A Matrix Characterization of $Near - MDS$ codes[1]

G.Viswanath[2] and B.Sundar Rajan[2] [3]

Abstract

It is well known that a linear code over a finite field with the systematic generator matrix $[I \mid P]$ is MDS (Maximum Distance Separable) if and only if every square submatrix of P is nonsingular. In this correspondence we obtain a similar characterization for the class of Near-MDS codes in terms of the submatrices of P.

1 Introduction

The class of Near-MDS (NMDS)codes [3], [4], [5], [1] is obtained by weakening the restrictions in the definition of classical MDS codes. The support of a code C is the set of coordinate positions, where not all codewords of C are zero. The r-th generalized Hamming weight $d_r(C)$ of a code C is defined to be the cardinality of the minimal support of an (n, r) subcode of C, $1 \leq r \leq k$ [7], [8], [9]. Near-MDS ($NMDS$) codes are a class of codes where for an (n, k) code the i-th generalized Hamming weight $d_i(C)$ is $(n - k + i)$ for $i = 2, 3, \ldots, k$ and $d_1(C)$ is $(n - k)$. This class contains remarkable representatives as the ternary Golay code and the quaternary (11,6,5) and (12,6,6) codes as well as a large class of Algebraic Geometric codes. The importance of NMDS codes is that there exist NMDS codes which are considerably longer than the longest possible MDS codes for a given size of the code and the alphabet. Also, these codes have good error detecting capabilities [2].

It is well known that a linear MDS code can be described in terms of its systematic generator matrix as follows: If $[I \mid P]$ is the generator

[1]The paper was presented in part at the "International Workshop on Algebraic and Combinatorial Coding Theory", 18-24 June, 2000, Bansko, Bulgaria.

[2]Electrical Communication Engineering Department, Indian Institute of Science, Bangalore, India 560 012.
email:gviswa@protocol.ece.iisc.ernet.in, bsrajan@ece.iisc.ernet.in.

[3]This work was partly supported by the DRDO-IISc Program on Advanced Research in Mathematical Engineering through a grant to B. S. Rajan.

matrix then every square submatrix of P is nonsingular. In this paper, we obtain a similar characterization for the class of NMDS codes. Also, using a general property of generalized Hamming weights, we point out that an algebraic geometric code over an elliptic curve, if not MDS is necessarily NMDS.

2 Preliminaries

In this section we present the known results concerning NMDS codes and generalized Hamming weight hierarchy that will be used in the following sections.

A Near-MDS code can be characterized in terms of either an arbitrary generator matrix or a parity check matrix of the code as follows [3]: A linear $[n, k]$ code is NMDS iff a parity check matrix $\mathbf{H}$ of it satisfies the following conditions:

- any $n-k-1$ columns of $\mathbf{H}$ are linearly independent
- there exists a set of $n-k$ linearly dependent columns in $\mathbf{H}$
- any $n-k+1$ columns of $\mathbf{H}$ are of rank $n-k$

A linear $[n, k]$ code is NMDS iff a generator matrix $\mathbf{G}$ of it satisfies the following conditions:

- any $k-1$ columns of $\mathbf{G}$ are linearly independent
- there exists a set of k linearly dependent columns in $\mathbf{G}$
- any $k+1$ columns of $\mathbf{G}$ are of rank k

Several interesting properties of Hamming weight hierarchy are discussed in [9] and [8]. A basic property is that the sequence of Hamming weight hierarchy is strictly increasing, i.e.,

$$d_1(C) < d_2(C) < \ldots < d_k(C) = n. \tag{1}$$

The following result [9] relates the Hamming weight hierarchy of a code to that of its dual. If $C^{\perp}$ denotes the dual of the code C, then

$$\{d_r(C) \mid r = 1,2,...,k\} \bigcup \{n+1-d_r(C^{\perp}) \mid r = 1,2..,n-k\}$$
$$= \{1,2,...,n\}.$$

3 Systematic Generator Matrix Characterization of NMDS Codes

Theorem Let $G = [I|P]$ be the systematic generator matrix of a linear non-MDS code C over a finite field. Then C is NMDS iff every $(g, g+1)$ and $(g+1, g)$ submatrix of P has at least one (g, g) nonsingular submatrix.

Proof: First we prove the 'if part'. We have to show that $d_1(C) = n-k$ and $d_2(C) = n-k+2$. Consider any one dimensional subcode generated by a minimum weight codeword $\underline{c}$ of C. In terms of linear combination of rows of G, let

$$\underline{c} = \sum_{j=1}^{g} \alpha_j \underline{r}_{i_j} \tag{2}$$

where $i_j \in \{1,2,\ldots,k\}, j = 1,2,\ldots,g$ and $\underline{r}_{i_j}$ is the i_j-th row of G. The weight of $\underline{c}$ within the first k positions is g. We need to show that the weight in the last $n-k$ positions is $(n-k-g)$ or the number of zeros in the last $n-k$ positions is g. Let the number of zeros in the last $n-k$ positions of $\underline{c}$ be $\lambda > g$. Choose any $g+1$ of these λ positions and let these positions be $j_1, j_2, \ldots,, j_{g+1}$. Then

$$\begin{bmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_g \end{bmatrix} \begin{bmatrix} r_{i_1j_1} & r_{i_1j_2} & \cdots & r_{i_1j_{g+1}} \\ r_{i_2j_1} & r_{i_2j_2} & \cdots & r_{i_2j_{g+1}} \\ \vdots & \vdots & \cdots & \vdots \\ r_{i_gj_1} & r_{i_gj_2} & \cdots & r_{i_gj_{g+1}} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \ldots & 0 \end{bmatrix}$$

Since there is a (g, g) nonsingular submatrix $\alpha_1 = \alpha_2 = \ldots \alpha_g = 0$, which is a contradiction. Hence $\lambda \leq g$ and $d_1 = n-k$. Notice that this means there can be at most one zero in each row of P.

To prove that $d_2(C) = n - k + 2$ consider a two dimensional subcode generated by two codewords $\underline{c}$ and $\underline{d}$. If the size of the union of supports of $\underline{c}$ and $\underline{d}$ is at least $n - k + 2$ then we are through. So, we need to consider the case where the support of both $\underline{c}$ and $\underline{d}$ is within an identical set of $n - k + 1$ locations. Let g of these locations be within the first k positions and let

$$\underline{c} = \sum_{j=1}^{g} \alpha_j \underline{r}_{i_j} \text{ and } \underline{d} = \sum_{j=1}^{g} \beta_j \underline{r}_{i_j}. \tag{3}$$

Consider an arbitrary linear combination of $\underline{c}$ and $\underline{d}$, i.e.,

$$\underline{e} = a\underline{c} + b\underline{d} = \sum_{j=1}^{g} (a\alpha_j + b\beta_j) \underline{r}_{i_j} \tag{4}$$

There are $g - 1$ zeros in the last $n - k$ positions of e. Let these be $j_1, j_2, \dots j_{g-1}$. Then we have

$$\begin{bmatrix} a\alpha_1 + b\beta_1 & \dots & a\alpha_g + b\beta_g \end{bmatrix} \begin{bmatrix} r_{i_1 j_1} & r_{i_1 j_2} & \cdots & r_{i_1 j_{g-1}} \\ r_{i_2 j_1} & r_{i_2 j_2} & \cdots & r_{i_2 j_{g-1}} \\ \vdots & \vdots & \cdots & \vdots \\ r_{i_g j_1} & r_{i_g j_2} & \cdots & r_{i_g j_{g-1}} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \dots & 0 \end{bmatrix}$$

Since every $(g, g-1)$ submatrix of P has a $(g-1, g-1)$ nonsingular submatrix, without loss of generality we assume the first $g - 1$ rows to constitute this nonsingular submatrix and choose a and b such that $a\alpha_g + b\beta_g = 0$. Then it follows that $a\alpha_t + b\beta_t = 0$ for all $t = 1, 2, \dots g - 1$.

Now, if both α_g and β_g are nonzeros, then $\underline{c}$ and $\underline{d}$ are scalar multiple of one another which means the code is one dimensional. Hence $d_2(C) = n - k + 2$. (Note that from (1), $d_2(C) = n - k$ is not possible since $d_1(C) = n - k$.) If one of them is zero, say $\beta_g = 0$, then $a = 0$ and $b\beta_t = 0$ for all $t = 1, 2, \dots g - 1$ which is not true. This completes the proof for the if part.

To prove the 'only if' part: For $NMDS$ codes every $(k-1)$ columns of the generator matrix are linearly independent. This follows from the fact that for an $[n\ k]$ $NMDS$ code the dual code is also $NMDS$ and that the minimum distance of the dual code is k. Consider a set of $(k-1)$ columns of the generator matrix. If all the columns are from the P part of the generator matrix, then since every $(k-1)$ columns are linearly independent we have a $(k-1, k-1)$ nonsingular submatrix.

If $k-g$ columns (say $j_1, j_2, \ldots j_{k-g}$) are from I and the rest $g-1$ columns from P, then let A denote the $(k, k-1)$ submatrix consisting of these columns. By suitable row exchanges and appropriate elementary column operations A can be brought to the form

$$\begin{bmatrix} \mathbf{0}_{\mathbf{g}\times(\mathbf{k}-\mathbf{g})} & \mathbf{A^*}_{\mathbf{g}\times(\mathbf{g}-\mathbf{1})} \\ \mathbf{I}_{(\mathbf{k}-\mathbf{g})\times(\mathbf{k}-\mathbf{g})} & \mathbf{0}_{(\mathbf{k}-\mathbf{g})\times(\mathbf{g}-\mathbf{1})} \end{bmatrix}.$$

Note that the column rank has not changed by these operations and the submatrix A^* is indeed a submatrix of A. Moreover, since the above matrix has column rank $k-1$ the submatrix A^* has column rank $g-1$ and hence contains a $(g-1, g-1)$ nonsingular submatrix. Therefore every $(g+1, g)$ submatrix of P has atleast one (g, g) nonsingular submatrix.

To show that every $(g, g+1)$ submatrix has atleast one (g, g) submatrix we make use of the fact that the minimum distance of the $NMDS$ code is $(n-k)$. Therefore for $NMDS$ codes every $(n-k-1)$ columns of the parity check matrix are linearly independent. The parity check matrix of the code can be written as $[-P^{\perp}\ I]$. Following the arguments for the systematic generator matrix we can see that every $(g+1, g)$ submatrix of $-P^{\perp}$ has atleast one (g, g) submatrix which is nonsingular. Therefore every $(g, g+1)$ submatrix of P submatrix has atleast one nonsingular (g, g) submatrix. This completes the proof. □

4 Discussion

In this correspondence we have extended the well known $[I|P]$ matrix characterization of MDS codes to the class of Near-MDS codes. This characterization of NMDS codes will be helpful to obtain NMDS over finite fields.

References

[1] M.A.deBoer, "Almost MDS Codes", Designs, Codes and Cryptography Vol.9, 1996, pp.143-154.

[2] R.Dodunekova, S.M.Dodunekov and Torleiv Klove, "Almost-MDS and Near-MDS codes for error detection," *IEEE Trans. on Information Theory*, IT-Vol.43, No:1, Jan.1997, pp.285-290.

[3] S. D. Dodunekov and I. N. Landgev, "On Near-MDS Codes", Technical Report, No:LiTH-ISY-R-1563, Department of Electrical Engineering, Linkoping University, February, 1994.

[4] S.M.Dodunekov and I.N.Landgev, "On Near-MDS Codes", Proc. International Symposium on Information Theory, ISIT-1994, Trondheim, Norway, p.427.

[5] S.M. Dodunekov and I.N. Landjev, "Near-MDS codes over some small fields", Discrete Mathematics, Vol.213, 2000, pp.55-65.

[6] I.I.Dumer and V.A.Zinovev, "Some new maximal codes over GF(4)", Problems of Information Transmission, Vol.14, No:3, pp.24-34, Sept.1978.

[7] Tor Helleseth, Torleiv Klove and Oyvind Ytrehus, "Generalized Hamming Weights of Linear Codes", *IEEE Trans. on Information Theory*, IT-Vol.38, No:3, May 1992, pp.1133-1140.

[8] T. Helleseth, T. Klove, V. I. Levenshtein, O Ytrehus, "Bounds on the Minimum Support Weights", *IEEE Trans. Information Theory*, Vol.IT-41, No.2, Nov.1995, pp.432-440.

[9] V.K.Wei, "Generalized Hamming Weights for linear codes," *IEEE Trans. on Information Theory*, IT-Vol.37, No:5, Sept.1991, pp.1412-1418.