Abstract

Given any linear code C over a finite field $GF(q)$ we show how C can be described in a transparent and geometrical way by using the associated Bruen-Silverman code.

Then, specializing to the case of MDS codes we use our new approach to offer improvements to the main results currently available concerning MDS extensions of linear MDS codes. We also sharply limit the possibilities for constructing long non-linear MDS codes. Our proofs make use of the connection between the work of Rédei [18] and the Rédei blocking sets that was first pointed out over thirty years ago in [9]. The main results of this paper significantly strengthen those in [5],[11].

Maximum Distance Separable Codes and Arcs in Projective Spaces

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

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

R. Silverman
Mathematics
Wright State University
Dayton, OH
45431
U.S.A.
robert.silverman@wright.edu

1 Introduction

Maximum distance separable codes (MDS codes) are at the heart of combinatorics and finite geometries. In their book [16] MacWilliams and Sloane describe MDS codes as "one of the most fascinating chapters in all of coding theory". These codes can be linear or non-linear. We define them as follows.

Definition 1.1. An (n, k, q)-MDS code C is a collection of q^k n-tuples (or code words) over an alphabet $\mathcal{A}$ of size q satisfying the following condition: No two words of C agree in as many as k coordinate positions.

In the special case that $\mathcal{A} = GF(q)$ the finite field of order q and C is a linear vector space of dimension k and length n, we say that C is a *linear* (n, k, q)-MDS code. These linear MDS codes are fundamental in error correction. In part this is due to the fact that they are precisely the linear codes meeting the Singleton bound (see [8]) which states that

*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

the minimum Hamming distance d of a linear (n, k, q)-MDS code satisfies $d = n - k + 1$. In particular, a class of these MDS codes, the so-called Reed-Solomon codes, are a mainstay of modern industrial applications. Geometrically, these Reed-Solomon codes are precisely the normal rational curves. Fundamental new algorithmic results on decoding Reed-Solomon codes are described in the work of Madhu Sudan, the winner of the 2002 Nevanlinna Prize (see [29]). Concerning the possible applications of error correction we should also mention the important recent results of Calderbank and Shor [12] relating to the emerging area of quantum error correcting codes.

The following combinatorial result is shown in [21, 17].

Lemma 1.2. *Let C be an (n, k, q)-MDS code over the alphabet $\mathcal{A}$.*

(a) Fix any t coordinate positions $a_1 < a_2 < \cdots < a_t$, $t \leq k$, and choose $\alpha_1, \alpha_2, \ldots, \alpha_t \in \mathcal{A}$ (not necessarily distinct). Then there are exactly q^{k-t} code words in C such that the entry in position a_i equals α_i, $1 \leq i \leq t$.

(b) Fix $\alpha \in \mathcal{A}$ and fix some coordinate position j. Let C_1 denote the set of all code words in C having α in position j. Then by deleting the j'th coordinate position from C_1 we obtain an $(n-1, k-1, q)$-MDS code.

(c) If q is even then $n \leq q + k - 1$, if q is odd and $k > 2$ then $n \leq q + k - 2$.

The existence question for codes meeting the combinatorial bound in Lemma 1.2 (c) is largely an open one. For $k = 2$ we have $n \leq q + 1$, with $n = q + 1$ if and only if there exists an affine plane of order q. Such planes exist if q is a prime power. Whether or not this condition is necessary (i.e. " the prime power conjecture") has been one of the most important and outstanding open questions in finite geometries for over 50 years, since the publication of the Bruck-Ryser theorem. For $k = 3$, equality is also possible.

For $k = 4$ the only known result is that in the case of equality, 36 divides q [10], (so that q could not be a prime power in this case). From the results of [1] it follows that for $k \geq 4$, if q is even and 36 does not divide q then $n \leq q + k - 3$.

In searching for "long" MDS codes a natural approach is to begin with a fixed code C and attempt to "lengthen" the code, while preserving the MDS property.

Definition 1.3. Let C be an (n, k, q)-MDS code. A code C' is said to be an *extension* of C if C' is an (m, k, q)-MDS code where $m > n$ and upon deleting some fixed set of $m - n$ coordinate positions from each word of C' the code C is obtained. Equivalently, C is said to be *extendable* (to the code C'). An MDS code is said to be *maximal* if it admits no extensions.

The following is an immediate consequence of Lemma 1.2 *(b)*.

Lemma 1.4. *An (n, k, q)-MDS code C is extendable to an $(n+1, k, q)$-MDS code if and only if there exists a partition $\mathcal{P} = \{C_1, C_2, \ldots, C_q\}$ of C such that each C_i is an $(n, k-1, q)$-MDS code.*

Definition 1.5. An *n-arc* $\mathcal{K}$ in $PG(k,q)$ is a collection of $n \geq k+1$ points no $k+1$ of which are incident with a common hyperplane. A *dual n-arc* in $PG(k,q)$ is a collection of $n \geq k+1$ hyperplanes no $k+1$ of which are incident with a common point.

Suppose C is a linear (n,k,q)-MDS code (so $\mathcal{A} = GF(q)$) and choose a generator matrix G for C of size $k \times n$. The MDS property of C is equivalent to the condition that every collection of k columns of G is linearly independent (see [8]). As observed by B. Segre one can multiply the columns of G by nonzero scalars and still preserve the MDS property. The columns of G can therefore be regarded as points (or, by duality, as hyperplanes) belonging to an n-arc in $PG(k-1,q)$. *Hence any results on linear MDS codes can be translated to an equivalent theorem on arcs.* A *normal rational curve* in $PG(k,q)$, $2 \leq k \leq q-2$ is a $(q+1)$-arc projectively equivalent to the $(q+1)$-arc $\{(1,t,\ldots,t^k) \mid t \in GF(q)\} \cup \{(0,\ldots,0,1)\}$. The n-arcs which are subsets of normal rational curves correspond to *generalized Reed-Solomon* (GRS) codes. Linear $(q+1,k,q)$-MDS codes are therefore easily constructed.

Denote by $m(k,q)$ 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 [5, 11, 13, 26, 19]). The Main Conjecture for linear MDS codes, always taking $q > k$, is the following:

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

The Main Conjecture has not been proved in general. It has been verified in many cases. In their paper [11] Bruen, Thas, and Blokhuis show it to hold at least asymptotically. The existence and possible structure of long MDS codes was a central theme in the address of J.A. Thas to the International Congress of Mathematicians in 1998 [26]. The question of the existence of MDS codes meeting the combinatorial bound remains largely an open one. In his engineering textbook, ([28], page 193), Wicker describes the analogous question for arcs as "one of the more interesting problems in projective geometry over Galois fields".

Consider a linear (n,k,q)-MDS code C over $\mathcal{F} = GF(q)$ with associated 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. In order to consider general (not necessarily linear) extensions of C we let M be a $q^k \times n$ array whose rows are precisely the words of C. This is called the *matrix form* of C. A general extension of C 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 an extension of C grows exponentially when one considers general as well as linear extensions.

Our main result (Theorem 6.6) shows that linear MDS codes of reasonable length do not admit non-linear extensions. In particular this gives a strengthening of results in the two papers mentioned above. Consequently, in the search for MDS codes close to the combinatorial bound, the approach of extending long linear codes in a non-linear fashion is fruitless. Moreover, by results such as those of Bruen, Thas and Blokhuis [11], there are many linear MDS codes of reasonable length that admit no linear extensions. Now we can show that these codes admit no extensions whatsoever.

2 2-Dimensional MDS Codes, Bruck Nets

A *Bruck net* (see [8]) $\mathcal{N}$ is a finite incidence structure of points and certain subsets of points called lines satisfying the following axioms.

(a) Any two points are contained in (lie on) at most one line.

(b) Given a line ℓ and point P off ℓ, there is a unique line through P failing to meet ℓ.

(c) There exists a triangle in $\mathcal{N}$ i.e. a set of three non-collinear points A, B, C such that the point pairs AB, AC, and BC are joined in $\mathcal{N}$.

Let us suppose that some line of $\mathcal{N}$ contains exactly q points. Then all lines of $\mathcal{N}$ contain exactly q points and q is called the *order* of $\mathcal{N}$. From axiom (b) it follows that the lines of $\mathcal{N}$ fall into n *parallel classes*. Each parallel class has exactly q lines no two of which meet. Two lines from distinct parallel classes meet in a unique point. The total number of points in $\mathcal{N}$ is q^2 and the total number of lines is nq. The parameter n is called the *degree* of $\mathcal{N}$. To extend a net $\mathcal{N}$ is to append one or more parallel classes of lines (thereby increasing the degree). It can be shown that $n \leq q+1$ with equality if and only if $\mathcal{N}$ consists of the points and lines of an affine plane of order q. In particular, a net of order q and degree $q+1$ can not be extended.

Lemma 2.1. *A Bruck net of order q and degree n is equivalent to a $(n, 2, q)$-MDS code.*

This is shown in [8]. Briefly, each of the q^2 points P of $\mathcal{N}$ give a code word as follows. Label the n parallel classes of $\mathcal{N}$ as $\{1, 2, \ldots, n\}$ where $n \geq 3$. Within each parallel class, label the lines from $\{1, 2, \ldots, q\}$. If the point P lies on the line α_i from parallel class number i, $1 \leq i \leq n$, we associate with P the code word $(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Two points are joined in the net if and only if the corresponding code words share a common entry.

Each coordinate of an $(n, 2, q)$-MDS code corresponds to a parallel class of lines in the related net and so we have a natural correspondence between extending the code and extending the net.

3 Linear Codes, BRS Codes

In the sequel we need to discuss equivalence of codes. Let C_1 and C_2 be codes of length n over an alphabet $\mathcal{A}$. Identify each code with a matrix, the rows of each matrix being the code words. Then C_2 is said to be *equivalent* to C_1 if C_2 can be obtained from C_1 by a sequence of operations of the following three types:

1. A permutation of the rows of C_1 ;
2. A permutation of the columns of C_1 ;
3. A permutation of the alphabet $\mathcal{A}$ is applied (entry-wise) to a column of C.

If two codes are equivalent then corresponding parameters such as minimum distance are equal, so the codes are essentially identical. A code that is equivalent to a linear code is referred to as a code of *type LE*, or an *LE code*. An LE code 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 and will therefore not be linear.

Let C be any linear code of length n and dimension k over the finite field $\mathcal{F} = GF(q)$. Associated with C is a $k \times n$ generator matrix G of rank k over $\mathcal{F}$. Each vector of C is a linear combination of the rows of G. Denote the entries of G as follows.

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

Then a code word w of C can be written as

$$w = \sum_{i=1}^{k} \alpha_i R_i \tag{3.1}$$

where R_i denotes the i^{th} row of G.

We want to get a better geometrical picture of C. This can be done as follows.

Associate with C a projective space $\Sigma = PG(k, q)$ having homogeneous coordinates $(x_1, x_2, \ldots, x_{k+1})$. Assume the hyperplane at infinity Σ_∞ has equation $x_{k+1} = 0$. So Σ_∞ has projective dimension $k-1$. Each column in G, say the i^{th} column, gives rise to a hyperplane Π_i in Σ_∞. The subspace Π_i of projective dimension $k-2$ is defined to be the solution set of the following system of equations:

$$\begin{cases} x_{k+1} = 0, \\ a_{1i}x_1 + a_{2i}x_2 + \cdots a_{ki}x_k = 0. \end{cases}$$

Let $E = \Sigma \setminus \Sigma_\infty$ denote the associated affine (or vector) space of dimension k. Thus E has q^k points or vectors. Each point P in E has homogeneous coordinates $(\alpha_1, \alpha_2, \ldots, \alpha_k, 1)$. We wish to associate with P a code word $(\lambda_1, \lambda_2, \ldots, \lambda_n)$. We have that P lies on a certain hyperplane labelled $H_i(P)$ containing the subspace Π_i for each i, $1 \leq i \leq n$. If we label the q hyperplanes of Σ other than Σ_∞ containing Π_i, then P will lie on say the hyperplane labelled λ_i. In this way we will end up with a code C_1 consisting of q^k code words $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ of length n over $\mathcal{F}$. The code C_1 will be a *Bruen-Silverman (BRS) code* associated with C.

Note that the construction of C_1 is analogous to the construction of the MDS code associated with a Bruck net in the previous section. The idea of a BRS type construction was first introduced in [10]. The BRS construction was first introduced in [2].

The code C_1 will depend on the labelling of $H_i(P)$. To fix coordinates, let us proceed in the following way. Assume that the point $U = (0, 1, 0, \ldots, 0)$ is not contained in any of the subspaces Π_i, $1 \leq i \leq n$. It follows that in G, a_{2i} is nonzero $1 \leq i \leq n$. Multiplying any column of G by a nonzero constant yields a generator matrix for a code equivalent to C.

Hence, we may assume $a_{2i} = 1$, $1 \leq i \leq n$. Let V denote the point $(0, 0, \ldots, 0, 1)$ so that V is a point of E. Then any point of E on the line $\ell = UV$ has coordinates $(0, \gamma, 0, \ldots, 0, 1)$. Let $P = (\alpha_1, \alpha_2, \ldots, \alpha_k, 1)$ be an affine point. The hyperplane $H_i(P)$ containing P and Π_i meets ℓ in a point $(0, \gamma_i, 0, \ldots, 0, 1)$ and γ_i gives the i^{th} coordinate entry of the code word $(\gamma_1, \gamma_2, \ldots, \gamma_n)$ in C associated with the point P.

Let us calculate γ_i. Any hyperplane other than Σ_∞ containing Π_i has an equation of the form

$$a_{1i}x_1 + a_{2i}x_2 + \cdots + a_{ki}x_k + bx_{k+1} = 0 \tag{3.2}$$

If the hyperplane contains $P = (\alpha_1, \alpha_2, \ldots, \alpha_k, 1)$ then we have

$$a_{1i}\alpha_1 + a_{2i}\alpha_2 + \cdots + a_{ki}\alpha_k + b = 0$$

which gives

$$b = -\left(a_{1i}\alpha_1 + a_{2i}\alpha_2 + \cdots + a_{ki}\alpha_k\right) \tag{3.3}$$

The hyperplane given by (3.2) meets the line ℓ in the point $(0, \gamma_i, 0, \ldots, 0, 1)$ so that $\gamma_i a_{2i} + b = 0$. Since we have $a_{2i} = 1$ we get

$$\gamma_i = -b = a_{1i}\alpha_1 + a_{2i}\alpha_2 + \cdots + a_{ki}\alpha_k$$

But then the code word of C_1 associated with P is precisely the code word of C in (3.1) associated with the coefficients $\alpha_1, \alpha_2, \ldots, \alpha_k$. We have shown the following.

Theorem 3.1. *The code C_1 is identical to the original code C. In particular C_1 is linear.*

To summarize, we now have a completely new way of looking at the original code C, as follows. We can identify a code word w in C with the set of coefficients $\alpha_1, \alpha_2, \ldots, \alpha_k$ as in formula 3.1. Alternatively, the code word can be thought of as a point $P = (\alpha_1, \alpha_2, \ldots, \alpha_k, 1)$ in an affine space. To find the i^{th} coordinate of w, given P, we calculate the label of the unique hyperplane H_i of Σ (the underlying projective space) containing Π_i and P (using ℓ) as above. Here Π_i is a subspace of Σ of codimension 2 corresponding to the i^{th} column of G, the generator matrix of C.

The power of this new approach will be demonstrated in section 5. From this picture it is clear that the set of code words with a given symbol in the i^{th} coordinate position corresponds to the points of E contained in a certain hyperplane H_i of Σ. The code words with given symbols in two fixed positions i and j correspond to the intersection $H_i \cap H_j$ of two hyperplanes, and so on. Hence, two code words w_1 and w_2 corresponding to the affine points P and Q will have t common entries if and only if the line PQ intersects Σ_∞ in a point belonging to t of the Π_i's.

In what follows we will need the following concept.

Definition 3.2. Let $\mathcal{K}$ be a dual arc in $\Pi = PG(k, q)$, $k \geq 2$ and let $\Sigma = PG(k+1, q)$. A point set S in $\Sigma - \Pi$ is called a *transversal set* of $\mathcal{K}$ if every line of Σ on a k-fold point of $\mathcal{K}$ intersects S in at most one point. Here, a k-fold point of $\mathcal{K}$ is a point incident with precisely k members of $\mathcal{K}$.

In the special case that the columns of G correspond to a dual arc we see that a transversal set corresponds to a collection of code words, no two of which agree in as many as k coordinates.

4 Primitive Sets, Slope Sets, Directions

Let π be any projective plane of order q say and let ℓ be a line of π. Let S be a set of points of π not on ℓ, so $S \subset \pi \setminus \{\ell\}$. The *Rédei set* of S with respect to ℓ, denoted by $R_\ell(S)$, is defined to be the set of all points of the form $PQ \cap \ell$, where P and Q are distinct points of S and PQ denotes the line joining them.

Definition 4.1. Let π, ℓ and S be as above with $|S| = q$. Let A be a subset of the points of ℓ. Then A is said to be *primitive* if whenever $R_\ell(S) \subset A$, the set S must be contained in a line of π.

Theorem 4.2. *Let π be a projective plane of order q (not necessarily a prime power) with a distinguished line l_∞. Let A be a subset of l_∞ and S a set of q points of $\pi \setminus \{l_\infty\}$ with the following property. The line joining any two points of S intersects l_∞ within A i.e. $R_\ell(S) \subset A$. If $|A| < \sqrt{q} + 1$, then S is a subset of a line of π.*

Proof. See: [6], [7] and [9]. The result is also implicit in earlier work of R.H. Bruck and T.G. Ostrom. □

Corollary 4.3. *Let π be a projective plane of order q with a distinguished line l_∞. Let A be a subset of l_∞. If $|A| < \sqrt{q} + 1$, then A is primitive.*

Theorem 4.4. *Let $\pi = PG(2, p)$, p a prime with a distinguished line ℓ at infinity. Let S be a set of p affine points and let $A \subset \ell$ with $R_\ell(S) \subset A$. Then if $|A| < (p+3)/2$, S is a subset of a line of π.*

Proof. See: [15]. □

Definition 4.5. For q a prime power we denote by $\mathcal{P}(q)$ the size of the smallest non-primitive set of (collinear) points in $PG(2, q)$.

Theorem 4.6. *Let $\pi = PG(2, q)$ with a distinguished line l_∞. Let $q = p^h$, p a prime and let $t < h$ be maximal such that t divides h. Let S be a set of q affine points and let $A \subset \ell$ with $R_\ell(S) \subset A$. Then if $|A| < p^{t-h} + 1$, S is a subset of a line of π.*

Proof. See: [4],[3]. □

From Theorems 4.4 and 4.6 we get the following.

Corollary 4.7. *Let $\pi = PG(2, q)$ where $q = p^h$, p prime, and let $t < h$ be maximal such that t divides h. Let A be a set of points on a line ℓ. If $|A| < \epsilon$ where*

$$\epsilon = \begin{cases} \frac{1}{2}(q+3) & h = 1 \\ p^{h-t} + 1 & \textit{otherwise.} \end{cases} \tag{4.1}$$

then A is primitive. In particular we have

$$\mathcal{P}(q) \geq \begin{cases} \frac{1}{2}(q+3) & h=1 \\ p^{h-t}+1 & \textit{otherwise} \end{cases}$$

Let $\pi = PG(2,q)$ with a distinguished line ℓ and let S be a set of q points in $\pi \setminus \{\ell\}$. If the points of S do not determine all directions (i.e. if $R_\ell(S) \subsetneq \ell$) then S may be regarded as a function on $GF(q)$. (Briefly, let $\mathcal{L}$ be the set of all lines incident with at least two points of S. By assumption there exists a point $Q \in \ell$ not incident with any line of $\mathcal{L}$. Assign homogeneous coordinates (x_1, x_2, x_3) in such a way that ℓ is given by $x_3 = 0$ and $Q = (0,1,0)$. Then $S = \{(a_i, b_i, 1) \,|\, i = 1 \ldots q\}$ yields a function $f(x)$ where $f(a_i) = b_i$.) Conversely, any function can be regarded as such a set S. Associated with a function f is the corresponding Rédei set $\mathcal{R}$ where

$$\mathcal{R} = \left\{ \frac{f(a_i) - f(a_j)}{a_i - a_j} \;\middle|\; i \neq j \right\} \tag{4.2}$$

Thus, according to the Definition 4.1 we have the following lemma.

Lemma 4.8. *Let $\pi = PG(2,q)$ with a distinguished line l_∞. Let A be a subset of l_∞. If the only functions for which A contains the associated Rédei set are linear functions, then A is primitive.*

Remark 4.9. We can also think of $\mathcal{R}$ as the slope set (including infinity) or the set of directions associated with f.

Using Theorems 4.4 and 4.6 we get the following.

Corollary 4.10. *Let $\pi = PG(2,q)$ with a distinguished line l_∞. Suppose $q = p^h$, p prime, and let $t < h$ be maximal such that t divides h. Let A be a subset of l_∞ contain the Rédei set of the function f. If $|A| < \epsilon$ where*

$$\epsilon = \begin{cases} \frac{1}{2}(q+3) & h=1 \\ p^{h-t}+1 & \textit{otherwise.} \end{cases} \tag{4.3}$$

then f is a linear function.

There is voluminous literature discussing Rédei sets beginning with [9]. We mention also [4], [3], and [23]. The case where the set is a group is discussed in [9].

Theorem 4.11. *Let ℓ be a line in $\pi = PG(2,q)$ containing the primitive set A. Embed π in $\Sigma = PG(3,q)$. Then A is primitive in each plane of Σ containing ℓ.*

Proof. Let π' be a plane of Σ containing ℓ. Suppose by way of contradiction that $S \subseteq \pi' \setminus \{\ell\}$ is a set of q points such that the line through any two points of S intersects ℓ in A and that S is not a subset of a line. Select any point P in $\Sigma \setminus \{\pi \cup \pi'\}$. Let ϕ be the projection through P mapping π' to π. Then ϕ is a collineation fixing ℓ. Hence $\phi(S)$ is not a subset of a line, yet any line on two points of $\phi(S)$ intersects ℓ within A. This contradicts the assumption that A is primitive in π. □

We generalize the property of being primitive to higher dimensions as follows. Let $\Sigma = PG(k,q)$ let Π be a hyperplane of Σ and let $E = \Sigma \setminus \Pi$ be the associated affine space. Let S be a set of points of E. The *Rédei set* of S with respect to Π, denoted by $R_\Pi(S)$, is defined to be the set of all points of the form $PQ \cap \Pi$, where $P, Q \in E$.

Definition 4.12. Let Σ, Π and S be as above with $|S| = q^{k-1}$ and let A be a subset of the points of Π. Then A is said to be *primitive* if whenever $R_\Pi(S) \subset A$, the set S must be contained in a hyperplane of Σ.

The proof of the following is entirely similar to that of Theorem 4.11.

Lemma 4.13. *Let Π be a hyperplane of $PG(k,q)$ containing the primitive set A. Embed $PG(k,q)$ in $\Sigma = PG(k+1,q)$. Then A is primitive in every hyperplane of Σ containing Π.*

5 Linear Three-Dimensional MDS Codes

Let C be a linear $(n,3,q)$-MDS code. The associated generator matrix G is of rank 3 over $\mathcal{F} = GF(q)$. Again, let $\Sigma = PG(3,q)$ be the underlying projective space of projective dimension 3 as described in section 3. The n columns of G give rise to a dual arc $\mathcal{K}$ in the plane at infinity, denoted here by Π. Thus $\mathcal{K} = \{\ell_1, \ell_2, \ldots, \ell_n\}$ is a set of n lines of Π with no three collinear. We want to examine the extensions of C to an MDS code.

A point of Π lying on exactly two lines of $\mathcal{K}$ is called a *secant point*. If the point lies on exactly one line of $\mathcal{K}$ then it is called a *tangent point*. We note that each line of $\mathcal{K}$ contains exactly $n-1$ secant points and $q+1-(n-1) = q-n+2$ tangent points.

Definition 5.1. Let $\mathcal{K}$ be a dual arc in the projective plane π. Let ℓ be a line of $\mathcal{K}$ and let A denote the set of tangent points of $\mathcal{K}$ on ℓ. Then ℓ is said to be *primitive with respect to* $\mathcal{K}$ (or, simply *primitive*) if A is a primitive set (in π).

If $\mathcal{K}$ is a dual arc and x is a line not in $\mathcal{K}$ such that $\mathcal{K} \cup \{x\}$ is a dual arc then x is said to *extend* $\mathcal{K}$, and x is an *extending line* of $\mathcal{K}$.

Lemma 5.2. *Let $\mathcal{K}$ be a dual n-arc in a projective plane of order q. If $n > q - \mathcal{P}(q) + 2$ then every line of $\mathcal{K}$ is primitive.*

Proof. Simply observe that each line of $\mathcal{K}$ is incident with precisely $q-n+2 < \mathcal{P}(q)$ tangent points. □

Recall, (Definition 3.2) that a set S in $\Sigma - \Pi$ is called a transversal set with respect to $\mathcal{K}$ if every line of Σ on a secant point of $\mathcal{K}$ intersects S in at most one point.

Theorem 5.3. *Let $\mathcal{K}$ be a dual n-arc in $\pi = PG(2,q)$ with $\pi \subset \Sigma = PG(3,q)$. Let $E = \Sigma - \pi$ be the associated affine space. Suppose S is a transversal set of $\mathcal{K}$ with $|S| = q^2$. Assume there exist two primitive lines in $\mathcal{K}$. Then S is a hyperplane of E. Moreover, if H is the hyperplane of Σ containing S, then $H \cap \pi$ is an extending line of $\mathcal{K}$.*

Proof. Let ℓ and ℓ' be primitive with respect to $\mathcal{K}$. Let $\{\pi_1, \pi_2, ...\pi_q\}$ be the pencil of planes other than π containing ℓ. Now $|S| = q^2$. Let $T = S \cap \pi_1$. We claim $|T| = q$. This follows since any of the q lines of π_1 other than ℓ on a secant point of $\mathcal{K}$ can meet T in at most one point. Thus, π_1 and indeed any of the planes π_i meet S in at most, and hence in exactly, q points. By the primitivity of ℓ, $\pi_i \cap S$ must be an affine line ℓ_i in π_i, $1 \leq i \leq q$. Let $m_1, m_2, \ldots, m_q$ be the corresponding projective lines, so that $m_i = \ell_i \cup P_i$ and $m_i \cap \ell = P_i$, $1 \leq i \leq q$, with P_i on ℓ.

(a) No two of the lines in $\{m_1, m_2, \ldots, m_q\}$ are skew. For suppose m_1 and m_2 are skew. Then through every point Q of π off ℓ, such as a secant point, there is a line meeting ℓ_1 and ℓ_2. This contradicts the fact that S is a transversal set. We conclude that the lines $m_1, m_2, \ldots, m_q$ pass through a fixed point P.

(b) We claim that all of the lines $m_1, m_2, \ldots, m_q$ lie in a plane. To see this, fix a plane $\psi \neq \pi$ through ℓ'. As above ψ meets S in a line (through say $P' \in \ell'$). Thus ψ meets each of $\ell_1, \ell_2, \ldots, \ell_q$ in collinear points $Q_1, Q_2, \ldots, Q_q$. Therefore, the lines $\ell_1, \ell_2, \ldots, \ell_q$ all lie in the plane γ containing P above and $Q_1, Q_2, \ldots, Q_q$. Thus, the points of S are the points of γ in E. Moreover, since S is a transversal set, γ meets π in an extending line of $\mathcal{K}$.

□

Remark 5.4. Associated with ℓ, ℓ' are points P, P' as above. We note that $P \neq P'$ since $\ell \cap \ell'$ is a 2-fold point of $\mathcal{K}$ and S is a transversal set of $\mathcal{K}$. Also, ℓ' is not on P.

Corollary 5.5. *Let $\mathcal{K}$ be a dual n-arc in $\pi = PG(2, q)$, let $\Sigma = PG(3, q)$ and $E = \Sigma - \pi$ be the associated affine space. Let S be a transversal set of $\mathcal{K}$ with $|S| = q^2$. Assume that $n > q + 2 - \mathcal{P}(q)$. Then S is a hyperplane of E. Moreover, if H is the hyperplane of Σ containing S, then $H \cap \pi$ is an extending line of $\mathcal{K}$.*

Proof. This follows immediately from Lemma 5.2 and Theorem 5.3. □

Theorem 5.6. *Let C be a linear $(n, 3, q)$-MDS code. Let $\mathcal{K}$ be a dual n-arc giving rise to C (as a BRS code). If $\mathcal{K}$ contains two primitive lines then any arbitrary $(n + 1, 3, q)$-MDS code extending C must be LE.*

Proof. As a BRS code, let C be constructed within $\Sigma = PG(3, q)$. Here π is the hyperplane (= plane) at infinity containing the dual n-arc $\mathcal{K}$, and $E = \Sigma - \pi$.

Let C' be an $(n + 1, 3, q)$-MDS code extending C. Then C' arises via a partition $\mathcal{P}$=$C_1, C_2, \ldots C_q$ of C where each C_i is an $(n, 2, q)$-MDS code (Lemma 1.4). The partition $\mathcal{P}$ corresponds to a partition $\mathcal{P}' = \{S_1, S_2, \ldots, S_q\}$ of E. Each S_i is a set of q^2 code words satisfying all conditions of S in Theorem 5.3. As such each S_i is a set of q^2 points lying in a plane π_i of Σ, $1 \leq i \leq q$. Let $\pi_i \cap \pi = \ell_i$. As in the proof of Theorem 5.3, each ℓ_i is an extending line of $\mathcal{K}$.
Now any two planes π_i, π_j of Σ meet in a line. Also, $\pi_i \cap E = S_i$ and $\pi_j \cap E = S_j$ are disjoint if $i \neq j$, $1 \leq i, j \leq q$. It follows that $\ell_1 = \ell_2 = \cdots = \ell_q = x$ and x is an extending line of $\mathcal{K}$. Moreover, (by re-labelling the $(n+1)^{th}$ coordinate of C' if necessary) C' is equivalent to the linear $(n + 1, 3, q)$-BRS code associated with the dual arc $\mathcal{K} \cup \{x\}$. □

With Lemma 5.2 and Theorem 5.6 we get the following.

Theorem 5.7. *Let C be a linear $(n,3,q)$-MDS code. If $n > q+2-\mathcal{P}(q)$ then any arbitrary $(n+1,3,q)$-MDS code C' extending C must be LE.*

Corollary 5.8. *Let C be a linear $(n,3,q)$-MDS code. Suppose $q=p^h$, p prime, and let $t<h$ be maximal such that t divides h. If $n>\beta$, where*

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

then any arbitrary $(n+1,3,q)$-MDS code C' extending C must be LE.

Let us discuss an easy application of this result. The following appears in [14] as Theorem 9.30.

Theorem 5.9. *In $PG(2,q)$, $q \equiv 3$ (mod 4), there exist maximal n-arcs with $n=\frac{1}{2}(q+5)$. Equivalently, for such q there exist linear $(\frac{1}{2}(q+5),3,q)$-MDS codes admitting no linear extensions.*

We can now state a stronger result for certain q by appealing to Corollary 5.8.

Lemma 5.10. *If $p \equiv 3$ (mod 4) is prime then maximal $(\frac{p+5}{2},3,p)$-MDS codes exist.*

6 Higher Dimensions

A dual n-arc $\mathcal{K}$ in $PG(k,q)$ is a collection $\{\Pi=\Pi_1,\Pi_2,\ldots,\Pi_n\}$, $n \geq k+1$, of hyperplanes such that no $k+1$ lie on a point, no k lie on a line,..., no 3 lie on a $(k-2)$-flat, and no 2 lie on a $(k-1)$-flat. Consequently, If we let $\Lambda_i = \Pi \cap \Pi_i$, $1<i\leq n$ then $\mathcal{K}'=\{\Lambda_1,\Lambda_2,\ldots,\Lambda_{n-1}\}$ is a dual $(n-1)$-arc in Π. In this sense we say the remaining members of $\mathcal{K}$ *cut out* a dual $(n-1)$-arc in Π.

Definition 6.1. Let $\mathcal{K}$ be a dual arc in $\Pi=PG(k,q)$,$k\geq 2$. Let Λ be a member of $\mathcal{K}$ and let B denote the set of k-fold points of $\mathcal{K}$. Then Λ is said to be *primitive* with respect to $\mathcal{K}$ (or, simply primitive) if the point set $A=\Lambda\setminus B$ is a primitive set.

Theorem 6.2. *Let $\mathcal{K}$ be a dual n-arc in $\Pi=PG(k,q)$, $k\geq 2$. Let $\Sigma=PG(k+1,q)$ and let S be a transversal set of $\mathcal{K}$ with $|S|=q^k$. If $\mathcal{K}$ contains two primitive members then S is a subset of a hyperplane $\mathcal{H}$ of Σ. Moreover, $\mathcal{H}\cap\Pi$ extends $\mathcal{K}$.*

Proof. Let Λ be a primitive member of $\mathcal{K}$. Let $\{\Pi_1,\Pi_2,\ldots,\Pi_q\}$ be the pencil of hyperplanes of Σ other than Π containing Λ. As in the proof of Theorem 5.3 Π_1, and indeed any of the hyperplanes Π_i meet S in exactly q^{k-1} points and (by the primitivity of Λ) $\Pi_i\cap S$ is an affine $(k-1)$-flat $\mathcal{L}_i$ in Π_i, $1\leq i\leq q$. Let $\mathcal{M}_1,\mathcal{M}_2,\ldots,\mathcal{M}_q$ be the corresponding projective $(k-1)$-spaces so that $\mathcal{M}_i\cap\Lambda=\lambda_i$ and $\mathcal{M}_i=\mathcal{L}_i\cup\lambda_i$, $1\leq i\leq q$.

We claim the λ_i's coincide. Indeed, suppose the point P is in $\{\lambda_1\}\setminus\{\lambda_2\}$ and consider a line ℓ in $\mathcal{M}_1$ where $\ell\cap\Pi=P$. In particular, ℓ and $\mathcal{M}_2$ are disjoint. Through each point Q in Π off Λ there is a unique line meeting both ℓ and $\mathcal{M}_2$ (necessarily in points of S). But

then, since S is a transversal set, Q can not be a k-fold point of $\mathcal{K}$. Thus, the $(k-1)$-spaces $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_q$ form a pencil on, say, λ, where $\lambda = \lambda_1 = \cdots = \lambda_q$.

We claim the $(k-1)$-spaces $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_q$ lie in a hyperplane of Σ. Briefly, suppose $\mathcal{M}_1$, $\mathcal{M}_2$, and $\mathcal{M}_3$ are not contained in a common hyperplane. Let Π_{12} be the unique hyperplane of Σ containing $\mathcal{M}_1$ and $\mathcal{M}_2$. Let $\Lambda' \neq \Lambda$ be a primitive member of $\mathcal{K}$. Choose a hyperplane Π' other than Π on Λ'. Denote by τ_i the $(k-2)$-flat $\mathcal{M}_i \cap \Pi'$, $1 \leq i \leq 3$. By assumption τ_3 is not contained in Π_{12}. By primitivity there is a $(k-1)$-flat H_1 in Π' containing τ_1, τ_2, and τ_3. Let $H_2 = \Pi' \cap \Pi_{12}$. As τ_1 and τ_2 are (disjoint) $(k-2)$-flats, at most one $(k-1)$-flat contains both. But then it follows that $H_1 = H_2$ so τ_3 is contained in Π_{12}. The second conclusion of the theorem is clear. □

Theorem 6.3. *Let $\mathcal{K}$ be a dual n-arc in $\Pi = PG(k,q)$, $k \geq 2$. If $n > q - \mathcal{P}(q) + k$ then every member of $\mathcal{K}$ is primitive.*

Proof. Our proof is inductive on k. The case $k = 2$ is given by Lemma 5.2. Assume the result to hold in $PG(k-1,q)$. Let $\mathcal{K}$ be a dual n-arc in $\Pi = PG(k,q), k > 2$ with $n > q - \mathcal{P}(q) + k$. Let B denote the set of all k-fold points of $\mathcal{K}$. Choose $\lambda \in \mathcal{K}$, let $A = \lambda \setminus B$ and suppose S is a collection of q^{k-1} points of $\Pi - \lambda$ such that any line on a point of B intersects S in at most one point (i.e. $R_\lambda(S) \subset A$). The remaining members of $\mathcal{K}$ cut out a dual $(n-1)$-arc $\mathcal{K}'$ in $\lambda = PG(k-1,q)$ so that in particular S is a transversal set of $\mathcal{K}'$. By the induction hypothesis, every member of $\mathcal{K}'$ is primitive. It follows (Theorem 6.2) that S is contained in a hyperplane of Π whence Λ is primitive. □

The proof of the following is entirely similar to that of Theorem 5.6.

Theorem 6.4. *Let C be a linear (n,k,q)-MDS code, $k \geq 3$. Let $\mathcal{K}$ be a dual n-arc giving rise to C (as a BRS code). If $\mathcal{K}$ contains two primitive members then any arbitrary $(n+1,k,q)$-MDS code extending C must be LE.*

The last two theorems give the following.

Theorem 6.5. *Let C be a linear (n,k,q)-MDS code. If $n > q - \mathcal{P}(q) + k$ then any arbitrary $(n+1,k,q)$-MDS code C' extending C must be LE.*

Corollary 6.6. *Let C be a linear (n,k,q)-MDS code. Suppose $q = p^h$, p prime, and let $t < h$ be maximal such that t divides h. If $n > \beta$, where*

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

then any arbitrary $(n+1,k,q)$-MDS code C' extending C must be LE.

7 Some Applications and Further Results

We summarize some existing results and our corresponding improvements.

7.1 Applications for q even

Theorem 7.1. *Let $\mathcal{K}$ be an n-arc in $PG(2,q)$, $n > \frac{q+2}{2}$ with q even. Then $\mathcal{K}$ is contained in a unique maximal arc.*

Proof. See: [22]. □

The following Theorem is found in [5] with a proof using results of algebraic geometry. For an inductive proof see [27].

Theorem 7.2. *Let $\mathcal{K}$ be an n-arc in $PG(k,q)$, $k \geq 2$ with q even. If $n > \frac{q}{2} + k - 1$. Then $\mathcal{K}$ is contained in a unique maximal arc.*

The above theorem together with Corollary 6.6 gives the following result.

Theorem 7.3. *Let C be a linear $(n, k+1, q)$-MDS code over $GF(q)$, $q = 2^h$. Let $t < h$ be maximal such that t divides h and suppose $n > q - 2^{h-t} + k - 1$. Let S be the collection of codes consisting of C and all extensions of C. Then*
(i) all members of S are LE;
(ii) there is (up to equivalence) a unique maximal code in S.

We now proceed to another application strengthening Theorem 7.4 below.

Theorem 7.4. *Let $\mathcal{K}$ be an n-arc in $PG(2,q)$ with $n > q - \sqrt{q} + 1$. Then $\mathcal{K}$ can be extended to a $(q+2)$-arc (a hyperoval) $\mathcal{K}'$ uniquely determined by $\mathcal{K}$.*
Equivalently, let C be a linear $(n, 3, q)$-MDS code over $GF(q)$ with $n > q - \sqrt{q} + 1$. Let S be the collection of codes consisting of C and all linear extensions of C. Then S contains a $(q+2, 3, q)$-MDS code C' and (up to equivalence) C' is the only maximal code in S.

Proof. See [20]. □

Corollary 6.6 can be used to strengthen Theorem 7.4 as follows.

Theorem 7.5. *Let C be a linear $(n, 3, q)$-MDS code, $n > q - \sqrt{q} + 1$ with q even. Then (up to equivalence) there is exactly one maximal extension C' of C. Moreover C' is an LE $(q+2, 3, q)$-MDS code.*

Next we improve Theorem 7.6 below.

Theorem 7.6. *Let $\mathcal{K}$ be a $(q+1)$-arc in $PG(k,q)$, q even, with either (a) $k = 3, 4$; or (b) $k \geq 5$ and $q \geq (k-2)^3$. Then $\mathcal{K}$ is complete.*
Equivalently, let C be a linear $(n, k+1, q)$-MDS code satisfying (a) or (b). Then C can not be extended to a linear $(q+2, k+1, q)$-MDS code.

Proof. For (a) see [13] and for (b) see [11] □

Corollary 6.6 strengthens the above to the following:

Theorem 7.7. *Let C be a linear $(q+1, k+1, q)$-MDS code with either (a) $k = 3, 4$; or (b) $k \geq 5$ and $q \geq (k-2)^3$. Then C is maximal.*

Theorem 7.8. *Let $\mathcal{K}$ be an n-arc in $PG(k,q)$ $k \geq 4$ and $n \geq q - \sqrt[3]{q} + k$. Then $\mathcal{K}$ lies in a normal rational curve uniquely determined by $\mathcal{K}$.*
Equivalently, let C be a linear $(n, k+1, q)$-MDS code over $GF(q)$ with $k \geq 4$ and $n \geq q - \sqrt[3]{q} + k$. Let S be the collection of codes consisting of C and all linear extensions of C. Then up to equivalence there is an unique maximal code C' in S. Moreover C' is (equivalent to) a GRS-code.

Proof. See [11]. □

Using Corollary 6.6 we have the following improvement to Theorem 7.8.

Theorem 7.9. *Let C be a linear $(n, k+1, q)$-MDS code over $GF(q)$ with $k \geq 4$ and $n \geq q - \sqrt[3]{q} + k$. Then up to equivalence there is an unique maximal extension C' of C. Moreover C' is (equivalent to) a GRS-code.*

7.2 Applications for q odd

Theorem 7.10. *Let $\mathcal{K}$ be an n-arc in $PG(2,q)$ with $n > \frac{2}{3}(q+2)$ and q odd. Then $\mathcal{K}$ is contained in a unique maximal arc.*

Proof. See: [22]. □

The following can be found in [5].

Theorem 7.11. *Let $\mathcal{K}$ be an n-arc in $PG(k,q)$, $k \geq 2$ with q odd. If $n > \frac{2}{3}(q-1)+k$. Then $\mathcal{K}$ is contained in a unique maximal arc.*
Equivalently, let C be a linear $(n, k+1, q)$-MDS code over $GF(q)$ with $n > \frac{2}{3}(q-1)+k$ and let S be the collection of codes consisting of C and all linear extensions of C. Then (up to equivalence) there is a unique maximal code in S.

Corollary 6.6 strengthens the above to the following in the case that q is prime.

Theorem 7.12. *For q an odd prime, let C be a linear $(n, k+1, q)$-MDS code over $GF(q)$ with $n > \frac{2}{3}(q-1)+k$. Let S be the collection of codes consisting of C and all extensions of C, then,*
(i) all members of S are LE;
(ii) there is (up to equivalence) a unique maximal code in S.

If q odd is not prime then $q \geq 9$, so n integral gives

$$n > q - \sqrt{q} + k - 1 \Rightarrow n > \frac{2}{3}(q-1) + k.$$

Hence, Theorem 7.11 and Corollary 6.6 give the following.

Theorem 7.13. *For q odd not a prime, let C be a linear $(n, k+1, q)$-MDS code over $GF(q)$. Let S be the set of codes consisting of C and all extensions of C. If $n > q - \sqrt{q} + k - 1$, then,*
(i) all members of S are LE;
(ii) there is (up to equivalence) a unique maximal code in S.

The previous result can be considerably improved in most cases by observing that if $q = p^h$ and $t < h$ with $p^t > 3$ then

$$n > q - p^{h-t} + k - 1 \Rightarrow n > \frac{2}{3}(q-1) + k.$$

Hence, Theorem 7.11 and Corollary 6.6 give the following.

Theorem 7.14. *Let C be a linear $(n, k+1, q)$-MDS code over $GF(q)$, where $q = p^h$ is odd. Let $t < h$ be maximal such that t divides h. Let S be the set of codes consisting of C and all extensions of C. If $p^t > 3$ and $n > q - p^{h-t} + k - 1$, then,*
(i) all members of S are LE;
(ii) there is (up to equivalence) a unique maximal code in S.

We now want to improve Theorem 7.15 below.

Theorem 7.15. *Let $\mathcal{K}$ be a dual $(q+1)$-arc in $PG(k, q)$, q odd, with either*
(a) $k = 2, 3$, or 4; or (b) $q > (4k - 23/4)^2$. Then $\mathcal{K}$ is complete.
Equivalently, let C be a linear $(q+1, k+1, q)$-MDS code satisfying (a) or (b) above, then C can not be extended to a linear $(q+2, k, q)$-MDS code.

Proof. For (a) see [19] and for (b) see [24, 25] □

Corollary 6.6, combined with Theorem 7.15 now gives the following improvement of Theorem 7.15.

Theorem 7.16. *Let C be a linear $(q+1, k+1, q)$-MDS code, q odd, with (a) $k = 2, 3$, or 4; or (b) $q > (4k - 23/4)^2$. Then C is maximal.*

Theorem 7.17. *Let $\mathcal{K}$ be a n-arc in $PG(k, q)$, q odd, with $n > q - \frac{1}{4}\sqrt{q} + k - \frac{7}{4}$ and either (a) $k = 2, 3$; or (b) $q > (4k - \frac{23}{4})^2$. Then $\mathcal{K}$ is contained in an unique (necessarily maximal) $(q+1)$-arc $\mathcal{K}'$. Moreover $\mathcal{K}'$ is the point set of a normal rational curve.*
Equivalently, let C be a linear $(n, k+1, q)$-MDS code over $GF(q)$ with $n > q - \frac{1}{4}\sqrt{q} + k - \frac{7}{4}$ and either (a) k=2,3; or (b) $q > (4k - \frac{23}{4})^2$. Let S be the collection of codes consisting of C and all linear extensions of C. Then S contains an unique maximal code C', moreover C' is (equivalent to) a GRS-code.

Proof. If $k = 2$ or 3 then every $q+1$ arc is the point set of a normal rational curve ([19, 20]). For any k, if $q > (4k - \frac{23}{4})^2$ then every $q+1$ arc is the point set of a normal rational curve ([24, 25]). For any k, if $n > q - \frac{1}{4}\sqrt{q} + k - \frac{7}{4}$ then $\mathcal{K}$ is contained in an unique normal rational curve ([24, 25]). □

Corollary 6.6 strengthens Theorem 7.17 as follows.

Theorem 7.18. *Let C be a linear $(n, k+1, q)$-MDS code over $GF(q)$ with q odd, $n > q - \frac{1}{4}\sqrt{q} + k - \frac{7}{4}$, and either (a) k=2,3; or (b) $q > (4k - \frac{23}{4})^2$. Then (up to equivalence) there is an unique maximal code C' extending C. Moreover, C' is (equivalent to) a GRS-code.*

References

[1] T. L. Alderson. Extending MDS codes. *Ann. Comb.*, 9(2):125–135, 2005.

[2] T.L. Alderson. On mds codes and bruen-silverman codes. *PhD. Thesis, University of Western Ontario*, 2002.

[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] 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.

[5] A. Blokhuis, A. A. Bruen, and J. A. Thas. Arcs in $\mathrm{PG}(n, q)$, MDS-codes and three fundamental problems of B. Segre—some extensions. *Geom. Dedicata*, 35(1-3):1–11, 1990.

[6] A. A. Bruen. Collineations and extensions of translation nets. *Math. Z.*, 145(3):243–249, 1975.

[7] A. A. Bruen. Nuclei of sets of $q + 1$ points in $\mathrm{PG}(2, q)$ and blocking sets of Redei type. *J. Combin. Theory Ser. A*, 55(1):130–132, 1990.

[8] A. A. Bruen and Mario A. Forcinito. *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.

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

[10] 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.

[11] A. A. Bruen, J. A. Thas, and A. Blokhuis. 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.

[12] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54:1098, 1996.

[13] Louis Reynolds Antoine Casse. 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.

[14] J. W. P. Hirschfeld. *Projective geometries over finite fields*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1998.

[15] L. Lovász and A. Schrijver. Remarks on a theorem of Rédei. *Studia Sci. Math. Hungar.*, 16(3-4):449–454, 1983.

[16] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. I.* North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[17] Carl Maneri and Robert Silverman. A vector-space packing problem. *J. Algebra*, 4:321–330, 1966.

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

[19] Beniamino Segre. Curve razionali normali e k-archi negli spazi finiti. *Ann. Mat. Pura Appl. (4)*, 39:357–379, 1955.

[20] Beniamino Segre. Introduction to Galois geometries. *Atti Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Natur. Sez. I (8)*, 8:133–236, 1967.

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

[22] T. Szőnyi. k-sets in $\mathrm{PG}(2, q)$ having a large set of internal nuclei. In *Combinatorics '88, Vol. 2 (Ravello, 1988)*, Res. Lecture Notes Math., pages 449–458. Mediterranean, Rende, 1991.

[23] Tamás Szőnyi. Around Rédei's theorem. *Discrete Math.*, 208/209:557–575, 1999. Combinatorics (Assisi, 1996).

[24] J. A. Thas. Normal rational curves and $(q + 2)$-arcs in a Galois space $S_{q-2,q}\,(q = 2^h)$. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8)*, 47:249–252 (1970), 1969.

[25] J. A. Thas. Complete arcs and algebraic curves in $\mathrm{PG}(2, q)$. *J. Algebra*, 106(2):451–464, 1987.

[26] Joseph A. Thas. Finite geometries, varieties and codes. In *Proceedings of the International Congress of Mathematicians, Vol. III (Berlin, 1998)*, number Extra Vol. III, pages 397–408 (electronic), 1998.

[27] F. Wettl. Internal nuclei of k-sets in finite projective spaces of three dimensions. In *Advances in finite geometries and designs (Chelwood Gate, 1990)*, Oxford Sci. Publ., pages 407–419. Oxford Univ. Press, New York, 1991.

[28] Stephen B. Wicker. *Error control systems for digital communication and storage.* Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1995.

[29] Avi Wigderson. On the work of madhu sudan. *Notices of the AMS*, pages 45–50, 2002.