A Characterization of certain Griesmer Codes: MMD Codes in a more general sense

Jonas Olsson, Student Member IEEE, Wolfgang Willems

Abstract

Let $\mathcal{C}$ be an $[n,k,d]_q$ linear code. The defect of $\mathcal{C}$ is the parameter $s = s(\mathcal{C}) = n-k+1-d$. If $k \geq m+1 \geq 2$ then by the Griesmer bound $d \leq \frac{q^m(q-1)}{q^m-1}(s+m)$. Our interest is in those linear codes having the maximum minimum distance, i.e. $d = \frac{q^m(q-1)}{q^m-1}(s+m)$. For $m=1$ we have $d = q(s+1)$ and the codes are maximum minimum distance (MMD) codes in the sense of [0]. Thus, we will consider MMD codes in a more general sense. We refer to them simply as MMD codes. All MMD codes with $m=1$ are known up to formal equivalence [0]. Note that two codes are formally equivalent if they have the same weight distribution. In this paper we classify up to formal equivalence the MMD codes with $m \geq 2$.

Keywords

Linear codes, defect of codes, weight distribution, optimal codes, Griesmer codes, maximum minimum distance

I. Preliminaries

Let $GF(q)$ denote the Galois field with q elements. An $[n,k,d]_q$ code $\mathcal{C}$ over $GF(q)$ is a k-dimensional subspace of the n-dimensional vector space over $GF(q)$ with minimum distance d. The corresponding $[n,n-k,d^\perp]_q$ dual code with minimum distance $d^\perp$ will be denoted by $\mathcal{C}^\perp$.

An $[n,k,d]_q$ code $\mathcal{C}$ satisfies the Singleton bound

$$d \leq n-k+1. \tag{1}$$

We define the *defect* $s(\mathcal{C})$ of $\mathcal{C}$ as the difference between the Singleton bound and the actual minimum distance d, i.e.

$$s(\mathcal{C}) := n-k+1-d.$$

The defect $s(\mathcal{C})$ is zero if and only if $\mathcal{C}$ is a Maximum Distance Separable (MDS) code. For all other codes the defect is positive. Similarily, the defect of the $[n,n-k,d^\perp]_q$ dual code $\mathcal{C}^\perp$ can be calculated as $s(\mathcal{C}^\perp) = k+1-d^\perp$. We usually write s and $s^\perp$ for $s(\mathcal{C})$ and $s(\mathcal{C}^\perp)$ respectively when it is clear from the context which code is involved. Furthermore, for convenience and with a slight abuse of language we sometimes refer to the parameter $s^\perp$ as the *dual defect* of $\mathcal{C}$.

The *support* of a vector $\mathbf{x} = (x_1, x_2, .., x_n)$ in $GF(q)^n$ is defined as $\chi(\mathbf{x}) := \{i : x_i \neq 0\}$. For a subset $U \subset GF(q)^n$ we put $\chi(U) := \bigcup_{\mathbf{x} \in U} \chi(\mathbf{x})$ and define the *support weight* of U by $w_S(U) := |\chi(U)|$. Hence, $w_S(U)$ is the number of positions where at least one vector of U is non-zero. If $U = \{\mathbf{x}\}$, then $w_S(U) = w_H(\mathbf{x})$ is the Hamming weight of $\mathbf{x}$.

Definition 1: Let $\mathcal{C}$ be an $[n, k, d]_q$ code. For $1 \leq r \leq k$ the r-th generalized Hamming weight d_r of $\mathcal{C}$ is defined by

$$d_r := \min\{w_S(D) : D \text{ is an } r\text{-dimensional subcode of } \mathcal{C}\}.$$

The sequence $d_1, d_2, .., d_k$ is called the *weight hierarchy* of $\mathcal{C}$.
In particular, $d_1 = d$ is the minimum distance of $\mathcal{C}$. The weight hierarchy of the corresponding dual code $\mathcal{C}^\perp$ will be denoted $d_1^\perp, d_2^\perp, .., d_k^\perp$. The concept of weight hierarchy of an $[n, k, d]_q$ code was introduced by Helleseth *et. al.* [0] and studied by Wei [0]. In [0] Forney called the weight hierarchy the *length/dimension profile.*

Wei [0] proved the inequalities

$$d_r < d_{r+1}, r = 1, 2, ..., k-1. \tag{2}$$

He also established the following relation between the weight hierarchy of $\mathcal{C}$ and the weight hierarchy of the dual code $\mathcal{C}^\perp$:

$$\{d_r : 1 \leq r \leq k\} = \{1, 2, ..., n\} \setminus \{n + 1 - d_r^\perp : 1 \leq r \leq n - k\}. \tag{3}$$

Combining (2) with the Singleton bound (1) and utilizing the obvious inequality $d_k \leq n$ we immediately obtain the *generalized Singleton bound* first observed by Wei [0]:

$$d_r \leq n - k + r, \; r = 1, 2, .., k. \tag{4}$$

In the sequel we always assume $d_k = n$. If this condition is not met then there exists a coordinate where all codewords of $\mathcal{C}$ have zeros. This implies that it is possible to delete that coordinate without changing the weight hierarchy of C.

The assumption $d_k = n$ implies that there always exists an integer $m \in \{1, 2, .., k-1\}$ such that for $r > m$ equality prevails in (4), i.e. there exist an integer $m \in \{1, 2, .., k-1\}$ such that $d_r = n - k + r$ for $r = m + 1, .., k$.

Lemma 1: Let $\mathcal{C}$ be an $[n,k,d]_q$ code of defect $s>0$. Then there exists a largest integer $m \in \{1,2,..,k-1\}$ such that $d_{m+1}-d_m \geq 2$. Furthermore, for this m we have

$$s^{\perp}=m.$$

Proof: Since $s>0$ and $d_k=n$ by assumption, there exists a largest $m \in \{1,2,\ldots,k-1\}$ such that $d_{m+1}-d_m \geq 2$. It is immediate from (2) and (4) that $d_i=n-k+i$ for $i=m+1,m+2,..,k$, and that $d_m \leq n-k+m-1$. By (3) this implies $d_1^{\perp}=k+1-m$ and the lemma follows. ■

Before we proceed to the next lemma we need the following inequality proved by Helleseth et al. [0]:

$$(q^r-1)d_l \leq (q^r-q^{r-l})d_r,\ 1 \leq l \leq r \leq k. \tag{5}$$

Lemma 2: Let $\mathcal{C}$ be an $[n,k,d]_q$ code and suppose that $d_{m+1}=n-k+m+1$ for some $m \in \{1,2,..k-1\}$. If

$$n > \frac{q^{m+1}-q}{q-1}+k-m$$

then $s^{\perp}=m$.

Proof: Suppose that $d_{m+1}-d_m=1$. Then since $d_{m+1}=n-k+m+1$ we have $d_m=n-k+m$. By (5) with $r=m+1$ and $l=m$ we get

$$(q^{m+1}-1)(n-k+m) \leq (q^{m+1}-q)(n-k+m+1).$$

Solving this inequality for n we obtain $n \leq \frac{q^{m+1}-q}{q-1}+k-m$, a contradiction. Since $d_{m+1}=n-k+m+1$ by assumption, the statements in (2) and (4) imply that m is the largest integer such that $d_{m+1}-d_m \geq 2$. Thus by Lemma 1, $s^{\perp}=m$. ■

We are now ready to prove the following theorem.

Theorem 1: Let $\mathcal{C}$ be an $[n,k,d]_q$ code of defect s. If there exists an integer $m \in \{1,2,..,k-1\}$ such that

(i) $s+m > \frac{q^m-1}{q-1}$

and

(ii) $d > \frac{q^m(q-1)}{q^m-1}(s+m-1)$,

then $s^{\perp}=m$.

Proof: For $t<m+1 \leq k$ it is convenient to define the following function

$$f_m(t)=\frac{q^{m+1}-1}{q^m-1}(s+t-1)+k-t.$$

Since

$$f_m(t+1) - f_m(t) = \frac{q^{m+1}-1}{q^m-1} - 1 = \frac{q^m(q-1)}{q^m-1} > 0,$$

the function $f_m(t)$ is strictly increasing with t. From the generalized Singleton bound (4) we get $d_{m+1} \leq n-k+m+1$. Suppose strict inequality holds, i.e. $d_{m+1} = n-k+t$ for some integers $t \leq m$. Then from (5) with $r = m+1$ and $l = 1$ we have

$$(q^{m+1}-1)(n-k+1-s) \leq (q^{m+1}-q^m)(n-k+t).$$

From this we obtain

$$n \leq \frac{q^{m+1}-1}{q^m-1}(t+s-1) + k - t = f_m(t).$$

As the function $f_m(t)$ is increasing with t it follows that $n \leq f_m(m)$ which contradicts (ii) since (ii) is equivalent to $n > f_m(m)$. Thus we have $d_i = n-k+i$ for $i = m+1, m+2, .., k$.

Furthermore, by condition (i)

$$n > f_m(m) \geq \frac{q^{m+1}-1}{q-1} + k - m > \frac{q^{m+1}-q}{q-1} + k - m$$

and Lemma 2 implies $s^\perp = m$. ■

Specializing $m = 1$ in Theorem 1 we have the following corollary, which is the same as Theorem 7 in [0].

Corollary 1: Let $\mathcal{C}$ be an $[n,k,d]_q$ code of dimension $k \geq 2$ and defect $s > 0$. If

$$d > sq$$

then $s^\perp = 1$.

The weight distribution of an $[n,k,d]_q$ code $\mathcal{C}$ is the sequence $A_0, A_1, .., A_n$ where A_i is the number of codewords of Hamming weight i. In the next section we need the following formula for the weight distribution. This formula has been discovered independently by the first author [0] and A. Faldum and the second author. Complete proofs can be found in [0] and [0].

Lemma 3: Let C be a code with parameters $[n,k,d]_q$, defect s and dual defect $s^\perp$. If $A_0, A_1, .., A_n$ is the weight distribution of $\mathcal{C}$ then

$$A_{n-k+v} = \binom{n}{k-v} \sum_{i=0}^{v-s^\perp} (-1)^i \binom{n-k+v}{i} (q^{v-i}-1) -$$

$$(-1)^{v-s^\perp} \sum_{i=1}^{s^\perp+s-1} \binom{k+s-i}{k-v} \binom{v-1+s-i}{v-s^\perp} A_{n-k-s+i} \tag{6}$$

for every $v \in \{s^\perp, s^\perp+1, ..., k\}$.

II. MMD Codes in a more general sense

Lemma 4: Let $\mathcal{C}$ be an $[n,k,d]_q$ code of defect s and let $m \geq 1$ be an arbitrary integer.

1. If $k \geq m+1$ then $d \leq \frac{q^m(q-1)}{q^m-1}(s+m)$.
2. If $k \geq m+2$ and $d = \frac{q^m(q-1)}{q^m-1}(s+m)$ then $s+m \leq \frac{q(q^m-1)}{q-1}$.

Proof: For the proof of statement 1 we suppose that $d > \frac{q^m(q-1)}{q^m-1}(s+m)$. Then by the Griesmer bound (cf. [0], p. 59)

$$n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil \geq d + \sum_{i=1}^{m} \frac{q^{m-i}(q-1)}{q^m-1}(s+m) + k - m$$

$$= d + (s+m) + k - m = n+1,$$

a contradiction. Thus $d \leq \frac{q^m(q-1)}{q^m-1}(s+m)$.

For $k \geq m+2$ and $d = \frac{q^m(q-1)}{q^m-1}(s+m)$ we have

$$n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil \geq d + \sum_{i=1}^{m} \frac{q^{m-i}(q-1)}{q^m-1}(s+m) + \lceil \frac{(q-1)}{q(q^m-1)}(s+m) \rceil + k - (m+2) =$$

$$n - 1 + \lceil \frac{(q-1)}{q(q^m-1)}(s+m) \rceil.$$

Hence $s+m \leq \frac{q(q^m-1)}{q-1}$ which proves statement 2. ■

Definition 2: Let $\mathcal{C}$ be an $[n,k,d]_q$ code of defect s and dimension $k \geq m+1 \geq 2$. If

$$d = \frac{q^m(q-1)}{q^m-1}(s+m)$$

then $\mathcal{C}$ is called a Maximum Minimum Distance (MMD) code.

Remark 1: Faldum and the second author [0] called an $[n,k,d]_q$ code $\mathcal{C}$ with $k \geq 2$ and defect s an MMD code if $d = (s+1)q$. Note that for $m = 1$ the two definitions coincide. Here we consider codes that are MMD in a more general sense. For convenience we simply refer to all of them as MMD codes.

In the next section we classify all these (in a more general sense) MMD codes. To do so we need

Theorem 2: Let $\mathcal{C}$ be an $[n,k,d]_q$ MMD code with $s+m > \frac{q^m-1}{q-1}$. Then $m = s^\perp$ and the weight distribution $A_0, A_1, .., A_n$ of $\mathcal{C}$ satisfies

(i) $A_d = \frac{\binom{n}{k-s^\perp}}{\binom{k+s-1}{k-s^\perp}}(q^{s^\perp}-1)$,

(ii) $A_{d+1} = A_{d+2} = \ldots = A_{n-k+s^\perp+1} = 0$,

and

(iii) $A_{n-k+v} = \binom{n}{k-v}\sum_{i=0}^{v-s^\perp}(-1)^i\binom{n-k+v}{i}(q^{v-i}-1) - \frac{(-1)^{v-s^\perp}(s+s^\perp-1)(q^{s^\perp}-1)}{(v+s-1)}\binom{n}{k-v}\binom{n-k+v}{v-s^\perp}$

for $v = s^\perp+2, s^\perp+3, \ldots, k$.

In particular, the parameters $[n,k,d]_q$ uniquely determine the weight distribution.

Proof: By Theorem 1 the dual defect of $\mathcal{C}$ is $s^\perp = m$. From Lemma 3 we obtain

$$A_{n-k+s^\perp} = \binom{n}{k-s^\perp}(q^{s^\perp}-1) - \sum_{i=1}^{s+s^\perp-1}\binom{k+s-i}{k-s^\perp}A_{n-k-s+i}$$

for $v = s^\perp$ and

$$A_{n-k+s^\perp+1} = \binom{n}{k-s^\perp-1}((q^{s^\perp+1}-1) - (n-k+s^\perp+1)(q^{s^\perp}-1)) +$$

$$\sum_{i=1}^{s+s^\perp-1}\binom{k+s-i}{k-s^\perp-1}(s^\perp+s-i)A_{n-k-s+i}.$$

for $v = s^\perp+1$. Since $A_{n-k+s^\perp} \geq 0$, $A_{n-k+s^\perp+1} \geq 0$ and $n-k+s^\perp+1 = \frac{q^{s^\perp+1}-1}{q^{s^\perp}-1}(s+s^\perp)$ we obtain

$$\sum_{i=2}^{s+s^\perp-1}\frac{(s+s^\perp)(s+s^\perp-i)+(i-1)}{(s+s^\perp-1)(s+s^\perp+1-i)}\binom{k+s-i}{k-s^\perp}A_{n-k-s+i} \leq$$

$$\binom{n}{k-s^\perp}(q^{s^\perp}-1) - \binom{k+s-1}{k-s^\perp}A_{n-k+1-s} \tag{7}$$

and

$$\sum_{i=2}^{s+s^\perp-1}\frac{(s+s^\perp)(s+s^\perp-i)}{(s+s^\perp-1)(s+s^\perp+1-i)}\binom{k+s-i}{k-s^\perp}A_{n-k-s+i} \geq$$

$$\binom{n}{k-s^\perp}(q^{s^\perp}-1) - \binom{k+s-1}{k-s^\perp}A_{n-k+1-s}. \tag{8}$$

Combining (7) and (8) we get

$$\sum_{i=2}^{s+s^\perp-1}\frac{i-1}{(s+s^\perp-1)(s+s^\perp+1-i)}\binom{k+s-i}{k-s^\perp}A_{n-k-s+i} \leq 0.$$

This implies $A_{n-k-s+2} = A_{n-k-s+3} = \cdots = A_{n-k+s^\perp-1} = 0$. By (7) and (8) it also follows that

$$A_{n-k+1-s} = \frac{\binom{n}{k-s^\perp}}{\binom{k+s-1}{k-s^\perp}}(q^{s^\perp} - 1),$$

and clearly $A_{n-k+s^\perp} = A_{n-k+s^\perp+1} = 0$ must hold. As $d = n-k+1-s$ the statements (i) and (ii) have been proved. Now, by inserting (i) and (ii) in Lemma 3, the formula in (iii) follows easily. ■

III. The classification up to formal equivalence

Let $\mathcal{C}$ be an $[n,k,d]_q$ MMD code of dimension $k \geq m+1 \geq 2$. By definition, the minimum distance of $\mathcal{C}$ satisfies

$$d = \frac{q^m(q-1)}{q^m-1}(s+m)$$

where s denotes the defect of $\mathcal{C}$.

The aim of this section is to classify all such codes up to formal equivalence. Remember that two codes are said to be formally equivalent if they have the same weight distribution.

First we consider two special cases. If $k=2$ then $m=1$ and for each $s \in \{0,1,2,..\}$ there exists up to equivalence exactly one MMD code $\mathcal{C}$ (see [0]). A generator matrix is given by

$$\begin{pmatrix} 0 & \cdots & 0 & 1 & \cdots & 1 & \cdots & 1 & \cdots & 1 \\ 1 & \cdots & 1 & \alpha_1 & \cdots & \alpha_1 & \cdots & \alpha_q & \cdots & \alpha_q \end{pmatrix}$$

where the blocks have length $s+1$ and $GF(q) = \{\alpha_1, \alpha_2, .., \alpha_q\}$. Obviously $\mathcal{C}$ is an $(s+1)$-times repeated Simplex code with parameters $[(s+1)(q+1), 2, (s+1)q]_q$. Thus in the sequel we may assume $k \geq 3$.

Secondly, if $s=0$, i.e. $\mathcal{C}$ is an MDS code, then by [0], Chap. 11,

$$d = m\frac{q^m(q-1)}{q^m-1} \leq q$$

which forces $m=1$ and by [0], $\mathcal{C}$ is the binary $[k+1,k,2]_2$ even weight code. Hence, we may also assume that $s \geq 1$.

The remainder of this section is devoted to the proof of the following theorem.

Theorem 3: Let $\mathcal{C}$ be an $[n,k,d]_q$ code of dimension $k \geq 3$ and defect $s \geq 1$. Then $\mathcal{C}$ is an MMD code if and only if $\mathcal{C}$ is formally equivalent to one of the following codes.

(i) The $[t\frac{q^k-1}{q-1}, k, tq^{k-1}]_q$ t-times repeated Simplex code, where $t \in \{1, 2, ..\}$.

(ii) The $[q^{k-1}, k, (q-1)q^{k-2}]_q$ generalized Reed-Muller code of first order. If $q = 2$ then $k \geq 4$.

(iii) The $[12, 6, 6]_3$ extended Golay code.

(iv) The $[11, 5, 6]_3$ dual Golay code.

(v) The $[q^2+1, 4, q^2-q]_q$ projective elliptic quadratic code with $q \neq 2$.

(vi) The $[(2^t-1)q+2^t, 3, (2^t-1)q]_q$ Denniston code with $1 \neq 2^t \mid q$.

Remark 2: Note that the codes in (iii)-(vi), the $[8, 4, 4]_2$ extended Hamming code, the $[\frac{q^3-1}{q-1}, 3, q^2]_q$ Simplex code and the $[q^2, 3, q^2-q]_q$ generalized Reed-Muller code of first order are up to formal equivalence exactly the MMD codes with $m = 1$, $k \geq 3$ and $s \geq 1$ (see [0]). Hence it suffices to prove that all MMD codes with $m \geq 2$, $k \geq 3$ and $s \geq 1$ are among those of (i) and (ii) of the list.

We first solve the exceptional case $k = m+1 \geq 2$ which covers again the 2-dimensional case.

Proposition 1: If $\mathcal{C}$ is an $[n, k, d]_q$ MMD code with $k = m+1 \geq 2$, then $\mathcal{C}$ is a repeated Simplex code.

Proof: We have $d = \frac{q^m(q-1)}{q^m-1}(s+m)$ and

$$n = d + k + s - 1 = \frac{q^m(q-1)}{q^m-1}(s+m) + k + s - 1 = \frac{q^{m+1}-1}{q^m-1}(s+m).$$

Clearly, $\frac{q^m-1}{q-1}$ divides $(s+m)$. First suppose that $s + m > \frac{q^m-1}{q-1}$. Then by Theorem 2 we have $s^\perp = m$ and

$$A_{d+1} = A_{d+2} = \cdots = A_{n-k+s^\perp+1} = 0.$$

But $n - k + s^\perp + 1 = n - k + (k-1) + 1 = n$. Thus $\mathcal{C}$ is a one-weight code and according to a result of Bonisoli [0], the code $\mathcal{C}$ is a repeated Simplex code. So we get the codes in Theorem 3(i) for $t \geq 2$.

If $s + m = \frac{q^m-1}{q-1}$ then $\mathcal{C}$ has parameters

$$[\frac{q^{m+1}-1}{q-1}, m+1, q^m]_q$$

which are those of the Simplex code and we have found all codes in Theorem 3(i). ■

According to Proposition 1 we may assume $k \geq m+2 \geq 4$ from now on. Since d is an integer we may apply Lemma 4 and get $d = iq^m$ and $s+m = i\frac{q^m-1}{q-1}$ with $1 \leq i \leq q$. Furthermore, for $i > 1$ we only have to classify the parameters since, by Theorem 2, they determine the code up to formal equivalence.

In the sequel we often refer to the following lemma which one obtains as a byproduct when prooving the Griesmer bound (cf. [0], p. 59).

Lemma 5: Let $\mathcal{C}$ be an $[n,k,d]_q$ code. Then there also exists an $[n-d, k-1, \geq \lceil \frac{d}{q} \rceil]_q$ code.

Proposition 2: Let $\mathcal{C}$ be an MMD of defect s and dimension $k \geq m+2 \geq 3$. If $s+m = q\frac{q^m-1}{q-1}$ then $\mathcal{C}$ is equivalent to one of the following codes.

(i) The $[2^{m+2}, m+3, 2^{m+1}]_2$ first order Reed-Muller code.

(ii) The $[\frac{q^{m+2}-1}{q-1}, m+2, q^{m+1}]_q$ Simplex code.

Proof: By assumption, $d = q^{m+1}$ and $n = q^{m+1}+q^m+\cdots+q+k-(m+1)$. Applying Lemma 5 exactly m times we get a code $\mathcal{C}_0$ with parameters

$$[q+k-(m+1), k-m, q]_q.$$

Obviously, $\mathcal{C}_0$ is an MDS code. Suppose $k \geq m+4$. Then by shortening we find an MDS code with parameters $[q+3, 4, q]_q$. But such an MDS code does not exist (see [0], Chap. 11). Thus $m+2 \leq k \leq m+3$. Suppose $k = m+3$. Again by shortening $\mathcal{C}_0$ we get an MDS code with parameter $[q+2, 3, q]_q$. Such a code exists only for q even (see [0], Chap. 11). If $q = 2$ the code $\mathcal{C}$ has parameters

$$[2^{m+2}, m+3, 2^{m+1}]_2$$

which are those of the binary Reed-Muller code of first order. It is well known that the first order binary Reed-Muller code is uniquely determined by its parameters. Finally suppose $q = 2^l > 2$. Applying Lemma 5 exactly $(m-1)$ times on $\mathcal{C}$ a code $\mathcal{C}_1$ with parameters

$$[q^2+q+k-(m+1), k-(m-1), q^2]_q = [q^2+q+2, 4, q^2]_q$$

arises. The defect of $\mathcal{C}_1$ is $s(\mathcal{C}_1) = q-1$. By definition, $\mathcal{C}_1$ is an MMD code with $m = 1$. According to [0] no such code exists for $q > 2$. Hence the case $k = m+2$ remains. Then

$\mathcal{C}$ has parameters

$$[\frac{q^{m+2}-1}{q-1}, m+2, q^{m+1}]_q$$

which are those of the Simplex code. Finally note that the Simplex code is uniquely determined by its parameters. ∎

Proposition 3: Let $\mathcal{C}$ be an $[n,k,d]_q$ MMD code of defect s and dimension $k \geq m+2 \geq 4$. If $s+m = (q-1)\frac{q^m-1}{q-1} = q^m - 1$ then $k = m+2$ and $\mathcal{C}$ is formally equivalent to the

$$[q^{k-1}, k, (q-1)q^{k-2}]_q$$

generalized Reed-Muller code of first order.

Proof: The parameters of $\mathcal{C}$ are

$$[q^{m+1} + k - (m+2), k, (q-1)q^m]_q.$$

Suppose $k \geq m+3$. By shortening $\mathcal{C}$ exactly $(k-(m+3))$ times we get a code $\mathcal{C}_0$ with parameters $[q^{m+1}+1, m+3, (q-1)q^m]_q$. Let $\mathcal{C}_1$ be the code which arises from $\mathcal{C}_0$ by applying Lemma 5 precisely $(m-2)$ times. Note that by assumption $m \geq 2$. The code $\mathcal{C}_1$ has parameters

$$[q^3+1, 5, (q-1)q^2]_q.$$

We may assume $q > 2$ since a binary $[9,5,4]_2$ does not exist (see Brouwer [0]). Obviously, the defect of $\mathcal{C}_1$ is $s(\mathcal{C}_1) = (q^2-1)-2$. Since $q > 2$ it follows by Theorem 1 that $s(\mathcal{C}_1^\perp) = 2$. Thus the code $\mathcal{C}_1^\perp$ has parameters $[q^3+1, q^3-4, 4]_q$. Hence any three columns of a generator matrix of $\mathcal{C}_1$ are linearly independent. This means that there exist q^3+1 points in the projective geometry $PG(4,q)$ such that no three are collinear. But the maximum number of such points is bounded by q^3 according to a result of Tallini [0]. We have therefore a contradiction. This proves $k = m+2$ for $q \geq 2$, and $\mathcal{C}$ has parameters

$$[q^{k-1}, k, (q-1)q^{k-2}]_q$$

which are those of a generalized Reed-Muller code of first order (see [0]). For $q = 2$ the code $\mathcal{C}$ has the parameters of the classical Reed-Muller code of first order, which is unique.

For $q > 2$ we have

$$s+m = (q-1)\frac{q^m-1}{q-1} > \frac{q^m-1}{q-1}$$

and thus, by Theorem 2, $\mathcal{C}$ is formally equivalent to a generalized Reed-Muller code of first order. ■

So far we have found all codes in the list of Theorem 3. Before we show that the list is complete we would like to improve a parameter in Brouwer's list [0].

Remark 3: In [0] the upper bound for the minimum distance d of an $[126, 5, d]_5$ code is given by $d \leq 100$. Suppose there exists a $[126, 5, 100]_5$ code $\mathcal{C}$. Such a code has defect $s = 22$. With $m = 2$ and $q = 5$ we get $s + m = 24 = q^m - 1$ and $d = \frac{q^m(q-1)}{q^m-1}(s+m) = 100$. Thus $\mathcal{C}$ is an MMD code with $s + m = q^m - 1$. By Proposition 3 such a code does not exist. Hence we have proved $d \leq 99$.

Proposition 4: There does not exist an $[n, k, d]_q$ MMD code over $GF(q)$ of defect s and dimension $k \geq m + 2 \geq 4$ with

$$s + m = (q - t)\frac{q^m - 1}{q - 1}$$

where $t \in \{2, 3, .., q - 1\}$.

Proof: Suppose $\mathcal{C}$ is an $[n, k, d]_q$ MMD code with $s + m = (q - t)\frac{q^m-1}{q-1}$ where $t \in \{2, 3, .., q - 1\}$. Note that $q > 2$. Now $\mathcal{C}$ has length

$$n = (q - t)(q^m + q^{m-1} + \cdots + q + 1) + k - (m + 1)$$

and minimum distance $d = (q - t)q^m$. First suppose that $k \geq m + 3$. Shortening $\mathcal{C}$ exactly $(k - (m + 3))$ times we end up with a code $\mathcal{C}_0$ with parameters

$$[(q - t)(q^m + q^{m-1} + \cdots + q + 1) + 2, m + 3, (q - t)q^m]_q.$$

Let $\mathcal{C}_1$ be the code that arises from $\mathcal{C}_0$ by applying Lemma 5 exactly $(m - 1)$ times. The code $\mathcal{C}_1$ has parameters

$$[(q - t)(q + 1) + 2, 4, (q - t)q]_q$$

and defect $s(\mathcal{C}_1) = (q - t) - 1$. Thus, by definition, $\mathcal{C}_1$ is an MMD code with $m = 1$. According to [0] such a code does not exist since $q > 2$ and $2 \leq t \leq q - 1$. Thus we have a contradiction. Hence $k = m + 2$ and $\mathcal{C}$ is a code with parameters

$$[(q - t)(q^m + q^{m-1} + \cdots + q + 1) + 1, m + 2, (q - t)q^m]_q.$$

Let $\mathcal{C}_2$ be the code which arises from $\mathcal{C}$ by using Lemma 5 now $(m-2)$ times. The code $\mathcal{C}_2$ has parameters

$$[n_2, k_2, d_2]_q = [(q-t)(q^2+q+1)+1, 4, (q-t)q^2]_q.$$

Furthermore the defect of $\mathcal{C}_2$ is $s(\mathcal{C}_2) = (q-t)(q+1) - 2$ and the minimum distance is $d_2 = (q-t)q^2 = \frac{q^2(q-1)}{q^2-1}(s(\mathcal{C}_2)+2)$. First we consider the case $t < q-1$. Then

$$s(\mathcal{C}_2) + 2 = (q-t)(q+1) > \frac{q^2-1}{q-1} = q+1$$

and by Theorem 1 we get $s(\mathcal{C}_2^\perp) = 2$. Moreover, by Theorem 2, the weight distribution of $\mathcal{C}_2$ satisfies $A_{d_2+1} = \cdots = A_{n_2-1} = 0$ and $A_{n_2} \neq 0$. Thus $\mathcal{C}_2$ is a two-weight code. Without loss of generality we may assume that $\mathcal{C}_2$ has a generator matrix of the form

$$G_2 = \left(\begin{array}{c|c} 1\cdots 1 & 0 \cdots 0 \\ u & v \\ z_{3,1} & z_{3,2} \\ z_{4,1} & z_{4,2} \end{array} \right) = \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix},$$

where $w_H(z_1) = d_2$ and $w_H(z_2) = w_H(u \mid v) = n_2$. For $a \in GF(q)\backslash\{0\}$ we define $\alpha_a := |\{i : u_i = a\}|$ where $u = (u_1, u_2, .., u_{d_2})$. Furthermore we put $z_a := az_1 - z_2$. Then $w_H(z_a) \in \{d_2, n_2\}$ since $\mathcal{C}_2$ is a two-weight code. In addition, for $\alpha_a \neq 0$ we have $d_2 = w_H(z_a) = d_2 - \alpha_a + (n_2 - d_2)$. Thus $\alpha := \alpha_a = n_2 - d_2 = (q-t)(q+1)+1$. Now we put $\beta := |\{a \in GF(q)\backslash\{0\} : \alpha_a \neq 0\}|$. Clearly $d_2 = \alpha\beta$. This yields

$$(q-t)q^2 = [(q-t)(q+1)+1]\beta = [q(q+1) - qt - (t-1)]\beta.$$

It follows that $(q-t) \mid \beta$ and by definition $\beta < q$. Hence $q \mid (t-1)$. Since $t > 1$ and $t < q-1$ by assumption, we have a contradiction. It remains to consider the case $t = q-1$. Then $\mathcal{C}_2$ has parameters $[q^2+q+2, 4, q^2]_q$ and defect $s(\mathcal{C}_2) = q-1$. Thus $\mathcal{C}_2$ is an MMD code with $m = 1$. But for $q > 2$ such a code does not exist according to [0]. ∎

References

[1] V.K. Wei, *Generalized Hamming Weights for Linear Codes*, IEEE Trans. on Information Theory, vol. 37, no 5, pp. 1412-1418, September, 1991.

[2] T.Helleseth, T. Kløve, V.I. Levenshtein, Ø. Ytrehus, *Bounds on the Minimum Support Weights*, IEEE Trans. on Information Theory, vol. 41, no. 2, pp. 432-440, March, 1995.

[3] A. Faldum and W. Willems, *Codes of Small Defect*, Designs, Codes and Cryptography, vol. 10, pp. 341-350, 1997.

[4] A. Faldum and W. Willems, *A Characterization of MMD Codes*, IEEE Trans. on Inf. Theory, vol. 44, no. 4, 1998.

[5] J.H. van Lint, *Introduction to Coding Theory*, Springer-Verlag 1982.

[6] J. Olsson, *On Near-Near-MDS Codes*, Fifth International Workshop on Algebraic and Combinatorial Coding Theory, pp. 231-236, June 1 - June 7, 1996, Sozopol, Bulgaria.

[7] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error Correcting Codes.* North-Holland 1977.

[8] E.F. Assmus and J.K. Key, *Designs and their Codes*, Cambridge University Press, 1993.

[9] T. Helleseth, T. Kløve and J. Mykkeltveit, *The weight distribution of irreducible cyclic codes with block lengths* $n_1((q^l-1)/N)$, Discr. Math., vol. 18, pp. 179-211, 1977.

[10] G.D. Forney, Jr., *Dimension/Length Profiles and Trellis Complexity of Linear Block Codes*, IEEE Trans. on Inf. Th. , vol. 40, no. 6, pp. 1741-1752, november, 1994.

[11] A. Bonisoli, *Every equidistant linear code is a sequence of dual Hamming codes*, Ars Combinatoria, vol. 18, pp. 181-186, 1983.

[12] G. Tallini, *Sulle k-calotte di uno spazio lineare finito*, Annali di Matematica, vol. 42, pp. 119-164, 1956.

[13] A.E. Brouwer, *Bounds on the minimum distance of linear codes*, [Online], Eindhoven University of Technology, Eindhoven, The Netherlands, Available: http://www.win.tue.nl/math/dw/voorlincod.html.

[14] J. Olsson, *Linear Codes with Performance close to the Singleton Bound*, Thesis No. 683, LIU-TEK-LIC-1998:18, Linköping University, Sweden.