Designs, Codes and Cryptography, 9, 143–155 (1996)

Almost MDS Codes

MARIO A. DE BOER mariob@win.tue.nl
Department of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, the Netherlands

Communicated by: D. Jungnickel

Received May 19, 1994; Accepted May 22, 1995

Abstract. MDS codes are codes meeting the Singleton bound. Both for theory and practice, these codes are very important and have been studied extensively. Codes near this bound, but not attaining it, have had far less attention. In this paper we study codes that almost reach the Singleton bound.

Keywords: MDS codes, bounds on codes

1. Introduction

1.1. Codes, Geometry and Designs

In this section we will state some well known results that establish the geometric and design-theoretic properties of codes.

In this paper we will only consider linear codes over finite fields $\mathbb{F}_q$ with parameters as usual denoted by $[n, k, d]$. For such codes the Singleton bound holds [14]: $d \leq n - k + 1$.

The following definition is natural in this context.

Definition 1. The *Singleton defect* of an $[n, k, d]$ code C is $s(C) = n - k + 1 - d$.

The projective space of r dimensions obtained from $\mathbb{F}_q$ will be denoted by $\mathrm{PG}(r, q)$. We say that a set of m points of $\mathrm{PG}(r, q)$ are in general position if they are not contained in a subspace of dimension $m - 2$.

The following generalization of a set of mutually orthogonal Latin squares, due to K. A. Bush, reveals some of the design-theoretic properties of codes.

Definition 2 ([4]). An $n \times M$ matrix A with entries from a set of $l \geq 2$ elements, is an *orthogonal array* of size M, n constraints, l levels, strength t and index λ, if each $t \times M$ submatrix of A contains all l^t possible t-tuples exactly λ times as a column. Then $M = \lambda l^t$ and the array will be denoted by $\mathrm{OA}_\lambda(t, n, l)$.

If the columns of A form a linear space over the finite field $\mathbb{F}_q$, the orthogonal array is *linear*.

We can now state the following important result by Bose and Bush.

THEOREM 1 ([2]) *The following are equivalent:*

1. *C is an* $[n, k, d]$ *code with* $s(C) = s$
2. *The columns of the parity check matrix of C are n points in* $PG(n-k-1, q)$ *each* $d-1$ *of which are in general position*
3. *The* $n \times q^{n-k}$ *matrix A having as columns the codewords of* $C^{\perp}$ *is a linear orthogonal array* $OA_{q^s}(d-1, n, q)$.

1.2. *MDS Codes*

Before we define almost MDS codes we will look at MDS codes.

Definition 3. A code C with $s(C) = 0$ is *maximum distance separable* (MDS for short). MDS codes of dimensions $k = 1$, $n-1$ and n are *trivial.*

Many properties of MDS codes have been proved by considering the geometric representation as in case 2 of Theorem 1.

Definition 4. An *n-arc* in $\mathrm{PG}(r, q)$ is a set of n points such that every $r+1$ of them are in general position.

From Theorem 1 we see that MDS codes, n-arcs and linear orthogonal arrays of index unity are equivalent objects.

The earliest results on MDS codes were obtained by Bush in [4], using the general setting of (not necessarily linear) orthogonal arrays. The following result will be used later.

THEOREM 2 ([4]) *Let A be an* $OA_1(t, n, l)$. *If* $l \leq t$, *then* $n \leq t+1$.

In the special case of (linear) MDS codes, Theorem 2 together with the fact that the dual of an MDS code is MDS, yield the well known result that for a nontrivial $[n, k, n-k+1]$ MDS code we have that $k < q$ and $n-k < q$.

One of the main problems in the theory of MDS codes is determining the maximum length of an MDS code. The following is a famous conjecture.

Main Conjecture on MDS codes. For a nontrivial $[n, k, n-k+1]$ MDS code we have that $n \leq q+2$ if q is even and $k = 3$ or $k = q-1$, and $n \leq q+1$ otherwise.

This conjecture is proven in a number of cases, for example for codes over fields $\mathbb{F}_q$ with $q \leq 19$, and for codes with dimensions $k \leq 5$ (for references see [12] chapter 11, [10] chapter 27, and the recent paper [5].)

In his paper, Bush discovered linear orthogonal arrays of strength unity that achieve the maximum length in the conjecture. The corresponding codes are the well known extended Reed Solomon codes.

1.3. Almost MDS Codes

We are now ready to define almost MDS codes.

Definition 5. A code C with Singleton defect $s(C) = 1$ is *almost MDS* (AMDS for short). AMDS codes of dimensions $k = 1,\ n-2,\ n-1$ and n are called *trivial.*

Since it is easy to construct trivial AMDS codes of arbitrary lengths, we will only be considering nontrivial AMDS codes.

Unlike the MDS case, the dual of an AMDS code need not be AMDS. To distinguish this property we follow Dodunekov and Landgev [7] in the following definition.

Definition 6. ([7]) A code C with $s(C) = s(C^{\perp}) = 1$ is a *near MDS code.*

In their paper [7], a preliminary version of which was published as [6], Dodunekov and Landgev study near MDS codes. Some of their results were discovered independently by the author and will be presented in this paper.

As in the MDS case we define sets of points in projective space that reflect the property of being AMDS.

Definition 7. An *n-track* is a set of n points in $\mathrm{PG}(r, q)$ such that every r of them are in general position. The maximum size of an n-track in $\mathrm{PG}(r, q)$ is denoted by $\mu(r, q)$. The maximum size of an n-track for which the dual is also an n-track is denoted by $\mu^e(r, q)$.

Theorem 1 yields that AMDS codes, n-tracks and linear orthogonal arrays of index q are equivalent objects. Hence $\mu(r, q)$ is the maximum length n for which there exists an $[n, n-r-1, r+1]$ code over $\mathbb{F}_q$, and $\mu^e(r, q)$ is the analogue in the case of near MDS codes. Equivalently, $\mu(r, q)$ is the maximal number of constraints of a linear orthogonal array of index q and strength r.

The aim of this paper is to derive bounds on $\mu(r, q)$ and find properties of AMDS codes, or equivalently, of tracks. We will use the construction of shortening codes, that is taking all codewords that have a 0 at a fixed position, and deleting that position. The shortened code of an $[n, k, d]$ code has parameters $[n-1, k-1, d]$ and thus has the same Singleton defect as the original code. In the language of tracks it means that one projects the n-track from one of its points onto a hyperplane. The resulting set is clearly an $(n-1)$-track. This proves the following.

LEMMA 1 $\mu(r, q) \leq \mu(r-1, q) + 1$.

2. Upper Bounds on $\mu(r, q)$

In this section we distinguish between two cases: $r < q$ and $r \geq q$.

2.1. *The Case $r < q$*

In view of Theorem 1, the following is a well known result.

THEOREM 3 *[cf. [2]]* $\mu(2, q) = q^2 + q + 1$.

Proof. The projective plane clearly is a maximal set that satisfies the conditions for a track. ■

The next theorem generalizes a result by Gulati [8].

THEOREM 4 *Let*

1. $q \leq 19$ *or* $r \leq 5$ *or* $r \geq q - 3$
2. $q = p^m$ *and* $q > r > 2$.

Then, if q is odd or $3 < r < q - 1$

$$\mu(r, q) \leq \begin{cases} q(q - r + 3) + 1 & \text{if } r = q - p^l + 3 \text{ for some } l \leq m \\ q(q - r + 3) & \text{otherwise.} \end{cases}$$

Proof. Let K be an n-track in $\mathrm{PG}(r, q)$, and let $P_1, \ldots, P_{r-1} \in K$. For the $q + 1$ hyperplanes $S_1, \ldots, S_{q+1}$ that contain $P_1, \ldots, P_{r-1}$ we have that $S_i \cap K$ is an arc in $\mathrm{PG}(r - 1, q)$. Condition 1 of the theorem implies that the main conjecture on MDS codes holds for codes of dimension r over $\mathbb{F}_q$. Since $q > r$, this yields that $|S_i \cap K| \leq q + 1$. Since two S_i only meet in the $(r - 2)$-space spanned by $P_1, \ldots, P_{r-1}$ we have that

$$\begin{aligned} |K| &\leq r - 1 + (q + 1)(q - r + 2) \\ &= q(q - r + 2) + q + 1 \\ &= q(q - r + 3) + 1. \end{aligned}$$

Now suppose $|K| = q(q - r + 3) + 1$. If S is any $(r - 1)$-space, then by the above we have that if $|K \cap S| \geq r - 1$, then $|K \cap S| = q + 1$. Now consider all $(r - 2)$-spaces passing through the points $P_1, \ldots, P_{r-2}$. There are $q^2 + q + 1$ of these and each of them intersects K in either $r - 2$ points (the points $P_1, \ldots, P_{r-2}$) or $q + 1$ points (a complete arc). Hence there must be an integer m such that

$$m(q - r + 3) + r - 2 = q(q - r + 3) + 1$$

and so we find that

$$q - r + 3 | q$$

which is impossible if $r \neq q - p^l + 3$ for some $l \leq m$. ■

Remark 1. The first condition in Theorem 4 is needed to assure that the main conjecture on MDS codes holds for codes of dimension r over $\mathbb{F}_q$. The condition can be replaced by other cases in which the main conjecture is known to be true.

Together with the fact that for any q there exist ovoids (sets of q^2+1 points in PG$(3,q)$ with the property that there are no 3 collinear, for example elliptic quadrics), Theorem 4 proves the q odd case of the following result, which was first proved in this case in [2]. The proof in the even case is due to Qvist [13].

THEOREM 5 ([2], [13]) *For $q \neq 2$ we have $\mu(3,q) = q^2+1$.*

2.2. *The Case $r \geq q$*

We start by giving a general upper bound on the maximum length of $[n,k,d]$ codes over $\mathbb{F}_q$ with $d > q$. It generalizes the Bush bound (Theorem 2) for linear orthogonal arrays.

THEOREM 6 *Let C be an $[n,k,d]$ code with Singleton defect s and $d > q$. Then*

$$n \leq d - 2 + 2\frac{q^{s+1}-1}{q-1}.$$

Proof. Set $r = n-k-1$. Then the columns of the parity check matrix of C can be considered as a set K of n points in PG(r,q), no $r-s+1$ in a codimension $(s+1)$ subspace. Fix $P_1, P_2, \ldots, P_{r-s} \in K$ and consider the $(r-s)$-dimensional spaces $S_1, \ldots, S_{\frac{q^{s+1}-1}{q-1}}$ passing through them. For $i = 1, \ldots, \frac{q^{s+1}-1}{q-1}$ the set $S_i \cap K$ is an arc with $r-s = d-2 \geq q-1$, so by Theorem 2 $|S_i \cap K| \leq r-s+2$ and we find

$$|K| \leq r-s+2\frac{q^{s+1}-1}{q-1} = d-2+2\frac{q^{s+1}-1}{q-1}. \qquad \blacksquare$$

For tracks the result of Theorem 6 is the following.

COROLLARY 1 *Let $r \geq q$. Then $\mu(r,q) \leq 2q+r+1$.*

In section 4 we will determine all codes that (almost) reach this upper bound.

Corollary 1 improves on the Plotkin and Hamming bound for these codes, and on the Griesmer bound for $r < 2q$. For $r \geq 2q$ the result of the Griesmer bound is strong: there are no AMDS codes with $r \geq 2q$. This was also noted by Dodunekov and Landgev in [7].

THEOREM 7 *[cf. [7]] If C is an $[n, n-r-1, r+1]$ AMDS code, then $r < 2q$.*

Proof. Let $r \geq 2q$. Then the Griesmer bound states

$$n \geq \sum_{i=0}^{n-r-2} \left\lceil \frac{r+1}{q^i} \right\rceil \geq n+1$$

which is a contradiction. $\blacksquare$

As also was remarked in [7], we can improve on this bound by rephrasing the following result from projective geometry. A plane 3-arc is a set of points in PG$(2,q)$ with at most

3 points on a line. The matrix having the points of a plane 3-arc as columns is a generator matrix of an $[n, 3, n-3]$ code. The converse is also true so that the concepts of a three-dimensional AMDS code and a plane 3-arc are equivalent. A result by Thas [15] shows that for $q > 3$ the number of points on a plane 3-arc cannot exceed $2q + 1$. This has the following consequence for AMDS codes.

THEOREM 8 [cf. [7]] *If C is an $[n, n-r-1, r+1]$ AMDS code over $\mathbb{F}_q$, $q > 3$, with $r \leq n-4$, then $r < 2q-2$.*

Proof. Shorten the code $n-r-4$ times. The resulting code is equivalent to a plane 3-arc of size $r+4$, and so $r+4 \leq 2q+1$. ■

Remark 2. For $[n, k, n-k]$ codes this can be rephrased as $n \leq k + 2q - 2$.

We now give a version of Theorem 8 for the case $r = n-3$.

THEOREM 9 *The maximal n for which there exists an $[n, 2, n-2]$ code over $\mathbb{F}_q$ is $n = 2q+2$.*

Proof. Let G be the generator matrix of an $[n, 2, n-2]$ code. Without loss of generality we assume that the first row of G has ones at the first w positions followed by $n-w$ zeros, $w \geq n-2$. At the first w positions of the second row of G every element of $\mathbb{F}_q$ may occur only twice. This proves $w \leq 2q$ and hence $n \leq 2q+2$. It is clear that equality can occur. ■

Theorem 9 can be used to give the values of $\mu(r, q)$ for $r = 2q-1$ and $r = 2q-2$.

COROLLARY 2 *If $q > 3$ then $\mu(2q-1, q) = 2q+2$ and $\mu(2q-2, q) = 2q+1$.*

Proof. Let $r = 2q-1$ or $r = 2q-2$. Then $r \geq 2q-2$ and Theorem 8 yields $r \geq n-3$, so $\mu(r, q) \leq r+3$. Equality follows from Theorem 9. ■

3. Duality and Near MDS Codes

As remarked in Section 1.3, the dual of an AMDS code need not be AMDS. Nevertheless, Dodunekov and Landgev show in [7], that for $r \geq q$ this is the case.

THEOREM 10 ([7]) *Let C be an $[n, n-r-1, r+1]$ AMDS code. If $r \geq q$ then $C^\perp$ is also AMDS.*

If some part of the main conjecture on MDS codes holds we can give a bound on the Singleton defect of the dual code $C^\perp$ in the case $r < q$.

THEOREM 11 *Let C be an AMDS code over $\mathbb{F}_q$ with $r < q$. Let $q \leq 19$ or $r \leq 5$ or $r \geq q-3$. Then*

$$s(C^\perp) \leq \begin{cases} q-r+2 & \text{if } r = 3 \text{ or } r = q-1 \text{ and } q \text{ even} \\ q-r+1 & \text{otherwise.} \end{cases}$$

Proof. Let C be an $[n, n-r-1, r+1]$ code and let the dual distance be $d^\perp$. Then shortening by the dual distance (construction Y1 in [12], page 592) yields an $[n-d^\perp, n-r-d^\perp, r+1]$ MDS code. Since the conditions of the theorem imply that for these parameters the main conjecture holds, this implies that $n - d^\perp \leq q + 2$ if $r = 3$ or $q - 1$ and q even, and $n - d^\perp \leq q + 1$ otherwise. This proves the theorem. ∎

Remark 3. As in Remark 1, the conditions on q or r that are needed to assure the validity of the main conjecture on MDS codes in Theorem 11 can be replaced by other cases in which the main conjecture is proven.

Remark 4. Since there are $[q^2+q+1, q^2+q-2, 3]$ and $[q^2+1, q^2-3, 4]$ codes, we have as a consequence of the above theorem that there exist $[q^2+q+1, 3, q^2]$ for arbitrary q and $[q^2+1, 4, q^2-q]$ codes for q odd. These parameters are quite good.

4. Extremal AMDS Codes

In this section we will find all $[n, n-r-1, r+1]$ codes, $r \geq q$, that (almost) reach the upper bound of Corollary 1, more precisely $n = 2q+r+1$ or $n = 2q+r$. It will turn out that these codes only exist over small fields.

We use the following form of the MacWilliams identities relating the weight distribution A_i of code C to the weight distribution $A_i^\perp$ of the dual code $C^\perp$ (cf. [12] chapter 5).

$$q^{v-k} \sum_{i=0}^{n-v} \binom{n-i}{v} A_i = \sum_{i=0}^{v} \binom{n-i}{n-v} A_i^\perp, \qquad v = 0, \ldots, n.$$

For near MDS codes this implies the following recursion on the $A_i^\perp$. See also [7] for a similar result.

$$\begin{cases} A_k^\perp &= A_{n-k} \\ A_{k+t}^\perp &= (q^t-1)\binom{n}{k+t} - \sum_{i=0}^{t-1} \binom{n-k-i}{t-i} A_{k+i}^\perp \qquad t = 1, \ldots, n-k. \end{cases} \tag{1}$$

This proves the well known fact that for near MDS codes the weight enumerator is known as soon as the number of minimal weight codewords has been determined.

In the extremal cases, where n differs at most one from the upper bound in Corollary 1, we can count the number of codewords of minimal weight.

LEMMA 2 *Let C be an $[n, n-r-1, r+1]$ code with $r \geq q$. For the number of minimal weight codewords A_{r+1} we have*

$$A_{r+1} = \begin{cases} \frac{\binom{n}{r-1}(q^2-1)}{\binom{r+1}{2}} & \text{if } n = 2q+r+1 \\ \frac{\binom{n}{r-1}q(q-1)}{\binom{r+1}{2}} & \text{if } n = 2q+r \end{cases}$$

Proof. We restrict to the case where $n = 2q + r + 1$ (the second case is quite the same). Let K be an n-track in PG(r, q). The number of minimal weight codewords is equal to $q - 1$ times the number of dependent $(r + 1)$-tuples of points of K. Fix $r - 1$ points $P_1, \ldots, P_{r-1}$ of K. Then there are $q + 1$ $(r - 1)$-spaces containing them and in each of them there is exactly one pair of points completing $P_1, \ldots, P_{r-1}$ to a set of $r + 1$ dependent points (they lie in an $(r - 1)$-space). Hence there are $(q - 1)(q + 1)$ minimal weight codewords with support containing $r - 1$ fixed coordinates. If we note that in this way we count every minimal weight codeword $\binom{r+1}{r-1}$ times, this completes the proof. ∎

Using equations (1) we find the following theorem.

THEOREM 12 *Let C be a $[n, n - r - 1, r + 1]$ near MDS code with $r \geq q$. Then for the number of codewords of low weight of $C^{\perp}$ we have:*

	$n = 2q + r + 1$	$n = 2q + r$
$A^{\perp}_{2q-1}$	0	$\frac{\binom{n}{r-1}q(q-1)}{\binom{r+1}{2}}$
$A^{\perp}_{2q}$	$\frac{\binom{n}{r-1}(q^2-1)}{\binom{r+1}{2}}$	$\binom{n}{r-1}\frac{q-1}{r}$
$A^{\perp}_{2q+1}$	0	0
$A^{\perp}_{2q+2}$	0	$\frac{1}{3}\binom{n}{r-2}q(q-1)(q-2)$
$A^{\perp}_{2q+3}$	$\frac{1}{3}\binom{n}{r-2}q(q-1)(q-2)$	$-\frac{1}{6}\binom{n}{r-3}q(q-1)(q-5)$
$A^{\perp}_{2q+4}$	$-\frac{1}{2}\binom{n}{r-3}q(q-1)(q-3)$	$\frac{1}{10}\binom{n}{r-4}q(q-1)(q-3)(2q^2+3)$

COROLLARY 3 *Let C be an $[n, n - r - 1, r + 1]$ near MDS code with $r \geq q$. If $n = 2q + r + 1$ then C is one of the following codes:*

q	*parameters*	*description*
2	[7,4,3]	*Hamming code*
2	[8,4,4]	*extended Hamming code*
3	[10,6,4]	*punctured Golay code*
3	[11,6,5]	*Golay code*
3	[12,6,6]	*extended Golay code*

If $n = 2q + r$ then C is one of the following codes:

q	*parameters*	*description*
2	*[6,3,3]*	*punctured Hamming code*
2	*[7,3,4]*	*Simplex code*
3	*[9,5,4]*	*shortened punctured Golay code*
3	*[10,5,5]*	*shortened Golay code*
3	*[11,5,6]*	*dual Golay code*

Proof. From Theorem 12 we find that $q = 2$ or $q = 3$ in the case $n = 2q + r + 1$ and $q = 2, 3, 4$ or $q = 5$ in the case $n = 2q + r$ (otherwise some $A_i^{\perp}$ would be negative). For the cases $q = 2$ and $q = 3$ note that the Golay and Hamming codes are uniquely determined by q, n, k and d. Since their automorphism groups are at least 2- (Golay code) respectively 1-transitive (Hamming code), also the punctured and shortened codes are unique.

Over $\mathbb{F}_4$ the cases that have to be checked are: $[12, 7, 5]$, $[13, 7, 6]$ and $[14, 7, 7]$. By Theorem 10 the duals of these codes have minimum distance 7. Applying Corollary 2 shows that these codes cannot exist. This proves the $q = 4$ case.

Over $\mathbb{F}_5$ the cases that have to be checked are: $[15, 9, 6]$, $[16, 9, 7]$, $[17, 9, 8]$. Again Corollary 2 together with Theorem 10 yields the nonexistence of these codes. ■

Remark 5. Except for the cases mentioned in this section we have that Corollary 1 can be sharpened to $\mu(r, q) \leq 2q + r - 1$.

5. Quadratic Embedding of a Plane 3-Arc

In this section we show that the existence of an $[n, 3, n - 3]$ code implies the existence of an $[n, n - 6, 6]$ code. We use the following embedding:

$$\phi : \mathrm{PG}(2, q) \longrightarrow \mathrm{PG}(5, q)$$

$$\phi(x_0 : x_1 : x_2) = (x_0^2 : x_0x_1 : x_0x_2 : x_1^2 : x_1x_2 : x_2^2).$$

To prove the theorem we need the following lemma due to Ying and Ikeda [17]. They prove it using a more general theorem of Justesen, Larsen, Jensen, Havemose and Høholdt [11]. Pellikaan gave the following direct proof.

LEMMA 3 ([17]) *Any 5 points P_1, P_2, P_3, P_4, P_5 on a plane 3-arc are mapped by ϕ to 5 independent points in $PG(5, q)$.*

Proof. Suppose the points $\phi(P_i), i = 1, \ldots, 5$, in $\mathrm{PG}(5, q)$ are dependent, so they lie in the intersection of two hyperplanes. This means that the $P_1, P_2, \ldots, P_5$ lie in the intersection of two plane quadrics which implies that, by Bézout's teorem, the quadrics must have a line in common containing at least four of the $P_i, i = 1, \ldots, 5$. This contradicts with P_i lying on a plane 3-arc. ■

THEOREM 13 *If there exists an* $[n, 3, n-3]$ *code over* $\mathbb{F}_q$, *then there is an* $[n, n-6, 6]$ *code over* $\mathbb{F}_q$.

Proof. The columns of the generator matrix of an $[n, 3, n-3]$ code over $\mathbb{F}_q$ form a plane 3-arc in PG$(2, q)$. Applying ϕ to these columns yields n points in PG$(5, q)$, every 5 of which are in general position by Lemma 3. The resulting matrix is hence a parity check matrix of an $[n, n-6, 6]$ AMDS code. ■

6. Lower Bounds on $\mu(r, q)$

Using algebraic geometric codes we can construct an infinite class of AMDS codes. The following result by Tsfasman and Vlăduţ was also used in [7].

THEOREM 14 ([16], Chapter 3.2) *Let* $q = p^m$. *Then, for all* r, $1 \leq r < 2q$

$$\mu^e(r, q) \geq \begin{cases} q + \lfloor 2\sqrt{q} \rfloor & \text{if } p \mid \lfloor 2\sqrt{q} \rfloor \text{ and } m \geq 3, \ m \text{ odd} \\ q + \lfloor 2\sqrt{q} \rfloor + 1 & \text{otherwise.} \end{cases}$$

Constructing other infinite classes of AMDS codes of considerable length appears to be hard.

Apart from the infinite class of codes from elliptic curves, the quadratic residue codes are candidates (they include the maximal $[8, 4, 4]$ over $\mathbb{F}_2$, $[12, 6, 6]$ over $\mathbb{F}_3$ and $[12, 6, 6]$ over $\mathbb{F}_4$). Using a computer to find the real minimum distances of quadratic residue codes over small fields we find the following almost MDS codes.

THEOREM 15 *The following QR codes are self dual AMDS codes.*

$\mathbb{F}_2$:	$[8, 4, 4]$	$\mathbb{F}_9$:	$[20, 10, 10]$
$\mathbb{F}_3$:	$[12, 6, 6]$	$\mathbb{F}_{11}$:	$[20, 10, 10]$
$\mathbb{F}_4$:	$[12, 6, 6]$	$\mathbb{F}_{13}$:	$[18, 9, 9]$
$\mathbb{F}_5$:	$[12, 6, 6]$	$\mathbb{F}_{17}$:	$[20, 10, 10]$

Remark 6. Over larger fields the construction of AMDS codes using quadratic residue codes gives codes of poor length. The QR construction gives no nice results in these cases.

The next construction we will consider is a free construction using a computer. In PG$(4, q)$ (yielding $[n, n-5, 5]$ codes) this gave the following results that improve on the constructions mentioned above.

THEOREM 16 *The following parity check matrices give AMDS codes:*

- *PG*$(4, 5)$*:* $[12, 7, 5]$ *code:*

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 4 & 4 & 1 & 1 & 0 & 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 1 & 2 & 4 & 1 \\ 0 & 0 & 0 & 4 & 4 & 0 & 2 & 1 & 0 & 2 & 2 & 1 \\ 0 & 0 & 0 & 4 & 1 & 3 & 1 & 0 & 4 & 3 & 4 & 2 \end{bmatrix}$$

- *PG*(4, 7)*: [16, 11, 5] code:*

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 3 & 3 & 4 & 4 & 4 & 5 & 6 & 6 \\ 0 & 0 & 0 & 1 & 3 & 5 & 1 & 6 & 5 & 4 & 2 & 2 & 6 & 0 & 0 & 6 \\ 0 & 6 & 0 & 0 & 3 & 0 & 5 & 5 & 3 & 4 & 0 & 4 & 4 & 6 & 4 & 0 \\ 0 & 5 & 0 & 0 & 0 & 3 & 4 & 2 & 2 & 4 & 2 & 6 & 3 & 6 & 2 & 4 \end{bmatrix}$$

For small q the maximum sizes of plane 3-arcs are known (see the Ph.D. thesis by Ball [1]).

THEOREM 17 ([1]) *The maximal length of a plane 3-arc is:*

q	3	4	5	7	8	9
n	9	9	11	15	15	17

For $q = 11$ *the maximal length of a plane 3-arc is bounded by* $21 \leq n \leq 22$ *and for* $q = 13$ *we have* $23 \leq n \leq 27$.

Rephrasing this result in terms of AMDS codes and using the embedding ϕ of the previous section we find the following.

COROLLARY 4 *AMDS codes with the following parameters exist:*

Field	*plane 3-arc*	*embedded code*
$\mathbb{F}_3$	[9, 3, 6]	[9, 3, 6]
$\mathbb{F}_4$	[9, 3, 6]	[9, 3, 6]
$\mathbb{F}_5$	[11, 3, 8]	[11, 5, 6]
$\mathbb{F}_7$	[15, 3, 12]	[15, 9, 6]
$\mathbb{F}_8$	[15, 3, 12]	[15, 9, 6]
$\mathbb{F}_9$	[17, 3, 14]	[17, 11, 6]
$\mathbb{F}_{11}$	[21, 3, 18]	[21, 15, 6]
$\mathbb{F}_{13}$	[23, 3, 20]	[23, 17, 6]

7. A Table of $\mu(r, q)$

In this section we will explicitely compute the upper bounds and compare them with the lower bounds by putting them in a table. We have chosen to make a table of $\mu(r, q)$ but we also could have taken $\mu^e(r, q)$ (the upper bounds in the right upper corner would be considerably lower).

Remark 7. The entries in the table below are implied by the following results:

- For $q = 2, 3$ and 4 the results are well known [3].
- For $r = 2$ see Theorem 3, for $r = 3$ see Theorem 5.

- For $r = 4, \ldots, q-1$ the Hamming bound is used together with Lemma 1, except for $(r, q) = (6, 7)$, $(8, 9)$ and $(10, 11)$ where Theorem 4 is used.
- For $r = q, \ldots, 2q-3$ use Remark 4.
- The cases $r = 2q-2$ and $2q-1$ follow from Corollary 2.
- The bound $r < 2q$ is Theorem 7.
- The codes giving the lower bounds for $r = 4, \ldots, 2q-3$ are constructed in Section 6 or are shortened versions of these, except for the [16, 2, 14] and [15, 2, 13] codes over $\mathbb{F}_7$ whose existence follows from Theorem 9.

		q							
d	r	2	3	4	5	7	8	9	11
3	2	7	13	21	31	57	73	91	133
4	3	8	10	17	26	50	65	82	122
5	4		11	11	12-20	16-30	14-36	16-43	22-57
6	5		12	12	12-14	15-31	15-37	17-44	23-58
7	6			9	10-15	13-28	14-34	17-39	18-49
8	7			10	11-16	13-20	14-35	18-40	18-50
9	8				11	13-21	14-23	19-36	19-50
10	9				12	13-22	14-24	20-26	20-51
11	10					14-23	14-25	16-27	18-44
12	11					15-24	15-26	16-28	18-32
13	12					15	15-27	16-29	18-33
14	13					16	16-28	17-30	18-34

Acknowledgement

The author would like to thank Ruud Pellikaan for the valuable discussions on the subject.

References

1. S. M. Ball, On sets of points in finite planes, Ph.D. Thesis, University of Sussex, U.K. (1994).
2. R. C. Bose and K. A. Bush, Orthogonal arrays of strength two and three, *Ann. Math. Stat*, Vol. 23 (1952) pp. 508–524.
3. A. E. Brouwer, private communication.
4. K. A. Bush, Orthogonal arrays of index unity, *Ann. Math. Stat.*, Vol. 23 (1952) pp. 426–434.
5. J. M. Chao and H. Kaneta, Rational arcs in PG(r, q) for $11 \leq q \leq 19$, preprint.
6. S. M. Dodunekov and I. N. Landgev, On Near MDS Codes, Report LiTH-ISY-R-1563, Department of Electrical Engineering Linköping University, Sweden, 1994-02-02.
7. S. M. Dodunekov and I. N. Landgev, On near-MDS codes, to appear in *J. of Geometry*.

8. B. R. Gulati, More about maximal (n, r)-sets, *Information and Control*, Vol. 20 (1972) pp. 188–191.
9. J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford University Press, Oxford (1979).
10. J. W. P. Hirschfeld and J. A. Thas, *General Galois Geometries*, Oxford University Press, Oxford (1991).
11. J. Justesen, K. J. Larsen, H. Jensen, A. Havemose and T. Høholdt, Construcion an decoding of a class of algebraic geometric codes, *IEEE Trans. Inform. Theory*, Vol. 35 (1989) pp. 811–821.
12. J. F. K. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam (1977).
13. B. Qvist, Some remarks concerning curves of the second degree in a finite plane, *Ann. Acad, Sci. Fen. Ser. A* Vol. 134 (1952).
14. R. C. Singleton, Maximum distance separable q-nary codes, *IEEE Trans. Inform. Theory*, Vol. 10 (1964) pp. 116–118.
15. J. Thas, Some results concerning $((q+1)(n-1), n)$-arcs, *J. Combin. Theory A*, Vol. 19 (1975) pp. 228–232.
16. M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-Geometric Codes*, Kluwer Academic Publishers, Dordrecht/Boston/London (1991).
17. J. Q. Ying and T. Ikeda, Analysis of the Parameters of Codes from Hermitian Surface over GF(4), Technical report of IEICE, IT93-6 (1993) pp. 29–34.