The duals of the MMD codes are proper for error detection

Rossitza Dodunekova[*]

Abstract A linear code, when used for error detection on a symmetric channel, is said to be *proper* if the corresponding undetected error probability increases monotonously in ε, the symbol error probability of the channel. Such codes are generally considered to perform well in error detection. A number of well-known classes of linear codes are proper, e.g., the perfect codes, the MDS codes, MacDonald's codes, the MMD codes, and some Near-MDS codes. The aim of this work is to show that also the duals of the MMD codes are proper.

Keywords linear code, error detection, proper code, dual code, MMD code.

1 Introduction

An $[n,k,d]_q$ code with symbols from a finite field $GF(q)$ of q elements is a k-dimensional subspace of the n-dimensional vector space over $GF(q)$, with minimum Hamming distance d. When looking for a linear code for error detection on a symmetric channel for information transmission, the choice of a proper code is considered to be sufficiently good. Many well-known classes of codes, such as the perfect codes, the MDS codes, MacDonald's codes, the MMD codes and some Near-MDS codes are proper (see, e.g., [14], [12], [6], [9], [5], [7]). The aim of this work is to show that the duals of the MMD codes are proper as well. For notions and results from Coding Theory used below we refer to [16].

The probability of undetected error $P_{ue}(C,\varepsilon)$ of an $[n,k,d]_q$ code C used for error detection on a q-nary symmetric channel depends on the symbol error probability

[*]This work was completed during the author's visit to the Institute of Mathematics and Mechanics of the Bulgarian Academy of Sciences in December 2001. She wishes to thank Prof. N. Yanev for his hospitality.

ε of the channel and involves the weight distribution $\{A_0, A_1, \dots, A_n\}$ of C, where A_i is the number of codewords of weight i in C, i.e.,

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

When ε is known, the best choice of an error detecting code in the class of all $[n,k]_q$ codes would be a code for which the undetected error probability (1) is as small as possible within the class. Unfortunately, there exists no general method for finding such a code, except exhaustive search [14]. Besides, the exact value of ε is often unknown and the best choice might depend on ε. This calls for a criterion by which we can judge the usefulness of a given code for error detection. The concept of a proper code provides such a criterion.

A linear code C is said to be *proper* for error detection if $P_{ue}(C,\varepsilon)$ as defined in (1) increases monotonously in $\varepsilon \in [0, \frac{q-1}{q}]$ (see [15], [12], and [14]). Such codes possess some regularity in the sense that the smaller the symbol error probability of the channel, the better they perform in error detection. In particular, they are *good* in the sense of [14], i.e., they perform worst for the worst case symbol error probability $\varepsilon = \frac{q-1}{q}$.

Again, there is no general efficient method for determining whether or not a given code with known weight distribution is proper. The work [6] provides a number of sufficient conditions in terms of the weight distribution for a linear code to be proper or good. In [1]-[5], [7], [9], and [13] these conditions were efficiently used for study of the error detecting capability of some classes of well known linear codes. In particular, the analysis in [13] showed that some standardized CRC codes are not even good, while some non-standardized CRC codes turn out to be proper.

In [8], sufficient conditions for a linear code C to be proper, derived in [6], were stated in terms of the weight distribution of the dual code $C^{\perp}$. The reason for doing this was that in some situations the “dual” sufficient conditions turned out to be technically more effective. In particular, this is the case when $C^{\perp}$ has a small dimension or a small number of non-zero weights.

In this paper we prove that the duals of the MMD codes are proper by making use of the dual sufficient conditions in [8]. For completeness, we present these conditions and describe briefly the MMD codes in Section 2 below. The main result and its proof are given in Section 3.

2 Preliminaries

Let C be an $[n,k,d]_q$ code and let $\{B_0,\ldots,B_n\}$ be the weight distribution of the dual code $C^{\perp}$ of minimum distance $d^{\perp}$. We introduce the coefficients

$$B_0^* = 0, \quad B_\ell^* = \sum_{i=1}^{\ell} \frac{\ell_{(i)}}{n_{(i)}} B_i, \quad \ell = 1,\ldots,n, \tag{2}$$

where $j_{(i)}$ denotes the i^{th} factorial moment $j(j-1)\ldots(j-i+1)$.

It was shown in [8] that if the inequalities

$$B_{n-\ell}^* \geq B_{n-\ell+1}^* - q^{n-k-\ell}(q-1), \quad \ell = d+1,\ldots,n \tag{3}$$

hold, then C is proper for error detection.

Remark. It should be noted that the above sufficient conditions immediately imply that the well known *maximum distance separable* (MDS) codes are proper, a result obtained earlier in [12]. For if C is an MDS code then $d^{\perp} = n-d+2 > n-d-1$, and (2) gives $B_{n-\ell}^* = 0$ for $\ell = d+1,\ldots,n$, i.e., the inequalities (3) hold true.

Following [17] we now give a short presentation of the MMD codes and their classification up to formal equivalence. Recall that two codes are said to be formally equivalent if they have the same weight distribution.

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 of C, i.e.,

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

If $s(C) = 0$, C is an MDS code. For all other codes the defect is positive. If s is the defect of C and $k \geq m+1$ for some integer $m \geq 1$, then

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

When

$$d = \frac{q^m(q-1)}{q^m-1}(s+m), \tag{4}$$

C is called a *maximum minimum distance* (MMD) code. In this case, if $s \geq 1$ then $m = s(C^\perp) =: s^\perp$.

The MMD codes have been classified in [17] (see also [11]) up to formal equivalence as follows.

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

A1. The $[t\frac{q^k-1}{q-1}, k, tq^{k-1}]$ t-times repeated Simplex code with $t = 1, 2, \ldots$.

A2. The $[q^{k-1}, k, (q-1)q^{k-2}]$ generalized Reed-Muller code of first order. Here, if $q = 2$ then $k \geq 4$.

A3. The $[q^2 + 1, 4, q^2 - q]_q$ projective elliptic quadratic code with $q \neq 2$.

A4. The $[(2^t - 1)q + 2^t, 3, (2^t - 1)q]_q$ Denniston code with $1 \neq 2^t | q$.

A5. The $[12, 6, 6]_3$ extended Golay code.

A6. The dual $[11, 5, 6]_3$ Golay code.

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

C. Let C be a q-nary MMD code of dimension k and defect $s = 0$. Then C is equivalent to the $[k+1, k, 2]_2$ 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 [17] as follows:

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

$$\begin{aligned} A_{n-k+v} = \binom{n}{k-v} \sum_{i=0}^{v-m} (-1)^i \binom{n-k+v}{i} (q^{v-i} - 1) \\ - \frac{(-1)^{v-m}(s+m-1)(q^m-1)}{v+s-1} \binom{n}{k-v} \binom{n-k+v}{v-m}, \end{aligned} \tag{5}$$

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

3 The main result and its proof

The following is the principal result of this work.

Theorem *The duals of the MMD codes are proper for error detection*

Proof. Let $C_0^{\perp}$ be the dual of some MMD code C_0. Then C_0 is formally equivalent to some code in **A1-A6**, **B** or **C**. When this code is from **A1** with $t = 1$, **A5**, **A6**, **B** with $s = 0$ or **C**, the statement that $C_0^{\perp}$ is proper is easily proved, so we start by considering these cases.

Assume first that C_0 is equivalent to the $[\frac{q^k-1}{q-1}, k, q^{k-1}]$ Simplex code in **A1** or to the $[q+1, 2, q]_q$ Simplex code in **B**. The dual of the Simplex code is a Hamming code which is proper ([14], p. 47). Hence $C_0^{\perp}$ itself is proper.

Now, let C_0 be formally equivalent to the $[12, 6, 6]_3$ extended Golay code in **A5.** The latter is proper (see, e.g., [9]) and is known to be self-dual. Thus $C_0^{\perp}$ is proper as well.

If C_0 is equivalent to the dual $[11, 5, 6]_3$ Golay code as in **A6** then $C_0^{\perp}$ is equivalent to the $[11, 6, 5]_3$ Golay code which is proper ([14], p. 106). Consequently, $C_0^{\perp}$ is proper. Note that this can also be concluded by using the sufficient conditions (3^0) in the proof of Lemma 2 below. Since for $C_0 \quad d-1 = 5$ and $n - d^{\perp} - 1 = 5$ in this case (3^0) contains only the inequality $0 \geq A_6^* - \frac{2}{3}$, which is true since $A_6 = 132$ by (5) and thus $A_6^* = A_6/\binom{11}{6} = 0.2857 < \frac{2}{3}$.

Furthermore, if C_0 is equivalent to the $[k+1, k, 2]_2$ MDS code as in **C**, then $C_0^{\perp}$ is an MDS code and is therefore proper (see [12] and also the Remark in the previous section).

Assume now that C_0 is formally equivalent to some code C from **A1** with $t \geq 2$, **A2-A4** or **B** with $s \geq 1$. We know that if the weight distribution of C_0 satisfies the inequalities (3), then $C_0^{\perp}$ is proper. Since C_0 and C' are formally equivalent, the inequalities (3) hold for C_0 if and only if they hold for C'. In this way, to complete the proof it suffices to show that the weight distributions of the codes in **A1** with $t \geq 2$, **A2-A4** and **B** with $s \geq 1$ satisfy the inequalities (3). This will be established in Lemma 2 below after a preliminary lemma, in which we reformulate the conditions (3) in a form more appropriate for the codes under consideration, reducing in this way the technical work of the proof of Lemma 2.

Lemma 1. *Let the code $C^\perp$ of defect $s^\perp$ and minimum distance $d^\perp$ be the dual of the $[n,k,d]_q$ code C of defect s and weight distribution $\{A_0,\dots,A_n\}$. If*

$$A_{d+1} = A_{d+2} = \dots = A_{n-d^\perp} = 0, \tag{6}$$
$$(q-1)(n-d^\perp) \le q(d-1), \tag{7}$$
$$(q-1)q^{s^\perp - 2} \ge \frac{(n-d^\perp-1)_{(d-1)}}{(n-1)_{(d-1)}} \cdot \frac{d}{n} A_d, \tag{8}$$

and

$$A_d \le (q-1)q^{-s}\binom{n}{d}, \tag{9}$$

then $C^\perp$ is proper.

Proof. Assume that (6)-(9) hold for C. The statement will follow if we show that (6)-(9) imply (3). Introduce the coefficients

$$A_0^* = 0, \quad A_{\ell'}^* = \sum_{i=1}^{\ell'} \frac{\ell'_{(i)}}{n_{(i)}} A_i, \quad \ell' = 1,\dots,n. \tag{10}$$

In terms of the parameters of the code C the conditions (3) take the form

$$A_{n-\ell'}^* \ge A_{n-\ell'+1}^* - q^{n-k^\perp-\ell'}(q-1), \quad \ell' = d^\perp + 1,\dots,n.$$

Denote $\ell = n - \ell'$, $\ell = 0,\dots,n-d^\perp-1$ and write these inequalities in the form

$$A_\ell^* \ge A_{\ell+1}^* - q^{\ell-k^\perp}(q-1), \quad \ell = 0,\dots,n-d^\perp-1.$$

From (6), $d \le n - d^\perp - 1$ and the above inequalities are then equivalent to

$$A_\ell^* \ge A_{\ell+1}^* - q^{\ell-k^\perp}(q-1), \quad \ell = d-1,\dots,n-d^\perp-1. \tag{3^0}$$

We now split these conditions into two parts by considering the case $\ell = d-1$ separately. Replacing $k^\perp$ with $n-k$ and $d-1-n+k$ with $-s$ we obtain that for the code under consideration the conditions (3) are equivalent to

$$A_{\ell+1}^* - A_\ell^* \le q^{\ell-n+k}(q-1), \quad \ell = d,\dots,n-d^\perp-1, \tag{$3'$}$$

$$A_d^* \le q^{-s}(q-1). \tag{$3''$}$$

However, ($3''$) holds for C, because $A_d^* = A_d/\binom{n}{d}$ by (10) and ($3''$) is then just (9). We will show that ($3'$) also holds for C by proving that because of (6) and

(7) the $n-d^{\perp}-d$ inequalities in $(3^{'})$ are in fact equivalent to the inequality (8). From (6) and (10), the coefficients A_{ℓ}^{*} involved in $(3^{'})$ are of the form

$$A_{\ell}^{*}=\frac{\ell_{(d)}}{n_{(d)}}A_{d},\quad \ell=d,\ldots,n-d^{\perp}.$$

In this way, for $\ell=d,\ldots,n-d^{\perp}-1$ we have

$$\frac{A_{\ell+1}^{*}}{A_{\ell}^{*}}=\frac{(\ell+1)_{(d)}}{\ell_{(d)}}=\frac{\ell+1}{\ell+1-d}=1+\frac{d}{\ell+1-d}$$

and thus

$$\begin{aligned}A_{\ell+1}^{*}-A_{\ell}^{*}&=\frac{d}{\ell+1-d}A_{\ell}^{*}=\frac{d}{\ell+1-d}\cdot\frac{\ell_{(d)}}{n_{(d)}}A_{d}\\&=\frac{d}{\ell+1-d}\cdot\frac{\ell(\ell-1)\ldots(\ell+1-d)}{n_{(d)}}A_{d}=\ell_{(d-1)}\cdot\frac{d}{n_{(d)}}A_{d}.\end{aligned}$$

Hence $(3^{'})$ is equivalent to

$$\frac{q^{\ell}}{\ell_{(d-1)}}\geq\frac{q^{n-k}}{q-1}\cdot\frac{d}{n_{(d)}}A_{d},\quad \ell=d,\ldots,n-d^{\perp}-1. \tag{$3^{'''}$}$$

Consider the ratio

$$\frac{q^{\ell+1}}{(\ell+1)_{(d-1)}}:\frac{q^{\ell}}{\ell_{(d-1)}}=q\frac{\ell+2-d}{\ell+1}$$

$$=q\Big(1-\frac{d-1}{\ell+1}\Big)<q\Big(1-\frac{d-1}{n-d^{\perp}}\Big),\quad \ell=d,\ldots,n-d^{\perp}-2$$

and apply (7) to get

$$\frac{q^{\ell+1}}{(\ell+1)_{(d-1)}}:\frac{q^{\ell}}{\ell_{(d-1)}}<q\Big(1-\frac{q-1}{q}\Big)=1,\quad \ell=d,\ldots,n-d^{\perp}-2,$$

and consequently

$$\min_{d\leq\ell\leq n-d^{\perp}-1}\frac{q^{\ell}}{\ell_{(d-1)}}=\frac{q^{n-d^{\perp}-1}}{(n-d^{\perp}-1)_{(d-1)}}.$$

Thus for the code C the $n-d^{\perp}-d$ inequalities in $(3^{'''})$ are actually equivalent to the one inequality

$$\frac{q^{n-d^{\perp}-1}}{(n-d^{\perp}-1)_{(d-1)}}\geq\frac{q^{n-k}}{q-1}\cdot\frac{d}{n_{(d)}}A_{d}$$

and hence to

$$(q-1)q^{k-d^{\perp}-1} \geq \frac{(n-d^{\perp}-1)_{(d-1)}}{(n-1)_{(d-1)}} \cdot \frac{d}{n} A_d,$$

which is in fact (8), since $k-d^{\perp}-1 = s^{\perp}-2$.

We have shown in this way that $(3')$ and $(3'')$ hold for C. Consequently, (3) holds for C and $C^{\perp}$ is thus proper. □

Lemma 2. *The codes in* **A1** *with* $t \geq 2$, **A2-A4** *and* **B** *with* $s \geq 2$ *satisfy the conditions (6)-(9).*

Proof. We start by the first case.

A1, $t \geq 2$. Let C be the $[t\frac{q^k-1}{q-1}, k, tq^{k-1}]_q$ $t-$times repeated Simplex code with $k \geq 3$, $\quad t = 2, 3, \ldots$. It easily follows from (4) and (5) that

$$\begin{aligned} &s = t\frac{q^k-1}{q-1} - k + 1 - tq^{k-1} = t\frac{q^{k-1}-1}{q-1} - k + 1, \\ &s^{\perp} = k-1, \quad d^{\perp} = 2, \quad A_d = q^k - 1, \quad A_{d+1} = \ldots = A_n = 0. \end{aligned} \tag{11}$$

As we see, (6) holds for C. We now check (7). Since $t + (q-2) > 0$, we have that

$$t(q^k-1) - 2(q-1) < tq^k - q,$$

or, equivalently, that

$$(q-1)(n-2) < q(d-1),$$

which is (7). By (11), for the present code (8) has the form

$$(q-1)q^{k-3} \geq \frac{(n-3)_{(d-1)}}{(n-1)_{(d-1)}} \cdot \frac{tq^{k-1}(q-1)}{t(q^k-1)}(q^k-1),$$

or, equivalently,

$$\frac{(n-1)(n-2)}{(n-d)(n-d-1)} \geq q^2.$$

But this inequality is valid since

$$\frac{n-1}{n-d} \cdot \frac{n-2}{n-d-1} > \Big(\frac{n-1}{n-d}\Big)^2 = \Big(\frac{q^k - 1 - \frac{q-1}{t}}{q^{k-1}-1}\Big)^2$$

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

$$= \Big(q + \frac{q-1}{q^{k-1}-1} \cdot \big(1 - \frac{1}{t}\big)\Big)^2 > q^2.$$

Hence (8) holds for C. To prove (9) we first note that

$$\binom{n}{d} = \binom{n}{n-d} = \prod_{j=0}^{n-d-1} \frac{n-j}{n-d-j} = (d+1) \prod_{j=0}^{n-d-2} \frac{n-j}{n-d-j}$$

$$> \left(\frac{n}{n-d}\right)^{n-d-1} \cdot d = \left(\frac{t\frac{q^k-1}{q-1}}{t\frac{q^{k-1}-1}{q-1}}\right)^{s+k-2} \cdot tq^{k-1}$$

$$= \left(\frac{q^k-1}{q^{k-1}-1}\right)^{s+k-2} tq^{k-1} > \left(\frac{q^k-q}{q^{k-1}-1}\right)^{s+k-2} q^{k-1} = q^{s+2k-3}.$$

Using this in the left-hand side of (9) we obtain

$$(q-1)q^{-s}\binom{n}{d} > (q-1)q^{-s}q^{s+2k-3}$$

$$= (q-1)q^{2k-3} = (q-1)q^{k-3} \cdot q^k \geq q^k > q^k - 1 = A_d,$$

where we have used the fact that $k \geq 3$ and that $q \geq 2$. In this way, (9) also holds for C.

A2. Now, let C be a $[q^{k-1}, k, (q-1)q^{k-2}]_q$ code with $k \geq 4$ when $q = 2$. In this case, (4) and (5) give

$$\begin{aligned} &s = q^{k-2} - k + 1, \quad s^{\perp} = k-2, \quad d^{\perp} = 3, \\ &A_d = q(q^{k-1} - 1), \quad A_{d+1} = \ldots = A_{n-1} = 0. \end{aligned} \tag{12}$$

Thus (6) holds for C. To prove (7) we use that $q > 3/2$ implies $q/(q-1) < 3$ and thus

$$q^{k-1} - 3 < q^{k-1} - \frac{q}{q-1}.$$

From this we obtain

$$(q-1)(q^{k-1} - 3) < q\Big((q-1)q^{k-2} - 1\Big)$$

which is (7). By (12), in this case (8) becomes

$$(q-1)q^{k-4} \geq \frac{(n-4)_{(d-1)}}{(n-1)_{(d-1)}} \cdot \frac{(q-1)q^{k-2}}{q^{k-1}} q(q^{k-1} - 1)$$

or, equivalently (note that since $k \geq 4$ when $q = 2$ there are no zero factors in the denominators below)

$$\frac{q^{k-1}-1}{q^{k-4}} \leq \frac{(n-1)(n-2)(n-3)}{(n-d)(n-d-1)(n-d-2)}$$

$$= \frac{(q^{k-1}-1)(q^{k-1}-2)(q^{k-1}-3)}{q^{k-2}(q^{k-2}-1)(q^{k-2}-2)}.$$

Thus in this case (8) is equivalent to

$$(q^{k-1}-2)(q^{k-1}-3) \geq q^2(q^{k-2}-1)(q^{k-2}-2) = (q^{k-1}-q)(q^{k-1}-2q)$$

which is evidently true. Finally, using (12) again we see that for the code C the inequality (9) becomes

$$q(q^{k-1}-1) \leq (q-1)q^{-q^{k-2}+k-1}\binom{n}{d}.$$

This is equivalent to

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

which is the same as

$$\frac{n(n-1)\dots(d+1)}{(n-d)(n-d-1)\dots 1} \geq \frac{q^{q^{k-2}-k+2}(q^{k-1}-1)}{(q-1)}.$$

Replacing n by q^{k-1} and d by $(q-1)q^{k-2}$ we get

$$\frac{q^{k-1}(q^{k-1}-1)\dots(q^{k-1}-q^{k-2}+1)}{q^{k-2}(q^{k-2}-1)\dots 1} \geq \frac{q^{q^{k-2}-k+2}(q^{k-1}-1)}{(q-1)}$$

and (9) becomes

$$\prod_{1}^{q^{k-2}-2} \frac{q^{k-1}-1-j}{q^{k-2}-j} \geq \frac{q^{q^{k-2}-k+1}}{q-1}.$$

To prove this inequality we note that $(q-1)j \geq 1$. Hence $qj \geq 1+j$ and therefore

$$q^{k-1}-1-j \geq q^{k-1}-qj = q(q^{k-2}-j).$$

Using this and that $k \geq 3$ we obtain

$$\prod_{1}^{q^{k-2}-2} \frac{q^{k-1}-1-j}{q^{k-2}-j} \geq q^{q^{k-2}-2} = q^{q^{k-2}-(3-1)} \geq q^{q^{k-2}-(k-1)} \geq \frac{q^{q^{k-2}-k+1}}{q-1}$$

and hence (9) is proved.

A3. Consider a $[q^2+1, 4, q^2-q]_q$ code C with $q \neq 2$. In this case (4) and (5) show

$$\begin{aligned}
&s = q-2, \quad s^{\perp} = 1, \quad d^{\perp} = 4; \\
&A_d = (q^2+1)q(q-1) = nd; \\
&A_{d+1} = \ldots = A_{n-2} = 0.
\end{aligned} \tag{13}$$

Thus (6) holds for C. We now check (7). Since $2q > 3$ we have

$$q^3 - q^2 - 3q + 3 < q^3 - q^2 - q$$

and

$$(q-1)(q^2-3) < q(q^2-q-1),$$

which is just (7). Next, by (13) we find that in this case (8) takes the form

$$(q-1)q^{-1} \geq \frac{(n-5)_{(d-1)}}{(n-1)_{(d-1)}} \cdot \frac{d}{n} \cdot nd$$

or, equivalently,

$$q^3(q-1) \leq \frac{(n-1)(n-2)(n-3)(n-4)}{(n-d)(n-d-1)(n-d-2)(n-d-3)},$$

where the right-hand side can be written as ($q \neq 2$)

$$\frac{q^2(q^2-1)(q^2-2)(q^2-3)}{(q+1)q(q-1)(q-2)} = \frac{q(q^2-2)(q^2-3)}{q-2} = \frac{q(q^4-5q^2+6)}{q-2}.$$

Therefore, in this case (8) is equivalent to the inequality

$$q^4 - 5q^2 + 6 \geq (q-2)(q^3-q^2) = q^4 - 3q^3 + 2q^2$$

and consequently to

$$3q^3 - 7q^2 + 6 \geq 0.$$

This is true, since

$$3q^3 - 7q^2 + 6 > 3q^3 - 7q^2 + 4 = 3(q-1)(q-2)(q+\frac{2}{3}) > 0.$$

Thus (8) is satisfied for C. Now, consider (9), which by (13) takes the form

$$(q^2+1)q(q-1) \leq (q-1)q^{-(q-2)}\binom{n}{d},$$

or, equivalently

$$\binom{n}{d} \geq q^{q-1}(q^2+1).$$

The latter holds true, since

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

$$= \frac{q^2+1}{q+1}\cdot q\prod_{j=1}^{q-1}\frac{q^2-j}{q-j} > \frac{q^2+1}{q+1}\cdot q\Big(\frac{q^2-1}{q-1}\Big)^{q-1}$$

$$= (q^2+1)q(q+1)^{q-2} > (q^2+1)q^{q-1}.$$

A4. Let C be a $[(2^t-1)q+2^t, 3, (2^t-1)q]_q$. For this code (4) and (5) give

$$\begin{aligned} &s = 2^t-2, \quad s^{\perp} = 1, \quad d^{\perp} = 3, \\ &A_d = \frac{n}{2^t}(q^2-1), \quad A_{d+1} = \ldots = A_{n-1} = 0. \end{aligned} \tag{14}$$

Again, (6) holds for C. By (14), in this case (7) becomes

$$(q-1)((2^t-1)q+2^t-3) \leq q((2^t-1)q-1)$$

or

$$q^2(2^t-1) - q(2^t-1) + (q-1)(2^t-3) \leq q^2(2^t-1) - q.$$

This is equivalent to

$$-q(2^t-1) + q(2^t-1) - 2q - 2^t + 3 \leq -q$$

and finally to

$$(2^t-1) + (q-2) \geq 0,$$

which is clearly true. Hence (7) holds for C. Using again (14) we find that in this case (8) is

$$(q-1)q^{-1} \geq \frac{(n-4)_{(d-1)}}{(n-1)_{(d-1)}}\cdot\frac{d}{n}\cdot\frac{n}{2^t}(q^2-1)$$

and consequently

$$\frac{(n-1)(n-2)(n-3)}{(n-d)(n-d-1)(n-d-2)} \geq \frac{2^t-1}{2^t}q^2(q+1).$$

Note that since the defect of the code under consideration is positive, we must have $t > 1$. The factor $n - d - 2 = 2^t - 2$ is thus positive and so are the other factors in the denominator of the right-hand side above. We now have

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

and

$$\frac{n-3}{n-d-2} > \frac{n-2}{n-d-1} = \frac{(2^t-1)q + 2^t - 2}{2^t - 1} = q + \frac{2^t-2}{2^t-1} > q,$$

so that

$$\frac{n-1}{n-d} \cdot \frac{n-2}{n-d-1} \cdot \frac{n-3}{n-d-2} > \frac{2^t-1}{2^t} q^2(q+1),$$

i.e., (8) holds for C. Furthermore, (9) is in this case

$$\frac{n}{2^t}(q^2-1) \leq (q-1)q^{-(2^t-2)}\binom{n}{d},$$

or,

$$\binom{n}{n-d} \geq \frac{n}{2^t} \cdot (q+1)q^{2^t-2}.$$

This is equivalent to

$$\frac{n(n-1)\ldots(d+1)}{(n-d)(n-d-1)\ldots 1} \geq \frac{n}{2^t}(q+1)q^{2^t-2}$$

and, since $n - d = 2^t$, to

$$\frac{(n-1)\ldots(d+1)}{(n-d-1)\ldots 1} \geq (q+1)q^{2^t-2}.$$

For the left-hand side above we have

$$\prod_{j=1}^{n-d-1} \frac{n-j}{n-d-j} > \left(\frac{n-1}{n-d-1}\right)^{n-d-1} = \left(\frac{(2^t-1)q + 2^t - 1}{2^t - 1}\right)^{2^t-1}$$

$$= (q+1)^{2^t-1} > (q+1)q^{2^t-2}.$$

Hence (9) also holds for C.

We have now come to the last case of the proof of Lemma 2.

B, $s \geq 1$. Let C be the $[(s+1)(q+1), 2, (s+1)q]_q$ $(s+1)$-times repeated Simplex code of defect s, $s = 1, \ldots,$ and dimension 2. We have shown in the case **A1** of this proof that the t-times repeated Simplex code of dimension $k \geq 3$ with $t = 2, \ldots$ satisfies (6)-(9). Since the proof of (6)-(8) did not take advantage of the fact that $k \geq 3$, it carries over to $k = 2$ as well. To prove (9) in this case, we notice that $A_d = q^2 - 1$ by (5) and (9) thus becomes

$$(q-1)q^{-s}\binom{n}{d} \geq q^2 - 1,$$

or, equivalently,

$$q^{-s}\binom{n}{d} \geq q + 1.$$

Since in this case $s = n - d - 1 \geq 1$ we have

$$\binom{n}{d} = \binom{n}{n-d} = \prod_{0}^{n-d-1} \frac{n-j}{n-d-j} > \left(\frac{n}{n-d}\right)^{n-d} = (q+1)^{s+1}$$

and

$$q^{-s}\binom{n}{d} > (q+1)\left(\frac{q+1}{q}\right)^{s} > q+1,$$

i.e., (9) is satisfied for C. □

To conclude, we have shown in Lemma 2 above, that the codes in **A1** with $t \geq 2$, **A2-A4** and **B** with $s \geq 1$ satisfy conditions (6)-(9). So do the MMD codes which are formally equivalent to codes considered in Lemma 2. By Lemma 1, the duals of these MMD codes are proper, and the proof of the Theorem is now complete. □

References

[1] T. Baicheva, S. M. Dodunekov, and P. Kazakov, On the cyclic redundancy-check codes with 8-bit redundancy, Computer Communications 21 (1998) 1030-1033.

[2] T. Baicheva, S. M. Dodunekov, and P. Kazakov, On the cyclic redundancy-check codes of 16-bit redundancy, in: Proc. VI Intern. Workshop on ACCT (Pskov, Russia, 1998) 17-21.

[3] T. Baicheva, S. M. Dodunekov, and P. Kazakov, On the error detection performance of some standardized CRC codes, in: Proc. Telecom 98 (Drujba, Bulgaria, 1998) 66-72.

[4] T. Baicheva, S. N. Dodunekov, and P. Kazakov, Undetected error probability performance of cyclic redundancy-check codes of 16-bit redundancy, IEEE Proc. Commun. 147 (2000), 253-256.

[5] R. Dodunekova and S. M. Dodunekov, On the probability of undetected error for Near-MDS codes, *preprint* 1995-25, Chalmers University of Technology and Göteborg University (1995) 13 p.

[6] R. Dodunekova and S. M. Dodunekov, Sufficient conditions for good and proper error detecting codes, IEEE Trans. Inform. Theory 43 (1997) 2023-2026.

[7] R. Dodunekova and S. M. Dodunekov, and T. Kløve, Almost-MDS codes and Near MDS codes for error detection, IEEE Trans. Inform. Theory 43 (1997) 285-290.

[8] R. Dodunekova and S. M. Dodunekov, Sufficient Conditions for Good and Proper Linear Error Detecting Codes via Their Duals, Mathematica Balkanica (New Series) 11 (1997) 375-381.

[9] R. Dodunekova and S. M. Dodunekov, The MMD codes are proper for error detection, *preprint* 2002:7, Chalmers University of Technology and Göteborg University (2002) 9 p.

[10] S. M. Dodunekov and I. N. Landgev, On Near-MDS codes, Journal of Geometry 54 (1995) 30-43.

[11] A. Faldum and W. Willems, A characterization of MMD codes, IEEE Trans. Inform. Theory 44 (1998) 1555-1558.

[12] T. Kasami and S. Lin, On the probability of undetected error for the Maximum Distance Separable Codes, IEEE Trans. Inform. Theory IT-25 (1979) 110-112.

[13] P. Kazakov, Application of Polynomials to CRC and Spherical Codes, PhD Thesis, Technishe Universitet Delft, 2000.

[14] T. Kløve and V. Korzhik, Error detecting codes, General Theory and Their Application in Feedback Communication Systems (Kluwer, Boston, MA 1995).

[15] S. K. Leung, E. R. Barnes, and D. U. Friedman, Some properties of undetected error probability of linear codes, IEEE Thans. Inform. Theory IT-25 (1979) 110-112.

[16] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes (North-Holland, New York, 1997).

[17] J. Olsson and W. Willems, A Characterization of Certain Griesmer Codes: MMD Codes in a More General Sense, IEEE Trans. Inform. Theory 45 (1999) 2138-2142.