Coprimitive Sets and Inextendable Codes

T. L. Alderson *
Mathematical Sciences
University of New Brunswick
Saint John, NB.
E2L 4L5
Canada
tim@combinatorics.ca

A. A. Bruen†
Electrical and Computer Engineering
University of Calgary
Calgary, AB
T2N 1N4
Canada
bruen@ucalgary.ca

Abstract

Complete (n, r)-arcs in $PG(k-1, q)$ and projective $(n, k, n-r)_q$-codes that admit no projective extensions are equivalent objects. We show that projective codes of reasonable length admit only projective extensions. Thus, we are able to prove the maximality of many known linear codes. At the same time our results sharply limit the possibilities for constructing long nonlinear codes. We also show that certain short linear codes are maximal. The methods here may be just as interesting as the results. They are based on the Bruen-Silverman model of linear codes (see [1, 2, 9] and [15]) as well as the theory of Rédei blocking sets first introduced in [8].

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 $\mathcal{A}$ of size q such that the minimum (Hamming) distance between any two codewords of C is d. Note that q need not be a prime power. In an $(n, k, d)_q$-code C there exist two codewords agreeing in $n-d$ coordinates and no two codewords agree in as many as $n-d+1$ (in particular, any $n-d+1$ coordinates form an information set). In the special case that $\mathcal{A} = GF(q)$ 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 whose columns can be considered as a projective multiset $\mathcal{G}$ of n points in $PG(k-1, q)$ at most $n-d$ per hyperplane. This multiset is called a *projective system* associated with C. Dually, $\mathcal{G}$ can be considered as a *projective system of hyperplanes* (of $PG(k-1, q)$) at most $n-d$ per point. The parameter n is the *length* of C.

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 therefore 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.

Two $(n, k, d)_q$-codes C_1 and C_2 over an alphabet $\mathcal{A}$ are *equivalent* if C_2 can be obtained from C_1 by a sequence of operations of the following two types.

1. A permutation on the set of coordinate positions (*positional permutation*);

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

2. A permutation of the alphabet $\mathcal{A}$ applied in a given coordinate position (*symbol permutation*).

If C_1 and C_2 are equivalent codes and C_1 is linear we say C_2 is *equivalent to linear*.

For $r \geq k$ an (n, r)-*arc* $\mathcal{K}$ in $PG(k, q)$ is an n-set of points such that each hyperplane is incident with at most r members of $\mathcal{K}$ and dually, a *dual* (n, r)-*arc* in $PG(k, q)$ is an n-set of hyperplanes such that each point is incident with at most r members of $\mathcal{K}$. An (dual) (n, r)-arc in $PG(k, q)$ is *complete* if it is not contained in an (dual) $(n + 1, r)$-arc in $PG(k, q)$.

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. Hence, an $(n, n - d)$-arc in $PG(k - 1, q)$ and a projective $(n, k, d)_q$-code are equivalent objects.
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 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.

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 [13] for a recent survey of results in the MDS case. Regarding the general problem some advances have been made through the construction of large complete (n, r)-arcs and therefore long projective codes admitting no projective extensions. We refer to the table in [4]. A fundamental question , which is the main focus of this paper , is as follows.

Question 1: Given a projective $(n, k, d)_q$ code C corresponding to a complete (n, r)-arc, under what conditions is C maximal?

It turns out (Corollary 3.10) that linear codes of reasonable length are necessarily projective. As such we ask the following more general question.

Question 2: Given a linear $(n, k, d)_q$ code C, under what conditions must all extensions of C be linear?

We are able to establish sufficient conditions in answer to both Question 1 (Lemma 3.5, Theorem 3.7, and Corollary 3.14) and Question 2 (Theorems 3.3 and 3.12). We also establish the maximality of certain non-projective codes (see Section 3.3). The central ideas to our approach are the Bruen-Silverman model of linear codes (first introduced in [1, 2]), coprimitive sets, and intersection sets. A set of points S 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*. Any set containing all of the points of a line is an intersection set.

Concerning nonlinear extensions of linear codes we make the following remark: Consider a linear $(n, k, d)_q$-code C over $\mathcal{F} = GF(q)$ with generator matrix G. A linear extension of C arises by augmenting G with an appropriate column vector. Over $\mathcal{F}$ there are in total q^k column vectors to check using (perhaps naively) an exhaustive search. But in order to consider general (not necessarily linear) extensions of C one must consider the $q^k \times n$ array M whose rows are the words of C. An extension then arises by augmenting M with an appropriate column vector. Over $\mathcal{F}$ there are a total of q^{q^k} possible column vectors! Hence the search for for an arbitrary extension of C grows exponentially when one considers general, and not just linear, extensions. In investigating the maximality of a given linear code it is therefore extremely useful to know when nonlinear extensions can be ruled out. Let us give just one example of this. Let p be be any prime. If π is any affine plane of order p, then the first two parallel classes of π give a linear code C over $GF(p)$. Suppose one could prove that any code D which is an extension of C is necessarily equivalent to a linear code. Then, a longstanding fundamental problem would be solved. Namely, it would follow, among other things, that π is necessarily Desarguesian!!

2 Coprimitive Sets

Let $\Pi = PG(k,q)$ and consider Π as embedded in $\Sigma = PG(k+1,q)$ where $E = \Sigma \backslash \Pi$ is the associated affine space. For any set S of (affine) points in E the *Rédei set* of S with respect to Π, denoted by $\mathcal{R}_\Pi(S)$, 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 2.1. 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 $\mathcal{R}_\Pi(S) \subseteq \Pi \setminus \{A\}$. A *transversal* of A is a (necessarily maximal) partial transversal of size q^k.

Remark 2.2. Let A be a set of n points in $PG(1,q)$ considered as embedded in $\pi = PG(2,q)$. The set A gives rise in a natural way to a Bruck net $\mathcal{N}$ of order q and degree n. We remark that a (partial) transversal of A as defined above is precisely a (partial) transversal of $\mathcal{N}$ as defined by Bruck [7].

Definition 2.3. The set A is *k-coprimitive* (or *coprimitive* if k is understood) where A is a pointset in $\Pi = PG(k,q) \subset \Sigma = PG(k+1,q)$ if every transversal of A necessarily composes an (affine) hyperplane in $\Sigma \setminus \Pi$.

Remark 2.4. In the definition, A is coprimitive if and only if the set $B = \Pi \setminus A$ is *primitive* as defined in [2].

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

Clearly a hyperplane of $PG(k,q)$, $k \geq 2$, possesses no transversals, so we have the following.

Lemma 2.6. *For $k \geq 2$ let A be a subset of $PG(k,q)$ containing a hyperplane, then A is k-coprimitive.*

In [8] various characterizations of certain blocking sets were described and the fundamental connection with the work of Redei ([14]) was first established. Building on this, Blokhuis, Ball, Brouwer, Storme, and Szonyi [6] proved theorems on the number of directions determined by q points in $AG(2,q)$. Some of those results were extended by Ball [3] as follows.

Theorem 2.7. *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 the graph of 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 2.8. *Let $\ell = PG(1,q) \subset \Pi = PG(2,q)$ where $q = p^h$, p prime, and let t be the largest proper divisor of h. Let A be a set of points in ℓ. If $|A| > t$ where*

$$t = \begin{cases} \frac{q-1}{2} & q \text{ is prime} \\ q - p^{h-t} & \text{otherwise.} \end{cases} \tag{2.1}$$

then A is coprimitive.

Lemma 2.9. *Let ℓ_1, ℓ_2 be lines in $\Pi = PG(2,q)$ and let $\phi : \ell_1 \to \ell_2$ be a projection through a fixed point $Q \notin \ell_1, \ell_2$. Let A_1 be a subset of the points of ℓ_1 and let $A_2 = \phi(A_1)$, then A_1 is 1-coprimitive if and only if A_2 is 1-coprimitive.*

Proof. Embed Π in $\Sigma = PG(3,q)$ and let Π_1, Π_2 be planes distinct from Π through ℓ_1 and ℓ_2 respectively. Let $\Phi : \Pi_1 \to \Pi_2$ be the projection through Q. Clearly a point set $T \subset \Pi_1$ is a transversal of A_1 if and only if $\Phi(T)$ is a transversal of A_2. As Φ maps lines to lines the result follows. □

Theorem 2.10. *Let A be a point set in $\Pi = PG(k,q)$, $k \geq 2$. Let λ_1 and λ_2 be hyperplanes of Π where $A_1 = A \cap \lambda_1$ and $A_2 = A \cap \lambda_2$. If*

1. *$A_1 \neq A_2$ are $(k-1)$-coprimitive, and*
2. *$A_1 \cap A_2 \neq \emptyset$.*

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 $\sigma = \lambda_1 \cap \lambda_2$. 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. Therefore, (as A_1 is $(k-1)$-coprimitive), each T_i is a subset of a $(k-1)$-flat say τ_i. By assumption $A_1 \neq A_2$, so we may assume there exists a point $P \in A \setminus A_1$ (if $A = A_1$ then we may interchange the roles of A_1 and A_2). 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).
Note that $\sigma_1 \neq \sigma$ since by assumption $\sigma \cap A \neq \emptyset$. We claim $\tau_1, \tau_2, \ldots, \tau_q$ belong to a hyperplane of Σ. 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 A_2 is coprimitive whence T' is contained in a $(k-1)$-flat, say τ'. Let $\tau' \cap \lambda_2 = \sigma_2$. Note that as above we have $\sigma_2 \neq \sigma$ hence $\sigma_2 \neq \sigma_1$. 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). □

Lemma 2.11. *For fixed k and q, denote by $\mathcal{M}(k,q)$ the size of the smallest k-coprimitive set, then*

$$\mathcal{M}(k,q) \leq k \cdot \mathcal{M}(1,q) - k + 1.$$

Proof. Let A_1 be a 1-coprimitive set in $\ell_1 = PG(1,q)$ with $|A_1| = \mathcal{M}(1,q)$ and let $P \in A_1$. Embed ℓ_1 in $\Sigma = PG(k,q)$ and let $\ell_2, \ell_3, \ldots, \ell_k$ be lines through P such that $\langle \ell_1, \ell_2, \ldots, \ell_k \rangle = \Sigma$. On each ℓ_i let A_1 be projected (as in Lemma 2.9) to a 1-coprimitive set A_i containing P and having cardinality $\mathcal{M}(1,q)$.
We claim $A = A_1 \cup A_2 \cup \cdots \cup A_k$ is $k-$coprimitive. The case $k = 1$ being clear we proceed inductively. Denote by H_1 and H_2 the hyperplanes of Σ spanned by $\ell_1, \ell_2, \ldots, \ell_{k-1}$ and by $\ell_2, \ell_3, \ldots, \ell_k$ respectively. By the induction hypothesis, $A \cap H_1$ and $A \cap H_2$ are $(k-1)$-coprimitive sets. Since $P \in H_1 \cap H_2$ it follows (Theorem 2.10) that A is a k-coprimitive set of size $k \cdot \mathcal{M}(1,q) - k + 1$. □

2.1 (n,r)-arcs in PG(k,q)

By $m_r(k,q)$ we denote the size of the largest (n,r)-arc in $PG(k,q)$. The following summarizes some existing bounds on (n,r)-arcs in the plane.

Theorem 2.12. *(a)* $m_r(2,q) \leq (r-1)(q+1)+1$

(b) $m_r(2,q) = (r-1)(q+1)+1$ *for* $(r,q) = (2^e, 2^h)$.

(c) $m_r(2,q) \leq (r-1)(q+1)-1$ *for* $(r,q) \neq (2^e, 2^h)$ *and* $2 < r < q$

(d) $m_r(2,q) \leq (r-1)(q+1) - \frac{\sqrt{q}}{4} + 1$ *for q odd, $r|q$.*

Proof. Simple counting gives (a); for (b) see [10]; (c) follows from the early work of Barlotti [5]; for (d) see [17]. □

Bounds on (n,r)-arcs in the plane give rise in a natural way to bounds in higher dimensions. The following result is likely well known; we include a proof for completeness.

Lemma 2.13. *For $k \geq 2$ and $s \geq 0$, $m_{k+s}(k,q) \leq m_{2+s}(2,q) + k - 2$*

Proof. We use the dual. The result clearly holds for $k = 2$. Fix $k > 2$ and let $\mathcal{K}$ be a dual $(n, k+s)$-arc in $PG(k,q)$ and let $\lambda \in \mathcal{K}$. By the respective intersections with λ the remaining members of $\mathcal{K}$ cut out a dual $(n-1, k+s-1)$-arc in $\lambda = PG(k-1,q)$. This gives $n - 1 \leq m_{k+s-1}(k-1,q)$ and the result follows inductively. □

Theorem 2.14. *Let K be a dual (n,r)-arc in $\pi = PG(2,q)$, $q = p^h$, where $r = 2 + s$ and let A be the collection of (r)-fold points of K. Let t be the largest proper divisor of h. If*

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

then A is a 2-coprimitive set.

Proof. Let X be an r-fold point of $\mathcal{K}$ and choose $\ell_1, \ell_2 \in \mathcal{K}$ both incident with X. Let $A_i = A \cap \ell_i$, $i = 1, 2$. From the bounds it follows that

$$|A_1| \geq \begin{cases} \frac{1}{2}(q+1) & \text{if } q \text{ is prime, and} \\ (q+1) - p^{h-t} & \text{otherwise.} \end{cases}$$

Therefore (Corollary 2.8) A_1 is a 1-coprimitive set. Similarly, A_2 is 1-coprimitive. As $X \in A_1 \cap A_2$ we see that A satisfies all hypotheses of Theorem 2.10 and is therefore 2-coprimitive. □

Theorem 2.15. *Let K be a dual (n,r)-arc in $\Pi = PG(k,q)$ $k \geq 2$ where $r = k + s$ and let A be the collection of (r)-fold points of K. Let t be the largest proper divisor of h. If*

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

then A is a coprimitive set in $PG(k,q)$.

Proof. We proceed by induction on k. Theorem 2.14 establishes the result for $k = 2$. For $k \geq 2$ let $K = \{\Lambda_1, \Lambda_2, \ldots, \Lambda_n\}$ be a dual (n,r)-arc in $PG(k+1,q)$, $r = k+1+s$ satisfying the bounds in the theorem. Let P be an r-fold point of $\mathcal{K}$ and assume with no loss of generality that $P \in \Lambda_{n-1} \cap \Lambda_n$. For each $i = 1, 2, \ldots, n-1$ let $\lambda_i = \Lambda_n \cap \Lambda_i$. Then $K' = \{\lambda_1, \lambda_2, \ldots, \lambda_{n-1}\}$ is a dual $(n-1, r-1)$-arc in $PG(k,q)$. From the induction hypothesis it follows that $A_1 = A \cap \Lambda_n$ is a k-coprimitive set. Similarly, $A_2 = A \cap \Lambda_{n-1}$ is a k-coprimitive set. Theorem 2.10 then yields the result. □

3 Extending Linear Codes

3.1 The BRS Model of Linear Codes

In [9] Bruen and Silverman introduce a construction of (a family of) three-dimensional MDS codes using dual arcs in PG(2,q). This construction was generalized to MDS codes of arbitrary dimension in [1] where the codes were also shown to be (equivalent to) linear. In [2] the construction was generalized to the case of arbitrary linear codes. That is, given any linear code C, it is possible to associate a family of codes with C. If D is any code in the family we refer to D as a Bruen-Silverman (BRS) code associated with C and shall speak of the BRS model of C. It is the case that any BRS code associated with C is equivalent to C. However, the BRS model affords a particularly convenient geometrical picture for visualizing the code C.

The model works as follows. Let $\mathcal{K} = \lambda_1, \lambda_2, \ldots, \lambda_n$ be an n-multiset of hyperplanes in $\Pi = PG(k-1,q)$ containing at least k members in general position and suppose that each point in Π is incident with at most t members of $\mathcal{K}$ (counting multiplicities). We construct a $(n, k, n-t)_q$-code associated with $\mathcal{K}$. Consider Π as embedded in $\Sigma = PG(k,q)$ where $E = \Sigma \backslash \Pi$ 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 λ_i. Let $\mathcal{A} = \{\alpha_1, \alpha_2, \ldots, \alpha_q\}$ be an alphabet of size q (with no loss of generality we may take

$\mathcal{A} = GF(q)$). For each i, j, associate with Π_{ij} the label $\mathcal{L}(\Pi_{ij}) = \alpha_j$. For each affine point $P \in E$ and for each i, $1 \leq i \leq n$ define the mappings

$$\Phi_i : E \to \mathcal{A} \quad \text{by} \quad \Phi_i(P) = \mathcal{L}\left(\langle \lambda_i, P \rangle\right)$$

and

$$\Phi : E \to \mathcal{A}^n \quad \text{by} \quad \Phi(P) = (\Phi_1(P), \Phi_2(P), \ldots, \Phi_n(P)).$$

Notice that if $P_1, P_2 \in E$ then $\Phi(P_1)$ and $\Phi(P_2)$ will have precisely m common coordinates if and only if the line P_1P_2 meets $\mathcal{K}$ in an m-fold point. It follows that $C = \{\Phi(P) | P \in E\}$ is an $(n, k, n-t)_q$-code. Moreover, if homogeneous coordinates are assigned in Π so that each λ_i has an equation of the form

$$a_{1i}x_1 + a_{2i}x_2 + \cdots a_{ki}x_k = 0$$

then C is equivalent to the linear code with generator matrix

$$G = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \end{bmatrix}$$

Notice that under the BRS model a positional permutation of the corresponding code equates to a reordering of the members of $\mathcal{K}$ whereas a symbol permutation is simply a relabeling of the q hyperplanes through a particular member of $\mathcal{K}$. In particular we have the following.

Theorem 3.1. *Let C be a linear $(n, k, d)_q$-code with generator G and let $\mathcal{G}$ be the associated projective system of hyperplanes in $\Pi = PG(k-1, q)$, then a given code is equivalent to C if and only if C admits a BRS model based on $\mathcal{G}$. That is, a code is equivalent to linear if and only if it admits a BRS model.*

The BRS model of linear codes brings a new interpretation of code extension. Indeed, let C be a linear $(n, k, d)_q$-code with a corresponding BRS model based on the projective system $\mathcal{G} = \{\Lambda_1, \Lambda_2, \ldots, \Lambda_n\}$ of hyperplanes in $\Pi = PG(k-1, q) \subset \Sigma = PG(k, q)$. Let A denote the collection of $(n-d)$-fold points of $\mathcal{G}$. An extension of C then corresponds to a partition $\mathcal{P} = S_1, S_2, \ldots, S_q$ of the points of $\Sigma^* = \Sigma \setminus \Pi$ into transversals of A. Moreover, any such extension will be (equivalent to) linear if and only if $\mathcal{P}$ corresponds to a parallel class of affine hyperplanes in Σ^* the projective points of which compose a (projective) $(k-2)$-flat (in Π) containing no points of A . This gives the following:

Lemma 3.2. *Let C be a linear $(n, k, d)_q$-code with $\mathcal{G}$ a corresponding projective system of hyperplanes. Let A be the set of $(n-d)$-fold points of $\mathcal{G}$. If A is an intersection set then C admits no linear extensions.*

Theorem 3.3. *Let C be a linear $(n, k, d)_q$-code with $\mathcal{G}$ an associated projective system of hyperplanes of $\Pi = PG(k-1, q)$. Denote by A the set of $(n-d)$-fold points of $\mathcal{G}$. If A is coprimitive then every extension of C is (equivalent to) linear.*

Proof. Consider the BRS model of C where $\mathcal{G} \subset \Pi \subset \Sigma = PG(k, q)$. Let $GF(q) = \{\alpha_1, \alpha_2, \ldots, \alpha_q\}$ and let C' be an $(n+1, k, d+1)_q$-code extending C. For each $i = 1, 2, \ldots, q$ denote by C_i the codewords in C' having $(n+1)$'st coordinate α_i. Denote by $\mathcal{C}_i$ the (affine) points of Σ corresponding to the codewords in C_i, $i = 1, 2, \ldots, q$. It follows that for any line ℓ of Σ incident with a point of A either $\ell \cap \mathcal{C}_i = \emptyset$, $i = 1, 2, \ldots, q$ (precisely when $\ell \subset \Pi$) or $|\ell \cap \mathcal{C}_i| = 1$, $i = 1, 2, \ldots, q$ (else in C' two codewords agree in $n - d + 1$ coordinates). Hence, each $\mathcal{C}_i$ is a transversal of A. Accordingly, if A is coprimitive then $\{C_1, C_2, \ldots, C_q\}$ is a partition of $\Sigma \setminus \Pi$ into affine hyperplanes and (from the BRS model) it follows that C' is equivalent to linear. □

Lemma 3.4. *Let C be a linear $(n, k, d)_q$-code with $\mathcal{G}$ a corresponding projective system of hyperplanes. Let A be the set of $(n-d)$-fold points of $\mathcal{G}$. If A is a coprimitive intersection set then C is maximal.*

Proof. Let C be a code meeting the conditions set out in the Lemma. By Theorem 3.3 all extensions of C are linear. By Lemma 3.2 C admits no linear extensions. □

3.2 Projective codes

Lemma 3.5. *Let $\mathcal{K}$ be a complete dual (n,r)-arc in $PG(k,q)$. Denote by A the set of r-fold points of $\mathcal{K}$. If A is k-coprimitive and each member of $\mathcal{K}$ contains at least one point of A then the projective $(n,k+1,n-r)_q$-code C corresponding to $\mathcal{K}$ is maximal.*

Proof. Suppose $\mathcal{K}$ is a complete dual (n,r)-arc satisfying the conditions set out in the Lemma. Let Π be a hyperplane of $PG(k,q)$. If $\Pi \notin \mathcal{K}$ then Π contains at least one point of A (since $\mathcal{K}$ is complete). If $\Pi \in \mathcal{K}$ then by assumption Π contains at least one point of A. Thus A is an intersection set and the result follows from Lemma 3.4. □

Lemma 3.6. *Let $\mathcal{K}$ be a complete dual (n,r)-arc in $PG(2,q)$ $n > (r-2)(q+1)+1$ then the set A of r-fold points of $\mathcal{K}$ is an intersection set. Consequently, if A is coprimitive then the projective $(n,3,n-r)_q$-code C corresponding to $\mathcal{K}$ is maximal.*

Proof. Assume $\mathcal{K}$ satisfies the conditions. As $\mathcal{K}$ is complete each line $\ell \notin \mathcal{K}$ contains at least one point of A. Since $n > (r-2)(q+1)+1$ simple counting shows each $\ell \in \mathcal{K}$ contains at least one point of A. □

Theorem 3.7. *For $k \geq 3$ let $\mathcal{K}$ be a complete dual (n,r)-arc in $PG(k-1,q)$ and let C be the corresponding projective $(n,k,n-r)_q$-code. If*

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

then the set A of r-fold points of $\mathcal{K}$ is an intersection set (in $PG(k-1,q)$). Consequently, if A is coprimitive then C is maximal.

Proof. Corollary 3.6 establishes the result for $k=3$; we proceed inductively. Suppose the result to hold for (n,r)-arcs in $PG(k-1,q)$. Let $\mathcal{K} = \Lambda_1, \Lambda_2, \ldots, \Lambda_n$ be a complete dual (n,r)-arc in $PG(k,q)$ with $n > (r-k)(q+1)+k-2$. As $\mathcal{K}$ is complete it suffices to show that each Λ_i contains at least one point of A. By the respective intersections with Λ_n the remaining members of $\mathcal{K}$ cut out a dual $(n-1,r-1)$-arc $\mathcal{K}' = \lambda_1, \lambda_2, \ldots, \lambda_{n-1}$ in $\Lambda = PG(k-1,q)$ (where say $\lambda_i = \Lambda_i \cap \Lambda_n \;\; i = 1,2,\ldots,n-1$). By assumption we have

$$n-1 > (r-k)(q+1)+k-3 = \big((r-1)-(k-1)\big)(q+1)+(k-1)-2$$

By the induction hypothesis each λ_i contains a $(r-1)$-fold point of $\mathcal{K}'$ and therefore a point of A. Therefore each Λ_i contains a point of A. □

3.3 Linear codes that are not projective

The following bound was established by Griesmer [11] for binary codes and was generalized in [16] for $q \geq 2$.

Theorem 3.8 (The Griesmer bound)**.** *A linear $(n,k,d)_q$ code satisfies* $n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$

The next Theorem is well known and follows from Theorem 2.16 of [12]. For the sake of completeness we include a proof.

Theorem 3.9. *A linear $(n,k,d)_q$ code C meeting the Griesmer bound and satisfying $d \leq q^{k-1}$ is necessarily projective.*

Proof. Let $\mathcal{G} = \{\Lambda_1, \Lambda_2, \ldots, \Lambda_n\}$ be a projective system of $(k-2)$-flats corresponding to C. Let Λ_n have multiplicity m in $\mathcal{G}$, where say $\Lambda_n = \Lambda_{n-1} = \cdots = \Lambda_{n-m+1}$. For each i, $1 \leq i \leq n-m$, let $\lambda_i = \Lambda_i \cap \Lambda_n$. It follows that $\{\lambda_1, \lambda_2, \ldots, \lambda_{n-m}\}$ is a projective system corresponding to an $(n-m, k-1, d)_q$-code. From the Griesmer bound we get $n-m \geq \sum_{i=0}^{k-2} \left\lceil \frac{d}{q^i} \right\rceil = \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil - 1 = n-1$. Hence, for $m > 1$ we arrive at a contradiction. □

Corollary 3.10. *If C is a linear $(n, k, d)_q$ code, $k \geq 3$ with $n \geq s(q+1)+k$, then C is projective.*

Proof. By substituting $s = n - d - k + 1$ we obtain

$$n \geq s(q+1)+k \iff n \leq d + \left\lfloor \frac{d+q-1}{q} \right\rfloor + k - 2 \iff n \leq d + \left\lceil \frac{d}{q} \right\rceil + k - 2.$$

It is clear that this condition is met if and only if $d \leq q^2$ and C meets the Griesmer bound. The result follows from Theorem 3.9. □

Example 1. We provide some examples of projective systems of lines in $PG(2, q)$ corresponding to linear non-projective codes meeting the theoretical bound in Corollary 3.10.

s=1: For q even let $\mathcal{K} = \{\ell_1, \ell_2, \ldots, \ell_{q+2}\}$ be a dual hyperoval and take $\mathcal{G} = \ell_1, \ell_1, \ell_2, \ldots, \ell_{q+2}$.

s=1: For q odd let $\mathcal{K} = \{\ell_1, \ell_2, \ldots, \ell_{q+1}\}$ be a dual conic. Let P be the (unique) tangent point on ℓ_1 and choose a line $\ell \notin \mathcal{K}$ incident with P. Take $\mathcal{G} = \ell_1, \ell_1, \ell_2, \ldots, \ell_{q+1}, \ell$.

s=2: For q even let $\mathcal{K}$ and $\mathcal{K}'$ be dual hyperovals having precisely two lines in common, say $\mathcal{K} \cap \mathcal{K}' = \{\ell_1, \ell_2\}$. Then take $\mathcal{G}$ to be the lines of $\mathcal{K} \cup \mathcal{K}'$ where ℓ_1 and ℓ_2 both have multiplicity 2 (in $\mathcal{G}$).

If C is a linear $(s(q+1)+k-1, k, d)_q$ code and C is not projective then (Corollary 3.10) C admits no linear extensions. The question then arises as to whether such a code is actually maximal. Notice that in each of the examples above, the set A of 3-fold points of $\mathcal{G}$ contains all of the points of a line. As such A is an intersection set and (Lemma 2.6) a coprimitive set. Therefore, in each case the corresponding code is maximal. We now establish that this property holds for all linear non-projective $(n, k, d)_q$ codes meeting the bound in Corollary 3.10.

Theorem 3.11. *Let C be a linear $(s(q+1)+k-1, k, d)_q$ code $k \geq 3$ where $S(C) = s$. If C is not projective then C is maximal.*

Proof. We first establish the result for $k = 3$. Let C be a non-projective linear $(s(q+1)+2, 3, d)_q$ code with corresponding projective system of lines $\mathcal{G}$ in $\Pi = PG(2, q)$. By Corollary 3.10 C admits no linear extensions. Hence (Theorem 3.3), it suffices to show the set A of $(n-d)$-fold points of $\mathcal{G}$ is coprimitive. Let $\ell \in \mathcal{G}$ have multiplicity $m > 1$. Each point of Π is incident with at most $n - d = s + 2$ members of $\mathcal{G}$ (counting multiplicity). In particular, each point of ℓ is incident with at most $s + 2 - m \leq s$ further members of $\mathcal{G}$. This gives

$$s(q+1)+2 = n \leq m + (s+2-m)(q+1) = s(q+1)+2-(m-2)q. \tag{3.1}$$

Therefore, $m = 2$ and we have equality throughout Equation (3.1). Each point of ℓ is therefore an $(n-d)$-fold point of $\mathcal{G}$. As A contains a line it is (Lemma 2.6) a coprimitive set and the result holds for $k = 3$.

We proceed by induction on k. Let C be a non-projective linear $(s(q+1)+k, k+1, d)_q$-code with associated projective system of hyperplanes $\mathcal{G} = \lambda_1, \lambda_2, \ldots \lambda_{s(q+1)+k}$ where say $\lambda_1 = \lambda_2$. Assume with no loss of generality that $\lambda_1 \neq \lambda_{s(q+1)+k}$. Let $\lambda_{s(q+1)+k}$ have multiplicity t in $\mathcal{G}$. For $i = 1, 2, \ldots, s(q+1)+k-t$ denote $\lambda_i' = \lambda_i \cap \lambda_{s(q+1)+k}$ and let C' be the code with projective system $\mathcal{G}' = \lambda_1', \lambda_2', \ldots, \lambda_{s(q+1)+k-t}'$. It follows that C' is a linear non-projective (n', k, d')-code with $S(C') = s' = s - t + 1$ where

$$n' = s(q+1)+k-t \geq s'(q+1)+k-1.$$

By the induction hypothesis C' is maximal. As any extension of C gives rise to an extension of C' we have C is maximal. □

3.4 The general case

Theorem 3.12. *Let C be a linear $(n,k,d)_q$-code of singleton defect $S(C)=s$, where $q=p^h$ 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 any extension of C is (equivalent to) linear.

Proof. Let C be a code meeting the conditions of the theorem and let $\mathcal{G}$ be a corresponding projective system of hyperplanes in $\Pi = PG(k-1,q)$. Denote by A the set of $(n-d)$-fold points of $\mathcal{G}$. By Corollary 3.10 C is projective, so $\mathcal{G}$ is an $(n,k-1+s)$-arc in $PG(k-1,q)$. By Theorem 2.15, A is a coprimitive set and therefore (Theorem 3.3) all extensions of C are (equivalent to) linear. □

Remark 3.13. By substituting $s=n-d-k+1$ we obtain

$$n > (s+\frac{1}{2})(q+1)+k-3 \iff n \le d + \left\lfloor \frac{d+\frac{1}{2}(q+1)}{q} \right\rfloor + k - 2 \ \left(\le d + \left\lceil \frac{d}{q} \right\rceil + k - 2 \right)$$

and

$$n > (s+1)(q+1)-p^{h-t}+k-3 \iff n \le d + \left\lfloor \frac{d+p^{h-t}}{q} \right\rfloor + k - 2 \ \left(\le d + \left\lceil \frac{d}{q} \right\rceil + k - 2 \right)$$

Consequently, any code satisfying the conditions of Theorem 3.12 meets the Griesmer bound and satisfy $d \le q^2$.

Corollary 3.14. *Let C be a projective $(n,k,d)_q$-code of singleton defect s corresponding to a complete (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.

Table 1 gives the values of N provided by Corollary 3.14 for which a complete (n,r)-arc in $PG(2,q)$ with $n > N$ corresponds to a maximal projective code. We have indicated in bold those values above which a complete (n,r)-arc is known to exist. Values for which the existence of an (n,r)-arc $n > N$ is unknown have been marked with an asterisk. For a summary of the size of the largest (n,r)-arcs in $PG(2,q)$ for small q see the table in [4] or the table available at http://www-ma4.upc.es/∼simeon/codebounds.html (maintained by Simeon Ball).

Table 1: Values of N for which a complete plane (n,r)-arc $n > N$ correspond to maximal codes.

r \ q	**3**	**4**	**5**	**7**	**8**	**9**	**11**	**13**	**16**	**17**	**19**
2	**2**	**3**	**3**	**4**	**5**	**7**	**6**	**7**	**13**	**9**	**10**
3		**8**	**9**	**12**	**14**	17	**18**	**21**	30*	**27**	**30**
4			**15**	**20**	**23**	**27**	**30**	**35**	**47**	**45**	**50**
5				**28**	**32**	37	**42**	49*	**64**	63*	70*
6				36	**41**	**47**	**54**	**63**	81*	81*	90*
7					50	57	**66**	**77**	98	99*	110*
8						67	78	**91**	**115**	117*	130*
9							90	105	132	**135**	150*
10							102	119	149	**153**	**170**
11								133	166	171	**190**

References

[1] T.L. Alderson. On MDS codes and Bruen-Silverman codes. *PhD. Thesis, University of Western Ontario*, 2002.

[2] T.L. Alderson, A. A. Bruen, and R. Silverman. Maximum distance separable codes and arcs in projective spaces. *J. Combin. Theory Ser. A (to appear)*.

[3] S. Ball. The number of directions determined by a function over a finite field. *J. Combin. Theory Ser. A*, 104(2):341–350, 2003.

[4] S. Ball and J. W. P. Hirschfeld. Bounds on (n, r)-arcs and their application to linear codes. *Finite Fields Appl.*, 11(3):326–336, 2005.

[5] Adriano Barlotti. Sui $\{k; n\}$-archi di un piano lineare finito. *Boll. Un. Mat. Ital. (3)*, 11:553–556, 1956.

[6] A. Blokhuis, S. Ball, A. E. Brouwer, L. Storme, and T. Szőnyi. 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.

[7] R. H. Bruck. Finite nets. II. Uniqueness and imbedding. *Pacific J. Math.*, 13:421–457, 1963.

[8] A. A. Bruen and B. Levinger. A theorem on permutations of a finite field. *Canad. J. Math.*, 25:1060–1065, 1973.

[9] A. A. Bruen and R. Silverman. On extendable planes, M.D.S. codes and hyperovals in $\mathrm{PG}(2, q), q = 2^t$. *Geom. Dedicata*, 28(1):31–43, 1988.

[10] R. H. F. Denniston. Some maximal arcs in finite projective planes. *J. Combinatorial Theory*, 6:317–319, 1969.

[11] J. H. Griesmer. A bound for error-correcting codes. *IBM J. Res. Develop.*, 4:532–542, 1960.

[12] R. Hill and D. E. Newton. Optimal ternary linear codes. *Des. Codes Cryptogr.*, 2(2):137–157, 1992.

[13] J. W. P. Hirschfeld. 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.

[14] L. Rédei. *Lacunary polynomials over finite fields*. North-Holland Publishing Co., Amsterdam, 1973. Translated from the German by I. Földes.

[15] Robert Silverman. A metrization for power-sets with applications to combinatorial analysis. *Canad. J. Math.*, 12:158–176, 1960.

[16] G. Solomon and J. J. Stiffler. Algebraically punctured cyclic codes. *Information and Control*, 8:170–179, 1965.

[17] Zsuzsa Weiner. On (k, p^e)-arcs in Desarguesian planes. *Finite Fields Appl.*, 10(3):390–404, 2004.