Classification of the $[n, 3, n-3]_q$ NMDS codes over $GF(7)$, $GF(8)$ and $GF(9)$

Stefano Marcugini, Alfredo Milani, Fernanda Pambianco
Dipartimento di Matematica e Informatica,
Università degli Studi di Perugia,
Via Vanvitelli 1, 06123 Perugia Italy
e-mail: {gino, milani, fernanda}@dipmat.unipg.it

Abstract

A linear $[n, k, d]_q$ code C is called NMDS if $d(C) = n - k$ and $d(C^\perp) = k$. In this paper the classification of the $[n, 3, n-k]_q$ NMDS codes is given for $q = 7, 8, 9$. It has been found using the correspondence between $[n, 3, n-k]_q$ NMDS codes and $(n, 3)$−arcs of $PG(2, q)$.

1 Introduction

Let F_q^n be the n−dimensional vector space over the Galois field $GF(q)$. The Hamming distance between two vectors of F_q^n is defined as the number of coordinates in which they differ. A q-ary linear $[n, k, d]_q$−code is a k−dimensional linear subspace of F_q^n with minimum distance d. The Singleton bound [15] states a relationship among n, k and d: $d \leq n - k + 1$. Codes meeting the Singleton bound are called MDS (Maximum distance separable). Bounds on the minimum distance of linear codes can be found in [3].

The projective space of dimension r obtained from $GF(q)$ will be denoted by $PG(r, q)$. A set of m points of $PG(r, q)$ are called in general position if they are not contained in a subspace of dimension $m - 2$. A set of n points in $PG(r, q)$ such that every $r + 1$ of them are in general position is called n−arc. A detailed description of the most important properties of these geometric structures can be found in [8], while [10] contains general bounds and particular values for the sizes of particular sets of points of $PG(r, q)$. The following theorem [2] states a relationship between linear codes and sets of points in $PG(r, q)$:

Theorem 1 *C is an $[n,k,d]$ linear code if and only if the columns of the parity check matrix of C are n points in $PG(n-k-1,q)$, each $d-1$ of which are in general position.*

In particular MDS codes and n-arcs are equivalent objects. A conjecture affirms that the maximum length of a non-trivial MDS code is less than or equal to $q+2$ if q is even and $k=3$ or $k=q-1$ and it is less than or equal to $q+1$ otherwise. The conjecture has been proved when $q \leq 19$ and when $k \leq 5$ ([4], [9], [11]). To have longer codes, the value of d has to be less than $n-k+1$. The Singleton defect of a $[n,k,d]$ code C, defined as $s(C)=n-k+1-d$, measures how far C is away from being MDS. Codes with $s(C)=1$ are called AMDS (almost MDS) and codes with $s(C)=s(C^{\perp})=1$ are called NMDS (near MDS). Such codes have been considered in [1], [5], [6], [7]. Not all the AMDS codes are NMDS [6], but the following theorem holds([5]):

Theorem 2 *If $n > k+q$, every $[n,k,n-k]$ code is NMDS.*

In [6] it is stated also that the following holds:

Theorem 3 *A linear $[n,k,d]$ code C is NMDS if and only if a generator matrix of C, say G_C, (and consequently each generator matrix) satisfies the following conditions:*
(N1) any $k-1$ columns of G_C are linearly independent;
(N2) there exist k linearly dependent columns in G_C;
(N3) any $k+1$ columns of G_C are of full rank.

Let C be a NMDS code with $k \geq 3$ and generator matrix $\mathbf{G}_C = [\mathbf{g}_1\ \mathbf{g}_2\ \ldots\ \mathbf{g}_n]$, where $\mathbf{g}_i \in F_q^n$. Since $k \geq 3$, the columns of $\mathbf{G}_C$ can be viewed as different points in the projective geometry $PG(k-1,q)$. Hence the existence of an $[n,k,n-k]$ NMDS code C is equivalent to the existence of a set S of points in $PG(k-1,q)$ having the following properties ([6]):

(N1') any $k-1$ points from S generate a hyperplane in $PG(k-1,q)$;
(N2') there exist k points lying on a hyperplane;
(N3') every $k+1$ points from S generate $PG(k-1,q)$.

When $k=3$ these properties reduce to the following:

(N2") there exist three collinear points in S;
(N3") no four points from S lie on a line.

A set S of points of $PG(2,q)$ satisfying the properties (N2") and (N3") is called $(n,3)$−arc. Every $[n,3,n-3]$ NMDS code is therefore equivalent to an $(n,3)$−arc in $PG(2,q)$.

In [6] the classification of the $[n, k, n-k]$ NMDS codes of maximal length is given for $q \leq 4$. The classification of the $(n,3)-$arcs in $PG(2,5)$ that gives also the classification of the $[n, k, n-k]_5$ NMDS codes can be found in [16]. This paper presents the classification of the $[n, 3, n-3]_q$ NMDS codes over $GF(7)$, $GF(8)$ and $GF(9)$. In particular it has been demonstrated that there are 19 non-equivalent NMDS codes of maximal length over $GF(8)$ and that there are 4 non-equivalent NMDS codes of maximal length over $GF(9)$. The classification of the NMDS codes has been obtained computing the number of non-equivalent $(n,3)-$arcs in $PG(2,q)$, $q = 7,8,9$ using a computer based exhaustive search. The classification given in this paper has been the starting point of an ongoing work concerning NMDS codes of dimension greater than three. Preliminary results concerning the existence and the classification of NMDS codes over $GF(5)$ and $GF(7)$ have been presented in [14].

The algorithm used is described in the next section. The third, the fourth and the fifth sections contain the classification of the $[n, 3, n-3]_q$ NMDS codes over $GF(7)$, $GF(8)$ and $GF(9)$, respectively.

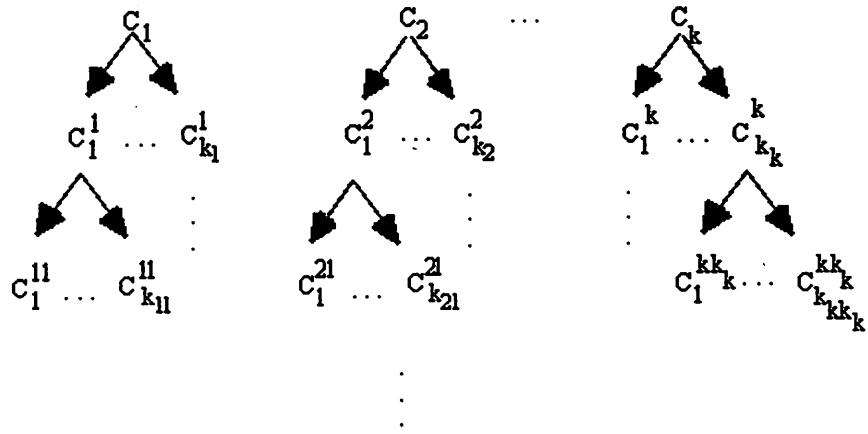
2 The algorithm for the classification of the $(n,3)$-arcs

In this section the algorithm used for the classification of the $(n,3)-$arcs in $PG(2,q)$ is described. It is a modification of the algorithm presented in [12]. It allows to find exactly one representative of each equivalence class of the $(n,3)$-arcs of a given size s. The following theorem [12], stating a lower bound on the size of the arcs that an $(n,3)$-arc contains, has been used to reduce the number of cases to examine:

Theorem 4 *An $(n,3)$-arc K in $PG(2,q)$, $n \geq \alpha + \binom{\alpha}{2}$, contains an arc of size $\alpha+1$.*

The first step of the algorithm is therefore the classification up to projective equivalence of the arcs in $PG(2,q)$ of size less than or equal to α. Start with $R = \{(0,0,1), (0,1,0), (1,0,0), (1,1,1)\}$ and define *Cand* to be the set of the points of the plane lying on no 2-secant of R. In *Cand* the following equivalence relation is introduced: $P \backsim Q$ if and only if $R \cup \{P\}$ is projectively equivalent to $R \cup \{Q\}$. Let $\{C_i\}_i$ be the set of the equivalence classes. Then not only can we limit the choice of the next point to one representative P_i from each class, but after having constructed all arcs

containing $R \cup \{P_i\}$, when considering the arcs containing $R \cup \{P_j\}$ with $i < j$, we may avoid to choose points in the classes C_k, with $k < j$: an arc containing such a point would in fact be projectively equivalent to an arc that was obtained previously. Iterate the process and obtain a tree structure of equivalence classes:



The depth of the tree is $\alpha - 4$. If $R \cup \{P_{i_1}\} \cup \ldots \cup \{P_{i_m}^{i_1 \ldots i_{m-1}}\} \cup \{P\}$ is projectively equivalent to $R \cup \{P_{i_1}\} \cup \ldots \cup \{P_{i_m}^{i_1 \ldots i_{m-1}}\} \cup \{Q\}$, where $P_s^{i_1 \ldots i_r} \in C_s^{i_1 \ldots i_r}$, then $P, Q \in C_j^{i_1 \ldots i_m}$.

The algorithm continues looking for $(n, 3)$-arcs containing one of the non-equivalent α-arcs. To extend each α-arc into an $(s, 3)$-arc, a procedure similar to the previous is adopted. In this case *Cand* will be the set of the points of the plane lying on no 3-secant of the current $(n, 3)$-arc. In *Cand* an equivalence relation similar to the above is introduced: $P \backsim Q$ if and only if $R \cup \{P_{i_1}\} \cup \ldots \cup \{P_{i_m}^{i_1 \ldots i_{m-1}}\} \cup \{P\}$ is projectively equivalent to $R \cup \{P_{i_1}\} \cup \ldots \cup \{P_{i_m}^{i_1 \ldots i_{m-1}}\} \cup \{Q\}$. Let $\{C_i\}_i$ be the set of the equivalence classes. Then the choice of the next point will be limited to one representative P_i from each class.

3 The $[n, 3, n-3]$ NMDS code over $GF(7)$

The classification of the $[n, 3, n-3]_7$ NMDS codes is reported in the following table:

$[5,3,2]_7$ NMDS codes	3
$[6,3,3]_7$ NMDS codes	14
$[7,3,4]_7$ NMDS codes	53
$[8,3,5]_7$ NMDS codes	180
$[9,3,6]_7$ NMDS codes	526
$[10,3,7]_7$ NMDS codes	907
$[11,3,8]_7$ NMDS codes	923
$[12,3,9]_7$ NMDS codes	395
$[13,3,10]_7$ NMDS codes	65
$[14,3,11]_7$ NMDS codes	4
$[15,3,12]_7$ NMDS codes	1

The classification of NMDS codes over $GF(7)$

It was obtained classifying the $(n,3)$-arcs in $PG(2,7)$ using the algorithm described above, as every $[n,3,n-3]$ NMDS code is equivalent to an $(n,3)-$arc in $PG(2,q)$. The description of the geometrical properties of the $(n,3)$-arcs in $PG(2,7)$ can be found in [13].

4 The $[n,3,n-3]$ NMDS code over $GF(8)$

The following table contains the classification of the $[n,3,n-3]_8$ NMDS codes:

$[5,3,2]_8$ NMDS codes	2
$[6,3,3]_8$ NMDS codes	7
$[7,3,4]_8$ NMDS codes	38
$[8,3,5]_8$ NMDS codes	175
$[9,3,6]_8$ NMDS codes	764
$[10,3,7]_8$ NMDS codes	2244
$[11,3,8]_8$ NMDS codes	4236
$[12,3,9]_8$ NMDS codes	4281
$[13,3,10]_8$ NMDS codes	1956
$[14,3,11]_8$ NMDS codes	297
$[15,3,12]_8$ NMDS codes	19

The classification of NMDS codes over $GF(8)$

It was obtained classifying the $(n,3)$-arcs in $PG(2,8)$. The study of the geometrical properties of the $(n,3)$-arcs in $PG(2,8)$ has not been completed yet.

5 The $[n, 3, n-3]$ NMDS code over $GF(9)$

The following table contains the classification of the $[n, 3, n-3]_9$ NMDS codes:

$[5,3,2]_9$ NMDS codes	3
$[6,3,3]_9$ NMDS codes	19
$[7,3,4]_9$ NMDS codes	119
$[8,3,5]_9$ NMDS codes	734
$[9,3,6]_9$ NMDS codes	4273
$[10,3,7]_9$ NMDS codes	18592
$[11,3,8]_9$ NMDS codes	56426
$[12,3,9]_9$ NMDS codes	105193
$[13,3,10]_9$ NMDS codes	106479
$[14,3,11]_9$ NMDS codes	48833
$[15,3,12]_9$ NMDS codes	8314
$[16,3,13]_9$ NMDS codes	382
$[17,3,14]_9$ NMDS codes	4

The classification of NMDS codes over $GF(9)$

It was obtained classifying the $(n, 3)$-arcs in $PG(2, 9)$. The study of the geometrical properties of the $(n, 3)$-arcs in $PG(2, 9)$ has not been completed yet.

Acknowledgments

This research is supported by Italian MURST, CNR and GNSAGA.

References

[1] M.A. de Boer, *Almost MDS Codes*, Designs, Codes and Cryptography 9 (1996), 143-154.

[2] R.C. Bose and K.A. Bush, *Orthogonal arrays of strength two and three*, Ann. Math. Stat. 23 (1952), 508-524.

[3] A.E. Brouer, Data base of bounds on the minimum distance of linear codes, URL http://www.win.tue.nl/~aeb/voorlincod.html.

[4] J.M. Chao and H. Kaneta, *Classical arcs in $PG(r, q)$ for $11 \leq q \leq 19$*, Discrete Math. 174 (1997), 87-94.

[5] S.M. Dodunekov and I. Landjev, *On near-MDS codes*, J. Geometry 54 (1995), 30-43.

[6] S.M. Dodunekov and I. Landjev, *Near-MDS codes over some small fields*, Discrete Math. 213 (2000), 55-65.

[7] A. Faldum and W. Willems, *Codes of small defect*, Designs, Codes and Cryptography 10 (1997), 341-350.

[8] J.W.P. Hirschfeld, *Projective geometries over finite fields* (Claredon Press, Oxford, 1998).

[9] J.W.P. Hirschfeld and J.A. Thas, *General Galois geometries*, (Claredon Press, Oxford, 1991).

[10] J.W.P. Hirschfeld and L. Storme, *The packing problem in statistics, coding theory and finite projective spaces*, J. Stat. Plann. Inference, 72 (1998), 335-380.

[11] J.F.K. MacWilliams, N.J.A. Sloane, *The theory of Error correcting codes*, North-Holland, Amsterdam(1977).

[12] S. Marcugini, A. Milani and F. Pambianco, *Maximal* $(n,3)-$*arcs in* $PG(2,11)$, Discrete Math. 208/209 (1999), 421-426.

[13] S. Marcugini, A. Milani and F. Pambianco, *Classification of the* $(n,3)-$*arcs in* $PG(2,7)$, submitted.

[14] S. Marcugini, A. Milani, F. Pambianco, *Existence and classification of* NMDS *codes over* $GF(5)$ *and* $GF(7)$, Proceedings of ACCT2000, the Seventh International Workshop on Algebraic and Combinatorial Coding Theory, Bulgaria June 2000 232-239.

[15] R.C. Singleton, *Maximum distance separable* $q-$*nary codes*, IEEE Trans. Inform. Theory, 10 (1964), 116-118.

[16] M.O. Yazdi, *The classification of* $(k;3)-$*arcs over the Galois field of order five*, PhD. Thesis, Univ. of Sussex, Brighton U.K. (1983).