_j)$ is $k-j \geq \bar{s}+1$, and $\langle B_j \rangle \cap C^\perp = \emptyset$.

Hence $\mu(B_{k-\bar{s}})$ is a top-down greedy cross-section of codimension $\bar{s}$, if and only if it is a maximum value cross-section of codimension $\bar{s}$. And thus there must be a minimum $\bar{i}$-subcode $D_{\bar{i}} = \langle B_{k-\bar{s}} \rangle \cap C^\perp$ where

$$d_s = \tilde{e}_s = n - e_{\bar{i}}^\perp = n - d_{\bar{i}}^\perp,$$

by Lemma 8.1 and Proposition 8.1. By Lemma 9.4, we get that $\bar{s} = k + \bar{i} - e_{\bar{i}}^\perp$; and the lemma follows for $s = \bar{s}$.

Suppose $\tilde{e}_{m+1} > \tilde{e}_m + 1$, and assume the lemma holds for all $s > m$. We will prove the lemma by induction. Define

$$t := \min\{t > m \mid \tilde{e}_{t+1} > \tilde{e}_t + 1\}.$$

Now consider a top-down greedy cross-section $\mu(B)$ of codimension m, where $B \subseteq \mathcal{B}$. Clearly there is $B' \subset B$ such that $\mu(B')$ is a top-down greedy subspace of codimension t. By the induction hypothesis, $B' = \beta(D_j)$ for some greedy j-subcode $D_j \subseteq C^\perp$ where $t = k - e_j^\perp + j$, and

$$\#B' = w(D_j) = e_j^\perp = n - \tilde{e}_t.$$

Note that we can make top-down greedy cross-sections of codimension x for $m < x \leq t$ by adding $t - x$ random elements b_y to B'. This implies also that there cannot be a subcode D_{j+1} of dimension $j+1$ such that $D_j \subset D_{j+1} \subseteq C$ and $w(D_{j+1}) \leq w(D_j) + 1 + t - x$. Hence

$$e_{j+1}^\perp \geq e_j^\perp + 1 + t - m = n - \tilde{e}_t + 1 + t - m. \tag{10.3}$$

Let $B'' = B_{k-(m+1)} \subseteq \mathcal{B}$ be such that $\mu(B'')$ is a top-down greedy cross-section of codimension $m+1$ with $B' \subset B'' \subset B$. Note that $D_j = \langle B'' \rangle \cap C^\perp$.

Let

$$z := \#B - \#B'' = (n - \tilde{e}_m) - (n - \tilde{e}_{m+1}) = \tilde{e}_{m+1} - \tilde{e}_m \geq 2. \tag{10.4}$$

Write $D := \langle B \rangle \cap C^\perp$. Since $\dim \mu(B) - \dim \mu(B'') = 1$, we must have $B = \beta(D)$, and there must be a chain of z subcodes

$$D_j \subset D_{j+1} \subset D_{j+2} \subset \ldots \subset D_{j+z-1} = D$$

where D_l has dimension l for $j \leq l < j+z$ and $w(D_l) = w(D_{l+1}) - 1$ for $j < l \leq j+z-2$. Moreover, by the bound (10.3), we get

$$w(D) = w(D_{j+z-1}) = n - \tilde{e}_t + t - m + z - 1 = e^\perp_{j+z-1}. \tag{10.5}$$

Thus we conclude that a maximum cross-section of codimension m is given as $\mu(\beta(D))$ where $D \subseteq C^\perp$ is a minimum i-subcode where $i = j+z-1$. To prove the lemma by induction, it remains to show that $m = k + i - e^\perp_i$. Since $w(D) = \#B$, we have $e^\perp_i = n - \tilde{e}_m$, so we get from (10.5) that

$$\begin{aligned} m &= n - e^\perp_i - \tilde{e}_t + t + z - 1 \\ &= n - e^\perp_i - \tilde{e}_t + k - e^\perp_j + j + z - 1 \\ &= -e^\perp_i + k + j + z - 1, \end{aligned}$$

as required. □

Theorem 10.2 (Duality)
Let $(\tilde{e}_1, \ldots, \tilde{e}_k)$ be the greedy weight hierarchy of a code C, and $(e^\perp_1, \ldots, e^\perp_{n-k})$ the top-down greedy weight hierarchies for $C^\perp$. Then

$$\{\tilde{e}_1, \tilde{e}_2, \ldots, \tilde{e}_k\} \quad \textit{and} \quad \{n+1-e^\perp_1, n+1-e^\perp_2, \ldots, n+1-e^\perp_{n-k}\}$$

are disjoint sets whose union is $\{1, \ldots n\}$.

Proof: Let $s_1 < s_2 < \ldots$ be the values of s for which $\tilde{e}_{s+1} > \tilde{e}_s + 1$. We have directly from Lemma 10.1, that there is i_x such that $n - \tilde{e}_{s_x} = e^\perp_{i_x}$ for each x, and $i_x > i_{x+1}$. By inspecting the proof of the lemma, with $t = s_{x+1}$ and $m = s_x$, we get $j = i_{x+1}$ and $i = i_x$. The subcodes $D_j, \ldots, D_i$ are minimum subcodes, and the top-down greedy cross-section $\mu(B'')$ of codimension $s_x + 1$ must have size $n - \tilde{e}_{s_x+1} \leq w(D_{j+1}) - 2 = e^\perp_{i_{x+1}+1} - 2$. Hence, for $s_{x+1} \geq s > s_x$, we have that $n - \tilde{e}_s + 1 < e^\perp_i$ for $i > i_{x+1}$ and $n - \tilde{e}_s + 1 > e^\perp_i$ for $i \leq i_{x+1}$. This holds for all x, hence the lemma. □

Since the CEZ weights does not form a monotonous sequence in general, an analogue of Theorem 10.2 would not make sense for CEZ weights.

10.5 Bounds on greedy weights

It is known that for any chained code, $d_r - d_{r-1} \leq q(d_{r+1} - d_r)$. The same relation holds for the top-down and bottom-up greedy weights of arbitrary codes.

Proposition 10.1
For any sequence of bottom-up greedy weights $(e_1, \ldots e_k)$ *or top-down greedy weights* $(\tilde{e}_1, \ldots, \tilde{e}_k)$*, we have*

$$e_r - e_{r-1} \leq q(e_{r+1} - e_r),$$
$$\tilde{e}_r - \tilde{e}_{r-1} \leq q(\tilde{e}_{r+1} - \tilde{e}_r),$$

for $1 \leq r < k$.

Proof: Let $\Pi_{r+1} \subset \Pi_r \subset \Pi_{r-1}$ be a chain of greedy subspaces of codimensions $r+1$, r, and $r-1$ respectively. Clearly $\gamma_C(\Pi_{r-1} \setminus \Pi_r) = e_r - e_{r-1}$ and $\gamma_C(\Pi_r \setminus \Pi_{r+1}) = e_{r+1} - e_r$.

There are q subspaces containing Π_{r+1} in Π_{r-1} in addition to Π_r, and each of them has value at most e_r. Hence $e_{r+1} - e_r \leq q(e_r - e_{r-1})$.

The proof for the top-down greedy weights is similar. □

The following is another analogue of known results on weight hierarchies of chained codes.

Proposition 10.2
Any set $(e_1, e_2, \ldots e_k)$ *of greedy weights can be split for any* i, $1 \leq i < k$, *into two sets of greedy weights,* $(e_1, \ldots e_i)$ *and* $(e_{i+1} - e_i, e_{i+2} - e_i, \ldots e_k - e_i)$.

Proof: Let C be a code with greedy weights $(e_1, e_2, \ldots e_k)$, and let

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

be a chain of greedy subcodes. The subcode D_i is an $[e_i, i]$ code with greedy weights $(e_1, \ldots e_i)$.

If C is punctured on $\chi(D_i)$, we get an $[e_k - e_i, k - i]$ code with greedy weights $(e_{i+1} - e_i, e_{i+2} - e_i, \ldots e_k - e_i)$. □

Remark 10.3
Also the top-down greedy weights have the property described by Proposition 10.2. The proof is similar.

11 Support weight distributions

Support weight distributions are probably the first parameters to be introduced concerning support weights of subcodes of dimension greater than one [HKM77]. We shall define the concept shortly and present a way to compute some of the higher order support weight distributions.

11.1 Definitions

Let $\mathfrak{V}_i^r(C)$ be the set of all r-spaces of value i, i.e.

$$\mathfrak{V}_i^r(C) = \{\Pi \leqq \mathsf{PG}(k-1,q) \mid \gamma_C(\Pi) = i, \dim \Pi = r\}.$$

We define the *value distribution* of γ_C to be

$$V_i^r(\gamma_C) = V_i^r(C) := \#\mathfrak{V}_i^r(C). \tag{11.1}$$

Let $\mathfrak{A}_i^r(C)$ be the set of r-dimensional subcodes of C with weight i. The support weight distribution of C is given by

$$A_i^r(C) := \#\mathfrak{A}_i^r(C).$$

By Lemma 2.2, there is a one-to-one correspondence between $\mathfrak{V}_i^r(C)$ and $\mathfrak{A}_{n-i}^{k-1-r}(C)$. Hence

$$V_i^r(\gamma_C) = V_i^r(C) = A_{n-i}^{k-1-r}(C).$$

We will mostly abbreviate and write $V_i^r = V_i^r(C)$, $A_i^r = A_i^r(C)$, $\tilde{A}_i^r = A_i^r(C^\perp)$, and $\tilde{V}_i^r = V_i^r(C^\perp)$.

Trivially, we have

$$V_0^{-1} = A_n^k = 1, \tag{11.2}$$

$$V_n^{k-1} = A_0^0 = 1. \tag{11.3}$$

When we determine A_i^r, we split the range of r into different intervals. Let

$$m_i = m_i(C) := d_i(C^\perp) - i - 1.$$

Obviously $m_0 = -1$ and $m_{n-k} = k-1$. We will determine V_i^r for $m_j \le r < m_{j+1}$ for $j = 0$ and for $j = 1$. First, let us observe a relatively simple but yet essential lemma.

Lemma 11.1
If $m_{j+1} > m_j$, then

$$V_{m_j+j+1}^{m_j} = \tilde{A}_{m_j+j+1}^{j},$$
$$V_i^{m_j} = 0, \quad i > m_j + j + 1.$$

Proof: Consider a subcode $D \subseteq C^\perp$ of dimension j and weight $m_j + j + 1 = d_j^\perp$. This is a minimum subcode, and because $m_{j+1} > m_j$ implies that there is r such that $n - d_r = d_j^\perp$, we get that $\gamma' = \mu(\beta(D))$ is a maximum size cross-section by Lemma 8.1. Furthermore, every maximum size cross-section of the same dimension can be written on the same form. By (8.1), γ' has projective dimension m_j. The first equation follows immediately. The second equation follows because $n - d_{m_j} = m_j + j + 1$. □

In this chapter, we will see that $A_i^r(C)$ can be computed for all $r > k + 2 - d_2(C^\perp)$ if we know the (first) weight enumerator for $C^\perp$. The result will be summarised in Theorem 11.4.

Definition 11.1
A projective multiset (or a code) is called r-DMDS (r-dual MDS) or $(k-1-r)$-MDS if $\Delta_r = r + 1$. A projective multiset (or code) is barely r-DMDS if it is r-DMDS and not $(r+1)$-DMDS.

An equivalent and more classic definition is that a code is r-MDS if it meets the r-th generalised singleton bound with equality, i.e. if $d_r = d_k - k + r$. Note that any i-DMDS code is $(i-1)$-DMDS, and being 0-DMDS is equivalent with being a projective code.

Consider now the code C' defined by $\gamma_{C'} := \gamma_C \circ \phi_{\Pi_m}^{-1}$, where ϕ_{Π_m} is the projection through an m-space $\Pi_m \leqq \mathsf{PG}(k-1, q)$. Every r-space in $\mathsf{PG}(k-2-m, q)$ is the image of an $(r+m+1)$-space containing Π_m in $\mathsf{PG}(k-1, q)$. Hence

$$\Delta_r(C') \leq \Delta_{r+m+1}(C) - \gamma_C(\Pi_m).$$

Hence, if Π_m has maximum value, then C' is $(m_1 - m - 2)$-DMDS.

We define the r-th support weight enumerator of C to be

$$A^r(Z; C) := \sum_{i=0}^{n} A_i^r(C) Z^i.$$

As usual, we write $A^r(Z) = A^r(Z; C)$ and $\tilde{A}^r(Z) = A^r(Z; C)$. We also define

$$[m]_r := \prod_{i=0}^{r-1} (q^m - q^i).$$

11.2 Previous results and motivation

We have mentioned that the support weight distribution was introduced in [HKM77], in the study of infinite classes of irreducible cyclic codes over $\mathsf{GF}(q)$. They started with an $[n_1, k_1]$ code V_1 over $\mathsf{GF}(q)$ and a generator matrix G for V_1. Viewing G as a matrix over $\mathsf{GF}(q^l)$, they got an $[n_1, k_1]$ code V_l over $\mathsf{GF}(q^l)$. The fundamental result from [HKM77], says that V_l has weight enumerator

$$A(Z; V_l) = \sum_{i=0}^{n_1} \sum_{r=0}^{k_1} A_i^r(V_1)[l]_r Z^i. \tag{11.4}$$

To obtain the infinite class of codes, we let $\hat{V}_l$ be the concatenation of V_l with a $[(q^l-1)/(q-1), l]$ simplex code S_l over $\mathsf{GF}(q)$. Thus $\hat{V}_l$ is an $[n_1(q^l-1)/(q-1), k_1 l]$ code over $\mathsf{GF}(q)$, and since every codeword of S_l has the same weight, the weight enumerator of $\hat{V}_l$ is easily computable from (11.4). An equivalent description would be to say that $\hat{V}_l = V_1 \otimes S_l$. Thus we get the following theorem.

Theorem 11.1 (Helleseth-Kløve-Mykkeltveit 1977)
Let C be an $[n, k]$ code and S_l the simplex code of dimension l. Then the weight enumerator of the product code $C \otimes S_l$ is given by

$$A(Z) = \sum_{i=0}^{n} \sum_{r=0}^{k} A_i^r(C)[l]_r(C) Z^{iq^{l-1}}.$$

The above results are general. We just note that if V_1 is an irreducible cyclic code, then also $\hat{V}_l$ is an irreducible cyclic code. In fact, any irreducible cyclic code with block length $n = n_1((q^l-1)/N)$ where $N|q-1$, $\mathsf{HCF}(n_1, N) = 1$, and $\mathsf{HCF}(l, N)$ can be decomposed as a product $C \otimes S_l$.

At least two more papers on support weight distributions appeared in the seventies, as well as a related result for the weight distribution of coset leaders [Hel79]. Helleseth treated two special classes of codes in [Hel78], and Kløve found some general results in [Kløv78]. The main result from the latter paper has been treated again and presented as generalised MacWilliams identities in [Kløv92].

Theorem 11.2 (MacWilliams-Kløve)
Let A^r be the r-th support weight enumerator of C, and $\tilde{A}^r$ that of $C^\perp$, then we have

$$\sum_{r=0}^{m} [m]_r \tilde{A}^r(Z) = q^{-mk}[1+(q^m-1)Z]^n \Big[\sum_{r=0}^{m} [m]_r A^r\Big(\frac{1-Z}{1+(q^m-1)Z}\Big)\Big].$$

Simonis [Sim94] has used a completely different technique to generalise the MacWilliams identities. He also present his results on a very different form. We have not been able to locate a proof showing that Simonis' and Kløve's results are equivalent, but they do seem to contain the same information as far as we have seen.

The proof due to Simonis is basically a generalisation of the original proof of MacWilliams [Mac63]. Kløve on the other hand, developes a sequence of codes and uses Theorem 11.1 to prove the identities.

Over the last few years we have seen the support weight distribution have been suggested for classification of self-dual codes. The Gleason theorems have been generalised for higher weights [DG01, DGO03]. The SWD-s of all the $[32, 16, 8]$ Type II codes have been studied in [MCC03], and the SWD-s of various isodual codes are treated in [Mil01b, Mil01a]. The trellis structure of selfdual codes was studied in [CC01], and this work contains some links to higher weights. The weight enumerator has often been used in existence and non-existence proofs for codes with certain parameters, and the SWD may be used in a similar manner.

A particularly interesting code is the $[72, 36, 16]$ self-dual code of Type II, i.e., where all the codewords have weight divisible by 4. We do not know if such a code exists, but if it does we know its weight enumerator [Dou01] and its second SWD [DG01]. If this $[72, 36, 16]$ code exists, it has the largest possible minimum weight. If we can prove that it does not exist, the largest possible minimum weight of a Type II code of length 72 must be 12.

In this chapter we devise a general technique to determine A_i^r for high values of r, given the weight enumerator of the dual code.

11.3 In the range $m_0 \leq r < m_1$

In this section, we will find the support weight distribution A_i^r for $k+1-d_1^\perp < r \leq k$. The results were first proved in [Klø78]. They are proved again here to provide a softer introduction to the next section.

Note that any code is barely R-DMDS where $R = m_1 - 1$. We write $\mathcal{V}_i^r(n,k) = V_i^r(C)$ for some R-DMDS $[n,k]$ code C, where $r \leq R$. We will see that this number is well-defined and independent of C. Observe that $\mathcal{V}_{n-i}^{k-1-r}(n,k) = A_i^r$ if and only if $k+1-d_1^\perp < r \leq k$.

When a code is R-DMDS, it means that for all $r \leq R$, any $(r+1)$-subset of γ spans an r-space of $\mathsf{PG}(k-1,q)$. It follows immediately that

$$\mathcal{V}_{r+1}^r(n,k) = \binom{n}{r+1}, \tag{11.5}$$

$$\mathcal{V}_j^r(n,k) = 0, \quad \forall j > r+1. \tag{11.6}$$

Lemma 11.2
For $0 \le r < m_1$, $\mathcal{V}_j^r(n,k)$ is well-defined, and we have

$$\mathcal{V}_0^r(n,k) = \begin{bmatrix} k \\ r+1 \end{bmatrix} - \sum_{j=1}^{r+1} \mathcal{V}_j^r(n,k), \tag{11.7}$$

$$\mathcal{V}_j^r(n,k) = \binom{n}{j} \mathcal{V}_0^{r-j}(n-j,k-j), \qquad 0 < j \le r+1, \tag{11.8}$$

$$\mathcal{V}_j^r(n,k) = 0, \qquad j > r+1. \tag{11.9}$$

Proof: Equation (11.9) comes from (11.6). For $j = r+1$, we get from (11.2) that (11.8) reduces to

$$\mathcal{V}_{r+1}^r(n,k) = \binom{n}{r+1},$$

which has been proved in (11.5). If we can prove (11.8) for $0 < j \le r$, then (11.7) follows by definition. Thus the lemma becomes trivial for $r = 0$, and we can proceed by induction. Hence assume (11.8) hold for $r-1$, and that $0 < j \le r$. Then also (11.7) holds for $r-1$.

An r-space Π_r of value j contains a unique $(j-1)$-space Π of value j. There are a total V_j^{j-1} such subspaces in the geometry, by the induction hypothesis. We consider the projection π_Π, which defines an $(m_1 - 1 - j)$-DMDS code C' by $\gamma_C \circ \pi_\Pi^{-1}$.

These r-spaces correspond to the $(r-j)$-spaces in $\operatorname{im} \pi_\Pi$. Hence Π_r has value j if and only if $\pi_\Pi(\Pi_r)$ has zero value. The number of such $(r-j)$-spaces is $\mathcal{V}_0^{r-j}(n-j,k-j)$ by the induction hypothesis. Hence

$$\mathcal{V}_j^r(n,k) = \mathcal{V}_j^{j-1}(n,k)\mathcal{V}_0^{r-j}(n-j,k-j).$$

By application of (11.5), we get (11.8). The result follows by induction. □

Lemma 11.3
For $-1 \le r < m_1$, $\mathcal{V}_0^r(n,k)$ is well-defined, and we have

$$\mathcal{V}_0^r(n,k) = \sum_{j=0}^{r+1} (-1)^j \begin{bmatrix} k-j \\ r+1-j \end{bmatrix} \binom{n}{j}.$$

Proof: For $r = -1$ and $r = 0$, the lemma reduces to

$$\mathcal{V}_0^{-1}(n,k) = 1,$$
$$\mathcal{V}_0^0(n,k) = \begin{bmatrix} k \\ 1 \end{bmatrix} - n,$$

which matches (11.2) and (11.7). We assume that the lemma holds for $r-1$ and proceed by induction.

We have from Lemma 11.2, that

$$\begin{aligned}\mathcal{V}_0^r(n,k) &= \begin{bmatrix} k \\ r+1 \end{bmatrix} - \sum_{j=1}^{r+1} \mathcal{V}_j^r(n,k) \\ &= \begin{bmatrix} k \\ r+1 \end{bmatrix} - \sum_{j=1}^{r+1} \binom{n}{j} \mathcal{V}_0^{r-j}(n-j,k-j).\end{aligned}$$

If we combine this with the induction hypothesis, we get

$$\mathcal{V}_0^r(n,k) = \begin{bmatrix} k \\ r+1 \end{bmatrix} - \sum_{j=1}^{r+1} \binom{n}{j} \sum_{i=0}^{r-j+1} (-1)^i \begin{bmatrix} k-j-i \\ r-j+1-i \end{bmatrix} \binom{n-j}{i}.$$

We set $m = i + j$ and rewrite to get

$$\begin{aligned}\mathcal{V}_0^r(n,k) &= \begin{bmatrix} k \\ r+1 \end{bmatrix} - \sum_{m=1}^{r+1} \begin{bmatrix} k-m \\ r+1-m \end{bmatrix} \sum_{i=0}^{m-1} (-1)^i \binom{n}{m-i} \binom{n-m+i}{i} \\ &= \begin{bmatrix} k \\ r+1 \end{bmatrix} - \sum_{m=1}^{r+1} \begin{bmatrix} k-m \\ r+1-m \end{bmatrix} \sum_{i=0}^{m-1} (-1)^i \binom{n}{m} \binom{m}{i} \\ &= \begin{bmatrix} k \\ r+1 \end{bmatrix} + \sum_{m=1}^{r+1} \begin{bmatrix} k-m \\ r+1-m \end{bmatrix} \binom{n}{m} (-1)^m \\ &= \sum_{j=0}^{r+1} \begin{bmatrix} k-j \\ r+1-j \end{bmatrix} \binom{n}{j} (-1)^j,\end{aligned}$$

as required. The lemma follows by induction. □

The following theorem is a direct result of Lemmata 11.2 and 11.3.

Theorem 11.3
For $-1 \leq r < m_1$, $\mathcal{V}_j^r(n,k)$ is well-defined, and we have

$$\mathcal{V}_j^r(n,k) = \binom{n}{j} \sum_{i=0}^{r-j+1} (-1)^i \begin{bmatrix} k-j-i \\ r-j+1-i \end{bmatrix} \binom{n-j}{i}.$$

11.4 In the range $m_1 \le r < m_2$

In this section we consider $m_1 \le r < m_2$. We know that $V_i^r = 0$ for all $i > r+2$.

Consider an r-space Π of value $r+2$. The cross-section $\gamma_C|_\Pi$ defines an $[r+2, r+1]$ code C'. Let $s := m_1(C')$. We say that Π has type s. Clearly $m_1 \le s \le r$. The set of r-spaces of type s is denoted by $\mathfrak{S}(r,s)$.

Given an r-space Π' of value $i \le r+1$, we say that Π' is Type I if it contains a $(i-2)$-space Π'' of value i. This $(i-2)$-space is unique when it exists. Clearly Π'' has type s for some s, and then we say that Π' is Type I(s).

If Π' is not Type I, we say that it is Type II, and then it contains a unique $(i-1)$-space of value i. Let $\mathfrak{U}_i^r(X)$ be the set of r-spaces of value i and Type X, where X is I, II, or I(s) for some s. Write $U_i^r(X) := \#\mathfrak{U}_i^r(X)$.

11.4.1 Subspaces of Maximum Value

If C is an $[n, n-1]$ code, there is a unique s such that $\delta_s(C) = 2$, and $\delta_i(C) = 1$ for $i \ne s$. Clearly $m_1(C) = s$. In this case, we call C an $[n, n-1]$ code of type s.

Lemma 11.4
Let γ_C be a projective multiset defining an $[n, n-1]$ code C of type s. Then there is a unique s-space Π_s of value $s+2$.

Proof: There exists at least one such s-space since $s = m_1 = \Delta_s(C) - 2$. Suppose there are two distinct s-spaces Θ_1 and Θ_2 of value $s+2$. Let i be the dimension of $\Theta := \Theta_1 \cap \Theta_2$. Clearly $i < s$ and thus $\gamma_C(\Theta) \le i+1$. We get

$$\gamma(\langle \Theta_1, \Theta_2 \rangle) \ge 2(s+2) - (i+1) = 2s - i + 3,$$

but

$$\dim\langle \Theta_1, \Theta_2 \rangle = 2s - i = 2s - i,$$

so

$$\gamma(\langle \Theta_1, \Theta_2 \rangle) \le \Delta_{2s-i}(C) = 2s - i + 2.$$

The lemma follows by contradiction. □

There is only one $[n, n-1]$ code of Type s up to equivalence. The corresponding projective multiset is obtained by taking a frame for a projective s-space and then adding projectively independent points to obtain an $(n-2)$-space.

Lemma 11.5
For any code C, if $m_1 \le s \le r < m_2$, we have

$$\#\mathfrak{S}(r,s) = \tilde{A}^1_{s+2} \binom{n-s-2}{r-s}.$$

Proof: The number of maximum r-spaces of type $r = s$ is

$$\#\mathfrak{S}(s,s) = \tilde{A}^1_{s+2}, \tag{11.10}$$

by Lemma 11.1.

An r-space Π_r of type s contains a unique s-space Π_s of value $s+2$ by Lemma 11.4. Hence there is a one-to-one correspondence between r-spaces of type s and pairs (Π_s, S) where $\Pi_s \in \mathfrak{S}(s,s)$ and $S \subset \gamma_C \backslash \Pi_s$ is a set of $r-s$ points. There are $\tilde{A}^1_{s+2}$ ways to choose Π_s by (11.10) and $\binom{n-s-2}{r-s}$ ways to choose S. Hence we get the result. □

Lemma 11.6
If $m_1 \le r < m_2$, then

$$V^r_{r+2} = \sum_{s=m_1}^{r} \tilde{A}^1_{s+2} \binom{n-s-2}{r-s},$$
$$V^r_i = 0, \quad i > r+2.$$

Proof: An r-space of value $r+2$ has type s for some s where $m_1 \le s \le r$. Thus we can take the sum of the equation in Lemma 11.5. Hence the result. □

11.4.2 When $n = k+1$

In this section we study an $[n, n-1]$ code C of type s. We will need the number $\mathcal{F}(j,n,s) := U_j^{n-3}(\mathrm{II})$ for C in the later sections.

We obviously have that $\mathcal{F}(j,n,s) = 0$ if $j \ge n-1$. When $n = s+2$, C is MDS, so

$$\mathcal{F}(j, s+2, s) = \mathcal{V}_j^{s-1}(s+2, s+1). \tag{11.11}$$

Lemma 11.7
For any $[n, n-1]$ code of type s, if $j \le n-2$, then $U_j^{n-3}(\mathrm{II})$ is given by

$$\mathcal{F}(i,n,s) = \sum_{j=0}^{i} \mathcal{V}_j^{s-1}(s+2, s+1) \binom{n-s-2}{i-j} (q-1)^{n-2-s-i+j}.$$

Proof: Note that if $n = s+2$, the lemma reduces to (11.11).

We consider the projective space $\mathsf{PG}(n-2,q)$. We want to find the number $\mathcal{F}(i,n,s)$ of hyperplanes of value i and Type II. Consider an arbitrary such hyperplane Π. There is a unique s-space $\Theta \leqq \mathsf{PG}(n-2,q)$ of value $s+2$. Every hyperplane must meet Θ in a subspace of dimension $s-1$ or more. Since Π has Type II, $\Theta' := \Theta \cap \Pi$ is exactly an $(s-1)$-space. Let $j = \gamma_C(\Theta')$.

Given j ($0 \leq j \leq s$), there are $\mathcal{F}(j, s+2, s)$ ways to choose Θ'. Let $\Pi' \leqq \Pi$ be the smallest subspace of value i and containing Θ'. Given Θ', we find Π' by choosing $i-j$ points among the $n-s-2$ points of positive value not contained in Θ. Given j, there are thus

$$\mathcal{F}(j, s+2, s)\begin{pmatrix} n-s-2 \\ i-j \end{pmatrix} = \mathcal{V}_j^{s-1}(s+2, s+1)\begin{pmatrix} n-s-2 \\ i-j \end{pmatrix}$$

ways to choose Π'.

Consider now the projection $\pi_{\Pi'}$. The multiset $\gamma'' := \gamma_C \circ \pi_{\Pi'}^{-1}$ defines an $[n-i, n-1-s-i+j]$ code. There is but one point x of value $\gamma''(x) = s+2-j$, namely $x = \pi_{\Pi'}(\Theta)$. The remaining points have value 0 or 1. We define a new projective multiset γ' by $\gamma'(x) = 1$ and $\gamma'(y) = \gamma''(y)$ for $y \neq x$. The corresponding code is a projective $[n', n']$ code where $n' = n-i-s-1+j$.

Finding $\Pi \geqq \Pi'$ of value i is the same as finding a hyperplane of zero value for γ', which is the same as counting one-dimensional subcodes of weight n' for the $[n', n']$ code. This number is $(q-1)^{n'-1}$. The lemma follows by summing over all j. □

11.4.3 Other subspaces

Now we return to the general $[n, k]$ code C, in order to determine V_j^r for $j \leq r+1$.

Proposition 11.1
For $m_1 \leq r < m_2$ and $r \geq i-2$, we have

$$U_i^r(\mathrm{I}(s)) = \mathcal{V}_0^{r+1-i}(n-i, k+1-i)\tilde{A}_{s+2}^1\begin{pmatrix} n-s-2 \\ i-s-2 \end{pmatrix},$$
$$U_i^r(\mathrm{I}) = \mathcal{V}_0^{r+1-i}(n-i, k+1-i)V_i^{i-2}.$$

For $r < i-2$, we have $U_i^r(\mathrm{I}) = U_i^r(\mathrm{I}(s)) = 0$.

Proof: We have from Lemma 11.5, that

$$U_i^{i-2}(\mathrm{I}(s)) = \tilde{A}_{s+2}^1\begin{pmatrix} n-s-2 \\ i-2-s \end{pmatrix}.$$

An r-space of value i and type s contains a unique $(i-2)$-space Π' of value i and type s. There are $U_i^{i-2}(\mathrm{I}(s))$ ways to choose Π'.

Consider then the multiset $\gamma' := \gamma_C \circ \pi_{\Pi'}^{-1}$ obtained by projection through Π'. We know that γ' defines an $[n-i, k+1-i]$ code C'. Finding an r-space $\Pi \geqq \Pi'$ of value i corresponds to finding an $(r+1-i)$-space of value 0 for γ'. Furthermore γ' defines a code with

$$\Delta_{m_2-i}(C') \leq \Delta_{m_2-1}(C) - i = m_2 + 1 - i.$$

Hence C' is (m_2-i)-DMDS, and since $r+1-i \le m_2-i$, there are $\mathcal{V}_0^{r+1-i}(n-i, k+1-i)$ ways to choose $\Pi \geqq \Pi'$. This proves the first equation, and the second one follows by summing over all s. □

Proposition 11.2
If $m_1 < j \le m_2$, we have

$$U_j^{j-1}(\mathrm{II}) = \binom{n}{j} - U_j^{j-2}(\mathrm{I}) - \sum_{s=m_1}^{j-1} (s+2) U_{j+1}^{j-1}(\mathrm{I}(s)).$$

For $i > j$, we have $U_i^{j-1}(\mathrm{II}) = 0$.

Proof: We consider all the $\binom{n}{j}$ possible ways to chose a set S of j points of positive value. To find $U_j^{j-1}(\mathrm{II})$, we must subtract the number of cases where these j points generate a subspace of type I.

Since $j-1 < m_2$, we have three cases:

1. $\dim\langle S\rangle = j-1$ and $\gamma_C(\langle S\rangle) = j$. (Type II)
2. $\dim\langle S\rangle = j-2$ and $\gamma_C(\langle S\rangle) = j$. (Type I)
3. $\dim\langle S\rangle = j-1$ and $\gamma_C(\langle S\rangle) = j+1$. (Type I)

The number of sets S giving the first case is $U_j^{j-1}(\mathrm{II})$, while for the second case, it is $U_j^{j-2}(\mathrm{I})$. The third case is more difficult, because S does not contain all points of positive value in $\langle S\rangle$. Suppose $\langle S\rangle$ has type s. Then $\langle S\rangle$ can be chosen in $U_{j+1}^{j-1}(\mathrm{I}(s))$ different ways. There is one point $x \notin S$ of positive value in $\langle S\rangle$, and x must be contained in the unique s-space $\Pi_s \leqq \langle S\rangle$ of value $s+2$. Moreover x can be any point of positive value in Π_s, hence there are $s+2$ different choices for S giving the same $\langle S\rangle$ of the third case. This gives the lemma. □

Let

$$\mathfrak{U}(r_1, v_1, X_1; r_2, v_2, X_2) = \{(\Pi_1, \Pi_2) \mid \Pi_1 \leqq \Pi_2, \Pi_j \in \mathfrak{U}_{v_j}^{r_j}(X_j), j = 1, 2\}.$$

We will write $v_j = *$ resp. $X_j = *$, when we allow any value of v_j resp. X_j.

Lemma 11.8
If $m_1 \le r < m_2$ and $0 \le j \le r$, then

$$U_j^r(\mathrm{II}) = \frac{q-1}{q^{r+1-j}-1}\left(U_j^{r-1}(\mathrm{II})\frac{q^{k-r}-1}{q-1} - \sum_{v=j+1}^{r+2} \#\mathfrak{U}(r-1, j, \mathrm{II}; r, v, *)\right).$$

Proof: We will count the number of elements of $\mathfrak{U}(r-1, j, \mathrm{II}; r, j, \mathrm{II})$ in two different ways. Consider a pair

$$(\Pi', \Pi) \in \mathfrak{U}(r-1, j, \mathrm{II}; r, j, \mathrm{II}).$$

There are $U_j^r(\mathrm{II})$ ways to choose Π. For Π', we can choose any $(r-1)$-space containing the unique $(j-1)$-space of value j in Π. Hence

$$\#\mathfrak{U}(r-1, j, \mathrm{II}; r, j, \mathrm{II}) = U_j^r(\mathrm{II}) \begin{bmatrix} r+1-j \\ r-j \end{bmatrix} = U_j^r(\mathrm{II}) \frac{q^{r+1-j}-1}{q-1}. \tag{11.12}$$

This gives the first of the two expressions we seek.

Now we observe that

$$\#\mathfrak{U}(r-1, j, \mathrm{II}; r, *, *) = \sum_{v=j}^{r+2} \#\mathfrak{U}(r-1, j, \mathrm{II}; r, v, *). \tag{11.13}$$

This number can equivalently be obtained by counting the number of $(r-1)$-spaces of value j and Type II, and the number of r-spaces containing each such space. This gives

$$\#\mathfrak{U}(r-1, j, \mathrm{II}; r, *, *) = U_j^{r-1}(\mathrm{II}) \begin{bmatrix} k-r \\ 1 \end{bmatrix} = U_j^{r-1}(\mathrm{II}) \frac{q^{k-r}-1}{q-1}. \tag{11.14}$$

Clearly we have that

$$\#\mathfrak{U}(r-1, j, \mathrm{II}; r, j, \mathrm{I}) = 0,$$

and if we combine this with with (11.13) and (11.14), we get

$$\#\mathfrak{U}(r-1, j, \mathrm{II}; r, j, \mathrm{II}) = U_j^{r-1}(\mathrm{II}) \frac{q^{k-r}-1}{q-1} - \sum_{v=j+1}^{r+2} \#\mathfrak{U}(r-1, j, \mathrm{II}; r, v, *),$$

which is our second expression for $\#\mathfrak{U}(r-1, j, \mathrm{II}; r, j, \mathrm{II})$. Combining this with (11.12), we get the lemma. □

Lemma 11.9
If $j < v-1$, then

$$\#\mathfrak{U}(r-1, j, \mathrm{II}; r, v, \mathrm{I}(s)) = U_v^r(\mathrm{I}(s)) \mathcal{F}(j, v, s) q^{r+2-v}.$$

Proof: Consider a pair

$$(\Pi', \Pi) \in \mathfrak{U}(r-1, j, \mathrm{II}; r, v, \mathrm{I}(s)).$$

There are $U_v^r(\mathrm{I}(s))$ ways to choose Π. There is a unique $(v-2)$-space $\Theta \leqq \Pi$ of value v and type s. The intersection $\Theta' := \Pi' \cap \Theta$ is a $(v-3)$-space of value j. There are $\mathcal{F}(j, v, s)$ ways to choose Θ'.

Consider the projection $\pi_{\Theta'}$. Finding Π' is the same as finding a hyperplane in $\mathsf{im}\,\pi_{\Theta'}$ not meeting $\pi_{\Theta'}(\Theta)$, which is a point. There are $(q^{r+3-v}-1)/(q-1)$ hyperplanes in $\mathsf{im}\,\pi_{\Theta'}$, of which $(q^{r+2-v}-1)/(q-1)$ meet $\pi_{\Theta'}(\Theta)$. Hence there are q^{r+2-v} hyperplanes not meeting $\pi_{\Theta'}(\Theta)$. □

Lemma 11.10
If $j < v$, then

$$\#\mathfrak{U}(r-1, j, \mathrm{II}; r, v, \mathrm{II}) = U_v^r(\mathrm{II})\mathcal{V}_j^{v-2}(v, v)q^{r+1-v}.$$

Proof: Consider a pair

$$(\Pi', \Pi) \in \mathfrak{U}(r-1, j, \mathrm{II}; r, v, \mathrm{II}).$$

There are $U_v^r(\mathrm{II})$ ways to choose Π. There is a unique $(v-1)$-space $\Theta \leqq \Pi$ of value v, and $\gamma_C|_\Theta$ defines a $[v, v]$ code. The intersection $\Theta' := \Pi' \cap \Theta$ is a $(v-2)$-space of value j. There are $\mathcal{V}_j^{v-2}(v, v)$ ways to choose Θ'.

Consider the projection $\pi_{\Theta'}$. Finding Π' is the same as finding a hyperplane in $\mathsf{im}\,\pi_{\Theta'}$ not meeting $\pi_{\Theta'}(\Theta)$, which is a point. There are q^{r+1-v} such hyperplanes. □

We define for brevity:

$$\mathfrak{F}(r, j) := \sum_{v=j+1}^{r+2} \#\mathfrak{U}(r-1, j, \mathrm{II}; r, v, *).$$

Proposition 11.3
We have

$$\mathfrak{F}(r, j) = \sum_{v=j+2}^{r+2} q^{r+2-v}\left[U_{v-1}^r(\mathrm{II})\mathcal{V}_j^{v-3}(v-1, v-1) + \sum_{s=m_1}^{r} U_v^r(\mathrm{I}(s))\mathcal{F}(j, v, s)\right].$$

Proof: First note that

$$\#\mathfrak{U}(r-1, j, \mathrm{II}; r, r+2, \mathrm{II}) = 0,$$

because $U_{r+2}^r(\mathrm{II}) = 0$, and that

$$\#\mathfrak{U}(r-1, j, \mathrm{II}; r, j+1, \mathrm{I}) = 0,$$

because there is no subspace of value j in a subspace of value $j+1$ and Type I. Now the result follows from Lemmata 11.9 and 11.10. □

Proposition 11.4
If $m_1 \leq r < m_2$ and $0 \leq j \leq r$, then

$$U_j^r(\mathrm{II}) = \frac{q^{k-r}-1}{q^{r+1-j}-1} U_j^{r-1}(\mathrm{II}) - \frac{q-1}{q^{r+1-j}-1} \mathfrak{F}(r,j),$$

where $\mathfrak{F}(r,j)$ is given by Proposition 11.3.

Proof: This is simply a rephrase of Lemma 11.8. □

If we combine all the results of this chapter, we get the following theorem as a conclusion.

Theorem 11.4
For $k \geq r > k+2-d_2(C^\perp)$, it is possible to compute $A_i^r(C)$ for all i provided we know the (first) weight enumerator of $C^\perp$. We have for $k+1-d_1(C^\perp) < r \leq k$, that

$$A_i^r(C) = \binom{n}{n-i} \sum_{j=0}^{k+i-r-n} (-1)^j \begin{bmatrix} k-n+i-j \\ k-r-n+i-j \end{bmatrix} \binom{i}{j},$$

and for $k+2-d_2(C^\perp) < r \leq k+1-d_1(C^\perp)$, that

$$A_i^r(C) = U_{n-i}^{k-1-r}(\mathrm{II}) + U_{n-i}^{k-1-r}(\mathrm{I}),$$

where $U_{n-i}^{k-1-r}(\mathrm{II})$ and $U_{n-i}^{k-1-r}(\mathrm{I})$ are given by Propositions 11.1, 11.2 and 11.4.

11.5 Discussion of future works

We have found formulæ for computing some high order support weight distributions. The formulæ are good for electronic computation of the parameters, and for instance computing the third through the 24th support weight distribution of the $[24, 12]$ Golay code is a matter of seconds. On the other hand, simplified formulæ more comprehensible to human readers would definitely be an improvement.

It will not be too difficult to continue and compute $A_i^r(C)$ for

$$k - d_2^\perp + 2 \geq r > k + 3 - \min\{d_3^\perp, 2d_1^\perp\},$$

provided the second support weight distribution of $C^\perp$ is known. We have omitted these results, because they would be too tedious, without adding significantly to the understanding of the subject.

To go below $k+3-2d_1^\perp$ is more difficult, because if $i \geq 2d_1^\perp$, we may have a codeword $\mathbf{c} \in C^\perp$ and a subcode $D \subseteq C^\perp$ of dimension more than one, such that $\chi(\mathbf{c}) = \chi(D)$. This codeword $\mathbf{c}$ will be counted in $\tilde{A}_i^1$, but for computing A_j^r, only D

should be counted. It is a long way to making a general statement for $r \leq k+3-2d_1^\perp$, but in special cases there may be possibilities.

We have tried to compute support weight distributions of the tentative $[72, 36, 16]$ Type II self-dual code. We have determined the 15th through the 36th SWD with Theorem 11.4. The MacWilliams-Kløve identities from Theorem 11.2 may be solved in reasonable time by first solving modulo (say) ten-digit primes and thereafter combining the solutions with the Chinese Remainder Theorem. Thus we have determined the 12th, 13th, and 14th SWD, and the 3rd through the 11th SWD are determined by linear formulæ in 30 free parameters. Listings of SWD-s of orders 1, 2, and 15-36 can be found in [Sch01b].

It is interesting to go on with this work and possibly determine more parameters from the SWD-s or the weight hierarchy. That might give us enough information on the structure of such a $[72, 36, 16]$ Type II code to prove existence or non-existence.

There are also plenty of other codes which may or may not exist, and which can be attacked with this technique.

12 Product codes

A product code $C_1 \otimes C_2$ is the tensor product of two linear codes, C_1 and C_2. The weight hierarchy of product codes was first studied by Wei and Yang in [WY93], a paper which is also remembered for having introduced the chain condition (Definition 2.2). They gave a conjecture on the weight hierarchy for products of two chained codes.

12.1 Introduction

The tensor product $C_1 \otimes C_2$ is the vector space generated by the vectors on the form

$$\mathbf{x} \otimes \mathbf{y} := (x_i y_j \mid 1 \leq i \leq n_1, 1 \leq j \leq n_2),$$

where $\mathbf{x} = (x_1, \ldots x_{n_1}) \in C_1$ and $\mathbf{y} = (y_1, \ldots y_{n_2}) \in C_2$. When C_1 and C_2 are $[n_1, k_1]$ and $[n_2, k_2]$ linear codes, $C_1 \otimes C_2$ is an $[n_1 n_2, k_1 k_2]$ code.

Definition 12.1
Given two linear codes C_1 and C_2, let

$$d_r^*(C_1 \otimes C_2) = \min \Big\{ \sum_{i=1}^{s} (d_i(C_1) - d_{i-1}(C_1)) d_{t_i}(C_2) \Big| \\ 1 \leq t_s \leq \ldots \leq t_1 \leq k_2, s \leq k_1, \sum_{i=1}^{s} t_i = r \Big\}.$$

Wei and Yang conjectured that $d_r = d_r^*$ for the product of chained codes. Barbero and Tena [BT95] studied d_r for $r \leq 4$ for arbitrary product codes, and when both component codes are chained, they found that their results coïncide with the Wei-Yang Conjecture. The number d_r^* is rather difficult to compute, but calculations for some special classes of codes are found in [HK96a, Par00b]. Park [Par00b] also verified the conjecture for the codes she studied. The first complete proof of the conjecture appeared in [Sch00], in the form of the following, stronger theorem.

Theorem 12.1
For any two linear codes C_1 and C_2, $d_r(C_1 \otimes C_2) \geq d_r^*(C_1 \otimes C_2)$ for $0 \leq r \leq k_1 k_2$. If C_1 and C_2 are chained codes, then equality holds for all r.

A second proof of the Wei-Yang conjecture, completely different, was presented by Martínez-Pérez and Willems in [MPW01], and it also covered product codes of more than two terms, but only products of chained codes. Following this second proof, Willems and the present author [SW03] proved a lower bound on the weight hierarchy of products of more than two codes, not necessarily chained, by using the techniques from [Sch00].

In this chapter, we include the proofs from [SW03], the preliminaries from [Sch00], and some special cases (Section 12.3) from [Sch00]. The original proof of Theorem 12.1 was modified to serve the general result, and only the modified version from [SW03] is included.

12.1.1 The Segre embedding

Our first step is to describe the projective multiset γ corresponding to $C = C_1 \otimes C_2$, in terms of the projective multisets γ_1 and γ_2 corresponding to C_1 and C_2.

Lemma 12.1 (Basis lemma)
If $\{\mathbf{x}_i \mid i = 1, \ldots k_1\}$ *and* $\{\mathbf{y}_i \mid i = 1, \ldots k_2\}$ *are bases for* C_1 *and* C_2*, then* $\{\mathbf{x}_i \otimes \mathbf{y}_j \mid 1 \leq i \leq k_1, 1 \leq j \leq k_2\}$ *is a basis for* $C_1 \otimes C_2$*.*

This is a well-known fact, so we omit the proof. With regard to product codes, it basically says that we can form a generator matrix for $C_1 \otimes C_2$, by taking as rows all possible product $\mathbf{x} \otimes \mathbf{y}$, where $\mathbf{x}$ is a row from some fixed generator matrix of C_1, and $\mathbf{y}$ is a row from a fixed generator matrix for C_2.

The following proposition says that we can equivalently form the generator matrix by taking products of columns.

Proposition 12.1
If C_1 *and* C_2 *are linear codes defined by the vector multisets* $\overline{\gamma}_1$ *and* $\overline{\gamma}_2$*, then the vector multiset defining* $C := C_1 \otimes C_2$ *is*

$$\overline{\gamma}_C = \{\mathbf{x} \otimes \mathbf{y} \mid \mathbf{x} \in \overline{\gamma}_1, \mathbf{y} \in \overline{\gamma}_2\},$$

considered as a multiset.

Proof: For any vector $\mathbf{x}$ we write $\mathbf{x}[i]$ for its ith coordinate. Let $\{\mathbf{a}_i\}$ and $\{\mathbf{b}_j\}$ be bases for C_1 and C_2 respectively, and let $\{\mathbf{c}_{ij} = \mathbf{a}_i \otimes \mathbf{b}_j\}$ be the induced basis for C. Let the code parameters be $[n_1, k_1]$ for C_1, $[n_2, k_2]$ for C_2, and $[n, k]$ for C.

Now, a codeword $\mathbf{c} \in C$ is written as

$$\mathbf{c} = \sum_{i=1}^{k_1} \sum_{j=1}^{k_2} \mathbf{m}[i, j]\mathbf{c}_{ij},$$

where $\mathbf{m}$ is a message word, i.e. a $k_1 \times k_2$ matrix over the base field.

The coordinates are given as

$$\begin{aligned}\mathbf{c}[a,b] &= \sum_{i=1}^{k_1}\sum_{j=1}^{k_2}\mathbf{m}[i,j]\mathbf{c}_{ij}[a,b] \\ &= \sum_{i=1}^{k_1}\sum_{j=1}^{k_2}\mathbf{m}[i,j]\mathbf{a}_i[a]\mathbf{b}_j[b] = \mathbf{g}_{ab}\mathbf{m},\end{aligned}$$

where $\mathbf{g}_{ab}$ is a vector of length k. In fact

$$\mathbf{g}_{ab} = (\mathbf{a}_i[a] : 1 \le i \le k_1) \otimes (\mathbf{b}_i[b] : 1 \le i \le k_2),$$

i.e. $\mathbf{g}_{ab}$ is the $\otimes$-product of one column from the generator matrix of C_1 and one from that of C_2. □

The definition of $(a,b) \mapsto a \otimes b$ works also for projective points, and then the map is known as the Segre embedding

$$\mathsf{PG}(k_1-1,q) \times \mathsf{PG}(k_2-1,q) \to \mathsf{PG}(k_1k_2-1,q),$$

which is well known from algebraic geometry. This map is bijective on its image, which is called a Segre variety Y. In other words, a point $c \in \mathsf{PG}(k_1k_2-1,q)$ can be decomposed as $c = a \otimes b$, $a \in \mathsf{PG}(k_1-1,q)$ and $b \in \mathsf{PG}(k_2-1,q)$, if and only if $c \in Y$. The decomposition is unique when it exists. The following theorem follows directly from the proposition above.

Theorem 12.2
Let γ_1, γ_2, and γ be the projective multisets defining C_1, C_2, and $C = C_1 \otimes C_2$ respectively. Then we have that

$$\begin{aligned}\gamma(a \otimes b) &= \gamma_1(a) \cdot \gamma_2(b), \\ &\qquad \forall a \in \mathsf{PG}(k_1-1,q), \forall b \in \mathsf{PG}(k_2-1,q), \\ \gamma(c) &= 0, \quad \forall c \notin Y.\end{aligned} \tag{12.1}$$

12.2 The general result

Consider now the tensor product $C = C_1 \otimes \ldots \otimes C_t$ of t component codes, where C_i has parameters $[n_i, k_i]$. Clearly, C is an $[n,k]$ code, where $n = n_1n_2\ldots n_t$ and $k = k_1k_2\ldots k_t$. We will state a generalisation of Theorem 12.1 for such codes. First we give a generalised definition of d_r^* due to [MPW01].

Define

$$\mathcal{M}_t := \{\mathbf{i} = (i_1, i_2, \ldots, i_{t-1}) \mid 1 \le i_j \le k_j, 1 \le j < t\}. \tag{12.2}$$

Definition 12.2 (Partitions)
Let π be a map $\mathcal{M}_t \to \{0, 1, \ldots, k_t\}$ given by $\mathbf{i} \mapsto t_{\mathbf{i}}$. We call π a $(k_1, k_2, \ldots, k_t)$-partition of r if

1. $\sum_{\mathbf{i} \in \mathcal{M}_t} t_{\mathbf{i}} = r$, *and*
2. π *is a decreasing function in each coordinate, i.e.*

$$t_{i_1,\ldots,i_j,\ldots,i_{t-1}} \leq t_{i_1,\ldots,i_j-1,\ldots,i_{t-1}}$$

for $j = 1, \ldots, t-1$ and $1 < i_j$.

Let $\mathcal{P}(k_1, k_2, \ldots, k_t; r)$ denote the set of all $(k_1, k_2, \ldots, k_t)$-partitions of r. For $\pi \in \mathcal{P}(k_1, k_2, \ldots, k_t; r)$, we define

$$\nabla(\pi) := \sum_{\mathbf{i} \in \mathcal{M}_t} d_{\pi(\mathbf{i})}(C_t) \prod_{j=1}^{t-1} (d_{i_j}(C_j) - d_{i_j-1}(C_j)). \tag{12.3}$$

Note that $\nabla(\pi)$ depends on the weight hierarchies of all the codes C_i. Now let

$$d_r^*(C_1 \otimes C_2 \otimes \ldots \otimes C_t) := \min \left\{ \nabla(\pi) \mid \pi \in \mathcal{P}(k_1, k_2, \ldots, k_t; r) \right\},$$

for $r = 1, 2, \ldots, k$. Note that this definition coïncides with Definition 12.1 for $t = 2$.

Theorem 12.3
Let $C = C_1 \otimes C_2 \otimes \ldots \otimes C_t$ be the product of linear codes C_i. Then $d_r(C) \geq d_r^*(C)$ for all $r = 1, 2, \ldots, k$. Moreover, equality holds if all the components C_i are chained.

The remainder of this section will be devoted to proving this theorem. We will first reformulate the result in terms of projective multisets, then we prove the bound for $t = 2$ in Section 12.2.2 and for $t > 2$ in Section 12.2.3. The case when the chain condition holds will be proved in Section 12.2.4.

12.2.1 Projective Multisets

We recall that $\Delta_r(C) = n - d_{k-1-r}(C)$. Analogously, we write $\Delta_r^*(C) := n - d_{k-1-r}^*(C)$. Evidently, Theorem 12.3 is equivalent to $\Delta_r(C) \leq \Delta_r^*(C)$ for $r = 0, 1, \ldots, k-1$, with equality if all the component codes are chained. This is what we will prove shortly.

Definition 12.3 (Sub-partition)
Let $\pi \in \mathcal{P}(k_1, k_2, \ldots, k_t; r)$, and take $s \in \{1, 2, \ldots, k_1\}$. The s-th sub-partition $\pi|_s$ of π is given by

$$\pi|_s(i_2, i_3, \ldots, i_{t-1}) = \pi(s, i_2, i_3, \ldots, i_{t-1}).$$

Clearly $\pi|_s \in \mathcal{P}(k_2, k_3, \ldots, k_t; r_s)$ for some integer r_s, and $r_1 + r_2 + \ldots + r_{k_1} = r$. Define also

$$\mathcal{M}_t^1 := \{\mathbf{i} = (i_2, i_3, \ldots, i_{t-1}) \mid 1 \leq i_j \leq k_j, 1 < j < t\}.$$

Definition 12.4 (Dual partition)
For every $\pi \in \mathcal{P}(k_1, k_2, \ldots, k_t; r)$, the dual partition is defined as

$$\pi^*(\mathbf{i}) := k_t - \pi((k_1 + 1, k_2 + 1, \ldots, k_{t-1} + 1) - \mathbf{i}).$$

Note that $\pi^* \in \mathcal{P}(k_1, k_2, \ldots, k_t; k - r)$ and $(\pi^*)^* = \pi$. We define $\Delta(\pi) := n - \nabla(\pi^*)$ for all $\pi \in \mathcal{P}(k_1, k_2, \ldots, k_t; r)$. By the definitions we get that

$$\Delta_r^*(C) = \max\left\{\Delta(\pi) \mid \pi \in \mathcal{P}(k_1, k_2, \ldots, k_t; r + 1)\right\}.$$

Lemma 12.2 (Dual sub-partition)
The dual $(\pi|_s)^*$ of $\pi|_s$ is the $(k_1 - s + 1)$-th sub-partition $\pi^*|_{k_1 - s + 1}$ of π^*.

Proof: We have

$$\begin{aligned}(\pi|_s)^*(\mathbf{i}) &= k_t - \pi|_s(k_2 + 1 - i_2, k_3 + 1 - i_3, \ldots, k_{t-1} + 1 - i_{t-1}) \\ &= k_t - \pi(s, k_2 + 1 - i_2, k_3 + 1 - i_3, \ldots, k_{t-1} + 1 - i_{t-1}).\end{aligned}$$

On the other hand, we have

$$\begin{aligned}\pi^*|_{k_1 - s + 1}(\mathbf{i}) &= \pi^*(k_1 - s + 1, i_2, i_3, \ldots, i_{t-1}) \\ &= k_t - \pi(s, k_2 + 1 - i_2, k_3 + 1 - i_3, \ldots, k_{t-1} + 1 - i_{t-1}).\end{aligned}$$

Comparing the two equations, we see that the lemma holds. □

Lemma 12.3
We have

$$\Delta(\pi) = \sum_{\mathbf{i} \in \mathcal{M}_t} \Delta_{\pi(\mathbf{i}) - 1}(C_t) \prod_{j=1}^{t-1} \delta_{i_j - 1}(C_j),$$

for all $\pi \in \mathcal{P}(k_1, k_2, \ldots, k_t; r + 1)$ and $0 \leq r \leq k - 1$.

Proof: The proof runs by induction on t. We prove first that it holds for $t = 2$, so consider

$$\begin{aligned}\Delta(\pi) = n - \nabla(\pi^*) &= n - \sum_{i \in \mathcal{M}_2} [d_i(C_1) - d_{i-1}(C_1)] d_{\pi^*(i)}(C_2) \\ &= n - \sum_{i \in \mathcal{M}_2} \delta_{k_1 - i}(C_1)(n_2 - \Delta_{k_2 - 1 - \pi^*(i)}(C_2)).\end{aligned}$$

Now we set $j = k_1 + 1 - i$ to get

$$\begin{aligned}\Delta(\pi) &= n - n_2 \sum_{j \in \mathcal{M}_2} \delta_{j-1}(C_1) + \sum_{j \in \mathcal{M}_2} \delta_{j-1}(C_1)\Delta_{\pi(j)-1}(C_2) \\ &= \sum_{j \in \mathcal{M}_2} \delta_{j-1}(C_1)\Delta_{\pi(j)-1}(C_2).\end{aligned}$$

This proves the lemma for $t = 2$. To proceed with induction, we assume that the lemma holds for $t-1$ and recall again the definition of $\nabla(\pi)$ from (12.3), to get

$$\begin{aligned}\nabla(\pi^*) &= \sum_{i_1=1}^{k_1} \Big[\sum_{\mathbf{i} \in \mathcal{M}_t^1} d_{\pi^*|_{i_1}(\mathbf{i})}(C_t) \prod_{j=2}^{t-1} \delta_{k_j - i_j}(C_j) \Big] \delta_{k_1 - i_1}(C_1) \\ &= \sum_{i_1=1}^{k_1} \Big[\sum_{\mathbf{i} \in \mathcal{M}_t^1} d_{(\pi|_{k_1+1-i_1})^*(\mathbf{i})}(C_t) \prod_{j=2}^{t-1} \delta_{k_j - i_j}(C_j) \Big] \delta_{k_1 - i_1}(C_1).\end{aligned}$$

The part in brackets is $\nabla((\pi|_{k_1+1-i_1})^*)$ computed for the code $C_2 \otimes \ldots \otimes C_t$. Hence we get

$$\begin{aligned}\nabla(\pi^*) &= \sum_{i_1=1}^{k_1} \big[n_2 \cdot n_3 \cdot \ldots \cdot n_t - \Delta(\pi|_{k_1+1-i_1}) \big] \delta_{k_1 - i_1}(C_1) \\ &= n - \sum_{i_1=1}^{k_1} \Delta(\pi|_{k_1+1-i_1}) \delta_{k_1 - i_1}(C_1).\end{aligned}$$

Hence

$$\Delta(\pi) = \sum_{i_1=1}^{k_1} \Delta(\pi|_{k_1+1-i_1}) \delta_{k_1 - i_1}(C_1) = \sum_{i_1=1}^{k_1} \Delta(\pi|_{i_1}) \delta_{i_1 - 1}(C_1). \tag{12.4}$$

By the induction hypothesis, we get

$$\begin{aligned}\Delta(\pi) &= \sum_{i_1=1}^{k_1} \Big[\sum_{\mathbf{i} \in \mathcal{M}_t^1} \Delta_{\pi(\mathbf{i})-1}(C_t) \prod_{j=2}^{t-1} \delta_{i_j - 1}(C_j) \Big] \delta_{i_1 - 1}(C_1). \\ &= \sum_{\mathbf{i} \in \mathcal{M}_t} \Delta_{\pi(\mathbf{i})-1}(C_t) \prod_{j=1}^{t-1} \delta_{i_j - 1}(C_j),\end{aligned}$$

as required. □

Define

$$\hat{\mathcal{P}}(k_1, k_2, \ldots, k_t; r) := \bigcup_{r' \leq r} \mathcal{P}(k_1, k_2, \ldots, k_t; r').$$

We have a partial ordering on $\hat{\mathcal{P}}(k_1, k_2, \ldots, k_t; r)$ by setting $\pi' \leq \pi$ if $\pi'(\mathbf{i}) \leq \pi(\mathbf{i})$ for all $\mathbf{i} \in \mathcal{M}_t$. If $\pi \in \mathcal{P}(k_1, k_2, \ldots, k_t; r)$ is a partition, write $\Sigma\pi = r$ for the sum of its values. Note that if we have a sequence of $(k_2, k_3, \ldots, k_t)$-partitions

$$\pi_1 \geq \pi_2 \geq \ldots \geq \pi_{k_1},$$

then the π_i define the sub-partitions $\pi|_i$ of some partition $\pi \in \mathcal{P}(k_1, k_2, \ldots, k_t; r)$, where $r = \Sigma\pi_1 + \Sigma\pi_2 + \ldots + \Sigma\pi_{k_1}$.

12.2.2 The simple case

In this section we study the case $t = 2$ only. Let $C = C_1 \otimes C_2$, where $\dim C = k$. Let γ_1, γ_2, and γ be the projective multiset corresponding to C_1, C_2, and C respectively.

Definition 12.5
Let $\Pi \leqq \mathsf{PG}(k-1, q)$. *For* $0 \leq i \leq k_1 - 1$, *let* $\Theta_i(\Pi)$ *be the set of points* $p \in \mathsf{PG}(k_2 - 1, q)$ *such that there is an* i*-space* $\Phi^i_\Pi(p) \leqq \mathsf{PG}(k_1 - 1, q)$ *with* $\Phi^i_\Pi(p) \otimes p \subseteq \Pi$. *The* associated partition *of* Π *is given by*

$$\pi(\Pi)(i) = \dim\langle \Theta_{i-1}(\Pi) \rangle + 1.$$

Obviously $\Theta_i(\Pi) \subseteq \Theta_{i-1}(\Pi)$, so $\pi(\Pi)$ is indeed a partition. When confusion is not likely, we will write Θ_i for $\Theta_i(\Pi)$. For brevity we write

$$t_i := \dim\langle \Theta_i \rangle = \pi(\Pi)(i+1) - 1.$$

For $x \in \mathsf{PG}(k_2 - 1, q)$ define

$$R(x) := \{ p \otimes x \in \Pi \mid p \in \mathsf{PG}(k_1 - 1, q) \}.$$

By the bilinearity of the Segre embedding we have $R(x) \leqq \mathsf{PG}(k-1, q)$.

Lemma 12.4
If $\Pi \leqq \mathsf{PG}(k-1, q)$ *is an* r*-space, then* $\pi(\Pi) \in \hat{\mathcal{P}}(k_1, k_2; r+1)$.

Proof: Let $b_0, b_1, \ldots, b_{k_2 - 1}$ be a basis for $\mathsf{PG}(k_2 - 1, q)$ such that $b_0, b_1, \ldots, b_{t_i} \in \Theta_i$. For each i where $0 \leq i < k_2$, let $b_i^0, b_i^1, \ldots, b_i^{r_i}$ be a basis for $R(b_i)$ where $r_i = \max\{ j \mid i \leq t_j \}$. Clearly $b_i^j = a_i^j \otimes b_i$ for some $a_i^j \in \mathsf{PG}(k_1 - 1, q)$.

Consider the set

$$B := \{b_i^j \mid 0 \le j \le k_1 - 1, 0 \le i \le t_j\}.$$

Clearly

$$\#B = \sum_{j=0}^{k_1-1} (t_j + 1).$$

The set B is a set of projectively independent points, and $B \subseteq \Pi$. Since $\dim \Pi = r$, we get

$$\Sigma\pi(\Pi) = \sum_{i=0}^{k_1-1} (t_i + 1) = \#B \le r + 1,$$

proving the lemma. □

Lemma 12.5
If $\Pi \leqq \mathsf{PG}(k-1, q)$, *then* $\gamma(\Pi) \le \Delta(\pi(\Pi))$.

Proof: For convenience, we write $\Theta_{k_1} := \emptyset$. If $b \in \Theta_i \setminus \Theta_{i+1}$, then $R(b) = \Phi_i(b) \otimes b$, where $\Phi_i(b)$ is an i-space in $\mathsf{PG}(k_1 - 1, q)$. We have

$$\Pi \cap Y = R(\Theta_0) = \bigcup_{b \in \Theta_0} R(b) = \bigcup_{i=0}^{k_1-1} \bigcup_{b \in \Theta_i \setminus \Theta_{i+1}} (\Phi_i(b) \otimes b),$$

where Y is the Segre variety. Note that the union is disjoint. Hence

$$\begin{aligned}
\gamma(\Pi) = \gamma\Big(\bigcup_{b \in \Theta_0} R(b)\Big) &= \sum_{i=0}^{k_1-1} \sum_{b \in \Theta_i \setminus \Theta_{i+1}} \gamma_1(\Phi_i(b)) \cdot \gamma_2(b) \\
&\le \sum_{i=0}^{k_1-1} \sum_{b \in \Theta_i \setminus \Theta_{i+1}} \Delta_i(C_1) \cdot \gamma_2(b) = \sum_{i=0}^{k_1-1} \delta_i(C_1) \sum_{b \in \Theta_i} \gamma_2(b) \\
&\le \sum_{i=0}^{k_1-1} \delta_i(C_1) \Delta_{t_i}(C_2) = \sum_{i=0}^{k_1-1} \delta_i(C_1) \Delta_{\pi(i+1)-1}(C_2) \\
&= \sum_{i=1}^{k_1} \delta_{i-1}(C_1) \Delta_{\pi(i)-1}(C_2) = \Delta(\pi(\Pi)).
\end{aligned} \tag{12.5}$$

Thus the lemma is proved. □

We observe that this lemma implies $\Delta_r(C_1 \otimes C_2) \le \Delta_r^*(C_1 \otimes C_2)$ and thus proves the bound from Theorem 12.3 for $t = 2$.

Lemma 12.6
If $\Pi' \leqq \Pi \leqq \mathsf{PG}(k-1,q)$, *then* $\pi(\Pi') \leq \pi(\Pi)$.

Proof: Let Θ_i and t_i be as in the definition of $\pi(\Pi)$, and let Θ'_i and t'_i be the corresponding objects for Π'. We only have to prove that $t'_i \leq t_i$ for all i. We obtain Π' from Π by removing points. Hence $\Theta'_i \subseteq \Theta_i$ for all i, and thus $t'_i \leq t_i$ as required. □

12.2.3 The general case

The t component codes C_i correspond to t projective multisets γ_i on $\mathsf{PG}(k_i-1,q)$ for $i = 1,2,\ldots,t$. Let γ be the multiset corresponding to $C = C_1 \otimes C_2 \otimes \ldots \otimes C_t$, and let $k := \dim C$.

Lemma 12.7
For every subspace $\Pi \leqq \mathsf{PG}(k-1,q)$ *of dimension* r *there is a well-defined associated partition* $\pi(\Pi) \in \hat{\mathcal{P}}(k_1,k_2,\ldots,k_t;r+1)$ *such that*

a. $\gamma(\Pi) \leq \Delta(\pi(\Pi))$; *and*

b. if $\Pi' \leqq \Pi \leqq \mathsf{PG}(k-1,q)$, *then* $\pi(\Pi') \leq \pi(\Pi)$.

Proof: We argue by induction on t. The base case, $t = 2$, is proved in Lemmata 12.4, 12.5, and 12.6. Write $k' := k_2 \cdot k_3 \cdot \ldots \cdot k_t$. Let γ' be the projective multiset corresponding to $C_2 \otimes C_3 \otimes \ldots \otimes C_t$.

Let $\Theta_i \subseteq \mathsf{PG}(k'-1,q)$ be the set of points p such that there exists an i-space $\Phi_i \leqq \mathsf{PG}(k_1-1,q)$ where $\Phi_i \otimes p \subseteq \Pi$. Obviously $\Theta_i \subseteq \Theta_{i-1}$. Let $t_i := \dim\langle\Theta_i\rangle$.

By the inductive hypothesis (b) there is a well-defined associated partition $\pi_i \in \hat{\mathcal{P}}(k_2,k_3,\ldots,k_t;t_i+1)$ to $\langle\Theta_i\rangle$ such that

$$\gamma'(\Theta_i) \leq \gamma'(\langle\Theta_i\rangle) \leq \Delta(\pi_i) \tag{12.6}$$

for each i. Furthermore $\pi_i \leq \pi_{i-1}$ by the inductive hypothesis (b) since $\Theta_i \subseteq \Theta_{i-1}$. Hence the π_i can be viewed as the k_1 sub-partitions of some partition

$$\pi \in \hat{\mathcal{P}}(k_1,k_2,\ldots,k_t;r'+1), \text{ where } r' := \sum_{i=0}^{k_1-1}(t_i+1)-1.$$

More precisely, $\pi(i_1,i_2,\ldots,i_{t-1}) = \pi_{i_1-1}(i_2,i_3,\ldots,i_{t-1})$. By an argument similar to that in the proof of Lemma 12.4, we get that $r' \leq r$. Hence

$$\pi \in \hat{\mathcal{P}}(k_1,k_2,\ldots,k_t;r+1).$$

For $x \in \mathsf{PG}(k'-1,q)$ define

$$R(x) := \{p \otimes x \in \Pi \mid p \in \mathsf{PG}(k_1-1,q)\}.$$

By the bilinearity of the Segre embedding, $R(x) \leqq \mathsf{PG}(k-1,q)$. If $b \in \Theta_i \backslash \Theta_{i+1}$, then $R(b) = \Phi_i(b) \otimes b$ for some i-space $\Phi_i(b) \in \mathsf{PG}(k_1-1,q)$.

Now we can write (as in the proof of Lemma 12.5),

$$\Pi \cap Y = R(\Theta_0) = \bigcup_{i=0}^{k_1-1} \bigcup_{b \in \Theta_i \backslash \Theta_{i+1}} R(b),$$

where Y is the Segre variety $\mathsf{PG}(k_1-1,q) \otimes \mathsf{PG}(k'-1,q)$. We get the value as follows,

$$\begin{aligned}
\gamma(\Pi) &= \sum_{i=0}^{k_1-1} \sum_{b \in \Theta_i \backslash \Theta_{i+1}} \gamma_1(\Phi_i(b))\gamma'(b) \\
&\leq \sum_{i=0}^{k_1-1} \Delta_i(C_1) \sum_{b \in \Theta_i \backslash \Theta_{i+1}} \gamma'(b) = \sum_{i=0}^{k_1-1} \delta_i(C_1) \sum_{b \in \Theta_i} \gamma'(b) \qquad (12.7) \\
&= \sum_{i=0}^{k_1-1} \delta_i(C_1)\gamma'(\Theta_i) \leq \sum_{i=0}^{k_1-1} \delta_i(C_1)\Delta(\pi_i) = \Delta(\pi).
\end{aligned}$$

The bound in the last line follows from (12.6), and the very last equality follows from (12.4). This proves (a) assuming that (a) and (b) holds for $t-1$. It remains to prove that (b) holds.

Let π' be the partition associated with $\Pi' \leqq \Pi$, and let $\pi'_i := \pi'|_i$ be the associated sub-partitions. It is sufficient to show that $\pi'_i \leq \pi_i$ for all i. Write $\Theta'_i = \Theta_i(\Pi')$, and recall that $\pi'_i = \pi(\langle \Theta'_i \rangle)$. We obtain Π' by removing points from Π. Hence $\langle \Theta'_i \rangle \leqq \langle \Theta_i \rangle$, and by the inductive hypothesis $\pi'_i \leq \pi_i$ as required. □

12.2.4 When the Chain Condition holds

Lemma 12.8
If $C_1, C_2, \ldots, C_t$ satisfy the chain condition, then for every

$$\pi \in \mathcal{P}(k_1, k_2, \ldots, k_t; r+1)$$

there is an r-space $\Pi \leqq \mathsf{PG}(k-1,q)$ such that $\pi(\Pi) = \pi$ and $\Delta(\pi) = \gamma(\Pi)$.

Moreover, if $\pi' \in \mathcal{P}(k_1, k_2, \ldots, k_t; r'+1)$ and $\pi' \leq \pi$, then there is an r'-space $\Pi' \leqq \Pi$ such that $\pi(\Pi') = \pi'$ and $\Delta(\pi') = \gamma(\Pi')$.

Proof: First consider the case where $t = 2$. Let $p_0, p_1, \ldots, p_{k_1-1}$ be a basis for $\mathsf{PG}(k_1-1,q)$ such that $\langle p_0, p_1, \ldots, p_i \rangle$ is an i-space of maximum value for C_1. Let

$$\emptyset = \Psi_{-1} \subset \Psi_0 \subset \ldots \subset \Psi_{k_2-1} = \mathsf{PG}(k_2-1,q)$$

be a chain of subspaces of maximum value for C_2. Write $t_i = \pi(i+1) - 1$ for $i = 0, 1, \ldots, k_1 - 1$, and let $\Pi = \langle p_i \otimes \Psi_{t_i} \mid i = 0, 1, \ldots, k_1 - 1 \rangle$. Observe that $\Theta_i(\Pi) = \Psi_{t_i}$, hence $\pi(\Pi) = \pi$ and $\dim \Pi = r$. As for the value, it is not hard to verify equality in (12.5). This proves the first statement of the lemma for $t = 2$.

Let $t'_i = \pi'(i+1) - 1$ for $i = 0, 1, \ldots, k_1 - 1$, and let $\Pi' = \langle p_i \otimes \Psi_{t'_i} \mid i = 0, 1, \ldots, k_1 - 1 \rangle$. Clearly $\Pi' \subseteq \Pi$, and the remaining properties of Π' follows by the argument above. Hence the lemma is proved for $t = 2$.

Assuming that the lemma holds for $t - 1$, the inductive step is similar. Let $k' = k_2 k_3 \ldots k_t$, and γ' the projective multiset corresponding to $C' = C_2 \otimes \ldots \otimes C_t$. Let $p_0, p_1, \ldots, p_{k_1 - 1}$ be a basis for $\mathsf{PG}(k_1 - 1, q)$ such that $\langle p_0, p_1, \ldots, p_i \rangle$ is an i-space of maximum value for C_1. Let $\pi_i = \pi|_{i+1}$ be the sub-partitions of π. By the inductive hypothesis, there is a chain

$$\Psi(\pi_{k_1 - 1}) \lneqq \Psi(\pi_{k_1 - 2}) \lneqq \ldots \lneqq \Psi(\pi_0) \lneqq \mathsf{PG}(k' - 1, q),$$

of subspaces of value $\gamma'(\Psi(\pi_i)) = \Delta'(\pi_i)$, where $\Delta'(\pi)$ is computed with the weight hierarchy of C'. The dimension is given by $\dim \Psi(\pi_i) = \Sigma \pi_i - 1$. We define

$$\Pi = \langle p_i \otimes \Psi(\pi_i) \mid i = 0, 1, \ldots, k_1 - 1 \rangle.$$

Observe that $\Theta_i(\Pi) = \Psi(\pi_i)$. Clearly $\dim \Pi = \sum_{i=0}^{k_1 - 1} \Sigma \pi_i - 1 = r$. The value is given by (12.7), and it may be verified that equality holds.

Consider at last a partition $\pi' \leq \pi$. We construct as above a chain of subspaces

$$\Psi(\pi'_{k_1}) \lneqq \Psi(\pi'_{k_1 - 1}) \lneqq \ldots \lneqq \Psi(\pi'_1) \lneqq \mathsf{PG}(k_1 - 1, q).$$

This can, by the induction hypothesis, be done such that $\Psi(\pi'_i) \lneqq \Psi(\pi_i)$. We define

$$\Pi' = \langle p_i \otimes \Psi(\pi'_i) \mid i = 0, 1, \ldots, k_1 - 1 \rangle.$$

Clearly $\Pi' \subseteq \Pi$, and the remaining properties are proved as in the previous paragraph. □

12.3 Some special cases

In this section, we return to the simple product code of two terms, to discuss certain special cases and specific examples.

Theorem 12.4
For any two codes C_1 and C_2, $d_r(C_1 \otimes C_2) = d_r^*(C_1 \otimes C_2)$ for $r \in \{0, 1, 2, k - 2, k - 1, k\}$.

Proof: For $r = 0$ this is trivial, and for $r = 1$ and $r = k$ it is well known. Wei and Yang [WY93] proved it for $r = 2$. Thus it suffices to prove that

$$\Delta_0(C_1 \otimes C_2) = \Delta_0^*(C_1 \otimes C_2) = \delta_0(C_1)\delta_0(C_2),$$
$$\Delta_1(C_1 \otimes C_2) = \Delta_1^*(C_1 \otimes C_2).$$

Let γ_1, γ_2, and γ be the projective multisets corresponding to C_1, C_2, and $C := C_1 \otimes C_2$. We know that $\Delta_i(C) \leq \Delta_i^*(C)$, so it remains only to prove that there exists a point $\wp \in \mathsf{PG}(k-1,q)$ of value $\gamma(\wp) = \delta_0(C_1)\delta_0(C_2)$ and a line $\ell \subseteq \mathsf{PG}(k-1,q)$ of value $\gamma(\ell) = \Delta_1^*(C)$.

The required point is $\wp := p_1 \otimes p_2$ where $\gamma_1(p_1) = \delta_0(C_1)$ and $\gamma_2(p_2) = \delta_0(C_2)$. Let l_1 and l_2 be lines of maximum value for C_1 and C_2 respectively. Then we have two lines: $l_1 \otimes p_2$ of value $\Delta_1(C_1)\delta_0(C_2)$ and $p_1 \otimes l_2$ of value $\delta_0(C_1)\Delta_1(C_2)$, and at least one of these lines has value $\Delta_1^*(C)$. □

Corollary 12.1
For any product code $C_1 \otimes C_2$ of dimension at most 5, $d_r(C_1 \otimes C_2) = d_r^*(C_1 \otimes C_2)$, $0 \leq r \leq k_1 k_2$.

The following examples show that for a six-dimensional product code this may or may not hold for $r = 3 = k - 3$.

Example 12.1
Let $a \in \mathsf{PG}(2,2)$ be a point and $\ell \not\ni a$ a line, and define a projective multiset by $\gamma_1(p) = 1$ for $p \in \ell$ or $p = a$, and $\gamma_1(p) = 0$ otherwise. Now γ_1 corresponds to a binary $[4,3]$ code C_1, which satisfies the chain condition and has difference sequence $(1,2,1)$.

We define a second projective multiset by $\gamma_2(a) = 5$, $\gamma_2(p) = 4$ for $p \in \ell$, and $\gamma_2(p) = 0$ otherwise. Thus γ_2 defines a binary $[17,3]$ code C_2, which does not satisfy the chain condition and whose difference sequence is $(5,7,5)$.

Now consider $C := C_1 \otimes C_2$. To find $\Delta_2^*(C)$ we consider the three possible partitions $\pi \in \mathcal{P}(k_1, k_2; 3)$ which we write as $[\pi(1), \pi(2), \pi(3)]$:

$$[3,0,0]: \quad \Delta(\pi) = \delta_0(C_1)\Delta_2(C_2) = 17,$$
$$[2,1,0]: \quad \Delta(\pi) = \delta_0(C_1)\Delta_1(C_2) + \delta_1(C_1)\Delta_0(C_2) = 22,$$
$$[1,1,1]: \quad \Delta(\pi) = \Delta_2(C_1)\Delta_0(C_2) = 20.$$

The maximum is $\Delta_2^*(C) = 22$, and we conclude that $d_3^* = 4 \cdot 17 - 22 = 46$.

The construction to obtain a plane P of value 22, assumes that all factorisable points in P are contained in the union of two intersecting lines. The best we can do with this approach is to take $P := \langle a' \otimes \ell \cup \ell \otimes b' \rangle$ where $a' \in \ell$ and $b' \in \ell$. This gives $\Delta_2(C) = \gamma(P) = 20 < 22$. Hence $d_3(C) = 48 > 46$.

Example 12.2
Take the previous example and reduce the length of C_2 by setting $\gamma_2(a) = 3$, and $\gamma_2(p) = 2$ for $p \in \varrho$. Now C_2 is a $[9,3]$ non-chain code with difference sequence $(3,3,3)$. This gives the following choices for the maximisation of $\Delta_2^*(C)$:

$$\begin{aligned}
[3,0,0]: &\quad \Delta(\pi) = \delta_0(C_1)\Delta_2(C_2) = 9\\
[2,1,0]: &\quad \Delta(\pi) = \delta_0(C_1)\Delta_1(C_2) + \delta_1(C_1)\Delta_0(C_2) = 12\\
[1,1,1]: &\quad \Delta(\pi) = \Delta_2(C_1)\Delta_0(C_2) = 12.
\end{aligned}$$

The maximum is $\Delta_2^*(C) = 12$, and this is realised by the plane $\mathsf{PG}(2,2) \otimes a$. Hence we get $d_3(C) = d_3^*(C) = 4 \cdot 9 - 12 = 24$.

Remark 12.1
If C_1 and C_2 are chained codes, $C_1 \otimes C_2$ may be chained or non-chained.

That $C_1 \otimes C_2$ may be chained is clear. Let for instance C_1 and C_2 be two simplex codes. Then it is simple to verify that the product code satisfies the chain condition. The example below shows a non-chained product code of two chained terms.

Example 12.3
Let $a, b, c \in \mathsf{PG}(2,2)$ be projectively independent points, and define two projective multisets as follows:

$$\begin{aligned}
\gamma_1(a) = \gamma_1(b) &= 3\\
\gamma_1(c) &= 1\\
\gamma_1(p) &= 0, \quad \forall p \notin \{a,b,c\}\\
\gamma_2(a) &= 3\\
\gamma_2(p) &= 1, \quad \forall p \neq a.
\end{aligned}$$

The projective multisets define two chained codes C_1 and C_2. The product $C = C_1 \otimes C_2$ corresponds to a projective multiset γ on $\mathsf{PG}(8,2)$. All points of positive value in $\mathsf{PG}(8,2)$ are located in three disjoint planes, Π_a, Π_b, and Π_c, consisting of the points with a, b, or c respectively as the first factor. We have

$$\begin{aligned}
\gamma(a \otimes a) = \gamma(b \otimes a) &= 9\\
\gamma(a \otimes p) = \gamma(b \otimes p) &= 3, \quad \forall p \neq a\\
\gamma(c \otimes a) &= 3\\
\gamma(c \otimes p) &= 1, \quad \forall p \neq a.
\end{aligned}$$

We see that the only line of maximum value is $\varrho := \langle a \otimes a, b \otimes a \rangle$, and the planes of maximum value are Π_a and Π_b, neither of which contains ϱ. Hence C is non-chain.

13 Greedy weights of product codes

In Chapter 10, we introduced the greedy weights and proved some duality relations concerning them. In this chapter, we will use techniques from Chapter 12 to find a lower bound on the greedy weights of product codes.

13.1 The result

We use the notation and terminology from Chapter 12. Recall in particular the definition of $\mathcal{M}_t$ from (12.2), and that of partitions from Definition 12.2. We define below the top-down and bottom-up greedy weight analogues of d_r^*, ∇, and Δ_r^*.

Define the greedy differences

$$\begin{aligned}\epsilon_i(C) &:= e_{k-i}(C) - e_{k-1-i}(C),\\ \tilde{\epsilon}_i(C) &:= \tilde{e}_{k-i}(C) - \tilde{e}_{k-1-i}(C).\end{aligned}$$

We define the greedy analogues of ∇ as follows.

$$\begin{aligned}\nabla_E(\pi) &:= \sum_{\mathbf{i}\in\mathcal{M}_t} e_{\pi(\mathbf{i})}(C_t)\prod_{j=1}^{t-1}\epsilon_{k_j-i_j}(C_j),\\ \tilde{\nabla}_E(\pi) &:= \sum_{\mathbf{i}\in\mathcal{M}_t} \tilde{e}_{\pi(\mathbf{i})}(C_t)\prod_{j=1}^{t-1}\tilde{\epsilon}_{k_j-i_j}(C_j).\end{aligned}$$

We also define e_r^* and $\tilde{e}_r^*$ analogously to d_r^*.

$$\begin{aligned}e_r^*(C_1\otimes C_2\otimes\ldots\otimes C_t) &:= \min\left\{\nabla_E(\pi) \mid \pi\in\mathcal{P}(k_1,k_2,\ldots,k_t;r)\right\},\\ \tilde{e}_r^*(C_1\otimes C_2\otimes\ldots\otimes C_t) &:= \min\left\{\tilde{\nabla}_E(\pi) \mid \pi\in\mathcal{P}(k_1,k_2,\ldots,k_t;r)\right\}.\end{aligned}$$

Theorem 13.1
We have

$$\begin{aligned}e_r(C_1\otimes C_2\otimes\ldots\otimes C_t) &\geq e_r^*(C_1\otimes C_2\otimes\ldots\otimes C_t),\\ \tilde{e}_r(C_1\otimes C_2\otimes\ldots\otimes C_t) &\geq \tilde{e}_r^*(C_1\otimes C_2\otimes\ldots\otimes C_t).\end{aligned}$$

The above bound may or may not be met with equality. This is obvious if we consider chained component codes. Then $d_j(C_i) = e_j(C_i)$, and $d_r = e_r^*$. If the product code is chained, then $e_r = d_r = e_r^*$. Otherwise $e_r > d_r = e_r^*$ for some r.

13.2 Redefining the problem

Analogously to the approach for weight hierarchies we will now reformulate the problem in terms of projective multisets. Let π^* be the dual partition of π, as defined in Definition 12.4.

Analogously to $\Delta_i(C)$, we define

$$E_i(C) := \sum_{j=0}^{i} \epsilon_i = e_k(C) - e_{k-1-i}(C), \tag{13.1}$$

$$\tilde{E}_i(C) := \sum_{j=0}^{i} \tilde{\epsilon}_i = \tilde{e}_k(C) - \tilde{e}_{k-1-i}(C), \tag{13.2}$$

and analogously to $\Delta(\pi)$, we let

$$E(\pi) := \sum_{\mathbf{i}\in\mathcal{M}_t} E_{\pi(\mathbf{i})-1}(C_t) \prod_{j=1}^{t-1} \epsilon_{i_j-1}(C_j), \tag{13.3}$$

$$\tilde{E}(\pi) := \sum_{\mathbf{i}\in\mathcal{M}_t} \tilde{E}_{\pi(\mathbf{i})-1}(C_t) \prod_{j=1}^{t-1} \tilde{\epsilon}_{i_j-1}(C_j). \tag{13.4}$$

Lemma 13.1
The above definition is equivalent to

$$E(\pi) = n - \nabla_E(\pi^*),$$
$$\tilde{E}(\pi) = n - \tilde{\nabla}_E(\pi^*).$$

Proof: We prove the first statement explicitly. The second statement is proved similarly by replacing $\epsilon_i(C_j)$ with $\tilde{\epsilon}_i(C_j)$.

First note that

$$\nabla_E(\pi^*) = \sum_{\mathbf{i}\in\mathcal{M}_t} e_{\pi^*(\mathbf{i})}(C_t) \prod_{j=1}^{t-1} \epsilon_{k_j-i_j}(C_j) = \sum_{\mathbf{i}\in\mathcal{M}_t} e_{\pi^*(\mathbf{k}+\mathbf{1}-\mathbf{i})}(C_t) \prod_{j=1}^{t-1} \epsilon_{i_j-1}(C_j),$$

where $\mathbf{k} = (k_1, \ldots, k_{t-1})$, and $\mathbf{1}$ is an all-1 vector. Hence

$$\nabla_E(\pi^*) = \sum_{\mathbf{i}\in\mathcal{M}_t} e_{k_t-\pi(\mathbf{i})}(C_t) \prod_{j=1}^{t-1} \epsilon_{i_j-1}(C_j).$$

We combine this with (13.3) to get

$$E(\pi)+\nabla_E(\pi^*) = \sum_{\mathbf{i}\in\mathcal{M}_t} (E_{\pi(\mathbf{i})-1}(C_t)+e_{k_t-\pi(\mathbf{i})}(C_t))\prod_{j=1}^{t-1}\epsilon_{i_j-1}(C_j)$$
$$= n_t \sum_{\mathbf{i}\in\mathcal{M}_t}\prod_{j=1}^{t-1}\epsilon_{i_j-1}(C_j).$$

It only remains to prove that

$$\sum_{\mathbf{i}\in\mathcal{M}_t}\prod_{j=1}^{t-1}\epsilon_{i_j-1}(C_j) = n_1\cdot n_2\cdot\ldots\cdot n_{t-1}. \tag{13.5}$$

This is obviously true if $t=2$, so we prove it by induction. We have

$$\sum_{\mathbf{i}\in\mathcal{M}_t}\prod_{j=1}^{t-1}\epsilon_{i_j-1}(C_j) = \sum_{i_{t-1}=1}^{k_{t-1}}\epsilon_{i_{t-1}-1}(C_{t-1})\sum_{\mathbf{i}\in\mathcal{M}_{t-1}}\prod_{j=1}^{t-2}\epsilon_{i_j-1}(C_j)$$
$$= n_{t-1}\sum_{\mathbf{i}\in\mathcal{M}_{t-1}}\prod_{j=1}^{t-2}\epsilon_{i_j-1}(C_j).$$

Hence (13.5) follows by induction, and the lemma is proved. □

Similarly to e_r^* and $\tilde{e}_r^*$, we define E_r^* and $\tilde{E}_r^*$, which will give bounds on E_r and $\tilde{E}_r$.

$$E_r^*(C_1\otimes C_2\otimes\ldots\otimes C_t) := \max\{E(\pi)\mid\pi\in\mathcal{P}(k_1,k_2,\ldots,k_t;r+1)\},$$
$$\tilde{E}_r^*(C_1\otimes C_2\otimes\ldots\otimes C_t) := \max\{\tilde{E}(\pi)\mid\pi\in\mathcal{P}(k_1,k_2,\ldots,k_t;r+1)\}.$$

Lemma 13.2
The following two statements are equivalent

$$e_r(C_1\otimes C_2\otimes\ldots\otimes C_t)\geq e_r^*(C_1\otimes C_2\otimes\ldots\otimes C_t),$$
$$E_r(C_1\otimes C_2\otimes\ldots\otimes C_t)\leq E_r^*(C_1\otimes C_2\otimes\ldots\otimes C_t).$$

Also the following two equations are equivalent

$$\tilde{e}_r(C_1\otimes C_2\otimes\ldots\otimes C_t)\geq \tilde{e}_r^*(C_1\otimes C_2\otimes\ldots\otimes C_t),$$
$$\tilde{E}_r(C_1\otimes C_2\otimes\ldots\otimes C_t)\leq \tilde{E}_r^*(C_1\otimes C_2\otimes\ldots\otimes C_t).$$

Proof: By Lemma 13.1, we get that

$$E_r^*(C_1\otimes C_2\otimes\ldots\otimes C_t)+e_r^*(C_1\otimes C_2\otimes\ldots\otimes C_t) = n.$$

By definition $E_r+e_r=n$. Hence the first equivalence follows. The second equivalence is proved in the same way. □

13.3 The proof

13.3.1 The Simple Case

We start with the simple case where $t = 2$. We shall proceed by induction on t in Section 13.3.2. Recall the definition of the associated partition $\pi(\Pi)$ from Definition 12.5. We write $\Phi_\Pi(x) = \Phi^i_\Pi(x)$ for the largest i for which this is defined.

Definition 13.1
Let $\Pi \leqq \mathsf{PG}(k-1,q)$ and $\pi = \pi(\Pi) \in \mathcal{P}(k_1,k_2;r+1)$. We call Π a normal subspace *associated with π if*

1. *all the $\langle\Theta_i(\Pi)\rangle$ are greedy subspaces;*
2. *for each i and for all $x \in \langle\Theta_i\rangle\backslash\langle\Theta_{i+1}\rangle$ with $\gamma_2(x) > 0$, $\Phi_\Pi(x)$ is a greedy i-space; and*
3. $\dim\Pi = r$.

Note that Part 2 of the definition implies that $\gamma_2(x) = 0$ for all $x \in \langle\Theta_i\rangle\backslash\Theta_i$ and consequently that $\gamma_2(\Theta_i) = \gamma_2(\langle\Theta_i\rangle)$.

Lemma 13.3
Let Π be a normal r-space, and let $\Pi'' < \Pi$. Then, for any partition $\pi' \in \mathcal{P}(k_1,k_2;r)$ such that $\pi(\Pi'') \leq \pi' < \pi(\Pi)$, we have $\gamma(\Pi'') \leq E(\pi')$. Equality holds if and only if Π'' is a normal subspace associated with π'.

Note that since Π is a normal subspace, $\Sigma\pi(\Pi) = r+1$, and $\Sigma\pi(\Pi') \leq \dim\Pi'' + 1 < r+1$. Hence $\pi(\Pi'') < \pi(\Pi)$ and there exists indeed some π'.
Proof: We write $\Theta''_i = \Theta_i(\Pi'')$ and $\Theta_i = \Theta_i(\Pi)$. Observe that

$$\gamma(\Pi'') = \sum_{i=0}^{k_1-1} \sum_{x\in\Theta''_i\backslash\Theta''_{i+1}} \gamma_2(x)\gamma_1(\Phi_{\Pi''}(x)). \tag{13.6}$$

We choose a partition π' according to the lemma. There is a unique s such that $\pi'(s+1) = \pi(s+1) - 1$. Let Θ'_s be an arbitrary subspace such that

$$\Theta''_s \subseteq \Theta'_s < \langle\Theta_s\rangle,$$
$$\dim\Theta'_s = \dim\Theta_s - 1 = \pi'(s+1) - 1.$$

Since $\langle\Theta_s\rangle$ is a greedy subspace, we get that $\gamma(\Theta'_s) \leq E_{\pi'(s+1)-1}(C_2)$. Write $\Theta'_i = \Theta_i$ for all $i \neq s$. Thus we get, for all i,

$$\Theta''_i \subseteq \Theta'_i, \tag{13.7}$$
$$\gamma_2(\Theta''_i) \leq \gamma_2(\Theta'_i) \leq E_{\pi'(i+1)-1}(C_2). \tag{13.8}$$

If $y \in \Theta_s \backslash \Theta'_s$, then $\Phi_{\Pi''}(y) < \Phi_\Pi(y)$. Since $\Phi_\Pi(y)$ is a greedy s-space whenever $\gamma_2(y) \neq 0$, we get that

$$\gamma_1(\Phi_{\Pi''}(y))\gamma_2(y) \leq E_{s-1}(C_1)\gamma_2(y).$$

Clearly $\Phi_{\Pi''}(x) \leqq \Phi_\Pi(x)$ for all $x \in \mathsf{PG}(k_2 - 1, q)$, and

$$\gamma_1(\Phi_\Pi(x))\gamma_2(x) \leq E_i(C_1)\gamma_2(x), \quad \forall x \in \Theta_i \backslash \Theta_{i+1}.$$

Hence we get for any i that

$$\gamma_1(\Phi_{\Pi''}(x))\gamma_2(x) \leq E_i(C_1)\gamma_2(x), \quad \forall x \in \Theta'_i \backslash \Theta'_{i+1}. \tag{13.9}$$

Thus we get from (13.6) that

$$\gamma(\Pi'') \leq \sum_{i=0}^{k_1-1} \sum_{x \in \Theta''_i \backslash \Theta''_{i+1}} \gamma_2(x) E_i(C_1). \tag{13.10}$$

This may be simplified further to

$$\begin{aligned}
\gamma(\Pi'') &\leq \sum_{i=0}^{k_1-1} E_i(C_1)\gamma_2(\Theta''_i \backslash \Theta''_{i+1}) \\
&= \sum_{i=0}^{k_1-1} E_i(C_1)(\gamma_2(\Theta''_i) - \gamma_2(\Theta''_{i+1})) \\
&= \sum_{i=0}^{k_1-1} E_i(C_1)\gamma_2(\Theta''_i) - \sum_{i=1}^{k_1} E_{i-1}(C_1)\gamma_2(\Theta''_i).
\end{aligned}$$

Now observe that Θ''_{k_1} is the empty set, and $\epsilon_0(C_1) = E_0(C_1)$. Hence

$$\gamma(\Pi'') \leq \sum_{i=0}^{k_1-1} \epsilon_i(C_1)\gamma_2(\Theta''_i) \leq \sum_{i=1}^{k_1} \epsilon_{i-1}(C_1) E_{\pi'(i)-1}(C_2) = E(\pi'),$$

by (13.8). This proves the bound in the lemma.

It remains to prove that equality depends on Π'' being a normal subspace associated with π'. Assume therefore that $\gamma(\Pi'') = E(\pi')$. To obtain this, we must have equality in (13.9), which means that $\Phi_{\Pi''}(x))$ is a greedy i-space whenever $\gamma_2(x) > 0$, proving Property 2 in the definition. Equality is also required in (13.8), which implies that $\langle \Theta''_i \rangle$ must be a greedy subspace of dimension $\pi'(i+1) - 1$, proving Property 1 and the fact that $\pi(\Pi'') = \pi'$.

Finally we observe that $\dim \Pi'' \leq r - 1$ since it is a proper subspace of Π. Also $\dim \Pi'' \geq \Sigma\pi' - 1 = r - 1$. Hence $\dim \Pi'' = r - 1$, which is the third property in the definition. The lemma follows by induction. □

Definition 13.2
A greedy basis of $\mathsf{PG}(k_i - 1, q)$ *is a basis* $p_0, p_1, \ldots, p_{k_1-1}$ *such that* $\langle p_0, p_1, \ldots, p_r \rangle$ *is a greedy* r*-space for each* r*.*

Lemma 13.4
Given a fixed greedy basis for each space $\mathsf{PG}(k_1 - 1, q)$ *and* $\mathsf{PG}(k_2 - 1, q)$*, there is a well-defined normal subspace* Π_π *associated with every partition* π*, such that if* $\pi' \leq \pi$*, then* $\Pi_{\pi'} \leqq \Pi_\pi$*.*

Proof: Let $b_0, b_1, \ldots, b_{k_2-1}$ be the greedy basis for $\mathsf{PG}(k_2 - 1, q)$. Write

$$\Psi_i = \langle b_0, b_1, \ldots, b_i \rangle.$$

Let $p_0, p_1, \ldots, p_{k_1-1}$ be the greedy basis for $\mathsf{PG}(k_1 - 1, q)$. We define Π_π by the following formula,

$$\Pi_\pi = \langle p_i \otimes \Psi_{\pi(i+1)-1} \mid 0 \leq i < k_1 \rangle.$$

It is straightforward to verify the properties of Π_π. □

Proposition 13.1
If $\Pi \leqq \mathsf{PG}(k - 1, q)$ *is a greedy subspace of dimension* r*, then* Π *is a normal subspace and* $\gamma(\Pi) = E(\pi)$ *where* $\pi = \pi(\Pi) \in \mathcal{P}(k_1, k_2; r + 1)$

We omit the proof, which is exactly identical to that of Proposition 13.2.

Corollary 13.1
For all codes C_1 *and* C_2*, we have*

$$E_r(C_1 \otimes C_2) \leq \max\{E(\pi) \mid \pi \in \mathcal{P}(k_1, k_2; r + 1)\}.$$

13.3.2 The General Case

We shall generalise the results from the last section by induction on t. We define normal subspaces recursively as follows.

Definition 13.3
Let $\Pi \leqq \mathsf{PG}(k - 1, q)$ *and* $\pi = \pi(\Pi) \in \mathcal{P}(k_1, k_2, \ldots, k_t; r + 1)$*. We call* Π *a* normal subspace *associated with* π *if*

1. *for each* i, $\langle \Theta_i(\Pi) \rangle$ *is a normal subspace associated with* $\pi|_{i+1}$*;*
2. *for each* i *and for all* $x \in \langle \Theta_i \rangle \backslash \langle \Theta_{i+1} \rangle$ *with* $\gamma'(x) > 0$, $\Phi_\Pi(x)$ *is a greedy* i*-space; and*
3. $\dim \Pi = r$*.*

Lemma 13.5
Let Π be a normal r-space, and let $\Pi'' < \Pi$ be a subspace. Then for any partition $\pi' \in \mathcal{P}(k_1, k_2, \ldots, k_t; r)$ such that $\pi(\Pi'') \le \pi' < \pi(\Pi)$, we have $\gamma(\Pi'') \le E(\pi')$. Equality holds if and only if Π'' is a normal subspace associated with π'.

Note that there must exist π' by the same reasoning used in conjunction with Lemma 13.3.

Proof: This was proved for $t = 2$ in Lemma 13.3. We assume that it holds for $t-1$ and prove it for t.

We write $\Theta''_i = \Theta_i(\Pi'')$ and $\Theta_i = \Theta_i(\Pi)$. Observe that

$$\gamma(\Pi'') = \sum_{i=0}^{k_1-1} \sum_{x \in \Theta''_i \setminus \Theta''_{i+1}} \gamma'(x)\gamma_1(\Phi_{\Pi''}(x)). \tag{13.11}$$

We choose an arbitrary partition π' according to the lemma. We write $u_i := \Sigma\pi|_{i+1} - 1$ and $u'_i := \Sigma\pi'|_{i+1} - 1$ for brevity. There is a unique s such that $u'_s = u_s - 1$. Let Θ'_s be an arbitrary subspace such that

$$\Theta''_s \subseteq \Theta'_s < \langle \Theta_s \rangle,$$
$$\dim \Theta'_s = \dim\langle \Theta_s \rangle - 1 = u'_s.$$

Since $\langle \Theta_s \rangle$ is a normal subspace, we get that $\gamma'(\Theta'_s) \le E(\pi'|_{s+1})$, by the induction hypothesis. Write $\Theta'_i = \Theta_i$ for all $i \ne s$. Thus we get, for all i,

$$\Theta''_i \subseteq \Theta'_i, \tag{13.12}$$
$$\gamma'(\Theta''_i) \le \gamma'(\Theta'_i) \le E(\pi'|_{i+1}). \tag{13.13}$$

If $y \in \Theta_s \setminus \Theta'_s$, then $\Phi_{\Pi''}(y) < \Phi_\Pi(y)$. Since $\Phi_\Pi(y)$ is a greedy subspace of dimension s whenever $\gamma'(y) > 0$, we get that

$$\gamma_1(\Phi_{\Pi''}(y))\gamma'(y) \le E_{s-1}(C_1)\gamma'(y).$$

Clearly $\Phi_{\Pi''}(x) \leqq \Phi_\Pi(x)$ for all $x \in \mathsf{PG}(k'-1, q)$, and

$$\gamma_1(\Phi_\Pi(x))\gamma'(x) \le E_i(C_1)\gamma'(x), \quad \forall x \in \Theta_i \setminus \Theta_{i+1}.$$

Hence we get for any i that

$$\gamma_1(\Phi_{\Pi''}(x))\gamma'(x) \le E_i(C_1)\gamma'(x), \quad \forall x \in \Theta'_i \setminus \Theta'_{i+1}. \tag{13.14}$$

From (13.11) we find that

$$\gamma(\Pi'') \le \sum_{i=0}^{k_1-1} \sum_{x \in \Theta''_i \setminus \Theta''_{i+1}} \gamma'(x) E_i(C_1). \tag{13.15}$$

This may be simplified further to

$$\begin{aligned}\gamma(\Pi'') &\leq \sum_{i=0}^{k_1-1} E_i(C_1)\gamma'(\Theta''_i \setminus \Theta''_{i+1}) \\ &= \sum_{i=0}^{k_1-1} E_i(C_1)(\gamma'(\Theta''_i) - \gamma'(\Theta''_{i+1})) \\ &= \sum_{i=0}^{k_1-1} E_i(C_1)\gamma'(\Theta''_i) - \sum_{i=1}^{k_1} E_{i-1}(C_1)\gamma'(\Theta''_i).\end{aligned}$$

Now observe that Θ''_{k_1} is the empty set, and $\epsilon_0(C_1) = E_0(C_1)$. Hence

$$\gamma(\Pi'') \leq \sum_{i=0}^{k_1-1} \epsilon_i(C_1)\gamma'(\Theta''_i) \leq \sum_{i=1}^{k_1} \epsilon_{i-1}(C_1)E(\pi'|_{i+1}) = E(\pi'),$$

by (13.13) and the induction hypothesis. This proves the bound in the lemma.

It remains to prove that equality depends on Π'' being a normal subspace associated with π'. Assume therefore that $\gamma(\Pi'') = E(\pi')$. Then we must have equality in (13.13), which requires equality in (13.12). It follows that $\pi(\Pi'') = \pi'$. Another necessary condition for equality in (13.13), is that all the Θ'_i be greedy subspaces. By the induction hypothesis it follows that Θ_i is a normal subspace associated with $\pi'|_{i+1}$, which is Property 1 in Definition 13.3

We must also have equality in (13.15), which in turn depends on equality in (13.14). Hence $\Phi_{\Pi''}(x)$ must be a greedy subspace for all $x \in \mathsf{PG}(k'-1,q)$ such that $\gamma'(x) > 0$. This proves Property 2 in Definition 13.3.

Finally we observe that $\dim \Pi'' \leq r-1$ since it is a proper subspace of Π. Also $\dim \Pi'' \geq \Sigma\pi' - 1 = r-1$. Hence $\dim \Pi'' = r-1$, which is the third property in the definition. The lemma follows by induction. □

Lemma 13.6
Given a fixed greedy basis for each space $\mathsf{PG}(k_i - 1, q)$*, there is a well-defined normal subspace* Π_π *associated with every partition* π*, such that if* $\pi' \leq \pi$*, then* $\Pi_{\pi'} \leqq \Pi_\pi$*.*

Proof: This holds for $t = 2$ by Lemma 13.4. We prove it for all t by induction. Therefore we assume that for every $\pi_r \in \mathcal{P}(k_2, k_3, \ldots, k_t; r+1)$, there is a well-defined normal subspace $\Psi_{\pi_r} \leqq \mathsf{PG}(k'-1,q)$ associated with π_r. Let $p_0, p_1, \ldots, p_{k_1-1}$ be a greedy basis for $\mathsf{PG}(k_1 - 1, q)$.

The Π_π may be given by the following formula,

$$\Pi_\pi = \langle p_{i-1} \otimes \Psi_{\pi|_i} \mid 1 \leq i \leq k_1 \rangle.$$

It is straightforward to verify the properties of this subspace. □

Proposition 13.2
If $\Pi \leqq \mathsf{PG}(k-1,q)$ *is a greedy subspace of dimension* r*, then* Π *is a normal subspace and* $\gamma(\Pi) = E(\pi)$ *where* $\pi = \pi(\Pi) \in \mathcal{P}(k_1, k_2, \ldots, k_t; r+1)$.

Proof: Note that $\mathsf{PG}(k-1,q)$ is a normal subspace associated with π where $\pi(\mathbf{i}) = k_t$ for all $\mathbf{i} \in \mathcal{M}_t$. Also $\mathsf{PG}(k-1,q)$ is the unique greedy $(k-1)$-space. Hence the lemma holds for $r = k-1$. Assume that the lemma holds for r. We will prove that then it also holds for $r-1$.

Let Π and Π' be greedy subspaces of dimensions r and $r-1$ respectively, such that $\Pi' < \Pi$. By the inductive hypothesis, Π is a normal subspace associated with some partition π. Also write $\pi' = \pi(\Pi')$. By Lemma 13.5, $\gamma(\Pi') \leq E(\pi'')$ for every partition $\pi'' \in \mathcal{P}(k_1, k_2, \ldots, k_t; r)$ with $\pi' \leq \pi'' < \pi$.

By Lemma 13.4, there exists, for every such partition π'', a normal subspace $\Pi_{\pi''} < \Pi$ of value $E(\pi'')$, so $E_{r-1} \geq E(\pi'')$, and thus $\gamma(\Pi') = E(\pi'')$ and Π' is a normal subspace by Lemma 13.5. The lemma follows by induction. □

Corollary 13.2
For any family codes $C_1, C_2, \ldots, C_t$*, we have*

$$E_r(C_1 \otimes C_2 \otimes \ldots \otimes C_t) \leq \max\{E(\pi) \mid \pi \in \mathcal{P}(k_1, k_2, \ldots, k_t; r+1)\}.$$

This proves the first bound of Theorem 13.1. We can in fact phrase a stronger result. We know that equality holds for $r = k-1$, since $E_{k-1} = \Delta_{k-1}$. Let $P_r \subseteq \mathcal{P}(k_1, k_2, \ldots, k_t; r+1)$ be the set of partitions achieving the maximum in the corollary. Then we have that

$$E_r(C) = \max\{E(\pi) \mid \pi \in \mathcal{P}(k_1, k_2, \ldots, k_t; r+1), \exists \pi' \in P_{r+1}, \pi \leq \pi'\}.$$

The problem with such an expression is of course that we must compute all the E_r in sequence, and we must find all partitions achieving maximum in each step.

13.3.3 Top-down Greedy Weights

The proof for top-down greedy weights is very similar to that for bottom-up greedy weights (and just as long). We will only list the definitions and the main lemmata for the induction step. The proofs can be filled in by following the pattern of the preceding sections.

Definition 13.4
Let $\Pi \leqq \mathsf{PG}(k-1,q)$ *and* $\pi = \pi(\Pi) \in \mathcal{P}(k_1, k_2, \ldots, k_t; r+1)$*. We call* Π *a* top-down normal subspace *associated with* π *if*

1. *for each* i, $\Theta_i(\Pi)$ *is a top-down normal subspace associated with* $\pi|_{i+1}$ *(or if* $t = 2$*, a top-down greedy* i*-space).*

2. *for each i and for all $x \in \Theta_i \backslash \Theta_i'$ with $\gamma'(x) > 0$, $\Phi_\Pi(x)$ is a top-down greedy i-space.*

3. $\dim \Pi = r$.

Lemma 13.7
Let Π be a top-down normal r-space, and let $\Pi'' > \Pi$ be an $(r+1)$-space. Then $\gamma(\Pi'') \leq E(\pi(\Pi''))$. Equality holds if and only if Π'' is a top-down normal subspace.

Definition 13.5
A top-down greedy basis $\mathsf{PG}(k_i - 1, q)$ is a basis $p_0, p_1, \ldots, p_{k_1-1}$ such that $\langle p_i \mid 0 \leq i \leq r \rangle$ is a top-down greedy r-space.

Lemma 13.8
Given a fixed top-down greedy basis for each space $\mathsf{PG}(k_i - 1, q)$, there is a well-defined top-down normal subspace Π_π associated with every partition π, such that if $\pi' \leq \pi$, then $\Pi_{\pi'} \leqq \Pi_\pi$.

Proposition 13.3
If $\Pi \leqq \mathsf{PG}(k-1, q)$ is a top-down greedy subspace of dimension r, then Π is a normal subspace and $\gamma(\Pi) = \tilde{E}(\pi)$ where

$$\pi = \pi(\Pi) \in \mathcal{P}(k_1, k_2, \ldots, k_t; r+1).$$

Corollary 13.3
For any family codes $C_1, C_2, \ldots, C_t$, we have

$$\tilde{E}_r(C_1 \otimes C_2 \otimes \ldots \otimes C_t) \leq \max\{\tilde{E}(\pi) \mid \pi \in \mathcal{P}(k_1, k_2, \ldots, k_t; r+1)\}.$$

This proves the second bound of Theorem 13.1.

14 Future research

The central theme of the thesis has been the relation between projective multisets and linear codes. From this single starting point, several problems have been studied, but even more problems remain. I do not think there are any limits to what coding problems we may try to solve with projective multisets. Below we will present some examples of such problems as well as some possible applications of the parameters we have studied. Recollect that we discussed problems regarding the SWD in Section 11.5.

14.1 Product codes

Product codes have been suggested for turbo coding schemes during the last couple of years. Usually their performance is estimated by simulation, but for some applications, extremely low bit error rates are required, and then simulation is not practically feasible. Hence it will be of great value to compute (or even estimate) the weight enumerator for such codes, from which the bit error rate may be computed analytically.

Projective multisets have been useful for computing the weight hierarchy of product codes, and they might become useful for computing support weight distributions as well. Then we must remember Theorem 11.1, which give weight enumerators from support weight enumerators. The low-order terms of the weight enumerator of an arbitrary product code is known from [TBHN98]. Our interest should therefore be in the high-order terms, and it is probably best to expect the best results for particular classes of codes.

Problem 14.1
Can the proof of Theorem 11.1 be modified or extended to give the weight enumerator for a product code $C \otimes P_l$ where P_l is an $[l+1, l]$ parity check code and C an arbitrary linear code with known SWD?

Similar questions may questions may be posed when P_l is replaced by other codes with well-known and simple structure.

The weight enumerator for product codes where the terms are $[n, n-1]$ parity check codes, first-order Reed-Muller codes, or simplex codes were studied in [And00]. By solving the following problem we will obtain weight enumerators for some three-term product codes by Theorem 11.1.

Problem 14.2
Compute the SWD for product codes where each component is a simplex code, an even parity check code, or a first-order Reed-Muller code.

A more difficult problem is *hyper-product codes* (HPC) as considered by Wang [Wan00]. An HPC is a product code, possibly multi-dimensional, with extra parity bits computed along each hyper-diagonal. Wang seems to get good estimates on the bit error rate for 2-D and 3-D HPC-s based on Hamming codes and even parity check codes, but nevertheless he relies to some extent on estimates and not accurate expressions for the weight enumerators. An important issue in his thesis is design rules to construct HPC-s with good properties.

Problem 14.3
Describe HPC-s in terms of projective multisets, and study their weight hierarchies.

Problem 14.4
Compute the weight enumerator of some HPC-s built from simple parity check codes.

14.2 Cyclic codes

The projective multisets corresponding to irreducible cyclic codes have a very nice structure. Consider an $[n,k]$ q-ary irreducible cyclic code C. We know that q-ary vectors of length k can be viewed as elements of the field $\mathsf{GF}(q^k)$. Taking a cyclic subgroup of the multiplicative group $\mathsf{GF}(q^k)^*$ and viewing the elements as vectors, we get the vector multiset $\overline{\gamma}_C$ corresponding to C.

Problem 14.5
Can we obtain results on the weight hierarchy or the support weight distribution for the vector multiset $\overline{\gamma}_C$ described above?

In the literature we find several partly answered questions about higher weights of cyclic codes.

Problem 14.6
The weight hierarchy of the binary Kasami codes was computed in [HK95]. Compute the weight hierarchy of the non-binary Kasami codes.

Problem 14.7
An irreducible cyclic $[n,k]$ code is said to be semiprimitive if $n = (2^k-1)/N$ where $N > 2$ divides 2^j+1 for some $j \geq 1$. The weight hierarchy of the semiprimitive codes where $k/2j$ is odd was found in [HK96b]. Can it be found in the remaining cases as well?

BCH codes have received much attention in the research on weight hierarchies. The most recent work we have seen is [Ich99] which deals with asymptotic weight hierarchy of BCH codes. Most other works deals with d_2 and d_3 for 2- and 3-error correcting BCH codes and their duals. Here seems to be plenty of interesting open problems.

14.3 Trellis complexity

According to Forney [For94b], the weight hierarchy gives on the trellis complexity a bound, which can only be met with equality if the code satisfies the two-way chain condition.

Problem 14.8
Can the greedy weights be used to improve the bound on the trellis complexity? If not, can new and better parameters for projective multisets be found to improve said bounds?

Problem 14.9
Can the trellis complexity of $C_1 \otimes C_2$ be computed from the individual complexities of C_1 and C_2?

14.4 Sub-chain conditions

A considerable part of this dissertation is occupied by the discussion of the weight hierarchy of extremal non-chain codes. This forms but a tiny part of a huge project undertaken by Wende Chen, Torleiv Kløve, and others, namely a classification of possible weight hierarchies with respect to the sub-chain conditions.

For chained codes, we approach a full classification of possible weight hierarchies. The most recent work we have seen is [LCF01]. There are substantial results for arbitrary q and arbitrary dimension. Ternary codes of dimension five is considered specifically and only a very few potential weight hierarchies remain open. The completists may want to solve the remaining cases.

Extremal non-chain codes have been studied in dimension four by Chen and Kløve. In this thesis we have found a general bound on the difference sequence of such codes. We have also proved the bounds to be optimal in dimension five (and partly in dimension six), but it would still be interesting to see optimal constructions working for arbitrarily high dimension.

In the binary case, Chen and Kløve have been more thorough [CK99b], by finding both upper and lower bounds. We have not yet seen any attempts to generalise these results to higher dimension nor for non-binary codes. Both these generalisations may be interesting.

We have also seen an extensive work on the remaining seven classes of codes in dimension four, with bounds in the non-binary case [CK97b] and a near full classification in the binary case [CK98a]. Similar work in higher dimension seems like an endless project at present, since the number of classes increases so rapidly. Yet, new works seem to appear steadily. The latest we have seen is [CK01b], which introduces a subcase of B-codes, defined by the so-called ‘almost chain condition’.

14.5 Other problems

Separating codes were introduced in [FGU69], and have been revitalised recently in the research on fingerprinting codes. Fingerprinting is a technique for copyright protection. A decent introduction to the topic may be found in [BS98]. Recent research [CES01] indicates some links between separating properties and higher weights.

Bibliography

[And00] Richard Andrew. The weight distributions of some product codes. In *Proc. IEEE Intern. Symp. Inform. Theory*, page 226, 2000. 14.1

[Beu80] Albrecht Beutelspacher. Blocking sets and partial spreads in finite projective spaces. *Geometrica Dedicata*, 9:425–449, 1980. 2.3, 3.2

[BS98] Dan Boneh and James Shaw. Collusion-secure fingerprinting for digital data. *IEEE Trans. Inform. Theory*, 44(5):1897–1905, 1998. Presented in part at CRYPTO'95. 14.5

[BT95] Angela I. Barbero and Juan G. Tena. Weight hierarchy of a product code. *IEEE Trans. Inform. Theory*, 41(5):1475–1479, September 1995. 12.1

[CC01] Houshou Chen and John T. Coffey. Trellis structure and higher weights of extremal self-dual codes. *Designs, Codes, and Cryptography*, 24(1–3):15–36, 2001. 1.1, 11.2

[CES01] GÃ©rard D. Cohen, Sylvia B. Encheva, and Hans Georg Schaathun. On separating codes. Technical report, Ecole Nationale SupÃ©rieure des TÃ©lÃ©communications, 2001. 14.5

[CEZ99] GÃ©rard D. Cohen, Sylvia B. Encheva, and Gilles ZÃ©mor. Antichain codes. *Designs, Codes, and Cryptography*, 18(1-3):71–80, 1999. 1.1, 2.2, 10, 10.2, 10.1, 10.2

[CK96] Wende Chen and Torleiv Kløve. The weight hierarchies of q-ary codes of dimension 4. *IEEE Trans. Inform. Theory*, 42(6):2265–2272, November 1996. 1.1, 1.3, 2.5

[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. 1.1, 1.2, 1.3, 2.5, 3, 3.3, 3.4

[CK97b] Wende Chen and Torleiv Kløve. Bounds on the weight hierarchies of linear codes of dimension 4. *IEEE Trans. Inform. Theory*, 43(6):2047–2054, 1997. 2.5, 9.3, 10.2, 10.2, 14.4

[CK98a] Wende Chen and Torleiv Kløve. Classification of the weight hierarchies of binary linear codes of dimension 4. Technical Report 147, Dept. of Informatics, University of Bergen, March 1998. 2.5, 14.4

[CK98b] Wende Chen and Torleiv Kløve. Weight hierarchies of linear codes satisfying the chain condition. *Designs, Codes, and Cryptography*, 11, 1998. 2.5

[CK99a] Wende Chen and Torleiv Kløve. On the second greedy weight for binary linear codes. In M. Fossorier et al., editor, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 1719 of *Springer Lecture Notes in Computer Science*, pages 131–141. Springer-Verlag, 1999. 1.1, 10

[CK99b] Wende Chen and Torleiv Kløve. Weight hierarchies of extremal non-chain binary codes of dimension 4. *IEEE Trans. Inform. Theory*, 45(1):276–289, 1999. 1.1, 1.3, 2.5, 3, 6, 6.1, 6.1, 6.3, 14.4

[CK01a] Wende Chen and Torleiv Kløve. On the second greedy weight for linear codes of dimension 3. *Discrete Math.*, 241(1–3):171–187, 2001. 1.1, 10

[CK01b] Wende Chen and Torleiv Kløve. Weight hierarchies of linear codes satisfying the almost chain condition. Technical Report 215, Dept. of Informatics, University of Bergen, May 2001. 14.4

[CS01] Antonio Cossidente and Alessandro Siciliano. A geometric construction of an optimal $[67, 9, 30]$ binary code. *IEEE Trans. Inform. Theory*, 47(3):1187–1189, March 2001. 1.2

[DG01] Steven Dougherty and Aaron Gulliver. Higher weights of self-dual codes. In Daniel Augot, editor, *Workshop on Coding and Cryptography*, pages 177–188, January 2001. 11.2

[DGO03] Steven Dougherty, Aaron Gulliver, and Manabu Oura. Higher weights and graded rings for binary self-dual codes. *Discrete Applied Mathematics*, 128:251–261, 2003. Special issue for WCC 2001. 11.2

[Dou01] Steven Dougherty. Does there exist a [72,36,16] Type II code?, 2001. `http://academic.scranton.edu/faculty/doughertys1/72.htm`. 11.2

[DS98] Stefan Dodunekov and Juriaan Simonis. Codes and projective multisets. *Electron. J. Combin.*, 5(1), 1998. Research Paper 37. 1.2, 2.4

[EK94] Sylvia Encheva and Torleiv Kløve. Codes satisfying the chain condition. *IEEE Trans. Inform. Theory*, 40:175–180, 1994. 2.5

[FGU69] A. D. Friedman, R. L. Graham, and J. D. Ullman. Universal single transition time asynchronous state assignments. *IEEE Trans. Comput.*, 18:541–547, 1969. 14.5

[FKLT93] Toru Fujiwara, Tadao Kasami, Shu Lin, and Toyoo Takata. On the optimum bit orders with respect to the state complexity of trellis diagrams for binary linear codes. *IEEE Trans. Inform. Theory*, 39(1):242–245, 1993. 1.1, 10.1

[For94a] G. David Forney, Jr. Density/length profiles and trellis complexity of lattices. *IEEE Trans. Inform. Theory*, 40(6):1753–1772, 1994. 1.1

[For94b] G. David Forney, Jr. Dimension/length profiles and trellis complexity of linear block codes. *IEEE Trans. Inform. Theory*, 40(6):1741–1752, 1994. 1.1, 10.1, 14.3

[Hel79] Tor Helleseth. The weight distribution of the coset leaders for some classes of codes with related parity-check matrices. *Discrete Math.*, 28(2):161–171, 1979. 11.2

[Hel78] Tor Helleseth. The weight enumerator polynomials of some classes of codes with composite parity-check polynomials. *Discrete Math.*, 20(1):21–31, 1977/78. 11.2

[Hir98] James W. P. Hirschfeld. *Projective Geometries over Finite Fields*. Oxford University Press, second edition, 1998. 2.3, 3.2

[HK95] Tor Helleseth and P. Vijay Kumar. The weight hierarchy of the Kasami codes. *Discrete Math.*, 145(1-3):133–143, 1995. 14.6

[HK96a] Tor Helleseth and Torleiv Kløve. The weight hierarchies of some product codes. *IEEE Trans. Inform. Theory*, 42(3):1029–1034, 1996. 12.1

[HK96b] Tor Helleseth and P. Vijay Kumar. On the weight hierarchy of the semiprimitive codes. *Discrete Math.*, 152(1-3):185–190, 1996. 14.7

[HKM77] Tor Helleseth, Torleiv Kløve, and Johannes Mykkeltveit. The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l-1)/n)$. *Discrete Math.*, 18:179–211, 1977. 1.1, 11, 11.2

[HKY92] Tor Helleseth, Torleiv Kløve, and Øyvind Ytrehus. Generalized Hamming weights of linear codes. *IEEE Trans. Inform. Theory*, 38(3):1133–1140, 1992. 1.2

[Ich99] Chzhan Ichun. Generalized spectra of binary BCH codes. *Problemy Peredachi Informatsii*, 35(3):3–17, 1999. 14.2

[Kløve78] Torleiv Kløve. The weight distribution of linear codes over $GF(q^l)$ having generator matrix over $GF(q)$. *Discrete Math.*, 23:159–168, 1978. 11.2, 11.3

[Kløve92] Torleiv Kløve. Support weight distribution of linear codes. *Discrete Math.*, 106/107:311–316, 1992. 11.2

[LCF01] Yuan Luo, Wende Chen, and Fang-Wei Fu. On the weight hierarchies satisfying the chain condition. In *Applied Algebra, Algebraic Algorithms and Error Correcting Codes. Proceedings*, November 2001. Abstract. 14.4

[Mac63] Jessie MacWilliams. A theorem on the distribution of weights in a systematic code. *Bell System Tech. J.*, 42:79–94, 1963. 11.2

[MCC03] Olgica Milenkovic, Sean T. Coffey, and Kevin J. Compton. The third support weight enumerators of the doubly-even, self-dual $[32, 16, 8]$ codes. *IEEE Trans. Inform. Theory*, 49(3):740–746, 2003. 11.2

[Mil01a] Olgica Milenkovic. Generalized Hamming and complete coset weight enumerators of isodual codes. Preprint, July 2001. 11.2

[Mil01b] Olgica Milenkovic. On the generalized Hamming weight enumerators and coset weight distributions of even isodual codes. In *Proc. IEEE Intern. Symp. Inform. Theory*, page 62, June 2001. 11.2

[MPW01] Conchita MartÃnez-PÃ©rez and Wolfgang Willems. On the weight hierarchy of product codes. Preprint submitted to *Designs, Codes, and Cryptography*, 2001. 12.1, 12.2

[OW84] L. H. Ozarow and A. D. Wyner. Wire-tap channel II. *AT&T Bell Laboratories Technical Journal*, 63(10):2135–2157, December 1984. 10.1, 10.1

[Par00a] Jeng Yune Park. The weight hierarchies of outer product codes. *Discrete Math.*, 224:193–205, September 2000.

[Par00b] Jeng Yune Park. The weight hierarchies of some product codes. *IEEE Trans. Inform. Theory*, 46(6):2228–2235, September 2000. 12.1

[RB98] Ilan Reuven and Yair Be'ery. Entropy/length profiles, bounds on the minimal covering of bipartite graphs, and the trellis complexity of nonlinear codes. *IEEE Trans. Inform. Theory*, 44(2):580–598, March 1998. 10.1

[RB99] Ilan Reuven and Yair Be'ery. Generalized Hamming weights of nonlinear codes and the relation to the Z_4-linear representation. *IEEE Trans. Inform. Theory*, 45(2):713–720, March 1999. 10.1

[Sch00] Hans Georg Schaathun. The weight hierarchy of product codes. *IEEE Trans. Inform. Theory*, 46(7):2648–2651, November 2000. 1.2, 5, 12.1, 12.1

[Sch01a] Hans Georg Schaathun. Duality and greedy weights for linear codes and projective multisets. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 2227 of *Springer Lecture Notes in Computer Science*, pages 92–101. Springer-Verlag, November 2001. 3

[Sch01b] Hans Georg Schaathun. Duality and weights for linear codes and projective multisets. Technical report, Dept. of Informatics, University of Bergen, 2001. Also available at `http://www.ii.uib.no/~georg/sci/inf/coding/public/`. 11.5

[Sch01c] Hans Georg Schaathun. Upper bounds on weight hierarchies of extremal non-chain codes. *Discrete Math.*, 241(1–3):449–469, 2001. 1

[Sim94] Juriaan Simonis. The effective length of subcodes. *Appl. Algebra Engrg. Comm. Comput.*, 5(6):371–377, 1994. 11.2

[Sle56] David Slepian. A class of binary signaling alphabets. *AT&T Bell Laboratories Technical Journal*, 35:203–234, 1956. 1.2

[SW03] Hans Georg Schaathun and Wolfgang Willems. A lower bound for the weight hierarchies of product codes. *Discrete Applied Mathematics*, 128:251–261, 2003. Special issue for WCC 2001. 12.1

[TBHN98] Ludo Tolhuizen, Stan Baggen, and Ewa Hekstra-Nowacka. Union bounds on the performance of product codes. In *Proc. IEEE Intern. Symp. Inform. Theory*, page 267, 1998. 14.1

[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. 1.2

[Wan00] Jian Wang. Performance bounds and design rules for product codes with hyper-diagonal parity. Master's thesis, Washington State University, August 2000. 14.1

[Wei91] Victor K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inform. Theory*, 37(5):1412–1418, 1991. 1.1, 2.2, 8, 10.1, 10.3

[WY93] Victor K. Wei and Kyeongcheol Yang. On the generalized Hamming weights of product codes. *IEEE Trans. Inform. Theory*, 39(5):1709–1713, 1993. 1.1, 1.3, 2.2, 8, 12, 12.3