(6,3)-MDS CODES OVER AN ALPHABET OF SIZE 4.

T.L. ALDERSON

Abstract. An $(n,k)_q$-*MDS code* C over an alphabet $\mathcal{A}$ (of size q) is a collection of q^k $n-$tuples over $\mathcal{A}$ such that no two words of C agree in as many as k coordinate positions. It follows that $n \leq q+k-1$. By elementary combinatorial means we show that every $(6,3)_4$-MDS code, linear or not, turns out to be a linear $(6,3)_4$-MDS code or else a code equivalent to a linear code with these parameters. It follows that every $(5,3)_4$-MDS code over $\mathcal{A}$ must also be equivalent to linear.

1. Introduction

A linear $[n,k]$-code of minimum distance d satisfies $d \leq n-k+1$–the Singleton bound [10]. A linear $[n,k]$-code meeting the Singleton bound is called a *linear Maximum Distance Separable*, or MDS code. Analogously, when no assumptions regarding linearity are made, an (n,k)-*MDS code* C over an alphabet $\mathcal{A}$ of size q (an $(n,k)_q$-MDS code) is a collection of q^k $n-$tuples over $\mathcal{A}$ such that no two words of C agree in as many as k coordinate positions. It follows that $n \leq q+k-1$ (with equality only if q is even). Such codes, when they exist may or may not be linear. Linear MDS codes are much studied in the mathematical and engineering sciences (see [5], [10], or [13]). Under the rubric of MDS codes there are many open questions. In particular, very little is known in the nonlinear case.

In this short note we are concerned with the structure of an arbitrary $(6,3)_4$-MDS code C. If C is in fact known to be linear, the structure of C is easily described as follows. We choose a basis for C as rows of a 3×6 matrix G over $GF(4)$ of rank 3. The MDS condition implies that in fact every set of 3 columns of G are linearly

1991 *Mathematics Subject Classification.* 94B25,51E14.

Key words and phrases. MDS Code, Bruen-Silverman Code, dual arc.

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

independent. Thus, if we regard the columns of G as points of $PG(2,4)$, we see that G is nothing more than an hyperoval in $PG(2,4)$. Conversely, any hyperoval in $PG(2,4)$ gives such a matrix (for more see [9]).

Let us proceed now to the general case. Our main result will be that any $(6,3)_4$-MDS code C is either linear or equivalent to linear. Specifically we show C to be a so called BRS (Bruen-Silverman) code as explained below. In [1], the author showed that such BRS codes are equivalent to linear–we need only the 3 dimensional case but the result holds in general. From a result in [2] it follows that every $(5,3)_4$-MDS code must also be equivalent to linear. We believe this to be a new result.

There is extensive literature on the structures relating to $PG(2,4)$ such as the hexacode, the mathieu designs etc. It is conceivable that our main result could be deduced by using this kind of machinery although we have not succeeded in doing so. Nor have we been able to locate a specific reference in the literature. Our main goal here was to construct a proof both elementary and self contained. It may transpire that the methods used in this paper are as interesting as the results. This is because it seems likely the methods can be extended to MDS codes of length 2^t+2 but our investigations are not yet complete.

In [11] R. Silverman discusses these general, not necessarily linear, $(n,k)_q$-MDS codes. Among the results in [11] are the following.

Lemma 1.1. *Let C be an $(n,k)_q$-MDS code over an alphabet $\mathcal{A}$. Fix any k coordinate positions. Then every $k-$tuple over $\mathcal{A}$ will occur exactly once in the fixed coordinate positions as we range over the words of C.*

Lemma 1.2. *Let C be an $(n,k)_q$-MDS code with $n=q+k-1$ (so the words of C have maximal length). Then any two words of C having $k-2$ common entries have $k-1$ common entries. In other words, if u and v are words of C and $d(u,v)\leq q+1$ then $d(u,v)=q$.*

We use the classical definition of equivalence of codes (see [12]).

Definition 1.3. Let C be a code of length n over an alphabet $\mathcal{A}$ of size q, let π be a permutation of the symbols in $\mathcal{A}$ and let π' be a permutation on n letters. We define two types of operations on the words of C.

(1) *positional permutation*: For each word $w = (w_1, w_2, \dots, w_n)$ of C, apply the transformation: $\pi' : w \mapsto w'$ defined by $w'_i = w_{\pi'(i)}$

(2) *symbol permutation*: Fix j. For each word $w = (w_1, w_2, \dots, w_n)$ of C, apply the transformation: $\pi' : w \mapsto w'$ defined by $w'_i = w_i \; i \neq j$, and $w'_j = \pi(w_j)$

If a code C' can be obtained from a code C by a sequence of positional or symbol permutations then C' and C are said to be *equivalent*. If C' is linear then C is said to be *equivalent to linear*.

2. The Incidence Structures $\mathcal{S}$ and $\mathcal{S}'$

An important construct shall be the following incidence structure.

Definition 2.1. Let C be a $(q+2, 3)_q$-MDS code and define the incidence structure $\mathcal{S}$ by:

Points of $\mathcal{S}$: The words of C.

Lines of $\mathcal{S}$: All words in C with fixed entries in two fixed positions.

Planes of $\mathcal{S}$: All words in C with a fixed entry in a fixed position.

By counting it can be easily shown [1] that $\mathcal{S}$ satisfies the following:

(1) Each line of $\mathcal{S}$ contains q points.

(2) Each plane of $\mathcal{S}$ contains q^2 points.

(3) The planes of $\mathcal{S}$ are divided into $q+2$ parallel classes, and each parallel class partitions the points of C.

(4) Any two planes from distinct parallel classes meet in a unique line.

(5) Any three planes from distinct parallel classes meet in a unique point.

(6) Each plane of $\mathcal{S}$ is an affine plane of order q.

We refer to the same objects as both *points* and *words* with the context being apparent. Two words are *joined* (resp. *unjoined*) if they have two (resp. no) common coordinates. Note that according to Lemma 1.2 any two words of C are either joined or unjoined.

Lemma 2.2. *Given a point P and a line l in $\mathcal{S}$, either P and l are coplanar (so P is joined to each point of l), or P is joined to exactly $\frac{q}{2}$ points of l.*

Proof. Assume P and l are not coplanar. Let $P = (a_1, a_2, \ldots, a_{q+2})$ and let l be the words in C of the form $(b_1, b_2, \_, \_, \_, \_)$ where $b_1 \neq a_1$ and $b_2 \neq a_2$ are fixed. For each i, $3 \leq i \leq q+2$, there is a unique word of C with first entry b_1, second entry b_2 and i'th entry a_i (Lemma 1.1). By Lemma 1.2 these words coincide in pairs, so exactly $\frac{q}{2}$ words of l are joined to P. □

Definition 2.3. Denote by $\Sigma_1, \Sigma_2, \ldots, \Sigma_q$ the parallel class of planes of $\mathcal{S}$ defined by the first coordinate where Σ_i consists of all words of the form (i, _, _, _, _, _).

Our aim is to give an embedding of $\mathcal{S}$ into $AG(3,q)$. To this end we augment $\mathcal{S}$ with new planes, $q-1$ through each line of $\mathcal{S}$. We detail the construction:

Definition 2.4 (New Plane)**.** Fix t. Let ℓ be a line of Σ_t and choose a point P not coplanar with ℓ. We define a new plane containing P and ℓ as follows. Let Q be one of the $\frac{q}{2}$ points of ℓ joined to P. The parallel class $[\ell]$ in Σ_t is determined by the intersection of Σ_t with each member of a parallel class of planes, $\Pi_1, \Pi_2, \Pi_3, \ldots, \Pi_q$, in $\mathcal{S}$. Denote by l_{ij} the line $\Sigma_i \cap \Pi_j$ and by $[l_{ij}]$ the parallel class of l_{ij} in Σ_i, $1 \leq i, j, \leq q$. Exactly q of the l_{ij}'s meet the line PQ (one of which is ℓ). The points of these q lines form a *new plane* on P and ℓ.

A natural question is whether these "new planes" are well defined. For general values of q an affirmative proof seems quite elusive. However, by restricting to an alphabet of size 4 the task becomes a manageable one.

For the remainder C shall denote a $(6,3)_4$-MDS code over $\mathcal{A} = \{1,2,3,4\}$. Let $\Pi_1, \Pi_2, \Pi_3, \Pi_4$ be the parallel class of planes based on position two, where each word of Π_i has second entry i. As above, $l_{ij} = \Sigma_i \cap \Pi_j$ and $[l_{ij}]$ is the parallel class of l_{ij} in Σ_i. Let $P_1 \in l_{11}$ be collinear with $P_2 \in l_{22}$ and let Π be the new plane on P_1 and l_{22} determined via P_1P_2. By Lemma 2.2, P_1 is joined to a second point, P_2'

of l_{22}. Let Π' be the new plane on P_1 and l_{22} determined via the line P_1P_2' (see Figure 1). To show the new planes are well defined it suffices to show $\Pi = \Pi'$.

Let $P_1 = (1, 1, a, b, c, d)$. P_2 and P_2' agree in the first two coordinate positions and hence have no further common entries. As such, we may assume the line P_1P_2 to consist of all words of the form $(\_, \_, a, b, \_, \_)$ and the line P_1P_2' to consist of all words of the form $(\_, \_, \_, \_, c, d)$. Let $P_3 = P_1P_2 \cap \Sigma_3$ and $P_3' = P_1P_2' \cap \Sigma_3$. P_3 and P_3' have a common first coordinate and (Lemma 2.2) must therefore have a second entry in common. Agreement in a further position other than the second would force three common entries with P_1, contradicting the MDS property of the code. Therefore $P_3P_3' \in [l_{33}]$ and so $\Pi \cap \Sigma_3 = \Pi' \cap \Sigma_3$. A similar argument shows $\Pi \cap \Sigma_4 = \Pi' \cap \Sigma_4$. Therefore $\Pi = \Pi'$ and we conclude that the new planes are well defined.

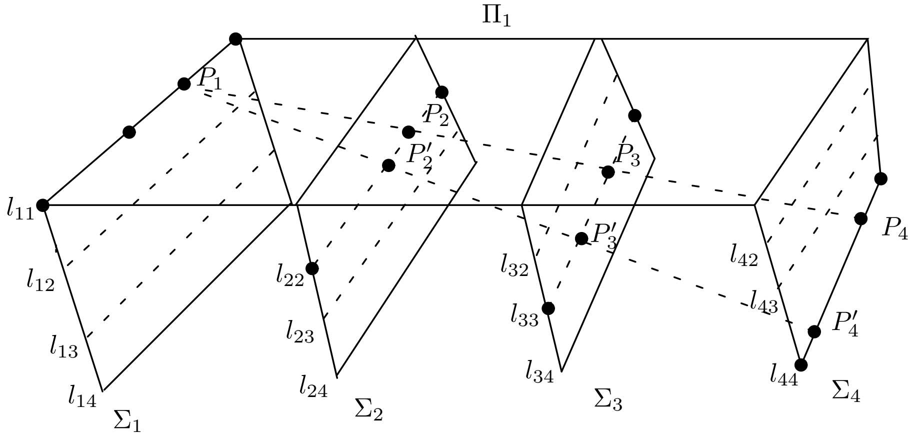

FIGURE 1. Constructing a new plane (the 16 dots).

We claim that no new plane other than Π contains both P_1 and l_{22}. Any such plane contains the line l_{11}. Let $Q_1 = (1, 1, e, f, g, h) \in l_{11}$ and let Π_Q be the new plane determined by Q_1 and l_{22}. We will have proved our claim upon showing $\Pi_Q = \Pi$. To this end, let $Q_2 \in l_{22}$ be collinear with Q_1 where Q_3 and Q_4 are the points of Q_1Q_2 on Σ_3 and Σ_4 respectively. We claim the coordinate positions defining Q_1Q_2 and those defining P_1P_2 are either disjoint, and therefore constitute positions three through six, or are equal. Suppose by way of contradiction that the positions overlap and constitute say entries 3, 4, and 5 then all words on P_1P_2 have the form $(\_,\_,a,b,\_,\_)$ while those on Q_1Q_2 have the form $(\_,\_,\_,f,g,\_)$. $P_1, Q_1 \in l_{11}$ so $b \neq f$ and $Q_2 \neq P_2$. In C there is a unique word of the form $W = (\_,\_,a,f,g,\_)$. Neither of the first two entries of W are from the set $\{1,2\}$ else W is distinct from yet shares three common entries with one of Q_1 or Q_2. W has the same third entry as P_1 and P_2 and so W, P_1 and P_2 agree in the last coordinate. But then P_1 and P_2 have three common entries contradicting $P_1 \neq P_2$. This proves the claim. Assume with no loss of generality that any word from P_1P_2 has the form $(\_,\_,a,b,\_,\_)$ whereas a word from Q_1Q_2 has the form $(\_,\_,\_,\_,g,h)$. As there is at most one word in C of the form $(\_,\_,a,b,g,h)$ we may assume (perhaps after applying a suitable symbol permutation) that $Q_2 \neq P_2$. In C there are words $V_1 = (x_1,x_2,a,b,g,x_3)$ and $V_2 = (y_1,y_2,a,b,y_3,h)$ where $\{x_1,x_2,y_1,y_2\} \cap \{1,2\} = \{\emptyset\}$ (else one of the V_i's has three common entries with and is distinct from one of P_1, P_2, Q_1 or Q_2). By Lemma 1.2, each V_i has two common entries with Q_1. This forces $x_3 = h$ and $y_3 = g$ and so $V_1 = V_2 = V$ say. Therefore $V \in P_1P_2 \cap Q_1Q_2$. V lies on Σ_3 or Σ_4, so Π and Π_Q intersect each of Σ_1, Σ_2, and say Σ_3 in the same sets. Since each Π_i and each Σ_i contains a unique point of P_1P_2 and a unique point of Q_1Q_2, $\Pi \cap \Sigma_4 = \Pi_Q \cap \Sigma_4$. We conclude that $\Pi = \Pi_Q$ and so through P_1 and l_{22} there is an unique new plane. Combinatorial reasoning then establishes the following.

Lemma 2.5. *A "new plane" Π is uniquely determined by one of its lines and one of its points each lying on distinct Σ_i's.*

Fix $i \neq j$. Any given line ℓ in Σ_i lies on two planes of $\mathcal{S}$, one of which intersects Σ_j in a line, say ℓ'. Through each of the three lines in Σ_j parallel to but not equal to ℓ' we form a new plane containing ℓ. Thus, in the manner above, through every line of Σ_i we construct three new planes.

Definition 2.6. Let $\mathcal{S}'$ be the incidence structure of $\mathcal{S}$ together with all new planes (where as in $\mathcal{S}$, two points are collinear if they lie on two common planes).

With a view to showing $\mathcal{S}'$ to be a linear space we establish the following three lemmas.

Lemma 2.7. *If Ψ_1 and Ψ_2 are distinct planes of $\mathcal{S}'$, then Ψ_1 and Ψ_2 are either disjoint or they intersect in exactly 4 points.*

Proof. If Ψ_1 and Ψ_2 are planes in the old sense (planes of $\mathcal{S}$) then the result is clear. If Ψ_1 is a new plane and Ψ_2 an old plane then we have two cases to consider, either Ψ_2 is a Σ_i or it is not. In the affirmative case, the construction of our new planes gives $|\Psi_1 \cap \Psi_2| = 4$. If Ψ_2 is not one of the Σ_i's, then it intersects each Σ_i in a line. For $i = 1..4$ define the lines l_i and m_i by $l_i = \Psi_1 \cap \Sigma_i$ and $m_i = \Psi_2 \cap \Sigma_i$. We have two subcases to consider:

Case 1: l_1 parallel to (or equal to) m_1.

In this case $[l_i] = [m_i]$ (in Σ_i) for each i. By the definition of a new plane, Ψ_1 will contain exactly one of the m_i's. As such we have $|\Psi_1 \cap \Psi_2| = 4$.

Case 2: l_1 intersects m_1 in a point.

In this case we will have l_i nonparallel to m_i for each i. This then gives exactly 4 points of intersection (one in each of the Σ_i's).

The final situation to consider is when Ψ_1 and Ψ_2 are both new planes. We have three subcases to consider:

$\boldsymbol{|l_1 \cap m_1| = 1}$**:** In this case, since l_1 and m_1 are not parallel, l_i will be nonparallel with m_i for each i. So Ψ_1 and Ψ_2 will have exactly one common point in each Σ_i giving $|\Psi_1 \cap \Psi_2| = 4$.

$\boldsymbol{|l_1 \cap m_1| = 4}$**:** Here, Ψ_1 and Ψ_2 have a common line in Σ_1. If Ψ_1 and Ψ_2 have a fifth point in common then (Lemma 2.5) they are equal.

$\boldsymbol{|l_1 \cap m_1| = 0}$**:** l_1 and m_1 are parallel, so l_i is parallel to m_i for each i. If Ψ_1 and Ψ_2 share two lines, they coincide. Hence, Ψ_1 and Ψ_2 share either no points or exactly one line (4 points).

□

With Lemma 2.7 in hand our definition of a line in $\mathcal{S}'$, as the intersection of two planes, is somewhat justified. The following Lemma strengthens our case.

Lemma 2.8. *If a line ℓ' of $\mathcal{S}'$ contains two points of a line ℓ of $\mathcal{S}$ then $\ell = \ell'$.*

Proof. Let P and Q be collinear in $\mathcal{S}$. It suffices to show that a new plane Π containing P and Q contains the line PQ. If P and Q lie in the same Σ_i then the result is clear. On the other hand, the line PQ intersects Σ_1 in a single point $P' \neq Q$ and Σ_2 in the point $Q' \neq P$. P' lies on the line $l = \Sigma_1 \cap \Pi$. Thus Π must be the plane determined by l and Q' and hence contains PQ. □

Lemma 2.9. *Let Π be a plane of $\mathcal{S}'$, and P a point not in Π. There exists a unique plane through P parallel to Π.*

Proof. Assume (perhaps after applying a suitable symbol permutation) $P \in \Sigma_1$. If Σ_1 is parallel to Π then we are done. So assume the contrary. For $i = 1, 2, 3, 4$ denote by λ_i the line $\Sigma_i \cap \Pi$. Since the Σ_i's are disjoint, the λ_i's are parallel in Π. Through P there exists a unique line l parallel (in Σ_1) to λ_1. Any plane parallel to Π and containing P must intersect Σ_1 in l. There are five planes containing the line l (one of which is Σ_1). According to Lemma 2.7, any plane on l intersecting Π will do so in exactly one line, moreover this line will be parallel (in Π) to λ_1. So four of the planes on l intersect π nontrivially (in a λ_i) leaving exactly one plane on l disjoint from Π. □

Theorem 2.10. *The incidence structure $\mathcal{S}'$ is a linear space.*

Proof. Every line of $\mathcal{S}'$ contains four points. As such, we need only show that any two points P and Q lie on a unique line. If P and Q are collinear in $\mathcal{S}$ then (Lemma 2.8) no other line contains both points. On the other hand P and Q are unjoined in $\mathcal{S}$, so P and Q appear in distinct Σ_i's. Assume (perhaps after applying a suitable symbol permutation) $P \in \Sigma_1$ and $Q \in \Sigma_2$. There are 5 new planes, say $\Psi_1, \Psi_2, \ldots, \Psi_5$, containing both P and Q (one for each pair of "parallel" lines, one on P and the other on Q). Let $m_i = \Psi_i \cap \Sigma_3$ and $n_i = \Psi_i \cap \Sigma_4$. We claim the m_i's share a common point as do the n_i's. If the m_i's are not incident at a point, then one of the lines, say m_1 contains at least three points of intersection with the other m_i's. By Lemma 2.2, m_1 contains exactly two points collinear in $\mathcal{S}$ with P.

Thus, one of the points of intersection, say $R = m_1 \cap m_2$ is collinear in $\mathcal{S}$ with P. Both Ψ_1 and Ψ_2 contain P and R. By Lemma 2.8 the line RP is precisely their intersection. But both Ψ_1 and Ψ_2 contain the point Q forcing Q to be contained in the line RP. This is a contradiction since Q was assumed unjoined to P in $\mathcal{S}$. A similar argument shows the n_i's to be incident at a point. We conclude that P and Q are contained in precisely one line. □

3. Main Results

An *n-arc* (resp. *dual n-arc*) in $PG(k, q)$ is a set $\mathcal{K}$ of $n \geq (k+1)$ points (resp. hyperplanes) such that no $k+1$ points (resp. hyperplanes) lie on a common hyperplane (resp. point). So in $PG(2, q)$, a dual n-arc is a set of n lines no three of which are incident at a point. In [8], Bruen and Silverman give a technique for constructing $(n, k)_q$-MDS codes over $GF(q)$. We define a Bruen-Silverman code as one that can be constructed using their technique.

Definition 3.1. (BRS-Code) In $\Sigma = PG(n, q)$ choose a hyperplane H_∞. In H_∞ choose a dual n-arc $\mathcal{K} = \{\lambda_1, \lambda_2, \cdots, \lambda_n\}$. Now, for each subspace λ_i in $\mathcal{K}$, label the q hyperplanes in Σ other than H_∞ containing λ_i with 1,2,...,q. Finally, let P be any of the q^k points of $\Sigma - H_\infty$. We define $\Phi(P) = (x_1, x_2, \cdots, x_n)$ where x_i is the label of the unique hyperplane of Σ containing both P and λ_i. Then $\{\Phi(P) \mid P \in \Sigma - H_\infty\}$ is a $(n, k)_q$-MDS code and is called an *$(n, k)_q$-Bruen-Silverman code*, or an *$(n, k)_q$-BRS code.*

In view of Definitions 1.3 and 3.1, if C is a BRS code and C' is equivalent to C, then C' is also a BRS code. In [1] the author showed the following:

Theorem 3.2. *C is an $(n, 3)_q$-BRS code if and only if C is equivalent to linear.*

We are now in a position to prove our main result.

Theorem 3.3. *Every $(6, 3)_4$-MDS code is equivalent to linear.*

Proof. We claim the incidence structure $\mathcal{S}'$ is exactly $AG(3, 4)$. To see this we demonstrate (see [4] p.86) that each of the following conditions hold in $\mathcal{S}'$:(1) $\mathcal{S}'$

is a linear space. (2) $\mathcal{S}'$ contains three points not on a line. (3) Every line of $\mathcal{S}'$ contains at least four points. (4) Every plane of $\mathcal{S}'$ is an affine plane.

Condition (1) is shown in Theorem 2.10 Conditions (2) and (3) are clear, leaving only (4) to be shown. To show that a plane Π of $\mathcal{S}'$ is an affine plane we need to show that Π has the following properties: (a) Π is a linear space (b) Π contains three points not on a line (c) Given a line l of Π and a point P not on l, then there exists a unique line through P parallel to l.

Property (a) is inherited from $\mathcal{S}'$. Property (b) is clear, leaving (c) to be shown. Suppose Π ,l, and P are as defined in (c). Let Ψ be a plane other than Π through l. By Lemma 2.9 there exists a unique plane Ψ' through P parallel to Ψ. Let $l' = \Psi' \cap \Pi$. Then l and l' are parallel and (c) is shown. Thus the incidence structure $\mathcal{S}'$ is AG(3,4).

The planes of $\mathcal{S}$ are precisely the planes of 6 parallel classes in $AG(3, q)$. Moreover, upon embedding $\mathcal{S}'$ in $PG(2, q)$ by appending a hyperplane Π_∞ at infinity, the planes in a given parallel class of $\mathcal{S}$ will share a common line in Π_∞. No three of these lines lie on a point (else three nonparallel planes of $\mathcal{S}$ share 4 points), so the aggregate of these lines form a dual 6-arc (or *hyperoval*) in Π_∞. It follows that C is of Bruen-Silverman type and by Theorem 3.2 we conclude that every $(6, 3)_4$-MDS code is equivalent to linear. □

Definition 3.4. An $(n, k)_q$-MDS code C is said to be an *extension* of an $(n-1, k)_q$-MDS code C' if upon deleting a fixed coordinate position from each word of C, the code C' results.

Theorem 3.5. *If C is a $(q + k - 2, k)_q$-MDS code with q even then C may be extended in a unique way to an $(q + k - 1, k)_q$-MDS code.*

Proof. See [2] (or [1] for $k = 3$). □

If C is an $(n, k)_q$-BRS code then the code C' obtained by deleting a fixed coordinate position from each word in C clearly remains a BRS code. Thus, by way of Theorems 3.3 and 3.5 we get the following corollary.

Corollary 3.6. *Every $(5, 3)_4$-MDS code is equivalent to linear.*

References

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

[2] T. L. Alderson, *Extending MDS Codes*, submitted to Ann.Comb., Dec. 2003.

[3] R. Baer, Nets and Groups, Trans AMS **46**, 1939, 110–141.

[4] Lynn M. Batten, *Combinatorics of Finite Geometries*, Cambridge Univ. Press , 1986.

[5] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, Cambridge Univ. Press, Cambridge, 1986.

[6] R.H.Bruck, Finite nets I, Numerical Invariants, Canad. J. Math. **3**, 1951, 94–107.

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

[8] A.A. Bruen and R. Silverman, On Extendable Planes, MDS Codes and Hyperovals in $PG(2, q)$, $q = 2^t$, Geom. Dedicata **28**, 1988, 31–43.

[9] A.A. Bruen, J.A. Thas, and A. Blokhuis, On MDS codes, arcs in $PG(n, q)$ with q even, and a solution of three fundamental problems of B. Segre, Invent. Math. **92**, 1988, 441–459.

[10] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam 1977.

[11] R. Silverman, A Metrization for Power-sets with Applications to Combinatorial Analysis, Canad. J. Math. **12**, 1960, 158–176.

[12] D. Welsh, *Codes and Cryptography*, Oxford University Press, 2000.

[13] Stephen B. Wicker, and Vijay Bhargava (Editors), *Reed-Solomon Codes and their Applications*, IEEE Press, New York, 1994.

Mathematical Sciences, University of New Brunswick, Saint John, Canada, E2L 4L5

E-mail address: `talderso@unb.ca`