Designs Codes & Cryptography manuscript No.
(will be inserted by the editor)

On the Maximality of Linear Codes

T. L. Alderson · András Gács

Received: date / Accepted: date

Abstract We show that if a linear code admits an extension, then it necessarily admits a linear extension. There are many linear codes that are known to admit no linear extensions. Our result implies that these codes are in fact maximal. We are able to characterize maximal linear $(n, k, d)_q$-codes as complete (weighted) $(n, n-d)$-arcs in $PG(k-1, q)$. At the same time our results sharply limit the possibilities for constructing long nonlinear codes. The central ideas to our approach are the Bruen-Silverman model of linear codes, and some well known results on the theory of directions determined by affine point-sets in $PG(k, q)$.

Keywords codes · non-linear codes · code extension · BRS model

Mathematics Subject Classification (2000) 94B27 · 51E20 · 94B65

The first author acknowledges support from the N.S.E.R.C. of Canada

The second author was supported by Bolyai grant and OTKA grants T 049662 and T 067867.

T. L. Alderson
Dept. of Mathematical Sciences
University of New Brunswick Saint John
Saint John, NB.
E2L 4L5
Canada
Tel.: +1-506-648-5622
Fax: +1-506-648-5513
E-mail: tim@unbsj.ca

András Gács
Department of Computer Science
Eötvös Loránd University
H-1117 Budapest
Pázmány Péter sétány 1/C,
HUNGARY
Tel.: +36-1-3722700/8604
Fax: +36-1-381-2156
E-mail: gacs@cs.elte.hu

1 Introduction

For $n \geq k$, an $(n,k,d)_q$-*code* C is a collection of q^k n-tuples (often called *words* or *codewords*) over an alphabet $\mathcal{A}$ of size q such that the minimum (Hamming) distance between any two codewords of C is d. That is to say, there exist two codewords agreeing in $n-d$ coordinates and no two codewords agree in as many as $n-d+1$ coordinates. In particular, any $n-d+1$ coordinates form an information set. In general, q need not be a prime power. In the special case that $\mathcal{A} = GF(q)$ and C is a vector space of dimension k over $GF(q)$, C is a *linear* $(n,k,d)_q$-code. In this case, the minimum distance property translates to the property that each nonzero codeword has at least d nonzero coordinates.
For an (n,k,d)-code over an alphabet $\mathcal{A}$ the Singleton bound:

$$|C| \leq |\mathcal{A}|^{n-d+1}$$

gives $d \leq n-k+1$. The *Singleton defect of* C, $S(C)$, is defined by $S(C) = n-k+1-d$. Codes with S(C)=0 are called Maximum Distance Separable (MDS) codes; those with $S(C) = 1$ are called Almost-MDS (AMDS) codes. A code C' obtained by deleting some fixed coordinate from each codeword of C is called a *punctured code* of C. In the case that $S(C') = S(C)$, C is said to be an *extension* 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 algebraic coding theory is that of determining the maximum length n for codes of fixed parameters k, q and singleton defect $S(C)$. This is a difficult open problem even if one restricts to linear MDS codes: the problem was first posed over 50 years ago by B. Segre. We refer to [16] for a survey of results in the MDS case. There are many texts which serve as an introduction to the basics of coding theory, a classic being [22]. For more recent texts we refer to any of [10,13,25,21].

In the present paper we investigate an intimately related problem–that of determining whether or not a given code is maximal. We provide necessary and sufficient condition for a linear $(n,k,d)_q$ code to be maximal, in terms of directions in $AG(k,q)$ (Theorem 2), and in terms of intersection sets in $PG(k-1,q)$ (Corollary 1). The main consequence of these characterizations is the following.

Theorem 1 *If a linear $(n,k,d)_q$ code can be extended to an $(n+1,k,d+1)_q$ code, then it can also be extended to a linear $(n+1,k,d+1)_q$ code.*

One way to construct a nonlinear code C is to begin with a linear code and attempt to extend it in a nonlinear way. In fact, if C is an $(n,k,d)_q$ MDS code then C may always be constructed in this way. Indeed, in any fixed k coordinates, C exhausts all possible k-tuples over the code alphabet. Consequently, if q is a prime power, C is (equivalent to) linear in these k coordinates. There are many linear codes that are known not to admit linear extensions. Theorem 1 shows such codes may not be extended in a nonlinear way; thus sharply limiting the possibilities for constructing nonlinear codes. In recent work it was shown, that linear codes of sufficient length admit only linear extensions (see [2] for the MDS case, [4,6] for the AMDS case, and [5] for the general case). These previous results imply that when a code is long enough and admits no linear extension, then it is maximal. Our result improves upon these previous results by omitting any assumption with regard to length.

The central ideas to our approach are the Bruen-Silverman model of linear codes first introduced in [3], and some well known results on the theory of directions determined by affine point-sets in $PG(k,q)$.

In Sections 2 and 3 we give the proof of our result. In section 4 we summarize some basic facts about the connection between codes and weighted arcs, and between projective codes and arcs, we also detail some of the consequences of our results.

2 Directions

In this section we shortly summarize definitions and results we need about directions.

Let U denote a set of q^{k-1} points in $AG(k,q)$. The *set of determined directions* by U is the set of parallel classes of lines joining pairs of points of U. By adding the hyperplane at infinity, $AG(k,q)$ can be embedded to $PG(k,q)$. After this, one can identify parallel classes of lines with the infinite points. Using coordinates we can take all k-tuples of the form $(X_0, X_1, ..., X_{k-1}, 1)$ for the affine points and all homogeneous k-tuples of the form $(X_0, X_1, ..., X_{k-1}, 0)$ for the infinite points. After this, the infinite point of the line joining $(X_0, X_1, ..., X_{k-1}, 1)$ and $(Y_0, Y_1, ..., Y_{k-1}, 1)$ is simply $(X_0 - Y_0, X_1 - Y_1, ..., X_{k-1} - Y_{k-1}, 0)$.

Sometimes a subset A of the infinite hyperplane of $PG(k,q)$ is fixed and one looks for a set U such that no point of A is determined by U. If this occurs, and $|U| = q^{k-1}$, then U is said to be *a transversal of* A.

There is a large literature about the direction problem, which has its roots in the work of Rédei [24]. For very deep algebraic results as well as the history of the problem, we refer to Ball [7], Blokhuis-Ball-Brouwer-Strome-Szőnyi [11] for the planar case, and Ball [8] for the non-planar case. In the present paper we only need the following lemma which may be found implicitly in Storme-Sziklai [29]. For the sake of completeness we include a proof.

Lemma 1 *Let $\Sigma = PG(k,q)$ where $AG(k,q) = \Sigma \setminus \Pi$ is the associated affine space. Let U be a set of q^{k-1} affine points and let D be the set of directions determined by U.*

(i) If there are at least $q^{l-1}+1$ points of U in an l-dimensional affine subspace, then all infinite points of that subspace are determined.
(ii) There exists at least one hyperplane of Π that is a subset of D.

Proof For (i) take an infinite point of the subspace in question. There are q^{l-1} lines within the subspace through this infinite point (in other words: there are q^{l-1} lines of this parallel class), so by the pigeon-hole principle, at least one line contains at least two points of U. This means that the infinite point in question is determined.

For (ii) suppose every hyperplane of Π contains at least one non-determined point. An arbitrary $(k-1)$-dimensional affine subspace V meets Π in a hyperplane. By the assumption, not all infinite points of V are determined by U. By (i) this implies $|U \cap V| \leq q^{k-2}$. By the next lemma, this is a contradiction.

Let us remark, that in fact more is true: the set D of determined directions is always the union of hyperplanes of Π, see Storme-Sziklai [29].

Lemma 2 *There is no set of $AG(k,q)$ of size q^{k-1} meeting every $(k-1)$-dimensional subspace in at most q^{k-2} points.*

Proof First note that since there are q $(k-1)$-dimensional subspaces in a parallel class, such set would have exactly q^{k-2} points in every $(k-1)$-dimensional subspace. We need to prove that this is impossible.

For $k = 2$ this is easy: q points in an affine plane cannot meet every line in 1 point. We proceed by induction on k. For $k \geq 3$, fix a subspace V of codimension 2 and suppose it contains x points. Counting the number of points in 1 codimensional subspaces through V, we find $x+(q+1)(q^{k-2}-x) = q^{k-1}$, which gives $x = q^{k-3}$. Hence our set meets every codimension 2 subspace in exactly q^{k-3} points. Fix a codimension 1 subspace W and consider the q^{k-2} points of U in W. Reformulating everything within W, we have a set of q^{k-2} points in $AG(k-1,q)$ meeting every $(k-2)$-dimensional subspace in exactly q^{k-3} points, contradicting the induction hypothesis.

3 Proof of Main Result

The next lemma gives a necessary and sufficient condition for the extendability of a code. The proof is straightforward.

Lemma 3 *Suppose C is an $(n,k,d)_q$ code. C is extendable to an $(n+1,k,d+1)_q$ code if and only if C can be partitioned into q subsets in such a way that two codewords from the same subset differ in at least $d+1$ coordinates.*

A linear $(n,k,d)_q$-code C may be described by an associated $k \times n$ generator matrix

$$G = \begin{bmatrix} a_{00} & a_{01} & \cdots & a_{0(n-1)} \\ a_{10} & a_{11} & \cdots & a_{1(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ a_{(k-1)0} & a_{(k-1)1} & \cdots & a_{(k-1)(n-1)} \end{bmatrix}.$$

The rows of G correspond to a basis of C over $GF(q)$. Here we assume that no column of G is the 0-vector (otherwise, the corresponding coordinate would be identically 0 in all codewords and therefore inessential). Multiplying any column of G by a nonzero scalar results in a code equivalent to the original. As such the columns may be considered as a multiset of points in $PG(k-1,q)$. This multiset is called a *projective system* associated with C. Dually, the columns of G may be considered as a multiset of hyperplanes in $PG(k-1,q)$ where the i'th column of G is associated with the hyperplane having equation $a_{0i}X_0 + a_{1i}X_1 + \cdots + a_{(k-1)i}X_{k-1} = 0$. In the sequel we often consider the dual case, and refer to the *projective system of hyperplanes* associated with C. Note that the minimum distance condition translates to the condition that each point of $PG(k-1,q)$ is incident with at most $n-d$ elements of any projective system of hyperplanes associated with C (counting multiplicities).

We shall have need of the Bruen-Silverman (BRS) model of linear codes first introduced in [3], and further developed in [5],[2]. We describe this model briefly. Let C be a linear $(n,k,d)_q$-code. Let $\Sigma = PG(k,q)$ and assign homogeneous coordinates $(X_0, X_1, \ldots, X_k)$. Let Π be the hyperplane (at infinity) with equation $X_k = 0$. Consider an associated generator matrix G and the corresponding projective system $\mathcal{G}$ of hyperplanes in Π. To be more precise, if $G = (a_{ij})$, $0 \leq i \leq k-1$, $0 \leq j \leq n-1$, then $\mathcal{G}$ consists of the following n hyperplanes of Π:

$$H_i = \{(X_0, ..., X_{k-1}, 0) : X_0 a_{0i} + X_1 a_{1i} + \cdots + X_{k-1} a_{(k-1)i} = 0\}, \quad (1)$$
$$i = 0, \ldots, n-1.$$

The elements of C are linear combinations of rows of G. Let $\boldsymbol{\lambda} = (\lambda_0, \lambda_1, \ldots, \lambda_{k-1})$. Under the BRS model the codeword $\boldsymbol{\lambda} \cdot G$ is identified with the affine point $(\lambda_0, \lambda_1, \ldots \lambda_{k-1}, 1)$.

Let $w_1 = \mathbf{x} \cdot G$ and $w_2 = \mathbf{y} \cdot G$ be two codewords corresponding to the affine points $X = (X_0, X_1, \ldots, X_{k-1}, 1)$ and $Y = (Y_0, Y_1, \ldots, Y_{k-1}, 1)$ respectively. It is clear that w_1 and w_2 will agree in the i'th coordinate (i fixed) if and only if $(\mathbf{x} - \mathbf{y}) \cdot G$ has i'th coordinate zero. Equivalently the infinite point $P = (X_0 - Y_0, X_1 - Y_1, ..., X_{k-1} - Y_{k-1}, 0)$ of the line joining X and Y satisfies the equation (1) defining H_i, so $P \in H_i$). It follows that under the BRS model, two codewords corresponding to respective affine points P_1 and P_2, will have precisely t common coordinates if and only if the infinite point P of the line $\langle P_1, P_2 \rangle$ is incident with precisely t members of $\mathcal{G}$ (again, counting with multiplicities). In this case we refer to P as a *t-fold point* of $\mathcal{G}$.

Let A denote the collection of $(n-d)$-fold points of $\mathcal{G}$. Recall from the previous section, that a transversal T of A is a collection of q^{k-1} affine points (in $\Sigma \setminus \Pi$) such that no line through a member of A is incident with as many as two points of T. In other words, A is a subset of the non-determined directions of T.

Regarding the extendability of C we have the following.

Lemma 4 *Let A denote the collection of $(n-d)$-fold points of $\mathcal{G}$. C is extendable if and only if there exists a partition $\mathcal{P} = S_1, S_2, \ldots, S_q$ of the affine points of Σ such that each S_i is a transversal of A.*

Proof From Lemma 3 it follows that C is extendable if and only if such a partition exists where each S_i is a partial transversal of A. From Lemma 1, and the fact that there exists at least one $(n-d)$-fold point of $\mathcal{G}$, we have $|S_i| \leq q^{k-1}$ for each $i = 1, 2, \ldots, q$. The result follows.

We now prove the main result which, in particular, implies Theorem 1.

Theorem 2 *Denote by A the set of $(n-d)$-fold points of $\mathcal{G}$. The following four conditions are equivalent.*

(i) There is a hyperplane of Π disjoint from A;
(ii) C can be extended to a linear $(n+1, k, d+1)_q$ code;
(iii) C can be extended to a not necessarily linear $(n+1, k, d+1)_q$ code;
(iv) A admits a transversal.

Proof Suppose *(i)* is true and let the hyperplane in question be given by the equations $a_0X_0 + \cdots + a_{k-1}X_{k-1} = X_k = 0$. Then it follows that augmenting G with the column $(a_0, ..., a_{k-1})^T$ produces a generator matrix of a linear $(n+1, k, d+1)_q$ code extending C. So *(i)* implies *(ii)*. Clearly, *(ii)* implies *(iii)*, and by Lemma 4 *(iii)* implies *(iv)*. What is left is to show that *(iv)* implies *(i)*. Let $T \subseteq AG(k, q)$ be a transversal of A and let D be the set of directions determined by T. By definition of a transversal, D is disjoint from A. By Lemma 2 *(ii)*, D contains a hyperplane of Π. The result follows.

The above may also be formulated in terms of blocking sets.

Definition 1 A set of points S in $PG(k-1, q)$ is an *intersection set* if each hyperplane contains at least one point of S. Such a set is also called a *1-intersection set* or – in the case S does not contain all of the points of a line – a *blocking set with respect to hyperplanes*.

The proof of the following follows easily from Theorem 2 and the definition of an intersection set.

Corollary 1 *Let C be a linear $(n,k,d)_q$-code with $\mathcal{G}$ a corresponding projective system of hyperplanes in $\Pi = PG(k-1,q)$. Let A be the set of $(n-d)$-fold points of $\mathcal{G}$. A necessary and sufficient condition for C to be maximal is that A is an intersection set in Π.*

Some remarks regarding Corollary 1 are in order: (1) We note that it has been known for a long time that a necessary and sufficient condition for a linear code to admit no *linear* extensions is that A be an intersection set. (2) The projective system $\mathcal{G}$ is a multiset of hyperplanes in Π at most $(n-d)$ per point, or in other words, a *dual weighted* $(n, n-d)$-*arc* (or a *dual* $(n, n-d)$-*multiarc*). Such a dual weighted arc is said to be *complete* if A is an intersection set. Consequently, the corollary gives an equivalence between maximal linear (n,k,d)-codes and complete weighted $(n, n-d)$-arcs in $PG(k-1,q)$. The case that $\mathcal{G}$ has no repeated elements is treated in the next section.

4 Maximal Projective Codes-Complete Arcs

A linear $(n,k,d)_q$-code for which every pair of columns in an associated generator matrix are linearly independent (essentially, a code with no repeated coordinates) is called a *projective* code. An associated projective system of hyperplanes $\mathcal{G}$, in $PG(k-1,q)$, is therefore a collection of n hyperplanes such that: (1) No point is incident with as many as $n-d+1$ members of $\mathcal{G}$. (2) At least one point is incident with $n-d$ members of $\mathcal{G}$. Such a system of hyperplanes is the dual of what is called an $(n, n-d)$-*arc*, or an n-arc of *degree* $n-d$. A (dual) arc of necessarily minimal degree k in $PG(k,q)$ is simply called a (dual) arc. Consequently, an $(n, n-d)$-arc in $PG(k-1,q)$ and a projective $(n,k,d)_q$-code are equivalent objects. In particular, linear $(n,k,d)_q$-MDS codes and dual arcs in $PG(k-1,q)$ are equivalent.

An extension of a projective code will be (equivalent to) either a projective code, a linear non-projective code (obtained through repeating a coordinate), or a nonlinear code. A (dual) (n,r)-arc in $PG(k,q)$ is *complete* if it is not contained in a (dual) $(n+1,r)$-arc in $PG(k,q)$. A complete (n,r)-arc in $PG(k-1,q)$ therefore corresponds to a projective (n,k,d)-code of Singleton defect $s = r-k+1$ that admits no projective extensions. We now summarize some known results and improvements regarding maximal projective codes.

4.1 MDS Codes

The maximality of MDS codes corresponding to complete arcs was investigated in [2]. It was shown that "large" arcs give rise to projective codes admitting only linear extensions, *ergo* large complete arcs provide maximal codes.

Theorem 3 ([2]) *Let C be a projective $(n,k,d)_q$-MDS-code corresponding to a complete (dual) arc in $PG(k-1,q)$. Let $q = p^h$ and let t be the largest proper divisor of h. If*

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

then C is maximal.

There is much literature dedicated to the construction (and existence questions) of complete arcs. Let $m(k,q)$ denote the size of the largest (dual) arc in $PG(k,q)$. Finding the value of $m(k,q)$ has been the focus of much research (see [12,14,15,27,32]). The Main Conjecture for linear MDS codes, always taking $q > k$, is the following:

$$m(k-1,q) = \begin{cases} q+2 & \text{if } k = 3 \text{ and } k = q-1 \text{ both with } q \text{ even} \\ q+1 & \text{in all other cases} \end{cases}$$

Arcs of size $q+1$ are known to exist in $PG(k,q)$ for all k, the canonical examples being the normal rational curves (NRC). Hyperovals ($(q+2)$-arcs) are also known to exist in $PG(2,q)$, for q even. The Main Conjecture has not been proved in general. It has been verified in many cases. In their paper [14] Bruen, Thas, and Blokhuis show it to hold at least asymptotically. We remark that the bounds above on linear MDS codes are also conjectured to hold for non-linear MDS codes.

Theorem 3 encapsulates many of the known large complete arcs in $PG(k,q)$. By no means, however, are all complete arcs within the bounds given in Theorem 3. Indeed, restricting to the case $k = 2$ (3-dimensional codes) there exist many examples of small complete arcs. Abatangelo [1], Korchmáros [20] and Szőnyi [31] provide constructions of complete n-arcs in the $PG(2,q)$, where $(q-1)/4+3 < n < (q-1)/2+3$. See also Marcugini *et al.* [23] and the table therein for complete arcs in $PG(2,q)$, q small. In [19], Kim and Vu show there are universal constants c and q_0 such that every plane of order $q \geq q_0$ has a complete arc of cardinality $\leq \sqrt{2q}\log^c q$. Moreover, an algorithm is given which constructs such an arc in polynomial time.
For higher dimensions, the literature is not so rich with examples of complete arcs. However, for all dimensions $k \geq 2$, there do indeed exist complete arcs in $PG(k,q)$ that are smaller than the bounds in the Theorem 3. See for example Storme [28], Szőnyi [31], and Storme-Szőnyi [30]. For an excellent summary of known complete arcs in projective spaces, see Hirschfeld [17].

Summarizing, we see that, in many cases, complete arcs give rise to maximal codes. On the other hand, there exist many complete arcs for which the maximality of the corresponding projective code has remained in question. The next theorem shows that in fact *all* complete arcs give rise to maximal codes.

Theorem 4 *Let C be a projective $(n,k,d)_q$-MDS-code. Let $\mathcal{G}$ be a corresponding projective system of hyperplanes in $\Pi = PG(k-1,q)$ (so that in particular $\mathcal{G}$ is a dual n-arc in Π). The code C is maximal if and only if $\mathcal{G}$ is a complete dual arc.*

Proof Let A be the set of $(k-1)$-fold points of $\mathcal{G}$. If C is maximal then (Corollary 1) A is an intersection set in Π. It follows that $\mathcal{G}$ is complete. On the other hand, suppose $\mathcal{G}$ is a complete dual n-arc. Since $\mathcal{G}$ is complete, each hyperplane of $\Pi \setminus \mathcal{G}$ is incident with at least one $(k-1)$-fold point of $\mathcal{G}$. Since $n > k-1$ and any $k-1$ hyperplanes of Π intersect nontrivially it follows that the set of $(k-1)$-fold points of $\mathcal{G}$ is an intersection set. The result follows from Corollary 1.

4.2 Codes of Arbitrary Singleton Defect

The maximality of projective codes corresponding to complete (n,r)-arcs was investigated in [5] for codes of arbitrary Singleton defect. As in the MDS case, "large" complete (n,r)-arcs provide maximal codes. Specifically, the following appears in [5].

Theorem 5 ([5]) *Let C be a projective $(n,k,d)_q$-code of singleton defect s corresponding to a complete (dual) (n,r)-arc in $PG(k-1,q)$. Let $q=p^h$ and let t be the largest proper divisor of h. If*

$$n > \begin{cases} (s+\frac{1}{2})(q+1)+k-3 & \text{if } q \text{ is prime, and} \\ (s+1)(q+1)-p^{h-t}+k-3 & \text{otherwise.} \end{cases}$$

then C is maximal.

Regarding arcs of higher degree, various constructions of large complete (n,r)-arcs in $PG(2,q)$ appear in the literature. We refer to the table in [9]. In order to improve the above result, we shall use the following Lemma, which appears in [5].

Lemma 5 ([5]) *If C is a linear $(n,k,d)_q$ code, $k \geq 3$ with $n > s(q+1)+k-1$, then C is projective.*

Theorem 6 *Let C be a projective $(n,k,d)_q$-code of Singleton defect s. Let $\mathcal{G}$ be an associated projective system of hyperplanes in $\Pi = PG(k-1,q)$ (so that in particular $\mathcal{G}$ is a dual $(n,n-d)$-arc in Π). If $\mathcal{G}$ is complete and*

$$n > s(q+1)+k-2$$

then C is maximal.

Proof Assume $\mathcal{G}$ is complete and $n > s(q+1)+k-2$. Since $\mathcal{G}$ is complete, C admits no projective extensions. By the Lemma 5, any linear extension of C must be projective. Therefore (Theorem 2) C is maximal.

4.3 NMDS codes and Plane Elliptic Curves

Projective AMDS codes are called Near-MDS (NMDS) codes. Such codes correspond to (n,k)-arcs in $PG(k-1,q)$. The rational points of an elliptic plane curve are well known to compose $(n,3)$-arcs (cubic arcs) in $PG(2,q)$. Regarding the completeness of the cubic arcs arising from nonsingular cubic curves we have the following.

Theorem 7 ([4]) *Let Γ be a non-singular cubic curve in $\pi = PG(2,q)$, $|\Gamma| = n$. If $n > q+7$, then Γ is a complete cubic arc.*

Theorems 7 and 6 give the following.

Corollary 2 *Let Γ be a non-singular cubic curve in $\pi = PG(2,q)$, $|\Gamma| = n$. If $n > q+7$, then the corresponding $(n,3,n-3)_q$-NMDS code C is maximal.*

Suppose the nonsingular cubic curve Γ is a complete $(n,3)$-arc in $PG(2,q)$ and let C be the corresponding $(n,3,n-3)_q$-NMDS code. From Theorem 6 it follows that if $n > q+2$ then C is maximal. (We remark that this improves the bound $n > p+4$ obtained in [4] where the case $q=p$ is prime is considered.)
From the work of Waterhouse [33] (and the subsequent work of Rück [26]) it follows that the number n of rational points on an elliptic curve satisfies $q+1-2\sqrt{q} \leq n \leq q+1+2\sqrt{q}$ and can take every value in this interval.

The following is a consequence of the classical theory. A proof can be found in [4].

Lemma 6 *Let Γ be a non-singular cubic curve in $\Pi = PG(2,q)$ with $|\Gamma| = n$. Let P be a point of Γ. Then there are at least $\frac{1}{2}(n-5)$ lines of Π on P, each containing 3 points of Γ.*

Theorem 8 *Let Γ be a nonsingular cubic curve in $PG(2,q)$. Suppose Γ is a complete $(n,3)$-arc. Let C be the corresponding NMDS code. If $n > 5$ then C is maximal.*

Proof It will be convenient to dualize Γ so that Γ may be thought of as a cubical set of n lines in $\Pi = PG(2,q)$. Let A be the set of 3-fold points of Γ. Let ℓ be a line. If $\ell \in \Pi \setminus \Gamma$ then (since Γ is complete) $\ell \cap A \neq \emptyset$. If $\ell \in \Gamma$ then (Lemma 6), $\ell \cap A \neq \emptyset$. Consequently, A is an intersection set and the result follows from the Corollary 1.

In [18], Hirschfeld and Voloch show the following.

Theorem 9 ([18]) *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.*

Theorems 8 and 9 give the following.

Corollary 3 *Let Γ be an elliptic curve in $\pi = PG(2,q)$, $q \geq 79$ not a power of 2 or 3, having n rational points. If the j-invariant $j(\Gamma) \neq 0$ then the corresponding $(n,3,n-3)_q$-NMDS code is maximal.*

References

1. Abatangelo, V.: A class of complete $[(q+8)/3]$-arcs of PG(2, q), with $q = 2^h$ and $h(\geq 6)$ even. Ars Combin. **16**, 103–111 (1983)
2. 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)
3. Alderson, T.L.: On MDS codes and Bruen-Silverman codes. PhD. Thesis, University of Western Ontario (2002)
4. Alderson, T.L., Bruen, A.A.: Codes from cubic curves and their extensions. Electron. J. Combin. **15**(1), Research paper 42, 9 (2008)
5. Alderson, T.L., Bruen, A.A.: Coprimitive sets and inextendable codes. Des. Codes Cryptogr. **47**(1-3), 113–124 (2008)
6. Alderson, T.L., Bruen, A.A.: Maximal AMDS codes. Appl. Algebra Engrg. Comm. Comput. **19**(2), 87–98 (2008)
7. Ball, S.: The number of directions determined by a function over a finite field. J. Combin. Theory Ser. A **104**(2), 341–350 (2003)
8. Ball, S.: On the graph of a function in many variables over a finite field. Des. Codes Cryptogr. **47**(1-3), 159–164 (2008)
9. 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)
10. Bierbrauer, J.: Introduction to coding theory. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL (2005)
11. 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)
12. Blokhuis, A., Bruen, A.A., Thas, J.A.: Arcs in PG(n,q), MDS-codes and three fundamental problems of B. Segre—some extensions. Geom. Dedicata **35**(1-3), 1–11 (1990)
13. Bruen, A.A., Forcinito, M.A.: Cryptography, information theory, and error-correction. Wiley-Interscience Series in Discrete Mathematics and Optimization. Wiley-Interscience [John Wiley & Sons], Hoboken, NJ (2005). A handbook for the 21st century

14. Bruen, A.A., Thas, J.A., Blokhuis, A.: On M.D.S. codes, arcs in 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. Hirschfeld, J.W.P.: The number of points on a curve, and applications. Arcs and curves: the legacy of Beniamino Segre. Rend. Mat. Appl. (7) **26**(1), 13–28 (2006)
17. Hirschfeld, J.W.P., Storme, L.: The packing problem in statistics, coding theory and finite projective spaces: update 2001. In: Finite geometries, *Dev. Math.*, vol. 3, pp. 201–246. Kluwer Acad. Publ., Dordrecht (2001)
18. 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)
19. Kim, J.H., Vu, V.H.: Small complete arcs in projective planes. Combinatorica **23**(2), 311–363 (2003)
20. Korchmáros, G.: New examples of complete k-arcs in PG(2, q). European J. Combin. **4**(4), 329–334 (1983)
21. van Lint, J.H.: Introduction to coding theory, *Graduate Texts in Mathematics*, vol. 86. Third edn. Springer-Verlag, Berlin (1999)
22. 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
23. Marcugini, S., Milani, A., Pambianco, F.: Complete arcs in PG$(2, 25)$: the spectrum of the sizes and the classification of the smallest complete arcs. Discrete Math. **307**(6), 739–747 (2007)
24. Rédei, L.: Lacunary polynomials over finite fields. North-Holland Publishing Co., Amsterdam (1973). Translated from the German by I. Földes
25. Roth, R.: Introduction to Coding Theory. Cambridge University Press, New York, NY, USA (2006)
26. Rück, H.G.: A note on elliptic curves over finite fields. Math. Comp. **49**(179), 301–304 (1987)
27. Segre, B.: Curve razionali normali e k-archi negli spazi finiti. Ann. Mat. Pura Appl. (4) **39**, 357–379 (1955)
28. Storme, L.: Small arcs in projective spaces. J. Geom. **58**(1-2), 179–191 (1997)
29. Storme, L., Sziklai, P.: Linear point sets and Rédei type k-blocking sets in PG(n, q). J. Algebraic Combin. **14**(3), 221–228 (2001)
30. Storme, L., Szőnyi, T.: Intersection of arcs and normal rational curves in spaces of even characteristic. J. Geom. **51**(1-2), 150–166 (1994)
31. Szőnyi, T.: Small complete arcs in Galois planes. Geom. Dedicata **18**(2), 161–172 (1985)
32. 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)
33. Waterhouse, W.C.: Abelian varieties over finite fields. Ann. Sci. École Norm. Sup. (4) **2**, 521–560 (1969)