Some new results on optimal codes over $\mathbb{F}_5$

Iliya Bouyukliev *
Institute of Mathematics and Informatics,
Bulgarian Academy of Sciences,
P.O.Box 323, 5000 V. Tarnovo, Bulgaria

Juriaan Simonis
Delft University of Technology
Faculty of Information Technology and Systems
Department of Mediamatics
P.O. Box 5031, 2600 GA Delft, The Netherlands

Abstract

We present some results on almost maximum distance separable (AMDS) codes and Griesmer codes of dimension 4 over $\mathbb{F}_5$. We prove that no AMDS code of length 13 and minimum distance 5 exists, and we give a classification of some AMDS codes. Moreover, we classify the projective strongly optimal Griesmer codes over $\mathbb{F}_5$ of dimension 4 for some values of the minimum distance.

1 Introduction

Let $\mathbb{F}_q^n$ be the n-dimensional standard vector space over the finite field $\mathbb{F}_q$ of q elements. The Hamming distance between two vectors of $\mathbb{F}_q^n$ is defined to be the number of coordinates in which they differ. A q-ary linear $[n,k,d]_q$ code is a k-dimensional linear subspace of $\mathbb{F}_q^n$ with minimum distance d.

Let $n_q(k,d)$ denote the smallest value of n for which an $[n,k,d]_q$ code exists. An $[n_q(k,d),k,d]_q$ code is called (length)-*optimal*. If an $[n+1,k+1,d]_q$ code exists, we can obtain an $[n,k,d]_q$ code by shortening it in one position. Similarly, if an $[n+1,k,d+1]_q$ code exists, we can obtain an $[n,k,d]_q$ code by puncturing it. A linear code is said to be *strongly optimal* if no $[n+1,k+1,d]_q$ or $[n+1,k,d+1]_q$ codes exist.

In this paper we investigate two classes of optimal codes. The first one is related to the Griesmer bound and the second one is related to the Singleton bound.

The Griesmer bound [15], [23] provides an important lower bound on $n_q(k,d)$:

$$n_q(k,d) \geq g_q(k,d) := \sum_{i=0}^{k-1} \lceil d/q^i \rceil.$$

Codes attaining this bound are called *Griesmer codes*. For $q=5$, the value of $n_5(k,d)$ is known for $k \leq 4$ for all except for 22 values of d, cf. [5]. We know that Griesmer codes with parameters $[6,4,3]_5$, $[12,4,8]_5$, $[16,4,11]_5$, $[26,4,20]_5$, $[39,4,30]_5$, $[70,4,55]_5$, $[76,4,60]_5$ and $[101,4,80]_5$ exist. These codes

*This work was supported in part by the Bulgarian NSF under Contract MM-901/1999

cannot be obtained from others by puncturing. Some of them, for instance $[26, 4, 20]_5$ and $[76, 4, 60]_5$ codes, are known to be unique up to equivalence , while Kapralov [19] proved that there exist exactly 16 inequivalent codes with parameters $[16, 4, 11]_5$. In this paper, we present a classification of the other Griesmer codes with the parameters given above.

If $\mathcal{C}$ is an $[n, k, d]_q$ code then

$$n \geq d + k - 1$$

This is the Singleton bound, and the codes attaining it are called *maximum-distance separable codes*, or *MDS codes*. Codes that almost reach this bound have been studied in [10] and [1]. The codes for which $n = k + d$ are called *almost MDS* or *AMDS*. For $q = 5$, it was not known whether AMDS codes of lengths between 13 and 20 and minimum distance 5 exist. We prove that such codes do not exist, and we classify all strongly optimal AMDS codes. It turns out that the Griesmer codes of dimension 4 and the AMDS codes over $\mathbb{F}_5$ are closely connected.

Our main tools are the dual transform and the software program Q-EXTENSION. These are presented in some detail in Section 2. Section 3 reports some new results on AMDS codes. In Section 4, we classify a few Griesmer codes of dimension 4. We summarize the classification results for codes of dimension 3 and $d \leq 5^2$ in Section 5.

2 Preliminaries

2.1 Dual transforms

For our purposes, it is useful to represent a linear code as a *projective multiset,* cf. [11]. Let G be a generator matrix of an $[n, k]_q$-code $\mathcal{C}$, i.e. a q-ary (k, n)-matrix whose row space is $\mathcal{C}$. Then we can associate to $\mathcal{C}$ the mapping

$$\gamma : \mathbb{P} := \mathbb{P}(\mathbb{F}_q^k) \to \mathbb{N}$$

for which $\gamma(p)$, $p \in \mathbb{P}(\mathbb{F}_q^k)$, is the number of times that the point p is represented by a column of G. The projective group $PGL(k, q)$ acts as a permutation group on $\mathbb{P}$ and hence on the set $\mathbb{N}^{\mathbb{P}}$ of the projective multisets by $\sigma\gamma := \gamma \circ \sigma^{-1}$. Different choices of generator matrices lead to projectively equivalent multisets. Conversely, any $PGL(k, q)$-orbit in $\mathbb{N}^{\mathbb{P}}$ whose elements have size $\leq n$ determines a unique equivalence class of $[n, i]$-codes with $i \leq k$. So we identify the code $\mathcal{C}$ with its projective multiset $\gamma_{\mathcal{C}}$. A non-zero codeword $\mathbf{c}$ of $\mathcal{C}$ determines a hyperplane $H \subset \mathbb{P}$, and the weight $w(\mathbf{c})$ of $\mathbf{c}$ is the number

$$\gamma(\mathbb{P} \setminus H) := \sum_{p \in \mathbb{P} \setminus H} \gamma(p).$$

(In general, we define $\gamma(S) := \sum_{p \in S} \gamma(p)$ for any subset $S \subseteq \mathbb{P}$.) The integer $\gamma(\mathbb{P})$ is called the *effective length* of $\mathcal{C}$. If the length of $\mathcal{C}$ is equal to its effective length, the code $\mathcal{C}$ is said to be of *full length*.

In [8], Brouwer and Van Eupen described a useful way to obtain new codes from old ones.

Definition 2.1 *Let W be the non-zero weight set of a k-dimensional q-ary code $\mathcal{C}$ of effective length n, and let $\alpha \neq 0, \beta \in \mathbb{Q}$ be such that the function $x \to \alpha x + \beta$ maps W into $\mathbb{N}$. Then the* dual (α, β)-transform *of $\gamma = \gamma_{\mathcal{C}}$ is the projective multiset*

$$D_{\alpha,\beta}(\gamma) : \mathbb{P}^* \to N, \quad D_{\alpha,\beta}(\gamma)(H) = \alpha \cdot \gamma(\mathbb{P} \setminus H) + \beta.$$

The code $D_{\alpha,\beta}(\mathcal{C})$ corresponding to this projective multiset $D_{\alpha,\beta}(\gamma)$ is called the projective dual(α, β)-transform of $\mathcal{C}$.

Note that if Δ is a *divisor* of $\mathcal{C}$, i.e. a common factor of its weights, and d is its minimum weight, one can choose $\alpha := \Delta^{-1}$ and $\beta := -d\Delta^{-1}$.

Example 2.2 *let C is a $[11, 3, 8]_5$ Griesmer code with non-zero weight set $W = \{8, 9, 10, 11\}$ and weight enumerators: $1 + 64z^8 + 28z^9 + 16z^{10} + 16z^{11}$*

The $(1, -8)$-dual transform of code $\mathcal{C}$ is a $[27, 3, 20]_5$ two-weight code $\mathcal{D}$. This code comes from code C by taking as multiset the 4 codwords of weight 11 (each taken tree times), the 4 codwords of weight 10 (each taken twice) and the 7 codewords of weight 9.

We list a few properties of $D_{\alpha,\beta}(\mathcal{C})$.

- The *length* of $D_{\alpha,\beta}(\mathcal{C})$ is equal to
$$\alpha n q^{k-1} + \beta \frac{q^k - 1}{q - 1}.$$
- Its *dimension* is $\leq k$. Equality holds if and only if the words $\mathbf{c} \in \mathcal{C}$ with $\alpha w(\mathbf{c}) + \beta \neq 0$ span $\mathcal{C}$. A dimension drop can only occur if
$$-\frac{q\beta}{\alpha} - (q - 1)n$$
is a value of $\gamma_{\mathcal{C}}$.
- Suppose that $\dim \mathcal{C}^{\alpha,\beta} = k$. Then the *minimum weight* of $D_{\alpha,\beta}(\mathcal{C})$ is equal to
$$\begin{cases} (\alpha n + \beta)q^{k-1} + \alpha(m - n)q^{k-2} & \text{if} \quad \alpha > 0, \\ (\alpha n + \beta)q^{k-1} + \alpha(M - n)q^{k-2} & \text{if} \quad \alpha < 0, \end{cases}$$
where $m := \min_{p \in \mathbb{P}} \gamma(p)$ and $M := \max_{p \in \mathbb{P}} \gamma(p)$.
If, in particular, the code $\mathcal{C}$ is *projective*, then $D_{\alpha,\beta}(\mathcal{C})$ is a 2-*weight code* with the weight set
$$\{(\alpha n + \beta)q^{k-1} - \alpha n q^{k-2}, \quad (\alpha n + \beta)q^{k-1} - \alpha(n - 1)q^{k-2}\}.$$
- Two $[n, k]_q$-codes $\mathcal{C}$, $\mathcal{D}$ are equivalent if and only if their dual transforms $D_{\alpha,\beta}(\mathcal{C})$, $D_{\alpha,\beta}(\mathcal{D})$ are equivalent. In fact, if both $\mathcal{C}$ and $\mathcal{C}' := D_{\alpha,\beta}(\mathcal{C})$ are of full length and have dimension k, then $\mathcal{C} = D_{\alpha',\beta'}(\mathcal{C}')$, with
$$\alpha' := \frac{q^{2-k}}{\alpha} \text{ and } \beta' := -\frac{q\beta}{\alpha} - (q - 1)n.$$

We describe two natural ways to derive new projective multisets. Let γ be the projective multiset of an $[n, k]$-code $\mathcal{C}$. Firstly, if $H \subset \mathbb{P}$ is the hyperplane corresponding to a non-zero word $\mathbf{c} \in \mathcal{C}$, then the *restriction* γ_H of γ to H is the projective multiset corresponding to the *residual code* $Res(\mathcal{C}, \mathbf{c})$ of $\mathbf{c}$. Secondly, let $p \in \mathbb{P}$ be a point. The quotient space $\mathbb{P}/p$ of $\mathbb{P}$ with respect to p is the $(k-2)$-dimensional projective space whose points are the lines L through p. The hyperplanes in $\mathbb{P}/p$ are the sets of lines through p that are contained in a hyperplane through p. Now we define the *quotient multiset* of γ by p to be the mapping $\gamma^p : \mathbb{P}/p \to \mathbb{N}$ given by
$$\gamma^p(L) := \gamma(L \setminus \{p\}), \quad L \in \mathbb{P}/p.$$

The quotient multisets γ^p correspond to the 1-codimensional subcodes of $\mathcal{C}$. Details can be found in section 2.3 of [11].

The next proposition describes how these derived multisets behave under a dual transform. For any subspace $M \subseteq \mathbb{P}$, let M^O denote the subspace of $\mathbb{P}^*$ consisting of the hyperplanes in $\mathbb{P}$ containing M.

Proposition 2.3 *Let $\gamma : \mathbb{P} := \mathbb{P}(\mathbb{F}_q^k) \to \mathbb{N}$ be a projective multiset such that its dual transform $D_{\alpha,\beta}(\gamma)$ is defined, and let $H \subset \mathbb{P}$ be a hyperplane.*
Then

$$D_{\alpha,\beta}(\gamma)^{H^O} = D_{\alpha',\beta'}(\gamma_H),$$

with $\alpha' := q\alpha$ and $\beta' := (q-1)\alpha\gamma(\mathbb{P} \setminus H) + q\beta$.

Proof. Let L be a hyperplane in H. Then L^O is a line in $\mathbb{P}^*$ through H^O, i.e. a point of the quotient space $\mathbb{P}^*/H^O$. The points of the line L^O correspond to a pencil $\{H_0 = H, H_1, \ldots, H_q\}$ of hyperplanes in $\mathbb{P}$. Now

$$\begin{aligned} D_{\alpha,\beta}(\gamma)^{H^O} &= \sum_{i=1}^{q} \{\alpha\gamma(\mathbb{P} \setminus H_i) + \beta\} = \\ &= \sum_{i=0}^{q} \alpha\gamma(\mathbb{P} \setminus H_i) - \alpha\gamma(\mathbb{P} \setminus H) + q\beta = \\ &= q\alpha\gamma(\mathbb{P}) - q\alpha\gamma(L) - \alpha\gamma(\mathbb{P}) + \alpha\gamma(H) + q\beta = \\ &= q\alpha\gamma(H \setminus L) + (q-1)\alpha\gamma(\mathbb{P} \setminus H) + q\beta. \end{aligned}$$

■

Corollary 2.4 *Let $\mathcal{C}$ be an $[n,k,d]_q$-code, and suppose that $\mathcal{D} := D_{1,-d}(\mathcal{C})$ has dimension k as well. Put $w := qd + iq^2$, where i be a nonnegative integer. Then the equivalence classes of the full-length projective $[n+w, k+1, w-iq]_q$-codes $\overline{\mathcal{C}}$ with divisor q and having $\mathcal{C}$ as residual code (with respect to a word of weight w) are in bijective correspondence with the equivalence classes of the full-length 2-weight codes $\overline{\mathcal{D}}$ that contain $\mathcal{D}$ and have the parameters*

$$[nq^{k-1} + i - d\frac{q^k-1}{q-1}, \quad k+1, \quad n(q-1)q^{k-2} - dq^{k-1}]_q.$$

Proof. Suppose an $[n+w, k+1, w-iq]_q$-code $\overline{\mathcal{C}}$ satisfies the conditions of the corollary. Then its dual transform $D_{\alpha,\beta}(\overline{\mathcal{C}})$ with $\alpha := q^{-1}$ and $\beta := -d - i(q-1)$ satisfies the conditions for $\overline{\mathcal{D}}$. Now use Proposition 2.3 and the fact that the dual transform is invertible. ■

Example 2.5 *The $(1,-11)$-dual transform of a $[15,3,11]_5$ Griesmer code $\mathcal{C}$ is a $[34,3,25]_5$-code $\mathcal{D}$. (There is no dimension drop.) The $[70,4,55]_5$ codes are known to be projective and with divisor 5. Now the corollary, with $i := 0$, implies that the equivalence classes of the $[70,4,55]_5$-codes with residual code $\mathcal{C}$ are in one-to-one correspondence with the equivalence classes of the 2-weight $[34,4,25]_5$-codes that contain $\mathcal{D}$. This correspondence is established by the $(5^{-1}, 11)$-dual transform. We could also start with a $[10,3,7]_5$-code $\mathcal{C}$ and take the parameter i equal to 1. Again the equivalence classes of the $[70,4,55]_5$-codes with residual code $\mathcal{C}$ (with respect to a word of weight 60) correspond one-to-one to the equivalence classes of the 2-weight $[34,4,25]_5$-codes that contain the $[33,3,25]_5$-code $D_{1,-7}(\mathcal{C})$.*

2.2 About Q-EXTENSION

The program contains two main approaches for extension of codes. The first one is the extension up to length which is the construction of an $[n, k, d]$ code on the basis of an $[n - w, k - 1, d']$ code as its residual code, or on the basis of an $[n - i, k, d']$ code. The second one is the extension up to dimension which is the extension of an $[n, k, d]$ code to $[n + i, k + i, d]$ or $[n + i + 1, k + i, d]$ code. If G is a generator matrix for a $[n, k, d]$ code, we extend it to

$$\left(\begin{array}{c|c} * & I_i \\ \hline G & 0 \end{array}\right) \quad \text{or} \quad \left(\begin{array}{c|c} * & 1\ I_i \\ \hline G & 0 \end{array}\right)$$

where I_i is the identity matrix. We take the matrix G in systematic form, thus we can fix k columns more. We will consider the following matrix

$$\left(\begin{array}{c|c|c} * & 0 & I_i \\ \hline G_1 & I_k & 0 \end{array}\right) \quad \text{or} \quad \left(\begin{array}{c|c|c} * & 0 & 1\ I_i \\ \hline G_1 & I_k & 0 \end{array}\right)$$

More information on this topic can be found in [6].

3 AMDS codes over $\mathbb{F}_5$

The *Singleton defect* of an $[n, k, d]$ code $\mathcal{C}$ is the nonnegative integer $s(\mathcal{C}) := n-k+1-d$. By definition, AMDS codes have Singleton defect 1. We shall use the following theorem.

Theorem 3.1 *[10] Let $\mathcal{C}$ be an $[n, n - r - 1, r + 1]_q$ AMDS code. If $r \geq q$ then $C^{\perp}$ is also AMDS.*

AMDS codes over $\mathbb{F}_5$ only exist for $d \leq 10$. In this section, we classify the *extremal* AMDS codes, i.e. the AMDS codes that are strongly optimal.

$d = 3$ In this case, the $[31, 28, 3]_5$ Hamming code is the unique extremal AMDS code.

$d = 4$ There exists a unique $[26, 22, 4]_5$ code. Its dual code is elliptic quadric. No $[27, 23, 4]_5$ code exists.

$d = 5$ **Theorem 3.2** *There exist exactly 36 $[12, 7, 5]_5$ extremal AMDS codes.*

Proof. Since codes with parameters $[7, 3, 5]_5$ do not exist, it follows that the dual distance of any putative $[13, 8, 5]_5$ code is at least 7. It is easy to see that there exist exactly two codes over $\mathbb{F}_5$ of length 8, dimension 7, and dual distance at least 7. By Q-EXTENSION we find that no one of them can be extended to a $[13, 8, 5]_5$ code. Hence no AMDS $[13, 8, 5]_5$ code exists and AMDS $[12, 7, 5]_5$ codes are extremal. We obtained exactly 36 inequivalent $[12, 7, 5]_5$ codes with the following weight enumerators:

$$1 + 364z^5 + 1228z^6 + 3996z^7 + 10240z^8 + 19060z^9 + 21540z^{10} + 16372z^{11} + 5324z^{12}$$
$$1 + 368z^5 + 1200z^6 + 4080z^7 + 10100z^8 + 19200z^9 + 21456z^{10} + 16400z^{11} + 5320z^{12}$$
$$1 + 360z^5 + 1256z^6 + 3912z^7 + 10380z^8 + 18920z^9 + 21624z^{10} + 16344z^{11} + 5328z^{12}$$
$$1 + 372z^5 + 1192z^6 + 4044z^7 + 10260z^8 + 18940z^9 + 21672z^{10} + 16308z^{11} + 5336z^{12}$$
$$1 + 356z^5 + 1264z^6 + 3948z^7 + 10220z^8 + 19180z^9 + 21408z^{10} + 16436z^{11} + 5312z^{12}$$
$$1 + 380z^5 + 1176z^6 + 3972z^7 + 10580z^8 + 18420z^9 + 22104z^{10} + 16124z^{11} + 5368z^{12}$$

$1 + 388z^5 + 1120z^6 + 4140z^7 + 10300z^8 + 18700z^9 + 21936z^{10} + 16180z^{11} + 5360z^{12}$
$1 + 368z^5 + 1220z^6 + 3960z^7 + 10400z^8 + 18800z^9 + 21756z^{10} + 16280z^{11} + 5340z^{12}$
$1 + 384z^5 + 1128z^6 + 4176z^7 + 10140z^8 + 18960z^9 + 21720z^{10} + 16272z^{11} + 5344z^{12}$
$1 + 396z^5 + 1084z^6 + 4188z^7 + 10320z^8 + 18580z^9 + 22068z^{10} + 16116z^{11} + 5372z^{12}$
$1 + 380z^5 + 1156z^6 + 4092z^7 + 10280z^8 + 18820z^9 + 21804z^{10} + 16244z^{11} + 5348z^{12}$
$1 + 376z^5 + 1184z^6 + 4008z^7 + 10420z^8 + 18680z^9 + 21888z^{10} + 16216z^{11} + 5352z^{12}$
$1 + 364z^5 + 1248z^6 + 3876z^7 + 10540z^8 + 18660z^9 + 21840z^{10} + 16252z^{11} + 5344z^{12}$
$1 + 392z^5 + 1112z^6 + 4104z^7 + 10460z^8 + 18440z^9 + 22152z^{10} + 16088z^{11} + 5376z^{12}$
$1 + 344z^5 + 1348z^6 + 3696z^7 + 10640z^8 + 18760z^9 + 21660z^{10} + 16352z^{11} + 5324z^{12}$
$1 + 336z^5 + 1384z^6 + 3648z^7 + 10620z^8 + 18880z^9 + 21528z^{10} + 16416z^{11} + 5312z^{12}$ ■

$d = 6$ **Theorem 3.3** *[22] There exist exactly 31 extremal AMDS* $[12, 6, 6]_5$ *codes.*

We give the different weight enumerators are:

$1 + 368z^6 + 960z^7 + 1560z^8 + 4080z^9 + 4464z^{10} + 3072z^{11} + 1120z^{12}$
$1 + 380z^6 + 888z^7 + 1740z^8 + 3840z^9 + 4644z^{10} + 3000z^{11} + 1132z^{12}$
$1 + 384z^6 + 864z^7 + 1800z^8 + 3760z^9 + 4704z^{10} + 2976z^{11} + 1136z^{12}$
$1 + 392z^6 + 816z^7 + 1920z^8 + 3600z^9 + 4824z^{10} + 2928z^{11} + 1144z^{12}$
$1 + 376z^6 + 912z^7 + 1680z^8 + 3920z^9 + 4584z^{10} + 3024z^{11} + 1128z^{12}$
$1 + 388z^6 + 840z^7 + 1860z^8 + 3680z^9 + 4764z^{10} + 2952z^{11} + 1140z^{12}$
$1 + 400z^6 + 768z^7 + 2040z^8 + 3440z^9 + 4944z^{10} + 2880z^{11} + 1152z^{12}$
$1 + 408z^6 + 720z^7 + 2160z^8 + 3280z^9 + 5064z^{10} + 2832z^{11} + 1160z^{12}$
$1 + 440z^6 + 528z^7 + 2640z^8 + 2640z^9 + 5544z^{10} + 2640z^{11} + 1192z^{12}$

$d = 7$ **Theorem 3.4** *[22] There exist exactly six AMDS* $[11, 4, 7]_5$ *codes.*

The $[11, 4, 7]_5$ codes have the following weight enumerators:

$1 + 132z^7 + 132z^8 + 132z^9 + 176z^{10} + 52z^{11}$
$1 + 128z^7 + 148z^8 + 108z^9 + 192z^{10} + 48z^{11}$
$1 + 136z^7 + 116z^8 + 156z^9 + 160z^{10} + 56z^{11}$
$1 + 140z^7 + 100z^8 + 180z^9 + 144z^{10} + 60z^{11}$

$d = 8$ **Theorem 3.5** *There exists a unique AMDS* $[12, 4, 8]_5$ *code.*

Proof. It is easy to check with Q-EXTENSION that there is a unique $[12, 4, 8]_5$ code. Its weight enumerator is

$1 + 192z^8 + 112z^9 + 96z^{10} + 192z^{11} + 32z^{12}$ ■

$d = 9$ There exists a unique $[11, 2, 9]_5$ code.

$d = 10$ There exists a unique $[12, 2, 10]_5$ code.

Table of some AMDS codes

d	AMDS codes	number	$g(k,d)$	$\mathcal{C}^\perp$	$s(\mathcal{C}^\perp)$	
3	$[31,28,3]$	1	30	$[31,3,25]$	4	extremal
4	$[26,22,4]$	1	25	$[26,4,20]$	3	extremal
5	$[8,3,5]$	16	8	$dd=2,3$		
	$[9,4,5]$	134	9	$dd=3,4$		
	$[10,5,5]$	558	10	$dd=4,5$		
	$[11,6,5]$	503	11	$dd=5,6$		
	$[12,7,5]$	36	12	$[12,5,6]$	2	extremal
	$[13,8,5]$	0				
6	$[9,3,6]$	16	9	$[9,6,3]$	1	
	$[10,4,6]$	93	10	$[10,6,4]$	1	
	$[11,5,6]$	60	11	$[11,6,5]$	1	
	$[12,6,6]$	31	12	$[12,6,6]$	1	extremal
7	$[10,3,7]$	7	10	$[10,7,3]$	1	
	$[11,4,7]$	6	11	$[11,8,4]$	1	
8	$[11,3,8]$	2	11	$[11,7,4]$	1	
	$[12,4,8]$	1	12	$[12,8,4]$	1	extremal
9	$[11,2,9]$	1	11	$[11,9,2]$	1	extremal
10	$[12,2,10]$	1	12	$[12,10,2]$	1	extremal

4 Classification of some 4-dimensional Griesmer codes

In this section, we classify the Griesmer codes with parameters $[39,4,30]_5$, $[70,4,55]_5$ and $[101,4,80]_5$. Before presenting the results, let us briefly discuss the possible weight distributions. By a general result of H. Ward [24],all weights in the three codes are divisible by 5. Moreover the codes are projective because $d \leq q^{k-1}$, cf. [18]. Now the MacWilliams identities leave only a few possibilities for the weight distributions. In fact, the $[39,4,30]_5$ codes have the unique weight enumerator

$$1 + 468z^{30} + 156z^{35}$$

and the $[70,4,55]_5$ codes have the unique weight enumerator

$$1 + 512z^{55} + 88z^{60} + 24z^{65}.$$

For the $[101,4,80]_5$ codes we find the three possibilities

$$\begin{array}{ll} (1) & 1 + 532z^{80} + 68z^{85} + 24z^{90}, \\ (2) & 1 + 520z^{80} + 100z^{85} + 4z^{100}, \\ (3) & 1 + 528z^{80} + 80z^{85} + 12z^{90} + 4z^{95}. \end{array} \tag{1}$$

In the sequel, we shall use the notation $[n,k,W]_q$ for the q-ary linear codes of length n and dimension k whose weight sets are contained in W.

4.1 [39,4,30]

A code with these parameters was found in [2]. Other examples have been presented by Van Eupen and Tonchev in [13].

Codes with these parameters are related to other combinatorial structures. It is well known that projective two-weight codes yield strongly regular graphs (N, K, λ, μ) [9]. In our case the parameters are $N = 625$, $K = 156$, $\lambda = 29$, and $\mu = 42$. Van Eupen and Tonchev have used $[39, 4, 30]_5$ codes to construct a reversible Abelian Hadamard difference set in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5^4$.

Theorem 4.1 *There exist exactly eight inequivalent* $[39, 4, 30]_5$ *codes.*

Proof. Landgev proved that there are exactly sixteen $[9, 3, 6]_5$ codes. By extension, we obtain eight inequivalent $[39, 4, 30]_5$ codes. We use the restrictions that the only nonzero weights are 30 and 35, and that a generator matrix does not contain columns with multiplicity 2. The constructed codes have generator matrices:

$$\begin{pmatrix} 1111111111111111111111111111000000000 \\ 1111112222223333334444440000001111111000 \\ 2233001334401122401122401334401234001 10 \\ 4023404142011423011320132342300443304 01 \end{pmatrix} \quad \begin{pmatrix} 1111111111111111111111111111000000000 \\ 1111112222223333334444440000001111111000 \\ 2233001334401122401122401334401234001 10 \\ 4010231242003412121423433103400443304 01 \end{pmatrix}$$

$$\begin{pmatrix} 1111111111111111111111111111000000000 \\ 1111112222223333334444440000001111111000 \\ 2233001334401122401122401334401234001 10 \\ 2024140131341412303030224132400443304 01 \end{pmatrix} \quad \begin{pmatrix} 1111111111111111111111111111000000000 \\ 1111112222223333334444440000001111111000 \\ 2233001334401122401122401334401234001 10 \\ 1412234302031023413424203101400443304 01 \end{pmatrix}$$

$$\begin{pmatrix} 1111111111111111111111111111000000000 \\ 1111112222223333334444440000001111111000 \\ 2334402234001133441123401122001234001 10 \\ 3144031024202334101240141323200443304 01 \end{pmatrix} \quad \begin{pmatrix} 1111111111111111111111111111000000000 \\ 1111112222223333334444440000001111111000 \\ 2334402234001133441123401122001234001 10 \\ 3124032014232434301400141223100443304 01 \end{pmatrix}$$

$$\begin{pmatrix} 1111111111111111111111111111000000000 \\ 1111112222223333334444440000001111111000 \\ 2234001122001133442334401123401234001 10 \\ 3403121412402323101343041240200344304 01 \end{pmatrix} \quad \begin{pmatrix} 1111111111111111111111111111000000000 \\ 1111112222223333334444440000001111111000 \\ 2334002334001124401122331124401234001 10 \\ 0402141124201432312334103023400334404 01 \end{pmatrix}$$

■

4.2 [70,4,55]

A $[70, 4, 55]_5$ code was constructed in [5]. The next theorem gives the whole picture.

Theorem 4.2 *There exist exactly fourteen inequivalent* $[70, 4, 55]_5$ *codes.*

Proof. We quote from the introduction to this section that any $[70, 4, 55]_5$ code $\overline{\mathcal{C}}$ is projective and has the weight enumerator $1 + 512z^{55} + 88z^{60} + 24z^{65}$. The residual code $\mathcal{C}$ with respect to a word of weight 65 is projective and has parameters $[5, 3, 3]_5$. Such a code is easily seen to be unique. Note that its dual transform $D_{1,-3}(\mathcal{C})$ is a full-length $[32, 3, \{25, 30\}]_5$ code. Now apply Corollary 2.4: The classification of the $[70, 4, 55]_5$ codes is equivalent to that of the full-length $[34, 4, \{25, 30\}]_5$ extensions of the unique full-length $[32, 3, \{25, 30\}]_5$ code. We can represent the generator matrices of these $[34, 4, \{25, 30\}]_5$ codes in the form

$$G_{34} := \begin{pmatrix} 11111111111111111111111111111 & 00001 \\ 44444433333322222211111100000 & 00010 \\ 33221144310043311044220043221 & 00100 \\ x & 11000 \end{pmatrix}.$$

Exhaustive computer search (using Q-EXTENSION) gives fourteen inequivalent solutions for G_{34}. Below follow the corresponding vectors x:

$$\begin{array}{ll}
44004040234412423033231033222, & 44340044043021322020343322231,\\
44004024304422013433201323223, & 44340044304012022323334023122,\\
44400030424423012433231023223, & 40443044221242312322330000343,\\
00404430222313320314223023444, & 33004423002211224433342420340,\\
44400020313332440420332222134, & 00333422042304434300243412122,\\
40004423201432022344302431332, & 34403322144423022300342300142,\\
44400014022303322240442333231, & 33443424424032210322304032001.
\end{array}$$

■

4.3 [101,4,80]

It is known that Griesmer $[q^3-q^2+1,4,q^3-2q^2+q]_q$ codes do exist for any prime power $q \geq 3$ [16]. In [17] it was shown that the $[19,4,12]_3$ code is unique, and a classification of the $[49,4,36]_4$ codes can be found in [4].

In the case $q=5$, we have $[101,4,80]$ codes $\overline{\mathcal{C}}$. We have seen in the introduction to this section that all of them are projective codes whose weights are divisible by 5. Moreover we listed exactly three feasible weight enumerators in (1). The dual transform $\overline{\mathcal{D}} := D_{5^{-1},-16}(\overline{\mathcal{C}})$ is a $[29,4,\{20,25\}]_5$ code, and the respective weight enumerators of (1) correspond to the respective maximal column multiplicities 2, 4 and 3 of $\overline{\mathcal{D}}$.

Theorem 4.3 *There exist exactly seven inequivalent* $[101,4,80]_5$ *codes.*

Proof. First, let us consider a $[101,4,80]_5$ code $\overline{\mathcal{C}}$ with weight enumerator (1). Its residual code with respect to a codeword of weight 90 has parameters $[11,3,8]_5$. In [21], the two equivalence classes for these codes have been identified. Using Corollary 2.4, we see that a generator matrix of the corresponding $[29,4,\{20,25\}]_5$ code $\overline{\mathcal{D}}$ may take the following form:

$$G_{29}^{1,1} = \begin{pmatrix}
11111111111111111111111 & 10000\\
14112333111223322230000 0 & 01000\\
42004333111004411103334 4 & 00100\\
x & 00011
\end{pmatrix}$$

or

$$G_{29}^{1,2} = \begin{pmatrix}
11111111111111111111111 & 10000\\
22333444222300023344400 1 & 01000\\
34333222000422210044434 3 & 00100\\
x & 00011
\end{pmatrix}.$$

The nonzero weights must be 20 and 25, and the generator matrix must contain columns with multiplicity at most 2. Using Q-EXTENSION, we found that no solution exists. So there is no $[101,4,80]_5$ code with weight enumerator (1).

Next we suppose that the $[101,4,80]_5$ code $\overline{\mathcal{C}}$ has weight enumerator (2) and hence that the generator matrices of $\overline{\mathcal{D}}$ a column of multiplicity four. Hence $\overline{\mathcal{D}}$ has a subcode of effective length 25, dimension

3, and minimum distance 20. A code with these parameters is unique. In fact, it is the $[25, 3, 20]_5$ MacDonald code. So we can take a generator matrix of $\overline{\mathcal{D}}$ in the following form

$$G_{29}^2 := \begin{pmatrix} 1111111111111111111111 & 1110000 \\ x_2 & 0001111 \\ x_3 & 0100000 \\ x_4 & 0010000 \end{pmatrix}.$$

With Q-EXTENSION, we found exactly six inequivalent solutions for G_{29}^2, namely

$$\begin{pmatrix} 11111111111111111111111110000 \\ 11112222333344444444400001111 \\ 11242240134012333344020100000 \\ 24231343142434123010200010000 \end{pmatrix} \begin{pmatrix} 11111111111111111111111110000 \\ 11112222333344444444400001111 \\ 11242240134012333344020100000 \\ 23241334441214123020300010000 \end{pmatrix}$$
$$\begin{pmatrix} 11111111111111111111111110000 \\ 11112222333344444444400001111 \\ 11242240134012333344020100000 \\ 24223034124331134010240010000 \end{pmatrix} \begin{pmatrix} 11111111111111111111111110000 \\ 11112222333344444444400001111 \\ 11242240134012333344020100000 \\ 34412032220313134024410010000 \end{pmatrix}$$
$$\begin{pmatrix} 11111111111111111111111110000 \\ 11112222333344444444400001111 \\ 11342340222311234440030100000 \\ 13202414134324012342300010000 \end{pmatrix} \begin{pmatrix} 11111111111111111111111110000 \\ 11112222333344444444400001111 \\ 11442233230011223344040100000 \\ 23341330242414401220310010000 \end{pmatrix}.$$

Finally we consider the case that $\overline{\mathcal{C}}$ has weight enumerator (3) and hence that the generator matrices of $\overline{\mathcal{D}}$ possess a column of multiplicity three (but not four). So $\overline{\mathcal{D}}$ has a subcode with effective length 26, dimension 3, and weights 20 and 2, and we can bring the generator matrix of $\overline{\mathcal{D}}$ in the form

$$G_{29}^3 := \begin{pmatrix} 11111111111111111111111 & 110000 \\ x_2 & 010000 \\ x_3 & 001000 \\ x_4 & 000111 \end{pmatrix}.$$

In this case, Q-EXTENSION gives us only one solution up to equivalence, namely

$$\begin{pmatrix} 11111111111111111111111110000 \\ 11112222233333444440000010000 \\ 22331334422330244002440001000 \\ 00404334024224014403141000111 \end{pmatrix}$$

■

Table for known codes over $\mathbb{F}_5$ with dimension 4 and $d \leq q^3$ attaining the Griesmer bound.

values of d for which $n_5(4,d) = g_5(4,d)$	codes	number
1–3	[6,4,3]	1
6–8	[12,4,8]	1
11	[16,4,11]	11 Kapralov
16–20	[26,4,20]	1 elliptic quadric
26–30	[39,4,30]	8
51–55	[70,4,55]	14
56–60	[76,4,60]	1 Bouyukliev and Kapralov
76–80	[101,4,80]	7
96–125		Type BV

Remark 4.4 *Using Q-EXTENSION, we proved that no* $[16, 5, 10]_5$ *code exists. This was the first open case for* $n_5(5, d)$*. Hence* $n_5(5, 10) = 16$ *and* $n_5(5, 11) = 18$*.*

5 Clasification of some codes in dimension 3

Table: Classification of some codes of dimension 3.

$[n,k,d]$	number	s(C)
$[5,3,3]$	1	0
$[6,3,4]$	1	0
$[8,3,5]$	16	1
$[9,3,6]$	16 Landgev	1
$[10,3,7]$	7 Landgev	1
$[11,3,8]$	2 Landgev	1
$[14,3,10]$	121	2
$[15,3,11]$	27 Kapralov	2
$[16,3,12]$	6 Bouyukliev and Kapralov	2
$[20,3,15]$	76	3
$[21,3,16]$	13	3
$[22,3,17]$	3	3
$[23,3,18]$	1 Van Eupen and Lisonek	3
$[24,3,19]$	1 Van Eupen and Lisonek	3
$[25,3,20]$	1 Van Eupen and Lisonek	3
$[27,3,21]$	3	4
$[28,3,22]$	2	4
$[29,3,23]$	1 Van Eupen and Lisonek	4
$[30,3,24]$	1 Van Eupen and Lisonek	4
$[31,3,25]$	1 Van Eupen and Lisonek	4

References

[1] M. de Boer, "Almost MDS codes", *Designs, Codes and Cryptography*, Vol. 9 (1996) pp. 143-155.

[2] I. Boukliev, "Some new optimal linear codes over F_5", *In Proc. 25th Spring Conference of the Union of Bulgarian Mathematicians*, Kazanlak, April 6–9, (1996) pp. 81-85.

[3] I. Boukliev and S. Kapralov, "The uniqueness of the Grismer $[76,4,60;5]$ code", *27th Spring Conference of the Union of Bulgarian Mathematicians*, Pleven, April, (1998) pp. 76-80.

[4] I. Boukliev and S. Kapralov, "Classification of the Griesmer $[49,4,36;4]$ codes", April, *Proceedings of the International Workshop ACCT*, Pskov, Russia, (1998) pp. 57-60.

[5] I. Boukliev, S. Kapralov, T. Maruta and M. Fukui, "Optimal linear codes of dimension 4 over F_5", *IEEE Trans. Info. Theory,* Vol. 43, No. 1 (1997) pp. 308-313.

[6] I. Bouyukliev and J. Simonis, "Some new results for optimal ternary linear codes", submitted to *IEEE Trans, Info. Theory.*

[7] A. E. Brouwer, "Bounds on the size of linear codes", in *Handbook of Coding Theory*, Edited by V.Pless and W.C.Huffman, Elsevier, Amsterdam etc., ISBN:0-444-50088-X, 1998. Online version: http://www.win.tue.nl/math/dw/voorlincod.html.

[8] A. E. Brouwer and M. van Eupen, "The correspondence between projective codes and 2-weight codes", *Designs, Codes and Cryptography*, Vol. 11 (1997) 262–266.

[9] A. R. Calderbank, and W. M. Kantor, "The geometry of two-weight codes," *Bull. London Math. Soc.* 18,(1986) pp. 97–122.

[10] S. Dodunekov, I. Landgev, "On near-MDS codes", *J. of Geometry*, **54**, pp. 30-34, 1995.

[11] S. Dodunekov, J. Simonis, Codes and projective multisets, *Electron. J. Combin.* 5 (1998), no. 1, 23 pp. (electronic).

[12] M. van Eupen and P. Lisonek ", Classification of some optimal ternary linear codes of small length", *Des. Codes Cryptogr.*, vol. 10, pp. 63–84, 1997,

[13] M. van Eupen and V.Tonchev, "Linear codes and the existence of a reversible Hadamard difference set in $Z_2 \times Z_2 \times Z_5^4$", *Proc. ACCT'96*, Sozopol, Bulgaria, June 1-7, (1996) pp. 295-301.

[14] P. Greenough and R. Hill, "Optimal linear codes over $GF(4)$", *Discrete Math.*, Vol. 125, (1994) pp. 187-199.

[15] J. H. Griesmer, "A bound for error-correcting codes", I.B.M.J Res. Develop, 4, (1960) pp. 532-542.

[16] N. Hamada, T. Helleseth, "On the construction of $[q^3 - q^2 + 1, 4, q^3 - 2q^2 + q; q]$ -code meeting the Griesmer bound", in Proc. ACCT, Voneshta Voda, Bulgaria, June 22-28, (1992) pp. 80-83.

[17] N. Hamada, T. Helleseth and O. Ytrehus,"There are exactly two nonequivalent [20,5,12;3]-codes", Ars Comb. Vol. 35 (1993) pp. 3-14.

[18] R. Hill, "Optimal linear codes: Cryptography and Coding II", (C. Mitchell, ed.), Oxford University Press, (1992) pp. 75–104.

[19] S. Kapralov, "Classification of some optimal linear codes over $GF(5)$", *Proceedings of the International Workshop OCRT*, Sozopol, Bulgaria,(1998) pp. 151-157.

[20] I. Landgev, "The geometry of $(n, 3)$-arcs in the projective plane of order 5", *Proc. ACCT'96*, Sozopol, Bulgaria, June 1-7, (1996) pp. 170-175.

[21] I. Landgev, T. Maruta, R. Hill. "On the nonexistence of quaternary [51,4,37] codes", *Finite Fields and their Applications*, 2, (1996) pp. 96-110.

[22] S. Marcugini,A. Milani and F. Pambianco, "Existence and classification of NMDS codes over GF(5) and GF(7)", *Proceedings of the International Workshop ACCT*, Bansko, Bulgaria, (2000) pp. 232-239.

[23] G. Solomon and J. J. Stiffler, "Algebraically punctured cyclic codes", *Inform. and Control*, 8, (1965) pp. 170-179.

[24] H. N. Ward, "Divisibility of codes meeting the Griesmer bound". *J. Comb. Theory Ser. A,* **83** (1998) pp. 79–93.

Iliya Bouyukliev
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
P.O. Box 323, 5000 V. Tarnovo, Bulgaria
E-mail: lpmivt@vt.bia-bg.com

Juriaan Simonis
Delft University of Technology
Faculty of Information Technology and Systems
Department of Mediamatics
P.O. Box 5031, 2600 GA Delft, The Netherlands

Keywords: Griesmer codes, AMDS codes, Optimal codes