Applicable Algebra in Engineering, Communication and Computing manuscript No.
(will be inserted by the editor)

T.L. Alderson · A.A. Bruen

Maximal AMDS codes

the date of receipt and acceptance should be inserted later

Abstract Complete (n,k)-arcs in $PG(k-1,q)$ and projective $(n,k)_q$-AMDS codes that admit no projective extensions are equivalent objects. We show that projective AMDS codes of reasonable length admit only linear extensions. Thus, we are able to prove the maximality of many known linear AMDS codes. At the same time our results sharply limit the possibilities for constructing long nonlinear AMDS codes. We also show that certain short linear AMDS codes are maximal. Central to our approach is the Bruen-Silverman (BRS) model of linear codes first introduced in [2, 1]).

Keywords NMDS codes · AMDS codes · (n,r)-arcs · arcs · cubic curves · complete arcs · code extension

The authors acknowledge support from the N.S.E.R.C. of Canada

T.L. Alderson
Mathematical Sciences
University of New Brunswick
Saint John, NB.
E2L 4L5
Canada
Tel.: +1-506-648-5622
E-mail: tim@unb.ca

A.A. Bruen
Electrical Engineering
University of Calgary
Calgary, AB
T2N 1N4
Canada
E-mail: bruen@ucalgary.ca

1 Introduction

For $n \geq k$, an $(n,k,d)_q$-code C is a collection of q^k n-tuples (or *codewords*) over an alphabet $\mathscr{A}$ of size q such that the minimum (Hamming) distance between any two codewords of C is d (that is, there exist two codewords agreeing in $n-d$ coordinates and no two codewords agree in as many as $n-d+1$). In the special case that $\mathscr{A} = GF(q)$ (the finite field of order q) and C is a vector space of dimension k, C is a *linear* $(n,k,d)_q$-code; C then has an associated generator matrix G. The columns of G can be considered as an n-multiset of points (or dually, hyperplanes) in $PG(k-1,q)$ at most $n-d$ per hyperplane (respectively, $n-d$ per point) called a *projective system* associated with C. Given a projective system $\mathscr{G}$ of points (respectively hyperplanes), a *t-fold hyperplane* (respectively *t-fold point*) of $\mathscr{G}$ is a hyperplane (respectively point) of $PG(k-1,q)$ incident with precisely t members of $\mathscr{G}$, counting multiplicity. A linear $(n,k,d)_q$-code is *projective* if every pair of columns in an associated generator matrix are linearly independent.
An (n,r)-*arc* $\mathscr{K}$ in $\Pi = PG(k,q)$, $k \leq r$ is an n-set of points such that each hyperplane of Π is incident with at most r points in $\mathscr{K}$ and some hyperplane is incident with $r-1$ points of $\mathscr{K}$. A *dual* (n,r)-*arc* is defined in the natural way. An (n,k)-arc in $PG(k,q)$ is an *n-arc*. A $(n,3)$-arc in $PG(2,q)$ is a *cubic arc*. An (n,r)-arc is *complete* if it is not contained in an $(n+1,r)$-arc. It follows that $(n,n-d)$-arcs in $PG(k-1,q)$ and a projective $(n,k,d)_q$-codes are equivalent objects.
From the Singleton bound it follows that an $(n,k,d)_q$ code satisfies $d \leq n-k+1$. The *Singleton defect* of an $(n,k,d)_q$ code is $S(C) = n-k+1-d$. An $(n,k,d)_q$ code C with $S(C) = 0$ is called a maximum distance separable (MDS) code [24]. The dual code of an MDS code is MDS. Codes of singleton defect 1 are called Almost-MDS (AMDS) codes [10]. In the case of MDS and AMDS codes, d is determined by n and k, so avoiding redundancy we shall refer to $(n,k)_q$-MDS or $(n,k)_q$-AMDS codes.
Let C be an $(n,k,d)_q$-code. A code C' obtained by deleting some fixed coordinate from each codeword of C is called a *punctured code* of C. An $(n+1,k,d+1)_q$-code C' is said to be an *extension* of C if C is a punctured code of C'. Equivalently, C is said to be *extendable* (to the code C'). A code is *maximal* if it admits no extensions.
A fundamental problem in coding theory is that of determining the maximum length of a code with k, q, and $S(C)$ fixed. A related problem is that of determining conditions under which a given code is maximal. Restricting discussions to AMDS codes, the majority of literature concerns projective codes admitting no projective extensions; that is complete (n,k)-arcs in $PG(k-1,q)$ (see for example [18,22]). All known general constructions of large complete cubic arcs fall far short of the theoretical bounds. This begs the question:

Question 1: Given a projective AMDS code C corresponding to a complete (n,k)-arc in $PG(k-1,q)$, can C be extended?

Given a linear $(n,k)_q$-AMDS code with generator G, a linear extension arises by augmenting G with an appropriate column vector. Hence, in searching for a linear extension a naive exhaustive search would include q^k possible column vectors. However; if one considers nonlinear extensions the problem grows exponentially as there are q^{q^k} possible ways of lengthening the codewords. We are able to show that linear AMDS codes of reasonable length admit only linear (in fact projective) extensions. Thus, on the one hand we are able to prove the maximality of many known linear AMDS codes and on the other we sharply limit the possibilities for constructing long nonlinear AMDS codes. Incidentally, along the way we are able to show that certain short linear AMDS codes are also maximal. Central to our approach is the Bruen-Silverman (BRS) model of linear codes first introduced in [2]. We describe this model in Section 4.

2 Long Linear Codes

Linear $(n,k)_q$-MDS codes and n-arcs in $PG(k-1,q)$ are equivalent objects. A *normal rational curve* (NRC) in $PG(k,q)$, $2 \leq k \leq q-2$ is a $(q+1)$-arc projectively equivalent to the $(q+1)$-arc $\{(1,t,\ldots,t^k)\,|\,t \in GF(q)\} \cup \{(0,\ldots,0,1)\}$. In the plane an NRC is called a conic. A conic in $PG(2,q)$ is a complete arc if q is odd and can be (uniquely) extended to a $(q+2)$-arc (a hyperoval) if q is even. The n-arcs which are proper subsets of normal rational curves correspond to *generalized Reed-Solomon* (GRS) codes. Linear $(q+1,k)_q$-MDS codes are therefore easily constructed. In most cases normal rational curves provide linear $(q+1,k)_q$-MDS codes that do not admit any linear extensions. Recently [1] it has been shown that these codes are in fact maximal. Therefore, in most cases NRC's furnish examples of maximal MDS codes and these are the best possible in the sense that no longer linear MDS code exists.

The situation for AMDS codes is quite different from that of MDS codes. First, the dual of an AMDS code need not be AMDS. A linear AMDS code C is near-MDS (NMDS) if the dual $C^{\perp}$ of C is also AMDS [10]. Consequently, for $k \geq 3$, a linear $(n,k)_q$-AMDS code C is NMDS if and only if C is projective.

Hence, a projective system $\mathscr{G}$ associated with an $(n,k)_q$-NMDS code is an (n,k)-arc in $PG(k-1,q)$. Adopting the notation of [17] we denote by $m'(k,q)$ the maximum possible length for which an $(n,k)_q$-NMDS code exists. Determining $m'(k,q)$ seems to be a hard problem. The best lower bounds on $m'(k,q)$ arise from algebraic geometry via elliptic curves.

The rational points of an elliptic plane curve compose a cubic arc. By $\mathscr{N}_q(1)$ we denote the maximum number of rational points on an elliptic curve over $GF(q)$. It follows that

$$\mathscr{N}_q(1) \leq m'(3,q)$$

and if $q = p^h$ from the work of Waterhouse ([32]) we have

$$\mathscr{N}_q(1) = \begin{cases} q + \lfloor 2\sqrt{q} \rfloor & \text{if } p \,\big|\, \lfloor 2\sqrt{q} \rfloor \text{ and } h \geq 3 \text{ is odd,} \\ q + \lfloor 2\sqrt{q} \rfloor + 1 & \text{otherwise.} \end{cases} \tag{1}$$

Regarding the completeness of the cubic arcs arising from elliptic curves, Hirschfeld and Voloch [22] show the following.

Theorem 1 *If $q \geq 79$ is not a power of 2 or 3, then an elliptic curve Γ with n rational points is a complete cubic arc unless the j-invariant $j(\Gamma) = 0$, in which case the completion of Γ has at most $n+3$ points.*

From Theorem 1 it follows that the rational points of suitable cubic curves give rise to projective $(n,3)_q$-AMDS codes that admit no projective extensions. For general upper bounds on $m'(k,q)$ we have the following.

Theorem 2 *Let k be a positive integer.*

(a) $m'(2,q) = 2q+2$
(b) $m'(k,q) \leq 2q+k$
(c) $m'(k,q) \leq 2q+k-2$*, for* $k,q \geq 3$

Proof See [17] Theorem 2.7. □

From our results it follows that a linear AMDS code meeting any of the bounds in Theorem 2 is maximal (see Corollary 7). Bounds on $m'(3,q)$ for small values of q (as found in [5]) appear in Table 1. Equality holds where only a single number appears. Unlike the case of MDS codes it appears that the best (i.e. longest) linear AMDS codes do not correspond to the points of rational curves. We show (Corollary 6) that the codes corresponding to the cubic arcs in Table 1 are indeed maximal.

Table 1 Values of $m'(3,q)$ for small q.

q	4	5	7	8	9	11	13	16	17	19
m'	9	11	15	15	17	21	23	28..33	28..35	31..39
ref	[23]	[23]	[11]	[8]	[7]	[21],[25]	[3],[26]	[12],[6]	[12],[6]	[12],[6]

3 Coprimitive Sets and Transversal Sets

Let $\Pi = PG(k,q)$ and consider Π as embedded in $\Sigma = PG(k+1,q)$ where $E = \Sigma \setminus \Pi$ is the associated affine space. For any set S of (affine) points in E the *Redéi set* of S with respect to Π, denoted by $\mathscr{R}_\Pi(S)$, is defined to be the set of all points of the form $PQ \cap \Pi$, where P and Q are distinct points of S and PQ denotes the line joining them.

Definition 1 Let A be a nonempty subset of $\Pi = PG(k,q) \subset \Sigma = PG(k+1,q)$. A *partial transversal* of A is a collection S of affine points such that $\mathscr{R}_\Pi(S) \subseteq \Pi \setminus \{A\}$. If $|S| = q^k$ then S is a *transversal* of A. A is *k-coprimitive* (or *coprimitive* if k is understood) if every transversal of A necessarily composes an (affine) hyperplane in $\Sigma \setminus \Pi$.

Remark 1 In the definition, A is coprimitive if and only if the set $B = \Pi \setminus A$ is *primitive* as defined in [1].

If T is a transversal of the set A, then T is a transversal of every nonempty subset of A. This observation gives the following.

Lemma 1 *Let* $A \subset B$ *be sets of points in* $\Pi = PG(k,q)$*. If* A *is coprimitive then so is* B*.*

For a moment let us restrict discussions to the plane $\pi = PG(2,q)$. Fix coordinates and consider a collection A of q affine points. The points of A can be identified with ordered pairs over $GF(q)$. The non-vertical lines then have equations of the form $y = mx + b$, where m is the slope (direction) of the line in question. Vertical lines determine the direction denoted ∞. The set of directions determined by A, when identified with points of ℓ_∞ is precisely $\mathscr{R}_{\ell_\infty}(A)$. We remark that any set of q affine points that does not determine all $(q+1)$ directions is affinely equivalent to the graph of a function. Building on the results of Rédei [27], Blokhuis, Ball, Brouwer, Storme, and Szonyi [9] proved a theorem on the number of directions determined by q points in $AG(2,q)$ which was subsequently improved by Ball [4] to the following.

Theorem 3 *Let f be a function from $GF(q)$ to $GF(q)$, $q = p^h$ for some prime p, and let N be the number of directions determined by f. Let s be maximal such that any line with a direction determined by f that is incident with a point of the graph of f is incident with a multiple of s points of the graph of f. One of the following holds:*

1. *$s = 1$, and $\frac{q+3}{2} \leq N \leq q+1$;*
2. *$GF(s)$ is a subfield of $GF(q)$ and $\frac{q}{s} + 1 \leq N \leq \frac{q-1}{s-1}$;*
3. *$s = q$ and $N = 1$.*

Moreover, if $s > 2$ then the graph of f is $GF(s)-$linear.

Corollary 1 *Let $\ell = PG(1,q) \subset \Pi = PG(2,q)$ where $q = p^h$, p prime, and let $t < h$ be maximal such that t divides h. Let A be a set of points in ℓ. If $|A| > \varepsilon^*$ where*

$$\varepsilon^* = \begin{cases} \frac{q-1}{2} & q \textit{ is prime} \\ q - p^{h-t} & \textit{otherwise.} \end{cases} \tag{2}$$

then A is coprimitive.

Definition 2 Let $\mathscr{G}$ be a projective system of hyperplanes associated with an $(n,k,d)_q$-code C and denote by A the set of all $(n-d)$-fold points of $\mathscr{G}$. An element $\lambda \in \mathscr{G}$ is said to be *primitive* if $\lambda \cap A$ is a $(k-2)$-coprimitive set.

Theorem 4 *Let $\mathscr{K}$ be a dual (n,k)-arc in $\Pi = PG(k,q)$, $k \geq 2$ and let A be the set of k-fold points of $\mathscr{K}$. If $\mathscr{K}$ contains two primitive members λ_1, λ_2 with $\lambda_1 \cap \lambda_2 \cap A \neq \emptyset$ and $A \cap \lambda_1 \neq A \cap \lambda_2$ then A is k-coprimitive.*

Proof Let $\Sigma = PG(k+1,q)$ and let $T \subset \Sigma \setminus \Pi$ be a transversal of A. Let $\sigma = \lambda_1 \cap \lambda_2$, let $A_i = A \cap \lambda_i$, $i = 1,2$ and choose $P \in A_1 \cap A_2$. Consider the collection $H_1, H_2, \ldots, H_q$ of hyperplanes of Σ other than Π containing λ_1 and let $T_i = H_i \cap T$ $i = 1,2\ldots,q$. As T is a transversal of A each T_i is a partial transversal (and therefore a transversal) of A_1. As λ_1 is primitive, each T_i is a subset of a $(k-1)$-flat say τ_i. By assumption there exists a point $P \in A \setminus A_1$ from which it follows that $\tau_1, \tau_2, \ldots, \tau_q$ is a q-pencil of $(k-1)$-flats intersecting λ_1 in say $\sigma_1 = PG(k-2,q)$ (else some line through P intersects T in at least two points).
By way of contradiction suppose $Q \in T_3$ and $Q \notin \Pi_{12} = \langle \tau_1, \tau_2 \rangle$. Let $\Pi' = \langle Q, \lambda_2 \rangle$ and let $T' = T \cap \Pi'$. By assumption λ_2 is primitive whence T' is contained in a $(k-1)$-flat, say τ'. Let $\tau' \cap \lambda_2 = \sigma_2$. Note that $\sigma_2 \neq \sigma_1$ since $P \in \sigma$. Let $\gamma_i = \tau_i \cap \Pi'$, $i = 1,2,\ldots,q$. Then $\Pi_{12} \cap \Pi' = \langle \gamma_1, \gamma_2 \rangle = \tau'$ which gives $Q \in \Pi_{12}$ (a contradiction). Therefore, T is a subset of Π_{12} and A is coprimitive. □

Lemma 2 *Let $\mathscr{K}$ be $(n,3)$-arc of lines in $\pi = PG(2,q)$ where $q = p^h$, p prime, and let $t < h$ be maximal such that t divides h. If $n > \beta$ where*

$$\beta = \begin{cases} \frac{3}{2}(q+1) & \textit{if } q \textit{ is prime, and} \\ 2q - p^{h-t} + 2 & \textit{otherwise,} \end{cases}$$

then the set A of 3-fold points of $\mathscr{K}$ is a coprimitive set.

Proof Let $\mathscr{K}$ be an $(n,3)_q$-arc of lines meeting the conditions. Let $\lambda \in \mathscr{K}$ and denote by A the set of 3-fold points of $\mathscr{K}$ on λ. Each point of λ is incident with at most two further members of $\mathscr{K}$ hence

$$|A| > \begin{cases} \frac{q-1}{2} & \text{if } q \text{ is prime.} \\ q - p^{h-t} & \text{otherwise,} \end{cases}$$

As λ is arbitrary, Corollary 1 and Theorem 4 give the result. □

Theorem 5 *Let $\mathscr{K}$ be (n,k)-arc of hyperplanes in $\Pi = PG(k-1,q)$ where $q = p^h$, p prime, and let $t < h$ be maximal such that t divides h. If $n > \beta$ where*

$$\beta = \begin{cases} \frac{3}{2}(q+1) + k - 3 & q \textit{ odd prime,} \\ 2q - p^{h-t} + k - 1 & \textit{otherwise,} \end{cases}$$

then the set A of k-fold points of $\mathscr{K}$ is a coprimitive set.

Proof The result holds for $k = 3$. Proceeding by induction let $\mathscr{K}$ be an $(n,k+1)$-arc of hyperplanes in $\Pi = PG(k,q) \subset \Sigma = PG(k+1,q)$. Let $P \in A$ be incident with $\lambda_1, \lambda_2 \in \mathscr{K}$. By the respective intersections, the remaining members of $\mathscr{K}$ cut out a dual $(n-1,k)$-arc $\mathscr{K}'$ in $\lambda_1 = PG(k-1,q)$. By the induction hypothesis $A \cap \lambda_1$ is a $(k-2)$-coprimitive set. Similarly $\lambda_2 \cap A$ is $(k-2)$-coprimitive. It follows (Theorem 4) that A is coprimitive. □

4 The BRS Model of Linear Codes

Let C be an $(n,k,d)_q$ code. A *positional permutation* of C is a permutation (on n letters) of the coordinates. A *symbol permutation* of C is a permutation (on q letters) of the alphabet $\mathscr{A}$ applied to a fixed coordinate. Any code obtained from C by symbol and positional permutations is called *equivalent* to C. Equivalent codes are essentially identical, they have the same parameters n,k,d and q and the same set of distances between codewords. A code that is equivalent to a linear code is said to be *equivalent to linear*. A code that is equivalent to linear need not be linear. For example, if we suitably permute the symbols in a given column of a linear code, the resulting code will not contain the zero vector.

In [13] Bruen and Silverman introduce a construction of MDS codes using dual arcs in projective spaces. In [2,1] the construction was generalized to linear codes. Briefly, let C be a linear $(n,k,d)_q$ code with generator G and corresponding projective system of hyperplanes $\mathscr{G} = \pi_1, \pi_2, \ldots, \pi_n$ in $\Pi = PG(k-1,q)$. We construct a $(n,k,d)_q$-Bruen-Silverman (BRS) code associated with $\mathscr{G}$ as follows: Consider Π as embedded in $\Sigma = PG(k,q)$ where $\Sigma^* = \Sigma \setminus \Pi$ is the associated affine space. For each i, $1 \leq i \leq n$ denote by $\Pi_{i1}, \Pi_{i2}, \ldots, \Pi_{iq}$ the hyperplanes other than Π containing π_i. For each i, j, associate with Π_{ij} the label $L(\Pi_{ij}) = j$. To each point $P \in \Sigma^*$ associate the $n-tuple$ $\Phi(P)$ defined by

$$\Phi(P) = \Big(L(P \vee \pi_1), L(P \vee \pi_2), \dots, L(P \vee \pi_n)\Big)$$

Theorem 6 *The code $C' = \{\Phi(P) | P \in \Sigma^*\}$ is an $(n,k,d)_q$-code equivalent to C.*

Proof See [1]. □

The code C' is called a *BRS model of C* (based on $\mathscr{G}$). Under this model a positional permutation on C' is simply a re-ordering of the members of $\mathscr{G}$. A symbol permutation of C' corresponds to a re-ordering of the hyperplanes incident with a particular member of $\mathscr{G}$. As such, the following is immediate.

Theorem 7 *A code C is (equivalent to) a linear $(n,k,d)_q$-code with generator matrix G if and only if C can be modeled as a BRS code based on the corresponding projective system of hyperplanes, $\mathscr{G}$.*

5 Extending AMDS Codes

The BRS model of linear codes gives a new geometric view of code extension. Indeed, let C be a linear $(n,k,d)_q$-code with a corresponding BRS model based on the projective system of hyperplanes $\mathscr{G} = \{\Lambda_1, \Lambda_2, \dots, \Lambda_n\}$ in $\Pi = PG(k-1,q) \subset \Sigma = PG(k,q)$. Let A denote the collection of $(n-d)$-fold points of $\mathscr{K}$. An extension of C then corresponds to a partition $\mathscr{P} = S_1, S_2, \dots, S_q$ of $\Sigma^* = \Sigma \setminus \Pi$ into transversals of A. From Theorem 7 it follows that such an extension is (equivalent to) linear if and only if the partition $\mathscr{P}$ is precisely a parallel class of affine hyperplanes. Thus, we have the following.

Theorem 8 *Let C be a linear $(n,k)_q$-AMDS code with associated projective system $\mathscr{G}$. Let A be the set of k-fold points of $\mathscr{G}$. If A is coprimitive then any extension of C is (equivalent to) linear.*

Corollary 2 *Let C be a linear $(n,k)_q$-AMDS code with $\mathscr{G}$ an associated projective system of hyperplanes in $PG(k-1,q)$. Let A be the set of k-fold points of $\mathscr{G}$. If $\lambda_1 \neq \lambda_2$ are primitive members of G with $\lambda_1 \cap \lambda_2 \cap A \neq \emptyset$ and $A \cap \lambda_1 \neq A \cap \lambda_2$ then every extension of C is (equivalent to) linear.*

Proof This follows immediately from Theorems 4 and 8. □

One approach to constructing cubic arcs in the plane is to begin with a conic and then to add points in such a way that a complete cubic arc is created. This method does not generally give rise to very large cubic arcs, but the following Corollary demonstrates that in many cases the corresponding codes are maximal.

Corollary 3 *Let $\mathscr{C}$ be a cubic arc in $PG(2,p)$, p an odd prime. If $\mathscr{C}$ contains a conic $\mathscr{K}$ and some 3-fold line of $\mathscr{C}$ is not a secant line of $\mathscr{K}$ then the NMDS code C corresponding to $\mathscr{C}$ admits only NMDS extensions. Consequently, if $\mathscr{C}$ is complete then C is maximal.*

Proof We argue dually. Denote by A the 3-fold points of $\mathscr{C}$. $\mathscr{C}$ is complete and contains a dual conic, $\mathscr{K}$. Simple counting gives $|\mathscr{C}| > p+2$ so that in particular, each member of $\mathscr{C}$ is incident with at least one 3-fold point. It follows that all linear extensions of C are projective. It therefore suffices to show that C admits only linear extensions.

By assumption there exists a 3-fold point of $\mathscr{C}$ and lines $l_1, l_2 \in \mathscr{C} \setminus \mathscr{K}$ incident at P. Let $A_i = A \cap l_i$, $i = 1,2$. Any line external to $\mathscr{K}$ is incident with either 0 or 2 tangent points of $\mathscr{K}$ (see [20] Lemma 8.10). As such $|A_1|, |A_2| \geq \frac{p-1}{2}$ from which it follows (Corollary 1) that l_1 and l_2 are primitive members of $\mathscr{C}$. By Theorem 8 all extensions of C are (equivalent to) linear. □

The following example demonstrates that the conditions in Corollary 2 are somewhat strong.

Example 1 Let $\mathscr{K} = \{l_1, l_2, \ldots, l_{q+1}\}$ be a dual $(q+1)$-arc (a conic) in $\pi = PG(2,p)$, p an odd prime. Let P be the unique tangent point on l_1 and let $\ell, \ell' \notin \mathscr{K}$ be two lines through P. Then the dual cubic arc $\mathscr{C} = \mathscr{K} \cup \{\ell, \ell'\}$ is a projective system corresponding to a projective $(p+3,3)_p$-AMDS code C admitting only projective extensions. However, the punctured code C' having projective system $\mathscr{C}' = \mathscr{C} \cup \ell$ does admit an extension that is not equivalent to linear.
Indeed, consider the BRS model of C' and let A be the 3-fold points of $\mathscr{C}'$ (note that $A \subset \ell$). Denote by $\pi_1, \pi_2, \ldots, \pi_p$ the planes other than π through ℓ'. Consider all affine points of π_{p-1} to be "painted" black, and all those in π_p to be painted white. Pick a black line u with projective point P and let v be the (white) affine line in $(l_1 \vee v)$. Reverse the colours of u and v and let $\mathscr{B}$ be the collection of black points and $\mathscr{W}$ the collection of white points. It is a simple matter to verify that $\mathscr{B}$ and $\mathscr{W}$ are transversals of A. Hence, the partition $\pi_1, \pi_2, \ldots, \pi_{p-1}, \mathscr{B}, \mathscr{W}$ of $PG(3,p) \setminus \pi$ gives rise to an extension of C'. As neither $\mathscr{B}$ nor $\mathscr{W}$ are affine planes this extension is not equivalent to linear (from the BRS model).

5.1 Short Maximal Codes

Theorem 9 *If $n > q+k$ then a linear $(n,k)_q$-AMDS code is NMDS.*

Proof See [16]. □

By the theorem above, if C is a linear $(n,k)_q$-AMDS code that is non-NMDS then n is bounded above by $q+k$. We now show that any such code meeting this bound is maximal.

Lemma 3 *Let C be a linear $(q+3,3)_q$-AMDS code that is not NMDS. Then C is maximal.*

Proof Let $\mathscr{G}$ be the projective system of lines in $PG(2,q)$ associated with C. It follows that $\mathscr{G}$ holds a repeated line comprising $q+1$ 3-fold points. As such, the set A of 3-fold points of $\mathscr{G}$ possesses no transversals and C is maximal. □

Theorem 10 *Let C be a linear $(q+k,k)_q$-AMDS code $k \geq 3$. If C is not NMDS then C is maximal.*

Proof By the previous Theorem the result holds for $k = 3$, we proceed by induction on k. Let C be a non-NMDS linear $(q+k+1,k+1)_q$-AMDS code with associated projective system of hyperplanes $\mathscr{G} = \lambda_1,\lambda_2,\dots\lambda_{q+k+1}$ where $\lambda_1 = \lambda_2$. Let C' be the linear code with projective system $\mathscr{G}' = \lambda_1',\lambda_2',\dots,\lambda_{q+k}'$ where $\lambda_i' = \lambda_i \cap \lambda_{q+k+1}$. C' is a linear non-NMDS $(q+k,k)_q$-AMDS code and is therefore (induction hypothesis) maximal. Clearly, any extension of C gives rise to an extension of C' whence C is maximal. □

In $PG(2,q)$, q even take a hyperoval $\mathscr{K} = l_1,l_2,\dots,l_{q+2}$. The multiset $\mathscr{G} = l_1,l_1,l_2,\dots,l_{q+2}$ is a projective system corresponding to a $(q+3,3)_q$-AMDS code which is not NMDS. In this sense the bound in Theorem 9 is best possible. However, for codes of dimension greater than three the bound can be improved in most cases (see Theorem 12 below). We first review some intermediary results on arcs.

Denote by $m(k,q)$ the size of the largest arc in $PG(k,q)$. Using combinatorial arguments Silverman [29] showed the following.

$$m(k,q) \leq \begin{cases} q+k & q \text{ even} \\ q+k-1 & q \text{ odd.} \end{cases} \tag{3}$$

Finding the value of $m(k,q)$ has been the focus of much research (see [14,15, 31,28]). The *Main Conjecture* for linear MDS codes, always taking $q > k+1$, is the following:

$$m(k,q) = \begin{cases} q+2 & \text{if } k=2 \text{ and } k=q-2 \text{ both with } q \text{ even} \\ q+1 & \text{in all other cases} \end{cases}$$

The Main Conjecture has not been proved in general but it has been verified in most cases. In the survey [19] of results relating to the Main Conjecture the following appears.

Theorem 11 *The Main Conjecture for Linear MDS Codes holds if*

(i) $2 \leq k \leq 4$ *or*

(ii) $k \geq 5$ *and* $q > \begin{cases} \left(2k-\frac{11}{2}\right)^2 & \textit{and } q \textit{ is even} \\ \left(4k-\frac{39}{4}\right)^2 & \textit{and } q \textit{ is odd} \\ 5(9k-28) & \textit{and } q \textit{ is prime} \end{cases}$

Lemma 4 *Let C be a linear $(n,k)_q$-AMDS code $k \geq 3$ with associated projective system of hyperplanes $\mathscr{G}$. Then no member of G has multiplicity $m > 2$ and at most one member has multiplicity 2.*

Proof Consider the BRS model of C where $\mathscr{G} = \pi_1,\pi_2,\dots,\pi_n \subset \Pi = PG(k-1,q) \subset \Sigma = PG(k,q)$. Suppose π_1 has multiplicity $t > 1$. By the respective intersections with π_1, the remaining members of $\mathscr{G}$ distinct from π_1 cut out a projective system of hyperplanes corresponding to an $(n-t,k-1,n-k)_q$-code. From the Singleton bound it follows that $t \leq 2$. For the second part, suppose $\pi_i \neq \pi_j$ both have multiplicity 2. Let $\lambda = \pi_i \cap \pi_j$. By the respective intersections with $\lambda = PG(k-3,q)$, the remaining members of $\mathscr{G}$ compose a projective system corresponding to an $(n-4,k-2,n-k)_q$-code. The Singleton bound then gives the contradiction $n-k \leq n-k-1$. □

Theorem 12 *A linear $(n,k)_q$-AMDS with $n > m(k-2,q)+2$ is NMDS.*

Proof Let C be a linear $(n,k)_q$-AMDS code with associated projective system of hyperplanes $\mathscr{G} = \lambda_1, \lambda_2, \ldots, \lambda_n$ in $PG(k-1,q)$. As C is not NMDS we may assume $\lambda_1 = \lambda_2$. By the previous lemma $\lambda_3, \lambda_4, \ldots, \lambda_n$ are distinct and therefore cut out (via the respective intersections with λ_1) a dual $(n-2)$-arc in λ_1 giving $n-2 \leq m(k-2,q)$. □

Teaming Theorem 11 with the above we get the following corollary.

Corollary 4 *If the conditions of the Main Conjecture are satisfied in $PG(k-2,q)$, then a linear $(n,k)_q$-AMDS code with*

$$n > \begin{cases} q+4 & \text{if } k=4 \text{ or } k=q, \text{ both with } q \text{ even} \\ q+3 & \text{otherwise,} \end{cases}$$

is NMDS.

Remark 2 For $k > 2$ let $\mathscr{K} = \{\pi_1, \pi_2, \ldots, \pi_{q+1}\}$ be a dual $(q+1)$-arc in $\Pi = PG(k-1,q)$. By the respective intersections the π_i's $i = 1,2,\ldots,l_q$ give a dual q-arc $\mathscr{K}'$ in $\pi_{q+1} = PG(k-2,q)$. Classical results show that for q suitably large, $\mathscr{K}'$ is not complete (see [30, 14]). Let λ be a hyperplane of Π_{q+1} where $\lambda \cup \mathscr{K}'$ is a dual $(q+1)-arc$. Let π be any $(k-2)$-flat other than π_{q+1} through λ. Then the multiset $\mathscr{G} = \pi_1, \pi_2, \ldots, \pi_{q+1}, \pi_{q+1}, \pi$ corresponds to a linear $(q+3,k)_q$-AMDS code which is not NMDS. In this sense the bound in the corollary above is sharp.

5.2 Long Maximal Codes

Theorem 13 *Let C be a linear $(n,k)_q$-AMDS code where $q = p^h$, p prime, and let $t < h$ be maximal such that t divides h. If $n > \beta$, where*

$$\beta = \begin{cases} \frac{3}{2}(q-1)+k & \text{if } q \text{ is prime, and} \\ 2q - p^{h-t} + k - 1 & \text{otherwise,} \end{cases} \tag{4}$$

then any arbitrary $(n+1,3,q)$-AMDS code C' extending C is (equivalent to) linear.

Proof By Theorem 9, C is NMDS so the associated projective system of hyperplanes $\mathscr{G}$ is a dual (n,k)-arc in $PG(k-1,q)$. Let A be the set of k-fold points of $\mathscr{G}$. By Theorem 5, A is coprimitive. Theorem 8 then gives the result. □

Corollary 5 *Let $\mathscr{C}$ be a complete (n,k)-arc in $PG(k-1,q)$ where $q = p^h$, p prime, and let $t < h$ be maximal such that t divides h. If $n > \beta$, where β is given by (4), then the projective $(n,k)_q$-AMDS code C corresponding to $\mathscr{C}$ is maximal.*

Proof All extensions of C are linear (Theorem 13) and in fact projective (Theorem 9). By the completeness of $\mathscr{C}$, C admits no projective extensions. □

Corollary 6 *The linear* $(9,3)_4$, $(11,3)_5$, $(15,3)_7$, $(15,3)_8$, $(17,3)_9$, $(21,3)_{11}$, *and* $(23,3)_{13}$ *NMDS codes corresponding to the entries in Table 1 are maximal.*

Corollary 7 *All linear $(2q+k,k)_q$-AMDS codes are maximal and for $k,q \geq 3$ all linear $(2q+k-2,k)_q$-AMDS codes are maximal.*

References

1. Alderson, T., Bruen, A.A., Silverman, R.: Maximum distance separable codes and arcs in projective spaces. J. Combin. Theory Ser. A **114**(6), 1101–1117 (2007)
2. Alderson, T.L.: On MDS codes and Bruen-Silverman codes. PhD. Thesis, University of Western Ontario (2002)
3. Ball, S.: Multiple blocking sets and arcs in finite planes. J. London Math. Soc. (2) **54**(3), 581–593 (1996)
4. Ball, S.: The number of directions determined by a function over a finite field. J. Combin. Theory Ser. A **104**(2), 341–350 (2003)
5. Ball, S., Hirschfeld, J.W.P.: Bounds on (n,r)-arcs and their application to linear codes. Finite Fields Appl. **11**(3), 326–336 (2005)
6. Barlotti, A.: Sui $\{k;n\}$-archi di un piano lineare finito. Boll. Un. Mat. Ital. (3) **11**, 553–556 (1956)
7. Barnabei, M., Searby, D., Zucchini, C.: On small $\{k;q\}$-arcs in planes of order q^2. J. Combinatorial Theory Ser. A **24**(2), 241–246 (1978)
8. Bierbrauer, J.: The maximal size of a 3-arc in $\mathrm{PG}(2,8)$. J. Combin. Math. Combin. Comput. **45**, 145–161 (2003)
9. Blokhuis, A., Ball, S., Brouwer, A.E., Storme, L., Szőnyi, T.: On the number of slopes of the graph of a function defined on a finite field. J. Combin. Theory Ser. A **86**(1), 187–196 (1999)
10. de Boer, M.A.: Almost MDS codes. Des. Codes Cryptogr. **9**(2), 143–155 (1996)
11. Bramwell, D.: PhD. Thesis, University of London (1973)
12. Braun, M., Kohnert, A., Wassermann, A.: Construction of (n,r)-arcs in $\mathrm{PG}(2,q)$. Innov. Incidence Geom. **1**, 133–141 (2005)
13. Bruen, A.A., Silverman, R.: On extendable planes, M.D.S. codes and hyperovals in $\mathrm{PG}(2,q), q=2^t$. Geom. Dedicata **28**(1), 31–43 (1988)
14. Bruen, A.A., Thas, J.A., Blokhuis, A.: On M.D.S. codes, arcs in $\mathrm{PG}(n,q)$ with q even, and a solution of three fundamental problems of B. Segre. Invent. Math. **92**(3), 441–459 (1988)
15. Casse, L.R.A.: A solution to Beniamino Segre's "Problem $I_{r,q}$" for q even. Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **46**, 13–20 (1969)
16. Dodunekov, S., Landgev, I.: On near MDS codes. J. Geom. **54**(1-2), 30–43 (1995)
17. Dodunekov, S.M., Landjev, I.N.: Near-MDS codes over some small fields. Discrete Math. **213**(1-3), 55–65 (2000). Selected topics in discrete mathematics (Warsaw, 1996)
18. Giulietti, M.: On the extendibility of near-MDS elliptic codes. Appl. Algebra Engrg. Comm. Comput. **15**(1), 1–11 (2004)
19. Hirschfeld, J.W.P.: Complete arcs. Discrete Math. **174**(1-3), 177–184 (1997). Combinatorics (Rome and Montesilvano, 1994)
20. Hirschfeld, J.W.P.: Projective geometries over finite fields, second edn. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York (1998)
21. Hirschfeld, J.W.P., Sadeh, A.R.: The projective plane over the field of eleven elements. Mitt. Math. Sem. Giessen (164), 245–257 (1984)
22. Hirschfeld, J.W.P., Voloch, J.F.: The characterization of elliptic curves over finite fields. J. Austral. Math. Soc. Ser. A **45**(2), 275–286 (1988)
23. Lunelli, L., Sce, M.: Considerazioni arithmetiche e risultati sperimentali sui $\{K;n\}_q$-archi. Ist. Lombardo Accad. Sci. Lett. Rend. A **98**, 3–52 (1964)
24. MacWilliams, F.J., Sloane, N.J.A.: The theory of error-correcting codes. II. North-Holland Publishing Co., Amsterdam (1977). North-Holland Mathematical Library, Vol. 16
25. Marcugini, S., Milani, A., Pambianco, F.: Maximal $(n,3)$-arcs in $\mathrm{PG}(2,11)$. Discrete Math. **208/209**, 421–426 (1999). Combinatorics (Assisi, 1996)
26. Marcugini, S., Milani, A., Pambianco, F.: Maximal $(n,3)$-arcs in $\mathrm{PG}(2,13)$. Discrete Math. **294**(1-2), 139–145 (2005)
27. Rédei, L.: Lacunary polynomials over finite fields. North-Holland Publishing Co., Amsterdam (1973). Translated from the German by I. Földes
28. Segre, B.: Curve razionali normali e k-archi negli spazi finiti. Ann. Mat. Pura Appl. (4) **39**, 357–379 (1955)
29. Silverman, R.: A metrization for power-sets with applications to combinatorial analysis. Canad. J. Math. **12**, 158–176 (1960)
30. Thas, J.A.: Normal rational curves and k-arcs in Galois spaces. Rend. Mat. (6) **1**, 331–334 (1968)

31. Thas, J.A.: Finite geometries, varieties and codes. In: Proceedings of the International Congress of Mathematicians, Vol. III (Berlin, 1998), Extra Vol. III, pp. 397–408 (electronic) (1998)

32. Waterhouse, W.C.: Abelian varieties over finite fields. Ann. Sci. École Norm. Sup. (4) **2**, 521–560 (1969)