The MMD codes are proper for error detection

R. Dodunekova
S. M. Dodunekov*

Abstract The undetected error probability of a linear code used to detect errors on a symmetric channel is a function of the symbol error probability ε of the channel and involves the weight distribution of the code. The code is *proper*, if the undetected error probability increases monotonously in ε. Proper codes are generally considered to perform well in error detection. We show in this paper that the Maximum Minimum Distance (MMD) codes are proper.

Index terms error detection, proper code, MMD codes

I Introduction

Let $GF(q)$ denote the Galois field with q elements. An $[n,k,d]_q$ code C is a k-dimensional subspace of the n-dimensional vector space over $GF(q)$ with minimum Hamming distance d. The weight distribution $\{A_0, A_1, \ldots, A_n\}$ of C consists of the numbers A_i of codewords of weight i in C, $0 \le i \le n$. When C is used to detect errors on a q-nary symmetric channel with symbol error probability ε, the probability of undetected error $P_{ue}(C,\varepsilon)$ is given by

$$P_{ue}(C,\varepsilon) = \sum_{i=d}^{n} A_i \Big(\frac{\varepsilon}{q-1}\Big)^i (1-\varepsilon)^{n-i}, \quad 0 \le \varepsilon \le \frac{q-1}{q}. \tag{1}$$

C is *proper*, if $P_{ue}(C,\varepsilon)$ is monotonously increasing in $\varepsilon \in [0, \frac{q-1}{q}]$ (see [6], [7], and [9]). A proper code is generally considered to perform well in error detection. In particular, such a code is *good* ([6], [7]), i.e., $P_{ue}(C,\varepsilon)$ becomes largest at $\varepsilon = \frac{q-1}{q}$, the worst case symbol error probability.

*This work was partially supported by the Bulgarian NSF under contract MM901/99.

A number of well-known classes of linear codes are known to be proper, such as the perfect codes, the MDS codes, MacDonald's codes, and some Near-MDS codes. (See, e.g., [1], [2], [3], [6].)

In this correspondence we show that the MMD codes are proper. Our proof takes advantage of the classification of the MMD codes up to formal equivalence given in [5] and [10], and uses sufficient conditions for a linear code to be proper, derived in [1]. For convenience, in Section II we give a short presentation of the MMD codes and their classification, and a description of the sufficient conditions mentioned above. The main result and its proof are presented in Section III.

II Preliminaries

An $[n, k, d]_q$ code C satisfies the Singleton bound

$$d \leq n - k + 1.$$

The defect $s(C)$ of C is defined as the difference between the Singleton bound and the minimum distance d of C, i.e.,

$$s(C) = n - k + 1 - d.$$

If the defect of C is zero, then C is a *maximum distance separable* (MDS) code. For all other codes the defect is positive. If $s = s(C)$ and $k \geq m + 1$ for some integer $m \geq 1$, then (see [10])

$$d \leq \frac{q^m(q-1)}{q^m - 1}(s + m).$$

When

$$d = \frac{q^m(q-1)}{q^m - 1}(s + m) \tag{2}$$

C is called a *maximum minimum distance* (MMD) code. It turns out that for a MMD code with positive defect, the corresponding number m in (2) is equal to the defect of the dual code.

Two codes with the same weight distribution are said to be formally equivalent. It follows from (1) that two formally equivalent codes have the same undetected error probability.

In [5] and [10], the MMD codes have been classified up to formal equivalence. Below we present this classification.

G1. Let C be an $[n,k,d]_q$ code of dimension $k \geq 3$ and defect $s \geq 1$. Then C is a MMD code if and only if C is formally equivalent to one of the following codes:

1. The $[t\frac{q^k-1}{q-1}, k, tq^{k-1}]_q$ t-times repeated Simplex code, where $t = 1, 2, \ldots$.
2. The $[q^{k-1}, k, (q-1)q^{k-2}]_q$ generalized Reed-Muller code of first order. If $q = 2$, then $k \geq 4$.
3. The $[12, 6, 6]_3$ extended Golay code.
4. The dual $[11, 5, 6]_3$ Golay code.
5. The $[q^2+1, 4, q^2-q]_q$ projective elliptic quadratic code with $q \neq 2$.
6. The $[(2^t-1)q + 2^t, 3, (2^t-1)q]_q$ Denniston code with $1 \neq 2^t | q$.

G2. Let C be a q-nary MMD code of dimension two and defect s. Then C is equivalent to the $[(s+1)(q+1), 2, (s+1)q]_q$ $(s+1)$-times repeated Simplex code.

G3. Let C be a MMD code of dimension k and defect $s = 0$. Then C is equivalent to the binary $[k+1, k, 2]$ MDS code.

The weight distribution of an $[n,k,d]_q$ MMD code with $s + m > \frac{q^m-1}{q-1}$ was determined in [10] as follows:

$$A_d = \frac{\binom{n}{k-m}}{\binom{k+s-1}{k-m}}(q^m - 1); \quad A_{d+1} = A_{d+2} = \ldots = A_{n-k+m+1} = 0;$$

$$\begin{aligned} A_{n-k+v} = &\binom{n}{k-v} \sum_{i=0}^{v-m} (-1)^i \binom{n-k+v}{i} (q^{v-i} - 1) \\ &- \frac{(-1)^{v-m}(s+m-1)(q^m-1)}{v+s-1} \binom{n}{k-v} \binom{n-k+v}{v-m}, \end{aligned} \tag{3}$$

$$v = m+2, \ldots, k.$$

Assume C has weight distribution $\{A_0, \ldots, A_n\}$. Define

$$A_\ell^* = \sum_{i=d}^{\ell} \frac{\ell_{(i)}}{n_{(i)}} A_i, \quad \ell = d, \ldots, n, \tag{4}$$

where $j_{(i)}$ denotes the i^{th} factorial moment $j(j-1)\dots(j-i+1)$ of the positive integer j. It was shown in [1], that the conditions

$$A^*_\ell \geq qA^*_{\ell-1}, \quad \ell = d+1, \dots, n, \tag{5}$$

are sufficient for C to be proper. In particular, if

$$\frac{d}{n} \geq \frac{q-1}{q}, \tag{6}$$

then the inequalities (5) hold and C is thus proper.

III The main result and its proof

Theorem *The MMD codes are proper for error detection.*

Proof. As mentioned in the previous section, it suffices to verify that the codes in the classification **G1-G3** of the MMD codes up to formal equivalence are proper. For most of these codes this will be done by taking advantage of the above sufficient conditions.

Assume first that C is an $[n,k,d]_q$ MMD code with weight distribution as in (3). By putting $\ell = d+j, \quad 0 \leq j \leq n-d$, we obtain for the coefficients A^*_ℓ defined in (4) that

$$A^*_d = \frac{A_d}{\binom{n}{d}}; \tag{7}$$

$$A^*_{d+j} = \frac{(d+j)_{(d)}}{n_{(d)}} A_d, \quad 1 \leq j \leq n-k+m+1-d; \tag{8}$$

$$A^*_n = \sum_d^n A_i = q^k - 1. \tag{9}$$

We first consider the codes in **G1.**

1. Let C be an $[t\frac{q^k-1}{q-1}, k, tq^{k-1}]_q$ code, $t = 1, 2, \dots$. Then

$$\frac{d}{n} = \frac{q^{k-1}(q-1)}{q^k-1} > \frac{q^{k-1}(q-1)}{q^k} = \frac{q-1}{q}$$

so that (6) holds. Thus C is proper.

2. Assume now that C is an $[q^{k-1}, k, (q-1)q^{k-2}]_q$ code. As above,

$$\frac{d}{n} = \frac{(q-1)q^{k-2}}{q^{k-1}} = \frac{q-1}{q},$$

i.e., (6) holds and C is thus proper. (For the case of $q = 2$, see also [8].)

3. Consider next the $[12, 6, 6]$ ternary extended Golay code. In this case, $s = 1$ and from (2), $m = 1$. Thus the code is a Near-MDS code (see [4]). The error detecting capability of Near-MDS codes was studied in [2] and [3]. In particular, it was shown there that if a Near-MDS code $[n, k, d]_q$ is such that

$$A_{n-k} \leq \binom{n}{k}\left(1 - \frac{1}{q}\right),$$

then (5) holds and the code is thus proper. Since an $[12, 6, 6]_3$ code has

$$A_{n-k} = A_6 = 264 = 4\binom{12}{2}$$

and

$$\binom{n}{k}\left(1 - \frac{1}{q}\right) = \binom{12}{6}\frac{2}{3} = \binom{12}{2}\frac{10 \cdot 9 \cdot 8 \cdot 7}{3 \cdot 4 \cdot 5 \cdot 6} \cdot \frac{2}{3} = \frac{28}{3}\binom{12}{2} > 4\binom{12}{2},$$

it is proper.

4. The dual $[11, 5, 6]_3$ Golay code is proper, according to [7], p. 106.

5. Now, let C be a code with parameters $[q^2 + 1, 4, q^2 - q]_q$. This time $s = q - 2$ and from (2), $m = 1$. The weight distribution of C is thus determined by (3) and hence

$$A_d = \frac{\binom{n}{3}}{\binom{q+1}{3}}(q-1) = \frac{n(n-1)(n-2)}{(q+1)q(q-1)}(q-1) = \frac{(q^2+1)q^2(q^2-1)}{(q+1)q} = nq(q-1);$$

$$A_{d+1} = A_{d+2} = \ldots = A_{n-2} = 0;$$

$$A_{n-1} = \binom{n}{1}\sum_{i=0}^{2}(-1)^i\binom{n-1}{i}(q^{3-i}-1) - (-1)^2\frac{(q-2)(q-1)}{q} \cdot \binom{n}{1}\binom{n-1}{2}$$

$$= n\sum_{i=0}^{2}(-1)^i\binom{n-1}{i}(q^{3-i}-1) - \frac{(q-2)(q-1)(q^2+1)q^2(q^2-1)}{2q}$$

$$= n\sum_{i=0}^{2}(-1)^i\binom{n-1}{i}(q^{3-i}-1) - \frac{(q^2-1)(q-2)}{2}A_d. \tag{10}$$

For $j = 1, 2, \ldots, n-2-d$, (7) and (8) give

$$\frac{A^*_{d+j}}{A^*_{d+j-1}} = \frac{d+j}{j} = \frac{d}{j} + 1 \geq \frac{d}{j_{max}} + 1 = \frac{d}{n-2-d} + 1$$

$$= \frac{n-2}{n-2-d} = \frac{q^2-1}{q-1} = q + 1 > q.$$

Thus (5) holds for $\ell = d + j = d + 1, \ldots, n-2$. Furthermore, (4) with $\ell = n-1$ gives in this case

$$A^*_{n-1} = \frac{(n-1)_{(d)}}{n_{(d)}} A_d + \frac{(n-1)_{(n-1)}}{n_{(n-1)}} A_{n-1}$$

$$= \frac{n-d}{n} A_d + \frac{1}{n} A_{n-1}. \tag{11}$$

From the above and (8) with $j = n-2-d$ we obtain

$$A^*_{n-1} - qA^*_{n-2} = \frac{n-d}{n} A_d + \frac{1}{n} A_{n-1} - q \frac{(n-2)_{(d)}}{n_{(d)}} A_d$$

$$= \Big(\frac{n-d}{n} - q \frac{(n-d)(n-d-1)}{n(n-1)} \Big) A_d + \frac{1}{n} A_{n-1}$$

$$= \frac{n-d}{n} \Big(1 - q \frac{n-d-1}{n-1} \Big) A_d + \frac{1}{n} A_{n-1}$$

$$= \frac{n-d}{n} \Big(1 - q \cdot \frac{q}{q^2} \Big) A_d + \frac{1}{n} A_{n-1} = \frac{1}{n} A_{n-1} > 0,$$

i.e., (5) holds for $\ell = n-1$. Furthermore, (9) and (11) give

$$A^*_n - qA^*_{n-1} = q^4 - 1 - q \left(\frac{n-d}{n} A_d + \frac{1}{n} A_{n-1} \right).$$

Here, by (10),

$$\frac{n-d}{n}A_d + \frac{1}{n}A_{n-1}$$

$$= \frac{n-d}{n}A_d + \sum_{i=0}^{2}(-1)^i \binom{n-1}{i}(q^{3-i}-1) - \frac{(q^2-1)(q-2)}{2}\frac{A_d}{n}$$

$$= \frac{A_d}{n}\Big(n-d-\frac{1}{2}(q^2-1)(q-2)\Big) + (q^3-1) - (n-1)(q^2-1) + \binom{n-1}{2}(q-1)$$

$$= q(q-1)\Big(q+1-\frac{1}{2}(q^2-1)q + (q^2-1)\Big)$$

$$+ (q-1)\Big(q^2+q+1-q^2(q+1)+\frac{1}{2}q^2(q^2-1)\Big)$$

$$= (q-1)\Big(q^2+q-\frac{1}{2}q^2(q^2-1)+q^3-q+q^2+q+1-q^3-q^2+\frac{1}{2}q^2(q^2-1)\Big)$$
$$= (q-1)(q^2+q+1) = q^3-1$$

and hence

$$A_n^* - qA_{n-1}^* = q^4 - 1 - q(q^3-1) = q-1 > 0.$$

Thus (5) also holds for $\ell = n$. Hence C is proper.

6. Let C be an $[(2^t-1)q+2^t, 3, (2^t-1)q]_q$ code. We then have $s = 2^t-2$ and from (2), $m = 1$. Since $s \geq 1$, then $t \geq 2$ and the weight distribution of C is thus determined in (3). We hence obtain

$$A_d = \frac{\binom{n}{2}}{\binom{2^t}{2}}(q-1) = \frac{n(n-1)}{2^t(2^t-1)}(q-1)$$

$$= \frac{n(2^t-1)(q+1)}{2^t(2^t-1)}(q-1) = \frac{n}{2^t}(q^2-1); \tag{12}$$

$$A_{d+1} = A_{d+2} = \ldots = A_{n-1} = 0.$$

If $j = 1, \ldots, n-1-d$, (7) and (8) give

$$\frac{A_{d+j}^*}{A_{d+j-1}^*} = \frac{d+j}{j} \geq \frac{d+n-1-d}{n-1-d} = \frac{(2^t-1)(q+1)}{2^t-1} = q+1 > q.$$

Thus (5) holds for $\ell = d + j = d + 1, \ldots, n - 1$. From (9), (8) with $j = n - 1 - d$, and (12) we get

$$\begin{aligned} A_n^* - qA_{n-1}^* &= q^3 - 1 - q\frac{n-d}{n}A_d \\ &= q^3 - 1 - q \cdot \frac{2^t}{n} \cdot \frac{n}{2^t}(q^2 - 1) \\ &= q^3 - 1 - q^3 + q = q - 1 > 0. \end{aligned}$$

Thus (5) holds also for $\ell = n$ and C is therefore proper.

We consider now an $[(s+1)(q+1), 2, (s+1)q]_q$ code from **G2.** Since

$$\frac{d}{n} = \frac{(s+1)q}{(s+1)(q+1)} = \frac{q}{q+1} > \frac{q-1}{q},$$

(6) holds and the code is proper.

Finally, a code with parameters $[k+1, k, 2]_2$ as in **G3** is a MDS code and is therefore proper, as shown in, e.g., [1] and [6].

Acknowledgement. This work has been completed during the visit of R. Dodunekova to the Department of Probability and Statistics, Institute of Mathematics and Informatics of the Bulgarian Academy of Sciences. She wishes to thank Prof. N. Yanev for his hospitality and excellent working conditions.

References

1. R. Dodunekova and S. M. Dodunekov, "Sufficient conditions for good and proper error detecting codes", *IEEE Trans. Inform. Theory*, vol. 43, pp. 2023-2026, Nov. 1997.

2. R. Dodunekova and S. M. Dodunekov, "On the probability of undetected error for Near-MDS codes", *preprint* no. 1995-25, Chalmers university of Technology and Göteborg university, 1995, p. 13.

3. R. Dodunekova, S. M. Dodunekov, and T. Kløve, "Almost-MDS and Near-MDS Codes for Error Detection", *IEEE Trans. Inform. Theory*, vol. 43 pp. 285-290, Jan. 1997.

4. S. M. Dodunekov and I. N. Landgev, "On Near-MDS Codes", *Journal of Geometry*, vol. 54, pp. 30-43, 1995.

5. A. Faldum and W. Willems, "A characterization of MMD codes", *IEEE Trans. Inform. Theory*, vol. 44, pp. 1555-1558, July 1998.

6. T. Kasami and S. Lin, "On the probability of undetected error for the Maximum Distance Separable Codes", *IEEE Trans. Commun.,* vol. COM-32, no. 9, pp. 998-1006, Sept. 1984.

7. T. Kløve and V. Korzhik, *Error detecting codes, General Theory and Their Application in Feedback Communication Systems.* Boston, MA: Kluwer, 1995.

8. T. Kløve, "Reed-Muller codes for error detection: The Good, The Bad, and The Ugly", *IEEE Trans. Inform. Theory,* vol. 42, pp. 1615-1622, Sept. 1996.

9. S. K. Leung, F. R. Barnes, and D. U. Friedman, "Some properties of undetected error probability of linear codes", *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 110-112, Jan. 1979.

10. J. Olsson and W. Willems, "A Characterization of Certain Griesmer Codes: MMD Codes in a More General Sense", *IEEE Trans. Inform. Theory*, vol. 45, pp. 2138-2142, Sept. 1999.