A Characterization of MMD Codes

A. Faldum
IDIR
Universität Jena
07740 Jena

W. Willems
Fachbereich Mathematik
Universität Mainz
55099 Mainz

faldum@bach.med.uni-jena.de
willems@mathematik.uni-mainz.de

Abstract Let C be a linear $[n, k, d]$-code over $\mathrm{GF}(q)$ with $k \geq 2$. If $s = n-k+1-d$ denotes the defect of C, then by the Griesmer bound, $d \leq (s+1)q$. Now, for obvious reasons, we are interested in codes of given defect s for which the minimum distance is maximal, i.e. $d = (s+1)q$. In this paper we classify up to formal equivalence all such linear codes over $\mathrm{GF}(q)$. Remember that two codes over $\mathrm{GF}(q)$ are formally equivalent if they have the same weight distribution. It turns out that such codes exist only in dimension 3 and 4 with the ternary extended Golay code, the ternary dual Golay code and the binary even weight code as exceptions. In dimension 4 they are related to ovoids in $\mathrm{PG}(3, q)$ except the binary extended Hamming code, and in dimension 3 to maximal arcs in $\mathrm{PG}(2, q)$.

Index terms linear code, defect of codes, weight distribution, ovoids, arcs, optimal codes, maximum minimum distance

1 Introduction

Let C be a linear $[n, k, d]$-code over $\mathrm{GF}(q)$ where n denotes the length, k the dimension and d the minimum distance of C. Sometimes we also say that C has parameters $[n, k, d]_q$. Furthermore let $s = n - k + 1 - d$ denote the defect of C. Then, if $k \geq 2$, the Griesmer bound

$$n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil$$

immediately yields

$$\frac{d}{q} \leq n - d - k + 2 = s + 1,$$

hence

$$d \leq (s+1)q. \tag{1}$$

If even $k \geq 3$ and $d = (s+1)q$, then again by the Griesmer bound

$$d + k + s - 1 = n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil \geq d + s + 1 + \lceil \frac{s+1}{q} \rceil + k - 3,$$

and hence

$$s \leq q - 1. \tag{2}$$

Definition 1.1 *A linear code C over* GF(q) *of defect s, minimum distance d and dimension $k \geq 2$ is called an* MMD *code* (<u>M</u>aximum <u>M</u>inimum <u>D</u>istance)*, if $d = (s+1)q$.*

Note that the length n of an MMD code is equal to $n = (s+1)q+k+s-1$.

Lemma 1.2 *For each nonnegative integer s there exists a 2-dimensional* MMD *code over $GF(q)$ of defect s and those are uniquely determined up to equivalence.*

Proof: If GF$(q) = \{a_1, \ldots, a_q\}$, then

$$\begin{pmatrix} 0 & \ldots & 0 & 1 & \ldots & 1 & \ldots & 1 & \ldots & 1 \\ 1 & \ldots & 1 & a_1 & \ldots & a_1 & \ldots & a_q & \ldots & a_q \end{pmatrix},$$

where the blocks have length $s+1$, defines the generator matrix of a $[(s+1)(q+1), 2, (s+1)q]$ MMD code over GF(q).

For the rest of the paper we may assume that an MMD code has dimension $k \geq 3$.

Definition 1.3 *Let C be a linear code over* $\mathrm{GF}(q)$*.*

a) C is called an ovoid code, if C has a four row generator matrix whose columns considered in the projective space $\mathrm{PG}(3,q)$ form an ovoid, i.e. a nonempty set $\mathcal{O} \subseteq \mathrm{PG}(3,q)$ which satisfies the following two conditions:

(i) Each line in $\mathrm{PG}(3,q)$ intersects $\mathcal{O}$ in at most two points.

(ii) For any $P \in \mathcal{O}$, the union of all lines that meet $\mathcal{O}$ only in P is a hyperplane of $\mathrm{PG}(3,q)$.

b) C is called a maximal arc code, if C has a three row generator matrix whose columns considered in $\mathrm{PG}(2,q)$ form a maximal arc, i.e. a nonempty set of points in $\mathrm{PG}(2,q)$ meeting every line in a fixed number of points or in non at all.

The reader who is not familiar with these geometrical objects is referred to the books of Dembowski [2] and Hirschfeld [6].

In this paper we mainly prove:

Theorem 1.4 *Let C be a linear code over $\mathrm{GF}(q)$ of dimension $k \geq 3$. Then C is an* MMD *code if and only if C is one of the following codes:*

- *the binary $[k+1, k, 2]$ even weight code*
- *the ternary $[12, 6, 6]$ extended Golay code*
- *the ternary $[11, 5, 6]$ dual Golay code*
- *the binary $[8, 4, 4]$ Hamming code*
- *a $[q^2+1, 4, q^2-q]$ ovoid code*
- *or a maximal arc code.*

Remarks 1.5 a) Applying results on the classification of maximal arcs we will get a description of the 3-dimensional MMD codes up to formal equivalence in section 5.
b) In the meantime the first author of this paper has obtained in his thesis [4] the bound $k \leq 4$ for a much larger class than MMD codes. More precisely, he proved that if $k \geq 4$, $s > 1$ and $d \geq \max\{\, sq+1,\ (s+1)q - \sqrt{s+1}\}$, then k has to be 4 and $s = q-2$. The main methods are similar to those presented here but involve an amount of manipulations with inequalities in the parameters.

2 The weight distribution

Definition 2.1 *A code of defect* 1 *is called an almost* MDS *code.*

For the proof of the next result we refer the reader to Theorem 7 of [5].

Lemma 2.2 *Let C be an $[n,k,d]$-code over* $\mathrm{GF}(q)$ *of defect $s \geq 1$. If $d > sq$, then the dual code $C^{\perp}$ is an almost* MDS *code.*

As an immediate consequence of Lemma 2.2 we have

Corollary 2.3 *The dual of an* MMD *code of defect $s \geq 1$ is an* almost MDS *code.*

The following Theorem is a slightly improved version of an earlier result.

Theorem 2.4 *Let C be an $[n,k,d]$ code over* $\mathrm{GF}(q)$ *of defect $s \geq 1$ and let $C^{\perp}$ have minimum distance $d^{\perp}$. Then the weight distribution A_i $(i = 0,\ldots,n)$ of C satisfies*

$$\begin{aligned} A_{n-d^{\perp}+r} &= (-1)^r r \binom{d^{\perp}}{r} \sum_{i=d}^{n-d^{\perp}} \binom{n-i}{d^{\perp}} \frac{A_i}{n-i-d^{\perp}+r} \\ &\quad + \binom{n}{d^{\perp}-r} \sum_{i=0}^{r-1} (-1)^i \binom{n-d^{\perp}+r}{i} (q^{k-d^{\perp}+r-i} - 1) \end{aligned}$$

for $r = 1,\ldots,d^{\perp}$.
In particular, $A_d,\ldots,A_{n-d^{\perp}}$ completely determine the weight distribution of C.

Proof: Because of Theorem 9 of [5] we only have to prove that

$$\sum_{j=d^{\perp}}^{n-d} \binom{j}{d^{\perp}-r} \left(\sum_{i=d^{\perp}}^{j} (-1)^{i-d^{\perp}+r} \binom{j-d^{\perp}+r}{j-i} \right) A_{n-j} =$$
$$(-1)^r r \binom{d^{\perp}}{r} \sum_{i=d}^{n-d^{\perp}} \binom{n-i}{d^{\perp}} \frac{A_i}{n-i-d^{\perp}+r}.$$

Since $\sum_{i=0}^{r}(-1)^i\binom{n}{i} = (-1)^r\binom{n-1}{r}$, we obtain

$$\sum_{j=d^\perp}^{n-d}\binom{j}{d^\perp - r}\left(\sum_{i=d^\perp}^{j}(-1)^{i-d^\perp+r}\binom{j-d^\perp+r}{j-i}\right)A_{n-j} =$$

$$\sum_{j=d^\perp}^{n-d}\binom{j}{d^\perp - r}\left(\sum_{i=r}^{j-d^\perp+r}(-1)^{i}\binom{j-d^\perp+r}{i}\right)A_{n-j} =$$

$$-\sum_{j=d^\perp}^{n-d}\binom{j}{d^\perp - r}\left(\sum_{i=0}^{r-1}(-1)^{i}\binom{j-d^\perp+r}{i}\right)A_{n-j} =$$

$$-\sum_{j=d^\perp}^{n-d}\binom{j}{d^\perp - r}(-1)^{r-1}\binom{j-d^\perp+r-1}{r-1}A_{n-j} =$$

$$\sum_{j=d^\perp}^{n-d}(-1)^r r\binom{d^\perp}{r}\binom{j}{d^\perp}\frac{A_{n-j}}{j-d^\perp+r} =$$

$$(-1)^r r\binom{d^\perp}{r}\sum_{i=d}^{n-d^\perp}\binom{n-i}{d^\perp}\frac{A_i}{n-i-d^\perp+r}.$$

Quite surprising is the next result which shows that the weight distribution of an MMD code is uniquely determined by the parameters of the code, i.e. MMD codes with the same parameters are formally equivalent.

Proposition 2.5 *Let C be an* MMD *code of defect $s \geq 1$ with parameters $[n,k,d]_q$ and $k \geq 3$. Then the weight distribution A_i $(i = 0,\ldots,n)$ satisfies*

$$\begin{aligned} A_d &= \frac{\binom{n}{k-1}}{\binom{k+s-1}{k-1}}(q-1), \\ A_{d+i} &= 0 \quad \textit{for } i = 1,\ldots,s+1, \\ A_{d+s-1+r} &= (-1)^r\frac{s(q-1)n!}{(s-1+r)(r-1)!(k-r)!(s+d)!} + \\ &\quad \binom{n}{k-r}\sum_{i=0}^{r-1}(-1)^i\binom{n-k+r}{i}(q^{r-i}-1) \\ &\quad \textit{for } r = 1,\ldots,k. \end{aligned}$$

Therefore the weight distribution is uniquely determined by n,k,d and q. (Note that for $r = 1,2$ we have $A_{d+s-1+r} = 0$.)

Proof: First we prove that

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

and

$$A_{d+1} = A_{d+2} = \ldots = A_{d+s+1} = 0 : \tag{3}$$

Let G be a generator matrix of C. Since $C^{\perp}$ is an almost MDS code, by 2.3, the minimum distance $d^{\perp}$ of $C^{\perp}$ equals $d^{\perp} = k$. By the assumption of the Proposition, $k \geq 3$. Thus we may regard the column vectors of G as different points in the projective space PG(k-1,q). Since $n = k + (s+1)q + s - 1$ and $d = (s+1)q$, at most $k + s - 1$ column vectors of G are in a hyperplane of PG(k-1,q). Furthermore, any set of $k-1$ column vectors of G generate a hyperplane in PG(k-1,q) as $d^{\perp} = k$ and any set of $k-2$ such vectors are contained in exactly $q+1$ hyperplanes. Thus we get

$$k + (s+1)q + s - 1 = n \leq (k-2) + (q+1)(s+1) = n.$$

This shows that a hyperplane containing at least $k-2$ column vectors of G contains exactly k+s-1 column vectors. Hence

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

as asserted above. Since $n - (k-2) = d + s + 1$ and $n - (k+s-1) = d$, we furthermore have $A_{d+1} = A_{d+2} = \ldots = A_{d+s+1} = 0$ and the claim has been proved. To obtain the complete weight distribution we use the formula in 2.4. Here we need again the assumption $s \geq 1$. Note that $n - d^{\perp} = n - k = d + s - 1$. By the results already proved the formula reduces to

$$\begin{aligned} A_{d+s-1+r} = \quad & (-1)^r r \binom{k}{r}\binom{n-d}{k}\frac{A_d}{r+s-1} \\ & + \binom{n}{k-r}\sum_{i=0}^{r-1}(-1)^i\binom{d+s-1+r}{i}(q^{r-i}-1). \end{aligned}$$

Finally, if we multiply $(-1)^r \frac{r}{r+s-1}\binom{k}{r}\binom{n-d}{k}$ by A_d, which we have computed already, we get the factor

$$(-1)^r \frac{s(q-1)n!}{(s-1+r)(r-1)!(k-r)!(s+d)!}$$

and the proof is complete.

3 Sporadic MMD codes

We start with the classification of MMD codes of defect $s = 0$.

Lemma 3.1 *Let* C *be an* MMD *code of dimension* $k \geq 4$ *and defect* 0. *Then* C *is the binary* $[k+1, k, 2]$ *even weight code.*

Proof: Remember that $n = (s+1)q + k + s - 1 = q + k - 1$ is the length of C. Repeated shortening leads to an MDS code with parameters $[q+3, 4, q]_q$. But such a code does not exist for $q \geq 3$, by ([7], Chap. 11, §7). For $q = 2$, the parameters of C are $[k+1, k, 2]_2$ and the assertion of the Lemma follows.

For the reader's convenience we restate part of ([5], Corollary 8) as

Lemma 3.2 *If* C *is an* MMD *code of defect* $s \geq 1$ *over* $\mathrm{GF}(q)$, *then* $\dim C \leq 2q$.

Proof: By 2.3, $C^\perp$ is of defect $s^\perp = 1$. Furthermore $\dim C^\perp = n - k = s + d - 1 \geq d = (s+1)q \geq 4$. Thus, by (1) of the introduction, the minimum distance of $C^\perp$ is bounded by $\mathrm{d}(C^\perp) = k \leq (s^\perp + 1)q = 2q$.

Lemma 3.3 *If* C *is a binary* MMD*-code of defect* $s \geq 1$ *and dimension* $k \geq 3$, *then* C *is the* $[7, 3, 4]$ *Simplex code or the* $[8, 4, 4]$ *extended Hamming code.*

Proof. The equation (2) of the introduction implies $1 \leq s \leq q - 1 = 1$. Thus C is a binary $[k+4, k, 4]$-code. By 3.2, $\dim C = k \leq 2q = 4$. As $k \geq 3$, C is the binary $[7, 3, 4]$ Simplex code or the binary $[8, 4, 4]$ extended Hamming code.

Lemma 3.4 *Let* C *be an* MMD *code with parameters* $[q^2 + q - 2 + k, k, q^2]_q$, *i.e. the bound* $s = q - 1$ *in* (2) *is reached. If* $q > 2$ *and* $k \geq 3$, *then* $k = 3$ *and* C *is the* $[q^2 + q + 1, 3, q^2]$ *Simplex code.*

Proof: First observe that $C^\perp$ is of defect 1, by 2.3. Suppose that $k \geq 4$. Then by repeated shortening we get a code, say C_0, of length $q^2 + q + 2$, of dimension 4 and with minimum distance at least q^2. In particular, C_0 is of defect $s_0 \leq q - 1$. Furthermore $s_0 \geq 1$, by (1) of the introduction. Since $q^2 > q^2 - q \geq s_0 q$, Lemma 2.2 implies that $C_0^\perp$ is an almost MDS code. Thus $C_0^\perp$ has parameters $[q^2+q+2, q^2+q-2, 4]_q$. In particular, any three column vectors of a generator matrix of C_0 are not collinear regarded as points in $\mathrm{PG}(3,q)$. Since $q > 2$, ([2], 1.4, 49(c), page 48) yields

$$q^2 + q + 2 \leq q^2 + 1,$$

a contradiction. Thus C is of dimension three and is therefore the Simplex code.

Lemma 3.5 *Let C be a $[q^2+1, 4, q^2-q]$ code over* $\mathrm{GF}(q)$ *with $q > 2$. Then C is an ovoid code.*

Proof: Clearly, C has defect $s = q-2$. Furthermore, the minimum distance d of C satisfies $d = q^2 - q = (q-1)q > sq$. Thus by 2.2, $C^\perp$ is an almost MDS code and has therefore minimum distance 4. In particular, any three column vectors of a generator matrix of C are linearly independent. Thus the set of all column vectors regarded in $\mathrm{PG}(3,q)$ form an ovoid, by ([2], 1.4, 49(c)) and the proof is complete.

Lemma 3.6 *Let C be a ternary* MMD *code of defect $s \geq 1$ and dimension $k \geq 4$. Then C is the $[12,6,6]$ extended Golay code, the $[11,5,6]$ dual Golay code or the $[10,4,6]$ ovoid code.*

Proof: By (2) of the introduction, we have $s \leq q-1 = 2$. If $s = 2 = q-1$, then 3.4 leads to a contradiction as $k \geq 4$. Hence $s = 1$ and C has minimum distance $d = (s+1)q = 6$. By 3.2, $k \leq 2q = 6$ and the assertion of the Lemma follows by [8] resp. 3.5 in case $k = 4$. Note that the ternary $[10,4,6]$ ovoid code is unique since it is the dual of the unique $[10,6,4]$ punctured Golay code.

4 MMD codes in dimension $k \geq 4$

In this section we will prove Theorem 1.4 in case that the dimension of the code is greater than three. By 3.1, we may assume that the defect of the code is not 0. According to 3.3 and 3.6 we may assume that the size q of the underlying field satisfies $q \geq 4$.

Proposition 4.1 *Let C be an $[n,k,d]$* MMD *code over* $\mathrm{GF}(q)$ *of defect $s \geq 1$. If $k \geq 4$, then $s = q-1$ or $s = q-2$.*

Proof: By (2), we know already that $s \leq q-1$. Thus it remains to show that $s \geq q-2$. To prove this we exploit the formula

$$\begin{aligned} A_{d+s-1+r} &= (-1)^r \tfrac{s(q-1)n!}{(s-1+r)(r-1)!(k-r)!(s+d)!} + \\ & \tbinom{n}{k-r} \sum_{i=0}^{r-1} (-1)^i \tbinom{n-k+r}{i} (q^{r-i}-1) \end{aligned}$$

stated in Proposition 2.5 for $r=4$. This is allowed since $k \geq 4$. We obtain

$$\begin{aligned} 0 \leq A_{d+s+3} &= \tfrac{n!}{6(k-4)!(s+d)!} \Big\{ \tfrac{s(q-1)}{s+3} + \\ & \tfrac{1}{\binom{s+d+3}{3}} \sum_{i=0}^{3} (-1)^i \tbinom{s+d+3}{i} (q^{4-i}-1) \Big\} . \end{aligned}$$

Hence

$$0 \leq s(q-1)\binom{s+d+3}{3} + (s+3)\sum_{i=0}^{3}(-1)^i\binom{s+d+3}{i}(q^{4-i}-1). \qquad (4)$$

Note that this inequality contains only s and q, since $d=(s+1)q$. Thus it defines a relation between s and q. Now the right hand side of (4) factors as

$$q(q-1)(qs+s+1-q)(s-q+2),$$

which proves $s \geq q-2$.

Proposition 4.2 *Let C be an $[n,k,d]$ MMD code over $\mathrm{GF}(q)$ of defect $s \geq 1$. If $k \geq 4$ and $q \geq 4$, then $k=4$ and C is a $[q^2+1, 4, q^2-q]$ ovoid code.*

Proof: By Proposition 4.1, we have $s=q-1$ or $s=q-2$. In the first case we get a contradiction to 3.4 as $k \geq 4$. Hence $s=q-2$ and C is a $[q^2+k-3, k, q^2-q]$ code, and by 2.2, the dual $C^\perp$ is a $[q^2+k-3, q^2-3, k]$ almost MDS code. According to Proposition 4 of [5] applied to $C^\perp$, we get a subcode $D \subseteq C^\perp$ of dimension $q-2$, of length smaller than $k+q-2$ and minimum distance greater or equal to k. Therefore D is a $[k+q-3, q-2, k]$ MDS code. By ([7], Chap. 11, Theorem 13), we get $k \leq 4$. Thus C is a $[q^2+1, 4, q^2-q]$-code and Lemma 3.5 completes the proof.

Up to this point we have proved the Theorem 1.4 for dimensions $k \geq 4$. So it remains to deal with 3-dimensional MMD codes. Before we do this in the next section we would like to make some remarks on the uniqueness of ovoid codes.

Remark 4.3 It is well-known that for q odd ovoids are projective elliptic quadrics (see [2], section 1.4). Thus in this case, ovoid codes are determined up to equivalence by its parameters. For q even, a classification of ovoids is still open. The only known examples are again the projective elliptic quadrics and in addition the Tits ovoids. For a fixed q these ovoids are non-isomorphic and the corresponding codes non-equivalent. However, they are formally equivalent. This can easily be seen from the definition of an ovoid code or directly by 2.5.

5 MMD codes in dimension 3

Proposition 5.1 *A 3-dimensional* MMD *code is a maximal arc code.*

Proof: Let C be a three-dimenional MMD code over $\mathrm{GF}(q)$ of length n and defect s. Let $\mathcal{G}$ be the set of column vectors of a generator matrix of C regarded as points in $\mathrm{PG}(2,q)$. If $s \geq 1$ Proposition 2.5 yields that the weights of C are in $\{0,d,n\}$. This is also true for $s=0$ by the well-known formula for the weight distribution of an MDS code (see for instance [7], Chap. 11, Theorem 6). Thus a line in $\mathrm{PG}(2,q)$ intersects $\mathcal{G}$ in exactly $n-d=s+2$ points or in non at all which means that $\mathcal{G}$ is a maximal arc in $\mathrm{PG}(2,q)$.

Proposition 5.2 *Let C be a 3-dimensional* MMD *code over* $\mathrm{GF}(q)$*. Then C is the $[q^2+q+1,3,q^2]$ Simplex code, a $[q^2,3,q^2-q]$ affine code or C has parameters $q-[(2^t-1)q+2^t,3,(2^t-1)q]$ with $1 \neq 2^t \mid q$. In the latter case, for a realization we may choose a maximal arc as defined by Denniston in* [3].

Proof: Obviously, $\mathrm{PG}(2,q)$ is a maximal arc which leads to the $[q^2+q+1,3,q^2]$ Simplex code. In this case, $q+1$ points of $\mathcal{G}$ (notation as in 5.1) are on each line. If q points are on each line which meets $\mathcal{G}$ nontrivially, then C has parameters $[q^2,3,q^2-q]_q$ and $\mathcal{G}$ is the complement of a line in $\mathrm{PG}(2,q)$, i.e. an affine two-dimenional space. Finally, suppose that each line meets $\mathcal{G}$ in less than q points, i.e. $\mathcal{G}$ is a nontrivial maximal arc. Note that a nontrivial intersection of $\mathcal{G}$ with a line contains exactly $s+2$ points. Hence $s+2 \mid q$, by ([6], 12.2.1). For q odd such arcs do not exist according to recent work [1] of Ball, Blokhuis and Mazzocca. In case q is even, for all possible s, i.e. such s which satisfy $s+2 \mid q$, there are examples, for instance the Denniston arcs as defined in [3]. The corresponding codes have parameters $[(2^t-1)q+2^t, 3, (2^t-1)q]_q$ with $1 \neq 2^t \mid q$.

Acknowledgments. We would like to thank J. Bierbrauer who brought paper [1] and [3] to our attention and the anonymous referees for helpful comments and in particular the factorization of the right hand side of (4) in 4.1.

References

[1] S. Ball, A. Blokhuis, F. Mazzocca, Maximal Arcs in Desarguesian Planes of Odd Order do not exist.
Preprint 1996.

[2] P. Dembowski, Finite Geometries.
Springer Verlag, Berlin 1968.

[3] R.H.F. Denniston, Some Maximal Arcs in Finite Projective Planes.
J. Combinatorial Theory 6 (1969), 317-319.

[4] A. Faldum, Codes mit optimalen Parametern.
Thesis, Magdeburg, 1997.

[5] A. Faldum and W. Willems Codes of Small Defect.
Designs, Codes and Cryptography 10 (1997), 341-350.

[6] J.W.P. Hirschfeld, Projective Geometries over Finite Fields.
Clarendon Press, Oxford, 1979.

[7] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes.
North-Holland, Amsterdam, sixth printing 1988.

[8] V. Pless, On the uniqueness of the Golay codes.
J. Combin. Theory 5 (1968), 215-228.