Extending MDS Codes

T. L. Alderson [*]

Abstract

A q-ary (n,k)-MDS code, linear or not, satisfies $n \leq q+k-1$. A code meeting this bound is said to have maximum length. Using purely combinatorial methods we show that an MDS code with $n = q+k-2$ can be uniquely extended to a full length code if and only if q is even. This result is best possible in the sense that there is, for example, a non-extendable 4-ary $(5,4)$-MDS code. It may be that the proof of our result is as interesting as the result itself. We provide a simple necessary and sufficient condition (property $\mathcal{P}$) for code extendability. In future work, this condition might be suitably modified to give an extendability condition for arbitrary (shorter) MDS codes.

AMS Subject Classification: 94B25, 51E21,05B15

Key Words: MDS Code, Latin Hypercube, Code Extension

[*] The author acknowledges support from the NSERC of Canada

1. Introduction

A linear $[n,k]$-code of minimum (Hamming) distance d satisfies $d \leq n-k+1$, the Singleton bound. A linear $[n,k]$-code meeting the Singleton bound is called a *linear Maximum Distance Separable*, or MDS code. Reed-Solomon (RS) codes, a mainstay in industry due to their powerful error correction and the availability of efficient decoding algorithms, are examples of linear MDS codes. see [25]. An (extended) $[n,k]$-RS code over $GF(q)$ satisfies $n \leq q+1$ unless $k=3$ and q is even, in which case $n \leq q+2$. The same bound has long been conjectured to hold for general linear MDS codes by dint of their relationship to arcs in projective spaces. Indeed, if C is a linear (n,k)-MDS code, the structure of C is easily described as follows. We choose a basis for C as rows of a $k \times n$ matrix G over $GF(q)$ of rank k. The MDS condition implies that every set of k columns of G are linearly independent. Thus, regarding the columns of G as points of $PG(k-1,q)$, collectively they form an n-arc in $PG(k-1,q)$. Conversely, any n-arc in $PG(k-1,q)$ gives such a matrix (see [16, 17]). An n-arc in $PG(k,q)$, $q>k$, $2 \leq k \leq 6$ satisfies $n \leq q+1$ (unless $k=2$ and q is even, in which case $n \leq q+2$), this bound has also been shown to hold, at least asymptotically, for dimensions $k>6$ [16–18]. With no assumptions regarding linearity, an (n,k)-*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. Such codes are the context here, all codes discussed being q-ary over the alphabet $\mathcal{A}=\{1,2,\ldots,q\}$. An $(n,2)$-MDS code C corresponds to a set of $n-2$ mutually orthogonal Latin squares or equivalently to a Bruck net of degree $n-2$, so that $n \leq q+1$. More generally, for $k>2$, C corresponds to a certain collection of mutually orthogonal Latin hypercubes ([22]). Very little is known about non-linear (n,k)-MDS codes where $k>2$. In [22], Silverman uses a counting argument to show the following.

Lemma 1.1. *If C is a q-ary (n,k)-MDS code, then $n \leq q+k-1$.*

An MDS code meeting the bound in Lemma 1.1 is said to have *maximum length*. For $k>3$ there is a widening gap between the combinatorial bound of Lemma 1.1 and the conjectured bound on the length of linear MDS codes. We now summarize some known existence results on maximal length MDS codes.

Theorem 1. ***(a)*** *A q-ary $(q+k-1,k)$-MDS code C does not exist if $q \equiv 1$ or 2 (mod 4) and the square free part of q is divisible by a prime of the form $4t+3$.*

(b) *A $(q+k-1,k)$-MDS code does not exist if q is odd.*

(c) *A $(q+k-1,k)$-MDS code does not exist if there exists a prime p such that $p<k$ and p divides $q-1$.*

(d) *If C is a $(q+k-1,k)$-MDS code with $k \geq 3$ and $q>2$ then 4 divides q.*

(e) *If C is a $(q+k-1,k)$-MDS code with $k>3$ and $q>2$ then 36 divides q.*

Proof. For (a) see [10], for (b) and (c) see [22], and for (d) and (e) see [14]. ∎

If a fixed coordinate position is deleted from each word of an (n,k)-MDS code C, an $(n-1,k)$-MDS code C' results. The code C is called an *extension* of C', and C' is said to be *extendable*.

Due to their connection with arcs in projective spaces, the literature is rich with results relating to the extendability of linear MDS codes (see [16–18, 24]). On the extendability of general MDS codes most results in the literature pertain only to the 2-dimensional codes, namely Bruck nets or sets of mutually orthogonal Latin squares (see [6, 8, 12, 13]). The results here are a first step toward filling the apparent gap in the theory. The main result of this paper is the following.

Theorem 2. *A q-ary $(q+k-2,k)$-MDS code C can be extended to a (unique) maximum length MDS code if and only if q is even.*

It is important to point out that we can not possibly improve Theorem 2 to include $(q+k-3)$-MDS codes. For example, any linear $(5,4)$-MDS code over $GF(4)$ is not extendable (Theorems 1(d) and 2). In our proofs we make repeated use of the following results, both found in [22].

Lemma 1.2. *Let C be a q-ary $(q+k-1,k)$-MDS code C. Then any two words $u,v \in C$ having $k-2$ common entries have exactly $k-1$ common entries.*

Lemma 1.3. *Let C be a q-ary (n,k)-MDS code over the alphabet $\mathcal{A}$, let $t \leq k$ be a positive integer and fix t coordinate positions. Then, every possible t-tuple over $\mathcal{A}$ will occur exactly q^{k-t} times in the fixed coordinate positions as we range over the words of C.*

1.1. Bruck Nets

Definition 1.1. *(Bruck Net) For $q > 2$ a positive integer, a (q,n)-Bruck Net $\mathcal{N}$ (or a (q,n)-net) is an incidence structure consisting of q^2 points and qn distinguished subsets called lines, such that each of the following conditions are met.*

(i) Every line of $\mathcal{N}$ contains exactly q points.

(ii) Parallelism (the property of being either equal or disjoint) is an equivalence relation on the lines of $\mathcal{N}$.

(iii) There are n parallel classes, each consisting of q lines.

(iv) Any two non-parallel lines meet exactly once.

The term “net” was first introduced in 1939 by Baer [2]. The name achieved popularity only after the much celebrated works of Bruck [8, 9], thus the often used *Bruck-nets*. Any n parallel classes of a finite affine plane of order q form a (q,n)-net (the converse is not always true). So a (q,n)-net has degree $n \leq (q+1)$. In view of this the *deficiency* δ associated with a (q,n)-net is the number such that $n+\delta = q+1$.

In his 1963 paper [9] Bruck defines a *partial transversal* of a (q,n)-net $\mathcal{N}$ to be a set of points no two of which are joined in $\mathcal{N}$. A *transversal* is a partial transversal of (necessarily maximal) size q. Also in [9] is the content of the following Lemma, proved using elementary counting techniques.

Lemma 1.4. *Let $\mathcal{N}$ be a (q,n)-net of deficiency δ, let P and Q be distinct points of $\mathcal{N}$, l a line of $\mathcal{N}$ and T a partial transversal. Then:*

(1) *$|T| \leq q$ with equality if and only if T meets every line of $\mathcal{N}$.*

(2) *P is joined to exactly $n(q-1)$ points and unjoined to $\delta(q-1)$ points.*

(3) *If $P \notin l$ thenP is collinear with $n-1$ points of l and unjoined to δ points of l.*

(4) *If T is a transversal and $P \notin T$ then P is joined to n points and unjoined to $\delta - 1$ points of T.*

From the discussion in [22] a q-ary $(n,2)$-MDS code is combinatorially equivalent to a (q,n)-net (where two words of the code are collinear if they have a common entry). To *extend* a (q,n)-net $\mathcal{N}$ is to partition the points of $\mathcal{N}$ into q transversals forming a new parallel class of lines yielding a $(q,n+1)$-net. To *embed* a (q,n)-net $\mathcal{N}$ is to successively extend $\mathcal{N}$ to an affine plane π (a $(q,q+1)$-net). In this case π is called a *completion* of $\mathcal{N}$. The center-piece of Brucks 1963 paper is the following theorem.

Theorem 3. *(Bruck's Completion Theorem) Define the polynomial p by $p(x) = \frac{1}{2}x^4 + x^3 + x^2 + \frac{3}{4}x$. Then any (q,n)-net $\mathcal{N}$ of deficiency δ satisfying $p(\delta-1) < q$ has an unique completion.*

The key to the proof of this theorem is an ingenious "clique and claw" method first used by Bruck(1963) [9] and Bose(1963) [7]. The method has subsequently been used for many other embedding theorems, see for example Beutelspacher and Metsch [4,5] for applications to linear spaces. The bound in Theorem 3 was slightly improved by Metsch ([20] (1991)). For the uniqueness of embedding Bruck actually proved the much better (and stronger) bound:

Theorem 4. *(Bruck's Uniqueness Theorem) Let $\mathcal{N}$ be a (q,n)-net with deficiency δ satisfying $q > (\delta-1)^2$. Then any two transversals of $\mathcal{N}$ intersect in at most one point and $\mathcal{N}$ has at most $q\delta$ transversals with equality holding if and only if $\mathcal{N}$ is embeddable. In the equality case, the completion of $\mathcal{N}$ is obtained by adjoining all $q\delta$ transversals, in particular, the completion of $\mathcal{N}$ is unique.*

Bruck also showed that the bound in Theorem 4 is best possible. All known examples of maximal nets are in fact transversal free. The first such examples were constructed by Bruen [11–13] using partial spreads in projective spaces.

2. Extending MDS codes

To repeat from our introduction.

Definition 2.1. *Let C be a q-ary (n,k)-MDS code. If a fixed coordinate position is deleted from each word of C, an $(n-1,k)$-MDS code C' results. The code C is called an extension of C', and C' is said to be extendable.*

Remark 1. *According to Theorem 3, a q-ary $(n,2)$-MDS code with $p(\delta-1) < q$ can be successively extended to yield a q-ary $(q+1,2)$-MDS code. Moreover, this extension is unique.*

Definition 2.2. *Let C be a q-ary (n,k)-MDS code over $\mathcal{A}$ and let $0 \le t \le k$. A t-residual code of C is defined as follows. Fix any t coordinate positions $\alpha_1, \alpha_2, \ldots, \alpha_t$ and any t-tuple $(\gamma_1, \gamma_2, \ldots, \gamma_t)$ over $\mathcal{A}$ there are precisely q^{k-t} words in C having γ_i in coordinate α_i, $i = 1, 2, \ldots, t$ (i.e. having t coordinates fixed). This collection of q^{k-t} words is a t-residual code of C. A 0-residual code is the entire code C. A 1-residual code is simply called a residual code.*

Definition 2.3. *Let C be a q-ary (n,k)-MDS code. For each j, $1 \le j \le q$, denote by C_j the residual code consisting of all words of C having first coordinate j.*

Remark 2. *Note that if C' is a t-residual code of a q-ary (n,k)-MDS code C then C' is residually a q-ary $(n-t, k-t)$-MDS code. That is to say, upon deleting the fixed t coordinate positions defining C', a q-ary $(n-t, k-t)$-MDS code results.*

Definition 2.4. *Let C' be a t-residual code of a q-ary (n,k)-MDS code C, where $0 \le t \le k-2$. (So C' is a collection of words in C having t fixed coordinates in common.) Any collection of q^{k-t-1} words of C' pairwise having no more than k-2 common entries is called a transversal of C'.*

Upon a moments reflection on Definitions 2.1 and 2.4, the following is clear.

Lemma 2.1. *A q-ary (n,k)-MDS code C can be extended if and only if there exists a partition $\{T_1, T_2, \ldots, T_q\}$ of C where each T_i is a transversal of C.*

3. Extending $(q+1,3)$-MDS Codes

Definition 3.1. *In a q-ary $(n,3)$-MDS code, two words u and v are tangent if $d(u,v) = n-1$, and secant if $d(u,v) = n-2$.*

Let C be a $(q+1,3)$-MDS code. Each of the residual codes $C_1, \ldots, C_q$ is residually a $(q,2)$-MDS code. By way of Theorem 3, any $(q,2)$-MDS code can be uniquely extended to a $(q+1,2)$-MDS code. It follows that for each i, $1 \le i \le q$, C_i can be uniquely partitioned into transversals, say $C_i = \{T_{i1}, T_{i2}, \ldots, T_{iq}\}$. Define the set $\mathcal{T}$ $= \{T_{ij} \,|\, 1 \le i, j \le q\}$.

Remark 3. *Observe that if $T \in \mathcal{T}$ then $|T| = q$ and all words in T have a common first entry. It follows (Lemma 1.3) that in each coordinate position other than the first, every member of $\mathcal{A}$ will occur exactly once as we range over the words of T.*

We state property $\mathcal{P}$ in the setting of $(n,3)$-MDS codes.

$\mathcal{P}$**:** Property $\mathcal{P}$ is said to hold in the $(n,3)$-MDS code C if no two words secant in C are tangent to a common word.

Definition 3.2. *Define the relation $\mathcal{R}$ on $\mathcal{T}$ as follows. $T_1 \mathcal{R} T_2$ if $T_1 = T_2$ or if there exist words $u \in T_1$ and $v \in T_2$ with u and v tangent.*

Lemma 3.1. *Suppose $\mathcal{P}$ holds in a q-ary $(q+1,3)$-MDS code and let $T_1, T_2 \in \mathcal{T}$ with $T_1 \mathcal{R} T_2$. Then each word of T_1 is tangent to each word of T_2.*

Proof. Suppose $T_1\mathcal{R}T_2$, then there exists $u \in T_1$ and $v \in T_2$ tangent. By property $\mathcal{P}$ u is secant to no word of T_2. From the Remark 3 it follows that u is tangent to each word of T_2. As u is tangent to all other words of T_1, it follows that no word of T_1 is secant to any word of T_2. We conclude each word of T_1 is tangent to each word of T_2. ∎

Lemma 3.2. *If property $\mathcal{P}$ holds in a q-ary $(q+1,3)$-MDS code C then $\mathcal{R}$ is an equivalence relation on $\mathcal{T}$. Moreover, each equivalence class of $\mathcal{R}$ is a transversal of C.*

Proof. $\mathcal{R}$ is clearly reflexive and symmetric. To see transitivity, suppose $T_1\mathcal{R}T_2$ and $T_2\mathcal{R}T_3$. If $u \in T_1$ and $v \in T_3$ are secant then (Lemma 3.1) any word w from T_1 together with u and v violate $\mathcal{P}$. From the Remark 3 it follows that u is tangent to each word of T_3 and hence $T_1\mathcal{R}T_3$. So $\mathcal{R}$ is an equivalence relation.

For the second part, let T_1 ba a transversal of C_1. It follows from Lemma 1.4 (4) that T_1 is $\mathcal{R}$-related to no other transversal of C_1. Let $u = (1, u_2, u_3, \ldots, u_{q+1}) \in T_1$ and fix $j \neq 1$. For each $i = 3, \ldots, q+1$ there exists an unique word in C with first entry j, second entry u_2, and i'th entry u_i (Lemma 1.3). By the MDS property of C, no two of these words coincide. Therefore, of the q words of the form $(j, u_2, \_, \_, \ldots, \_)$, exactly one word is tangent to u while the others are secant to u. It follows that T_1 is $\mathcal{R}$-related to exactly one transversal of C_j. As such, each equivalence class of $\mathcal{R}$ consists of q^2 words (consisting of a transversal from each C_i) no two agreeing in as many at two coordinate positions. In other words, each equivalence class of $\mathcal{R}$ is a transversal of C. ∎

Theorem 5. *A q-ary $(q+1,3)$-MDS code can be extended if and only if property $\mathcal{P}$ holds on C. Moreover, this extension is unique.*

Proof. For the necessary conditions, suppose $\mathcal{P}$ holds in C. By the above Lemma, there is a partition, say $\{T_1, T_2, \ldots, T_q\}$ of C (arising via $\mathcal{R}$) where each T_i is a transversal of C. By Lemma 2.1 C can be extended. For the sufficient conditions, assume by way of contradiction that C can be extended to C' by adding a (q+2)nd component to each word of C and that $\mathcal{P}$ does not hold in C. By Lemma 1.2 any two words in C' have distance $q+2$ or q from each other. As $\mathcal{P}$ does not hold in C there are words u, v, and w in C corresponding to the words u', v', and w' in C' satisfying $d(u,w) = q-1$, $d(u,v) = q$, and $d(v,w) = q$. As each pair of words have at least one common entry, we have, $d(u',v') = d(u',w') = d(v',w') = q$. Since $d(u,v) = d(u',v')$, u' and v' must have the same (q+2)nd component. Let α be the (q+2)nd component of u' and v'. Similarly v' and w' have a common (q+2)nd component, which must also be α. So u' and w' both have α as (q+2)nd component. As u and w are secant in C, u' and w' must have three common entries. This contradicts the MDS property of C'. We conclude that C can be extended if and only if property $\mathcal{P}$ holds.

For uniqueness, any extension of C requires C to be partitioned into q transversals (Lemma 2.1). Any given transversal T in this partition must contain a transversal of each of the residual codes $C_1, C_2, \ldots, C_q$ (briefly, by Lemma 1.4(4) a collection of more than q words from a given C_i contains at least two secant words. By the Pigeonhole Principle T must contain exactly q words—forming a transversal— from each C_i). By way of Theorem 4, each C_i has a unique decomposition into transversals. It follows that the partition of C arising via the extension of C and the partition induced by the relation $\mathcal{R}$ are identical. We conclude that the extension of C is unique. ∎

Lemma 3.3. *Let C' be a residual code of a q-ary $(q+1,3)$-MDS code C. If $w \in C - C'$ then w is tangent to exactly q words of C'. Moreover, if q is even, these q words form a transversal of C'.*

Proof. Assume with no loss of generality that $C' = C_1$ and $w = (2, w_2, \ldots, w_{q+1}) \in C_2$. For each choice of i and j , $2 \leq i < j \leq q+1$, there is an unique word of C_1 having ith entry w_i and jth entry w_j (Lemma 1.3). This gives precisely $\binom{n}{2}$ words of C_1 secant to w. For each i, $2 \leq i \leq q+1$, let $A_i = \{u \in C_1 | u_i = w_i\}$. Then for i, j, and k distinct, $|A_i| = q$, $|A_i \cap A_j| = 1$, and $|A_i \cap A_j \cap A_k| = 0$. So $|\cup A_i| = q^2 - \binom{q}{2} = (q^2+q)/2$ is the number of words in C_1 having at least one common entry with w. It follows that there are precisely $(q^2+q)/2 - \binom{q}{2} = q$ words in C_1 tangent to w.

For the second part suppose q is even and let T be the q words of C_1 tangent to w. Define the subset $B \subset C$ to be the q words of C having first entry 1 and second entry w_2. For each i, $3 \leq i \leq q+1$, there is an unique word of B having i'th entry w_i. No two of these words coincide (by the MDS property) leaving exactly one word of B tangent to w. Choose $\alpha \in \mathcal{A}$ with $\alpha \neq w_2$. Define the set D to be the collection of q words in C having first entry 1 and second entry α. For each i, $3 \leq i \leq q+1$, there is an unique word of D having i'th entry w_i. No three of these words coincide. By assumption $q-1$ is odd, so there is at least one word of D tangent to w. It follows that each element of $\mathcal{A}$ occurs exactly once in the second entry as we range over the words of T. The same argument holds for each coordinate position (other than the first). We conclude that T is a transversal. ∎

Theorem 6. *If C is a q-ary $(q+1,3)$-MDS code then C can be extended if and only if q is even. Furthermore, any extension of C is unique.*

Proof. The sufficiency condition is given by Theorem 1 (b). For the necessary condition, assume q is even. By Theorem 5 it suffices to show $\mathcal{P}$ holds in C. To this end let $u, v \in C$ be secant. Assume with no loss of generality that $u, v \in C_1$. The $q-1$ words in C_1 tangent to u are contained in a transversal of C_1 containing u. By Lemma 1.4 (4), no word of C_1 is tangent to both u and v. If $w \in C - C_1$ then (Lemma 3.3) since q is even, the words of C_1 tangent to w form a transversal of C_1. Since u and v are secant, w is not tangent to both u and v. Hence no word of C is tangent to both u and v and we conclude that property $\mathcal{P}$ holds in C. The uniqueness part is given by Theorem 5. ∎

Theorem 6 with Theorem 1 (d) give the following as an immediate consequence.

Corollary 3.1. *If $q > 2$ and $q \equiv 2$ mod 4 then no q-ary $(q+1,3)$-MDS codes exist.*

4. Extending $(q+k-2,k)$-MDS Codes

For $k > 3$ let C be a q-ary $(q+k-2,k)$-MDS code. Each residual code of C is residually a $(q+k-3,k-1)$-MDS code, whereas a transversal of a residual code is residually a

$(q+k-3,k-2)$-MDS code. Two words u and v in C are said to be *hypertangent* (resp. *hypersecant*) if u and v have precisely $k-2$ (resp. $k-1$) common entries. We restate property $\mathcal{P}$ in this setting.

$\mathcal{P}$**:** Property $\mathcal{P}$ is said to hold in the $(q+k-2,k)$-MDS code C if no two words hypersecant in C are hypertangent to a common word.

The main results of this section are the following theorems.

Theorem 7. *A $(q+k-2,k)$-MDS code C, $k \geq 3$, can be extended if and only if property $\mathcal{P}$ holds in C. Furthermore, any extension of C is unique.*

Theorem 8. *A q-ary $(q+k-2,k)$-MDS code C, $k \geq 3$, can be extended if and only if q is even. Furthermore, any extension of C is unique.*

With Theorem 1 (e) we get the following as an immediate consequence.

Corollary 4.1. *If 36 does not divide q and $k \geq 4$ then a q-ary (n,k)-MDS code satisfies $n \leq q+k-3$.*

Setting $k=4$ in the Corollary gives $n \leq q+1$. We point out that the arguments used in [14] are purely combinatorial. As pointed out in the introduction, linear q-ary (n,k)-MDS codes and n-arcs in PG$(k-1,q)$ are equivalent objects. In view of this we have essentially provided a new and elementary proof of the following well known result.

Corollary 4.2. *In $PG(3,q)$, q even, the maximal size of an arc is $q+1$.*

4.1. Proof of Theorem 7

let C be a $(q+k-2,k)$-MDS code. For the only if part we refer to the proof of Theorem 5. For the if part assume property $\mathcal{P}$ holds in C. Appealing to the results of the previous section we proceed by induction on k. Let $k>3$ and assume our result holds for all $(q+k-3,k-1)$-MDS codes. Each of the residual codes $C_1,C_2,\ldots,C_q$ is residually a $(q+k-3,k-1)$-MDS code. By our induction hypothesis, each C_i can be uniquely extended and hence partitioned in an unique way into transversals, say $C_i=\{T_{i1},T_{i2},\ldots,T_{iq}\}$. Let $\mathcal{T}=\{T_{ij}\,|\,1\leq i,j,\leq q\}$.

Lemma 4.1. *Assume property $\mathcal{P}$ holds in C. Let $u \in C_i$ and $v \in C_j$ be hypertangent. Denote by T the transversal of C_j containing v. In any fixed $k-2$ coordinate positions (excluding the first), there exists a word in T hypertangent to u in exactly those positions.*

Proof. By counting, the (unique) transversal of C_i containing u contains all words of C_i hypertangent to u. Thus if $i=j$ the result holds. Suppose $i \neq j$. As u and v are hypertangent, assume with no loss of generality that $u_t=v_t$, $t=2\ldots k-2$. Fix $k-2$ coordinate positions, say $1<\alpha_1,\alpha_2,\ldots,\alpha_{k-2}\leq q+k-2$. We claim there exists a word in T hypertangent to u and agreeing with u in coordinate positions $\alpha_1,\alpha_2,\ldots,\alpha_{k-2}$. Let $B=\{\alpha_i|i=1\ldots k-2\}$, and let $D=\{2,3,\ldots,k-1\}$. If $D=B$ then v is the required word. Suppose $\alpha_1 \notin D$. Since T is residually a $(q+k-3,k-2)$-MDS code, there exists an unique word, say v_1, in T agreeing with u in coordinates $3,4,\ldots,k-1,\alpha_1$. As v and

v_1 are hypertangent, u is not hypersecant to v_1 (property $\mathcal{P}$). Hence u is hypertangent to v_1. If $\alpha_2 \in D \setminus \{2\}$ set $v_2 = v_1$. Otherwise, by the same argument as above we can find $v_2 \in T$ hypertangent to u in positions $4, 5, \ldots, k-1, \alpha_1, \alpha_2$. Continuing in this manner we arrive at a word, $v_{k-2} \in T$ hypertangent to u in exactly the required coordinate positions. ∎

Lemma 4.2. *Assume property $\mathcal{P}$ holds in C. For fixed i, j let $u \in C_i$ and let T be a transversal of C_j. Then u is hypersecant to no word of T if and only if u is hypertangent to some word of T.*

Proof. By counting, the (unique) transversal of C_i containing u contains all words of C_i hypertangent to u. Thus if $i = j$ the result holds. Assume $i \neq j$. For the necessary conditions, let $v \in T$ be hypertangent to u. By way of contradiction suppose $w \in T$ is hypersecant to u, with no loss of generality assume $w_t = u_t, t = 2 \ldots k$. By the previous Lemma, there exists a word $x \in T$ hypertangent to u with $x_t = u_t$, $t = 2 \ldots k-1$. But then $x, w \in T$ are distinct and have $k-1$ common entries. This contradicts the transversal property of T. We conclude that u is hypersecant to no word of T.

For the sufficient conditions, assume u is hypersecant to no word of T. T is residually a $(q+k-3, k-2)$-MDS code. As such, in any fixed $k-2$ coordinate positions (excluding the first), there is an unique word in T agreeing with u in those positions. As u is assumed to be hypersecant to no word of T, u is hypertangent to each such word. We conclude that u is hypersecant to no word of T if and only if u is tangent to some word of T. ∎

Lemma 4.3. *Assume property $\mathcal{P}$ holds in C. Suppose $u, v \in C_i$ are hypertangent and $w \in C_j$ is hypertangent to u. If T_j is the transversal of C_j containing w then v is hypersecant to no word of T_j.*

Proof. By the previous Lemma, u is hypersecant to no word of T_j. As in the proof of the above Lemma, u and v are in a common transversal, say T_i, of C_i. If $i = j$ then, by the same argument, $w \in T_i$ and our result follows. Assume $i \neq j$. With no loss of generality assume $u_s = v_s$, $s = 1..k-2$. Let $\Lambda = \{x \in T_j \,|\, x_s = u_s, s = 2..k-2\}$. T_j is residually a $(q+k-3, k-2)$-MDS code. So $|\Lambda| = q$ and moreover, in each coordinate position t, $t > k-2$, each element of $\mathcal{A}$ will occur exactly once as we range over the words of Λ. It follows that each word in Λ is hypertangent to u. Fix $t > k-2$. There exists a word $y \in \Lambda$ with $y_t = v_t$. By property $\mathcal{P}$, v and y are not hypersecant and must therefore be hypertangent. By the previous Lemma we conclude that v is hypersecant to no word of T_j. ∎

Lemma 4.4. *Assume property $\mathcal{P}$ holds in C. Let $T_1, T_2 \in \mathcal{T}$, $u \in T_1$, $v \in T_2$. If u and v are hypertangent then no word of T_1 is hypersecant to any word of T_2.*

Proof. If $T_1 = T_2$ the result is clear. Assume $T_1 \neq T_2$, so u and v lie in distinct residual codes. Define the subsets $S_0 \subset S_1 \subset \cdots \subset S_{k-3}$ of T_1 by $S_i = \{w \in T_1 | w_j = u_j, j = 1, 2, .., k-2-i)\}$. So $S_0 = \{u\}$ and $S_{k-3} = T_1$. No two words in T_1 agree in as many as $k-1$ coordinate positions. All words in S_t $(t > 0)$ have the first $k-2-t$ coordinates in common. It follows that in any fixed t coordinate positions chosen from $k-1-$

$t, k-t, \ldots, k+q-2$, every ordered t-tuple will occur exactly once as we range over the words of S_t. As such, each word of S_t is either hypertangent or equal to at least one word of S_{t-1}, $t = 1 \ldots k-3$. By assumption u is tangent to some word of T_2 and hence(Lemma 4.2) is hypersecant to no word of T_2. Recursively applying Lemmas 4.2 and 4.3 to $S_1, S_2, \ldots, S_{k-3} = T_1$ we conclude that no word of T_1 is hypersecant to any word of T_2. ∎

Definition 4.1. *Define the relation $\mathcal{R}$ on $\mathcal{T}$ by $T_1 \mathcal{R} T_2$ if $T_1 = T_2$ or if there exist words $u \in T_1$ and $v \in T_2$ with u and v hypertangent.*

Lemma 4.5. *Suppose $\mathcal{P}$ holds in C. Then $\mathcal{R}$ is an equivalence relation on $\mathcal{T}$. Moreover, each equivalence class of $\mathcal{R}$ is a transversal of C.*

Proof. $\mathcal{R}$ is clearly reflexive and symmetric. Suppose by way of contradiction that $\mathcal{R}$ is not transitive. Say $T_1 \mathcal{R} T_2$, $T_2 \mathcal{R} T_3$ and T_1 is not $\mathcal{R}$ related to T_3. Then (Lemma 4.2) there exists $u \in T_1$ and $v \in T_3$ where say $u_i = v_i$, $i = 2 \ldots k$. Since $T_1 \mathcal{R} T_2$, there exists (Lemma 4.1) $w \in T_2$ with $w_i = u_i$, $i = 3 \ldots k$, where w and u are hypertangent. Since $T_2 \mathcal{R} T_3$, w and v are also hypertangent. So u, v, and w violate property $\mathcal{P}$, a contradiction. We conclude that $\mathcal{R}$ is an equivalence relation on $\mathcal{T}$. For the second part see the proof of Lemma 3.2. ∎

By assumption C is a $(q+k-2,k)$-MDS code in which $\mathcal{P}$ holds. Proceeding as in the proof of Theorem 5, the relation $\mathcal{R}$ gives the unique extension of C and Theorem 7 is proved.

4.2. Proof of Theorem 8

Let C be a $(q+k-2,k)$-MDS code. For the sufficient conditions we appeal to Theorem 1 (b). For the necessary conditions assume q is even. Once again we proceed by induction on k. By Theorem 6 the result holds for $k = 3$. Let $k > 3$ and assume our result holds for all $(q+k-3,k-1)$-MDS codes.

By Theorem 7 it suffices to show that property $\mathcal{P}$ holds in C. To this end let $u, v \in C$ be hypersecant. Assume with no loss of generality that $u_i = v_i$, $i = 2, 3, \ldots, k-2$ and that $u_1 = v_1 = 1$. We must show no word of C is hypertangent to both u and v. By our induction hypothesis, no word of C_1 is hypertangent to both u and v. Choose $w \in C - C_1$. Let $\alpha = (a_1, a_2, \ldots, a_{k-3})$ where the a_i's are distinct integers satisfying $2 \leq a_i \leq q+k-2$ for each $i = 1, 2, \ldots, k-3$. Define the sets $S_\alpha = \{x \in C | x_i = w_i, i = a_1, a_2, \ldots, a_{k-3}\}$ and $N_\alpha = S_\alpha \cap C_1$. So N_α is residually a $(q,2)$-MDS code and S_α is residually a $(q+1,3)$-MDS code. In fact, N_α is a residual code of S_α. It follows (Lemma 3.3) that there is a transversal T_α of N_α consisting of all words of N_α hypertangent to w.

By our induction hypothesis, $\mathcal{P}$ holds in C_1. As in the proof of Theorem 5 any word $y \in C_1$ lies in an unique transversal T of C_1. Further, by counting, y is hypertangent to no word of $C_1 - T$. It follows that T_α is contained in a transversal, say τ_α of C_1.

Let $\beta = (b_1, b_2, \ldots, b_{k-3})$ where b_i's are distinct integers satisfying $2 \leq b_i \leq q+k-2$ for each i. We claim $\tau_\beta = \tau_\alpha$. If $b_1 \in \{a_1, a_2, \ldots, a_{k-3}\}$ let $\alpha_1 = \alpha$. Otherwise let $\alpha_1 = (a_2, a_3, \ldots, a_{k-3}, b_1)$. In C_1 there are precisely q agreeing with w in positions

$a_1, a_2, \ldots, a_{k-3}, b_1$. By counting, exactly one such word is hypertangent to w. So $T_\alpha \cap T_{\alpha_1} \neq \emptyset$. Since each word of C_1 is contained in an unique transversal of C_1, we conclude that $\tau_\alpha = \tau_{\alpha_1}$. Similarly, if $b_2 \in \{a_3, a_4, \ldots, a_{k-3}\}$ let $\alpha_2 = \alpha_1$. Otherwise let $\alpha_2 = (a_3, a_4, \ldots, a_{k-3}, b_1, b_2)$. As above we arrive at $\tau_{\alpha_2} = \tau_{\alpha_1} = \tau_\alpha$. Continuing in this manner we arrive at $\tau_\alpha = \tau_\beta$.

It follows that all words of C_1 hypertangent to w belong to a common transversal (namely τ_α) of C_1. u and v are hypersecant and so belong to distinct transversals of C_1. Hence w is hypertangent to at most one of u and v. We conclude that property $\mathcal{P}$ holds in C.

References

1. T. L. Alderson, *On MDS Codes and Bruen-Silverman Codes*, PhD. Thesis, University of Western Ontario, 2002.
2. R. Baer, *Nets and Groups*, Trans AMS **46**, 1939, 110–141.
3. Lynn M. Batten, *Combinatorics of Finite Geometries*. Cambridge Univ. Press , 1986.
4. A. Beutelspacher, K. Metsch, *Embedding Finite Linear Spaces in Projective Planes*, Ann. Discr. Math. **30**, 39–56.
5. A. Beutelspacher, K. Metsch, *Embedding Finite Linear Spaces in Projective Planes II*, Discr. Math. **66**, 219–230.
6. Bose, R. C., Shrikhande, S. S., Parker, E. T., *Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture.*, Canad. J. Math. **12**, 1960 189–203.
7. R.C. Bose, *Strongly Regular Graphs, Partial Geometries and Partially Balanced Designs*, Pacific J. Math. **13**, 1963, 389–419.
8. R.H.Bruck, *Finite nets I, Numerical Invariants*, Canadian J. Math. **3**, 1951, 94–107.
9. R.H.Bruck, *Finite nets II, Uniqueness and embedding*, Pacific J. Math. **13**, 1963, 421–457.
10. R.H.Bruck, H.J.Ryser , *The nonexistence of certain finite projective planes*, Canadian J. Math.**1**, 1949, 88–93.
11. A.A. Bruen, *Partial Spreads and Replacable Nets*, Canadian J. Math. **23**, 1971, 381–391.
12. A.A. Bruen, *Unembeddable Nets of Small Deficiency*, Pacific J. Math. **43**, 1972, 51–54.
13. A.A. Bruen, *Collineations and Extensions of Translation Nets*, *Mathematische Zeitschrift* **145**, 1975, 243–249.

14. A.A. Bruen and R. Silverman, *On the nonexistence of certain MDS codes and projective planes*, *Mathematische Zeitschrift* **183**, 1983, 171–175.

15. 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.

16. A.A. Bruen, J.A. Thas, and A. Blokhuis, *MDS Codes and Arcs in Projective Spaces I*, *C.R. Math. Rep. Acad. Sci. Canada* **10**, 1988, 225–230.

17. A.A. Bruen, J.A. Thas, and A. Blokhuis, *MDS Codes and Arcs in Projective Spaces II*, *C.R. Math. Rep. Acad. Sci. Canada* **10**, 1988, 233–235.

18. Hirschfeld, J. W. P., *Complete arcs*, Discrete Math. **174**, 1997, no. 1-3, 177–184.

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

20. K. Metsch, *Improvement of Bruck's Completion Theorem*, Designs, Codes and Crypography **1**, 1991, 99–116.

21. C.R.Rao, *Hypercubes of strength d leading to confounded designs in factorial experiments*, Bulletin Calcutta Mathematics Society 38, 1946, 67-78.

22. R. Silverman, *A Metrization for Power-sets with Applications to Combinatorial Analysis*, Can. J. Math. **12**, 1960, 158–176.

23. R. Silverman, C. Maneri, *A Vector Space Packing Problem*, J. Algebra **4**, 1966, 321–330.

24. L. Storme and J.A. Thas, *M.D.S. codes and k-arcs in PG(n,q) with q even: An improvement of the bounds of Bruen, Thas and Blokhuis*, J. Combin. Theory, Series A **62**, No. 1, 1993, 139-154.

25. S.B. Wicker, and V. Bhargava (Editors), *Reed-Solomon Codes and their Applications*, IEEE Press, New York, 1994.