CHALMERS | GÖTEBORGS UNIVERSITET

PREPRINT

On the Error-Detecting Performance of Some Classes of Block Codes

R. DODUNEKOVA
S. M. DODUNEKOV
E. NIKOLOVA

Department of Mathematical Statistics
CHALMERS UNIVERSITY OF TECHNOLOGY
GÖTEBORG UNIVERSITY
Göteborg Sweden 2004

Preprint 2004:13

On the Error-Detecting Performance of Some Classes of Block Codes

R. Dodunekova
S. M. Dodunekov
E. Nikolova

Mathematical Statistics
Department of Mathematics
Chalmers University of Technology and Göteborg University
SE-412 96 Göteborg, Sweden
Göteborg, March 2004

NO 2004:13
ISSN 0347-2809

Matematiska Vetenskaper
Göteborg 2004

On the error-detecting performance of some classes of block codes

R. Dodunekova[1]
Mathematical Sciences
Chalmers University of Technology
and Göteborg University
412 96 Göteborg, Sweden

S. M. Dodunekov[2]
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
8 G. Bonchev Str.
1113 Sofia, Bulgaria

E. Nikolova
Computer Science
Bourgas Free University
101 Aleksandrovska Str.
8000 Bourgas, Bulgaria

Abstract We establish the properness of some classes of binary block codes with symmetric distance distribution, including the Kerdock codes and codes which satisfy the Grey-Rankin bound, and also the properness of the Preparata codes, thus augmenting the list of the very few known proper nonlinear codes.

Keywords error detection, proper code, Grey-Rankin bound, weight distribution.

1 Introduction

The performance of an $[n, k, d]_q$ linear code C in detecting errors on a q-ary symmetric memoryless channel with symbol error probability ε is estimated by the probability of undetected error $P_{ue}(C, \varepsilon)$. In terms of the Hamming weight

[1]Supported by the Swedish Research Council under grant 621-2003-5325.
[2] Partially supported by the Bulgarian NSF under Contract MM901/99.

distribution $\{A_0, A_1, \ldots, A_n\}$ of C this probability is expressed as

$$P_{ue}(C, \varepsilon) = \sum_{i=d}^{n} A_i \Big(\frac{\varepsilon}{q-1}\Big)^i (1-\varepsilon)^{n-i}, \quad 0 \le \varepsilon \le \frac{q-1}{q}, \tag{1.1}$$

and in terms of the dual Hamming weight distribution $\{B_0, B_1, \ldots, B_n\}$ as

$$P_{ue}(C, \varepsilon) = q^{-(n-k)} \sum_{i=0}^{n} B_i \Big(1 - \frac{q\varepsilon}{q-1}\Big)^i - (1-\varepsilon)^n, \quad 0 \le \varepsilon \le \frac{q-1}{q}. \tag{1.2}$$

We notice that when a nonlinear distance invariant code $C = (n, k, d)_q$ is used for error detection on a symmetric memoryless channel with symbol error probability ε, the probability of undetected error of the code is given by the right hand side of (1.1) with A_i replaced by the corresponding term of the distance distribution, i.e., by the number of pairs of codewords at distance i in C. In particular, (1.1) remains true for the probability of undetected error of a nonlinear distance invariant code for which the distance distribution and the code weight distribution coincide.

A code is *proper* for error detection on a q-ary symmetric memoryless channel with symbol error probability ε if the undetected error probability of the code increases in $\varepsilon \in [0, \frac{q-1}{q}]$ (see [7], [8]).

The problem of establishing properness of parametric classes of linear codes has been considered in a number of works, see the monograph [7] and the recent summary [2], and it has become clear that most often analytical study of the function $P_{ue}(C, \varepsilon)$ would not work, unless the formulas of the code weight distribution are relatively simple, which is the case here.

In this work we study several classes of block codes with respect to properness. For completeness, in Section 2 we recall basic facts about these codes, together with a technical lemma which will be used in the sequel. In Section 3 we establish the properness of binary block codes with sufficiently large minimum code distance, among which the Kerdock codes and codes which satisfy the Grey-Rankin bound, and in Section 4 we prove that the Preparata codes are proper. In this way we augment the list of the very few nonlinear codes known to be proper in error detection.

For all results and notions which are not introduced here we refer to the monographs [7] and [10].

2 Preliminaries

Here we recall some basic facts about the codes to be studied below.

The Kerdock codes [6] and the Preparata codes [11] are most interesting classes of nonlinear binary codes. They are both Hamming-distance invariant,

for both the distance distribution coincides with the code weight distribution, and their weight enumerators are MacWilliams dual just as if the codes were linear, see [14] and Sections 15.5 and 15.6 in [10]. The above phenomenon was explained in [4], where it was shown that Kerdock and Preparata codes are self-dual as Z_4-linear codes. Thus formulas (1.1) and (1.2) for the probability of undetected error apply for these codes as well.

For even integer m greater than two, the Kerdock code $\mathcal{K}(m)$ has basic parameters

$$n = 2^m, \quad |\mathcal{K}(m)| = 2^{2m}, \quad d = 2^{m-1} - 2^{\frac{m-2}{2}},$$

and the weight distribution is given by the following table.

weight i	the number of codewords of weight i
0	1
$2^{m-1} - 2^{\frac{m-2}{2}}$	$2^m(2^{m-1} - 1)$
2^{m-1}	$2^{m+1} - 2$
$2^{m-1} + 2^{\frac{m-2}{2}}$	$2^m(2^{m-1} - 1)$
2^m	1

The properness of the Kerdock codes will follow from Theorem 1 which establishes properness of codes with symmetric weight distribution, while the properness of the Preparata codes will be shown by using (1.2), which in this case involves the basic parameters and the weight distribution of the Kerdock codes.

Consider a binary code $C = (n, M, d)$ for which $\mathbf{1} + c \in C$ for every codeword $c \in C$. For such a code the number of pairs of codewords at distance i equals the number of pairs of codewords at distance $n - i$, i.e., the distance distribution of the code is symmetric. It has been shown that the parameters of C satisfy the inequality (see (17.46) in [10], Chapter 17)

$$M \leq \frac{8d(n-d)}{n - (n-2d)^2}, \tag{2.1}$$

provided the denominator is positive. The inequality is known as the Grey-Rankin bound, see [3] and [13]. As above, the properness of codes meeting or satisfying this bound will follow from Theorem 1. We provide also examples of interesting families of proper codes meeting the Grey-Rankin bound.

The following technical lemma will be used in the sequel.

Lemma. Let n, τ_1 and τ_2 be positive integers such that $0 < \tau_1 < \frac{n}{2} \leq \tau_2 \leq n$, and let $a > 0$, $b > 0$. Then the function

$$G(\varepsilon) = a\varepsilon^{\tau_1}(1-\varepsilon)^{n-\tau_1} + b\varepsilon^{\tau_2}(1-\varepsilon)^{n-\tau_2}$$

is increasing in $\varepsilon \in [0, \frac{1}{2}]$ if

$$a(n - 2\tau_1) \le b(2\tau_2 - n) \tag{2.2}$$

and if either

$$\tau_1 + \tau_2 \le n \text{ and } \frac{\tau_1\tau_2}{n} \ge \frac{(\tau_1 + \tau_2 - 1)^2}{4(n-1)} \tag{2.3}$$

or

$$\tau_1 + \tau_2 \ge n \text{ and } (n - 2\tau_1)(2\tau_2 - n) \le n. \tag{2.4}$$

Proof. Denote $\varepsilon_1 = \frac{\tau_1}{n} < \frac{1}{2}$ and $\varepsilon_2 = \frac{\tau_2}{n} \ge \frac{1}{2}$. From

$$[\varepsilon^{\tau_i}(1-\varepsilon)^{n-\tau_i}]' = n\varepsilon^{\tau_i - 1}(1-\varepsilon)^{n-\tau_i-1}(\varepsilon_i - \varepsilon) \tag{2.5}$$

we obtain

$$G'(\varepsilon) = nb\varepsilon^{\tau_2-1}(1-\varepsilon)^{n-\tau_2-1}(\varepsilon_2 - \varepsilon)\Big[1 - \frac{a}{b}\Big(\frac{1-\varepsilon}{\varepsilon}\Big)^{\tau_2-\tau_1}\frac{\varepsilon - \varepsilon_1}{\varepsilon_2 - \varepsilon}\Big]. \tag{2.6}$$

It follows from (2.5) that $G'(\varepsilon)$ is non-negative in $[0, \varepsilon_1)$. It thus suffices to establish that $G'(\varepsilon)$ is non-negative in $[\varepsilon_1, 1/2]$. Obviously, the sign of $G'(\varepsilon)$ in this interval is the same as the sign of the function in the brackets on the right side of (2.6). Setting

$$g(\varepsilon) = \Big(\frac{1-\varepsilon}{\varepsilon}\Big)^{\tau_2-\tau_1}\frac{\varepsilon - \varepsilon_1}{\varepsilon_2 - \varepsilon}, \quad \varepsilon_1 \le \varepsilon \le 1/2,$$

we get

$$g'(\varepsilon) = \Big(\frac{1-\varepsilon}{\varepsilon}\Big)^{\tau_2-\tau_1-1}\frac{1}{\varepsilon^2}\frac{\varepsilon_2 - \varepsilon_1}{(\varepsilon_2 - \varepsilon)^2}[(1-\varepsilon)\varepsilon - n(\varepsilon - \varepsilon_1)(\varepsilon_2 - \varepsilon)], \tag{2.7}$$

where the function in the brackets,

$$\begin{aligned}\tilde{g}(\varepsilon) &= (n-1)\varepsilon^2 + [1 - n(\varepsilon_1 + \varepsilon_2)]\varepsilon + n\varepsilon_1\varepsilon_2 \\ &= (n-1)\Big(\frac{\tau_1 + \tau_2 - 1}{2(n-1)} - \varepsilon\Big)^2 + \frac{\tau_1\tau_2}{n} - \frac{(\tau_1 + \tau_2 - 1)^2}{4(n-1)},\end{aligned}$$

takes its minimum at

$$\overline{\varepsilon} = \frac{\tau_1 + \tau_2 - 1}{2(n-1)} \ge \frac{2\tau_1}{2n} = \varepsilon_1.$$

Assume first that (2.3) holds. Then $\overline{\varepsilon} \le \frac{1}{2}$ and we have

$$\min_{\varepsilon_1 \le \varepsilon \le \frac{1}{2}} \tilde{g}(\varepsilon) = \tilde{g}(\overline{\varepsilon}) = \frac{\tau_1\tau_2}{n} - \frac{(\tau_1 + \tau_2 - 1)^2}{4(n-1)} \ge 0.$$

Assume (2.4). If the first part there holds with equality we have $\overline{\varepsilon} = 1/2$, otherwise $\overline{\varepsilon} > \frac{1}{2}$. Then

$$\min_{\varepsilon_1 \le \varepsilon \le \frac{1}{2}} \tilde{g}(\varepsilon) = \tilde{g}(1/2) = \frac{1}{4} - \frac{(n-2\tau_1)(2\tau_2 - n)}{4n} \ge 0.$$

Since in both cases $\tilde{g}(\varepsilon)$ is non-negative on $[\varepsilon_1,\ \frac{1}{2}]$, $g'(\varepsilon)$ in (2.7) is non-negative in this interval as well. Therefore

$$g(\varepsilon) \le g(1/2) = \frac{n-2\tau_1}{2\tau_2 - n},\ \ \varepsilon_1 \le \varepsilon \le 1/2,$$

and, by this and (2.2),

$$\frac{a}{b} g(\varepsilon) \le \frac{a(n-2\tau_1)}{b(2\tau_2 - n)} \le 1,\ \ \varepsilon_1 \le \varepsilon \le 1/2.$$

This shows that $G'(\varepsilon)$ in (2.6) is non-negative in $[\varepsilon_1, \frac{1}{2}]$, and the Lemma thus follows.

3 Codes with symmetric weight or distance distribution

For simplicity, we will let $\{A_0, A_1, \ldots, A_n\}$ denote as before the code weight distribution, when the code under consideration is linear, but also the distance distribution, when the code is nonlinear.

Theorem 1.

(i) A linear code $C = [n, k, d]$ with $d \ge \dfrac{n}{2} - \dfrac{\sqrt{n}}{2}$ and symmetric weight distribution is proper.

(ii) A nonlinear distance invariant code $C = (n, k, d)$ with $d \ge \dfrac{n}{2} - \dfrac{\sqrt{n}}{2}$ and symmetric distance distribution is proper.

Proof. In both cases, the probability of undetected error of C is given by (1.1) with $A_1, \ldots, A_n$ representing the code weight distribution in the first case and the distance distribution in the second one. Since $A_i = A_{n-i}$ for $1 \le i \le n-1$ we obtain in both cases

$$P_{ue}(C, \varepsilon) = \sum_{d \le i < n/2} \left[A_i \varepsilon^i (1-\varepsilon)^{n-i} + A_{n-i} \varepsilon^{n-i} (1-\varepsilon)^i \right] + A_{\frac{n}{2}} \varepsilon^{\frac{n}{2}} (1-\varepsilon)^{\frac{n}{2}} + A_n \varepsilon^n, \quad (3.1)$$

where $A_{\frac{n}{2}} = 0$ when n is odd, and A_n equals either 0 or 1. The functions

$$G_i(\varepsilon) = A_i \varepsilon^i (1-\varepsilon)^{n-i} + A_{n-i} \varepsilon^{n-i} (1-\varepsilon)^i, \quad d \le i < n/2,$$

satisfy the condition (2.2) of the Lemma since

$$A_i(n-2i) = A_{n-i}(2(n-i)-n),$$

and also the condition (2.4) since

$$i + (n-i) = n$$

and

$$(n-2i)(2(n-i)-n) = (n-2i)^2 \leq (n-2d)^2 \leq (n-(n-\sqrt{n}))^2 = n.$$

By the Lemma, the functions $G_i(\varepsilon)$, $d \leq i < n/2$ in (3.1) are increasing in $\varepsilon \in [0, \frac{1}{2}]$. Since also the sum of the last two terms in (3.1) is an increasing function in this interval, C is proper.

The Kerdock codes given in Section 2 satisfy the condition (ii) of Theorem 1 and we have therefore

Corollary 1. *The Kerdock codes $\mathcal{K}(m)$, $m = 2,\ 4, \ldots$, are proper.*

Assume now that $C = (n, M, d)$ is a binary code satisfying the Grey-Rankin bound (2.1). Since the distance distribution of C is symmetric and

$$n - (n-2d)^2 > 0 \quad \text{iff} \quad \frac{1}{2}(n-\sqrt{n}) < d < \frac{1}{2}(n+\sqrt{n}),$$

for such a code part (ii) of Theorem 1 implies the following.

Corollary 2. *Any binary distance invariant code which satisfies the Grey-Rankin bound is proper.*

Moreover, since a code satisfying the Grey-Rankin bound with equality is distance invariant (see [9]), the above corollary implies for such a code

Corollary 3. *Any binary code which meets the Grey-Rankin bound is proper.*

Examples. Below we give some interesting families of codes which meet the Grey-Rankin bound and thus are proper, by Corollary 3.

A. Brouwer constructed in [1] a family of q-ary two-weight projective codes (i. e., codes with minimum dual distance greater than two) with parameters

$$n = \frac{(q^{e-1}-1)(q^{se-e} + q^{\frac{se}{2}-e})}{q-1}, \quad k = se,$$

where s and e are arbitrary positive integers such that s is even and e is greater than one. The two weights are

$$\omega_1 = (q^{e-1}-1)q^{se-e-1}, \quad \omega_2 = \omega_1 + q^{\frac{se}{2}-1}.$$

In the case $q = 2$, $s = 2$, the resulting code $C_1(e)$ has parameters

$$n = 2^{2e-1} - 2^{e-1}, \quad k = 2e, \quad \text{and} \quad \omega_1 = 2^{2e-2} - 2^{e-1}, \quad \omega_2 = 2^{2e-2}.$$

The code $C(e)$, spanned by C_1 and the all-one vector $\mathbf{1}$, is a projective self-complementary $[n,\, k+1,\, \omega_1]$–code with nonzero weights ω_1, ω_2 and n, which meets the Grey-Rankin bound. The code is thus proper.

Consider the first order Reed-Muller code $RM(1, 2e)$. Since the code $C(e)$ is projective, the code

$$D(e) = RM(1, 2e) \setminus C(e),$$

which consists of the column set of $RM(1, 2e)$ with the columns of $C(e)$ deleted, has parameters

$$[n = 2^{2e-1} + 2^{e-1}, \quad k = 2e + 1, \quad d = 2^{2e-1}],$$

nonzero weights 2^{2e-2}, $\quad 2^{2e-2} + 2^{e-1}$ and $2^{2e-1} + 2^{e-1}$, and it meets the Grey-Rankin bound. Thus $D(e)$ is proper. We note that the codes $C(e)$ and $D(e)$ possess interesting combinatorial properties, see [9] and [5].

4 The Preparata codes

Theorem 2. *The Preparata codes $\mathcal{P}(m)$, $m = 2,\ 4, \ldots$, are proper.*

Proof. Consider a Preparata code $\mathcal{P}(m)$ of parameter m. We know that both formulas (1.1) and (1.2) apply for the probability of undetected error of this code. In terms of the formally dual Kerdock code $\mathcal{K}(m)$ this probability is then

$$P_{ue}(\mathcal{P}(m),\ \varepsilon) = \frac{1}{n^2} \sum_{i=0}^{4} A_{\tau_i} (1 - 2\varepsilon)^{\tau_i} - (1 - \varepsilon)^n, \quad 0 \le \varepsilon \le 1/2, \tag{4.1}$$

where, as given in Section 2,

$$\begin{aligned}
&\tau_0 = 0, && A_{\tau_0} = 1, \\
&\tau_1 = \frac{n - \sqrt{n}}{2}, && A_{\tau_1} = \frac{n(n-2)}{2}, \\
&\tau_2 = \frac{n}{2}, && A_{\tau_2} = 2(n-1), \\
&\tau_3 = \frac{n + \sqrt{n}}{2}, && A_{\tau_3} = \frac{n(n-2)}{2}, \\
&\tau_4 = n, && A_{\tau_4} = 1,
\end{aligned} \tag{4.2}$$

and $n = 2^m$ for $m = 2,\ 4,\ 6 \ldots$. We thus have

$$P'_{ue}(\mathcal{P}(m),\, \varepsilon) = -\frac{2}{n^2} \sum_{i=1}^{4} A_{\tau_i} \tau_i (1-2\varepsilon)^{\tau_i - 1} + n(1-\varepsilon)^{n-1}, \quad 0 \le \varepsilon \le 1/2, \quad (4.3)$$

and

$$\begin{aligned} \frac{P'_{ue}(\mathcal{P}(m),\, \varepsilon)}{n(1-\varepsilon)^{n-1}} &= 1 - \frac{2}{n^3} \sum_{i=1}^{4} A_{\tau_i} \tau_i \Big(\frac{1-2\varepsilon}{1-\varepsilon} \Big)^{\tau_i - 1} \Big(\frac{1}{1-\varepsilon} \Big)^{n-\tau_i} \\ &= 1 - \frac{2^n}{n^3} \sum_{i=1}^{4} A_{\tau_i} \tau_i \Big(1 - \frac{1}{2(1-\varepsilon)} \Big)^{\tau_i - 1} \Big(\frac{1}{2(1-\varepsilon)} \Big)^{n-\tau_i} \qquad (4.4) \\ &= 1 - \frac{2^n}{n^3} \sum_{i=1}^{4} A_{\tau_i} \tau_i \delta^{\tau_i - 1} (1-\delta)^{n-\tau_i}, \end{aligned}$$

where we have put

$$\delta = 1 - \frac{1}{2(1-\varepsilon)}, \quad 0 \le \delta \le 1/2. \qquad (4.5)$$

Obvioulsly, to prove the theorem it suffices to show that the last expression to the right in (4.4) is a non-negative function of $\delta \in [0,\ 1/2]$, i.e., that the function

$$S(\delta) = \sum_{i=1}^{4} A_{\tau_i} \tau_i \delta^{\tau_i - 1} (1-\delta)^{n-\tau_i} \qquad (4.6)$$

satisfies

$$S(\delta) \le \frac{n^3}{2^n}, \quad 0 \le \delta \le 1/2. \qquad (4.7)$$

We first claim that the above inequality holds for $\delta \in [\delta_0,\ 1/2]$, where

$$\delta_0 = \frac{1}{2} - \frac{3}{n-6}. \qquad (4.8)$$

Indeed, since for the minimum code distance of the code $\mathcal{P}(m)$ we have $d = 6$ for all possible values of m, all terms $\varepsilon^i (1-\varepsilon)^{n-i}$ appearing in the right hand side of formula (1.1) applied to this code are increasing functions of ε in the interval $[0,\ \frac{6}{n}]$, as is easily seen from (2.5). Consequently, $P'_{ue}(\mathcal{P}(m),\, \varepsilon) \ge 0$ in this interval and thus the last expression to the right in (4.4) is a nonnegative function of δ when, cf. (4.5),

$$\frac{1}{2} \ge \delta \ge 1 - \frac{1}{2(1-\frac{6}{n})} = \frac{n-12}{2(n-6)} = \frac{1}{2} - \frac{3}{n-6} = \delta_0,$$

i.e., the inequality of (4.7) holds in the above interval, and, in particular,

$$S(\delta_0) \le \frac{n^3}{2^n}. \qquad (4.9)$$

It follows therefore that (4.7) now has to be established only for $\delta \in [0,\ \delta_0]$.

Put $\delta_i = \frac{\tau_i - 1}{n-1}$ so that

$$\begin{aligned}
\delta_1 &= \frac{n - \sqrt{n} - 2}{2(n-1)} = \frac{1}{2} - \frac{1}{2(\sqrt{n}-1)}, \\
\delta_2 &= \frac{n-2}{2(n-1)} = \frac{1}{2} - \frac{1}{2(n-1)}, \\
\delta_3 &= \frac{n + \sqrt{n} - 2}{2(n-1)} = \frac{1}{2} + \frac{1}{2(\sqrt{n}+1)}, \\
\delta_4 &= 1.
\end{aligned} \tag{4.10}$$

Note that the function $S(\delta)$ in (4.6) is increasing in the interval $[0,\ \delta_1]$ since all its terms $\delta^{\tau_i - 1}(1-\delta)^{n-\tau_i}$ are, by (2.5). When $n = 2^4$ we obtain from (4.10) and (4.8) that $\delta_1 = 1/3 > 1/5 = \delta_0$, which implies that $S(\delta)$ increases in $0 \le \delta \le \delta_0$ and hence

$$S(\delta) \le S(\delta_0) \le \frac{n^3}{2^n}, \quad 0 \le \delta \le \delta_0, \tag{4.11}$$

where we have used (4.9). Thus the theorem is valid for $n = 2^4$ and we can then assume in the rest of this proof that $n \ge 2^6 = 64$. It is easily seen that for these values of n we have $\delta_1 < \delta_0$ and $\delta_i > \delta_0$ for $i = 2$, 3, and 4, which shows that except for the first term of $S(\delta)$ all other terms are increasing functions in $[0,\ \delta_0]$, while the first function increases in $[0,\ \delta_1]$ and decreases in $[\delta_1,\ \delta_0]$. Nevertheless, the function $S(\delta)$ turns out to be increasing in $[0,\ \delta_0]$ which follows from the next proposition.

Proposition. *The function*

$$G_1(\delta) = \tau_1 \delta^{\tau_1 - 1}(1-\delta)^{n-\tau_1} + \tau_3 \delta^{\tau_3 - 1}(1-\delta)^{n-\tau_3}$$

increases in the interval $[0,\ \delta_0]$.

Proof. It suffices to show that the derivative of $G_1(\delta)$ is positive in $(0,\ \delta_0]$. This function is of the same form as the one considered in the Lemma of Section 2. As (2.6) shows, $G_1'(\delta)$ will be positive in $(0,\ \delta_0]$ if

$$1 - \frac{\tau_1}{\tau_3}\Big(\frac{1-\delta}{\delta}\Big)^{\tau_3 - \tau_1}\frac{\delta - \delta_1}{\delta_3 - \delta} > 0 \tag{4.12}$$

in this interval. As in (2.7), the derivative of the function

$$g_1(\delta) = \Big(\frac{1-\delta}{\delta}\Big)^{\tau_3 - \tau_1}\frac{\delta - \delta_1}{\delta_3 - \delta}$$

is

$$g_1'(\delta) = \Big(\frac{1-\delta}{\delta}\Big)^{\tau_3-\tau_1-1}\frac{1}{\delta^2}\frac{\delta_3-\delta_1}{(\delta_3-\delta)^2}[(1-\delta)\delta-(n-1)(\delta-\delta_1)(\delta_3-\delta)], \quad (4.13)$$

where by using (4.10) the quadratic function in the brackets is computed to be

$$\tilde{g_1}(\delta) = (n-2)\delta^2-(n-3)\delta+\frac{n-4}{4}.$$

It is easily seen that the solutions of $\tilde{g_1}(\delta)=0$ are the points $\frac{1}{2}-\frac{1}{n-2}$ and $\frac{1}{2}$ and since

$$\frac{1}{2}-\frac{1}{n-2} > \frac{1}{2}-\frac{3}{n-6} = \delta_0,$$

$\tilde{g_1}(\delta)$ is positive in $(0,\ \delta_0]$ which means that $g_1' > 0$ in this interval and hence, after a simple calculation,

$$\max_{0<\delta\le\delta_0} g_1(\delta) = g_1(\delta_0) = \frac{\tau_3}{\tau_1}\cdot\frac{\sqrt{n}-6}{\sqrt{n}+6}\Big(1+\frac{12}{n-12}\Big)^{\sqrt{n}}.$$

In this way the desired inequality (4.12) is equivalent to

$$\Big(1+\frac{12}{n-12}\Big)^{\sqrt{n}} < \frac{\sqrt{n}+6}{\sqrt{n}-6}, \quad (4.14)$$

where, we recall, $n \ge 64$. Put $x=\sqrt{n}$ and consider for $x \ge 8$

$$f(x) = \ln\frac{x+6}{x-6} - x\ln\Big(1+\frac{12}{x^2-12}\Big).$$

We have

$$f'(x) = -\frac{12}{x^2-36} - \ln\Big(1+\frac{12}{x^2-12}\Big)+\frac{24}{x^2-12}.$$

Using the Taylor series of the logarithmic function we obtain

$$\begin{aligned}
-\ln\Big(1+\frac{12}{x^2-12}\Big) &= \sum_{k=1}^{\infty}\frac{(-1)^k}{k}\Big(\frac{12}{x^2-12}\Big)^k \\
&= -\frac{12}{x^2-12}+\frac{1}{2}\Big(\frac{12}{x^2-12}\Big)^2-\sum_{k=3}^{\infty}\frac{(-1)^{k-1}}{k}\Big(\frac{12}{x^2-12}\Big)^k \\
&= -\frac{12}{x^2-12}+\frac{1}{2}\Big(\frac{12}{x^2-12}\Big)^2 \\
&-\Big\{\Big[\frac{1}{3}\Big(\frac{12}{x^2-12}\Big)^3-\frac{1}{4}\Big(\frac{12}{x^2-12}\Big)^4\Big]+\Big[\frac{1}{5}\Big(\frac{12}{x^2-12}\Big)^5-\frac{1}{6}\Big(\frac{12}{x^2-12}\Big)^6\Big]+\dots\Big\} \\
&< -\frac{12}{x^2-12}+\frac{1}{2}\Big(\frac{12}{x^2-12}\Big)^2
\end{aligned}$$

where the last inequality is due to the fact that

$$0 < \frac{12}{x^2 - 12} < 1, \quad x \geq 8$$

so that the terms in the brackets on the line next to the last are positive. Hence

$$\begin{aligned} f'(x) &< -\frac{12}{x^2 - 36} + \frac{12}{x^2 - 12} + \frac{1}{2}\Big(\frac{12}{x^2 - 12}\Big)^2 \\ &= -\frac{2 \cdot 12^2}{(x^2 - 36)(x^2 - 12)} + \frac{1}{2}\Big(\frac{12}{x^2 - 12}\Big)^2 \\ &= \Big(\frac{12}{x^2 - 12}\Big)^2 \Big[\frac{1}{2} - \frac{2(x^2 - 12)}{x^2 - 36}\Big] \\ &< \Big(\frac{12}{x^2 - 12}\Big)^2 \Big[\frac{1}{2} - 2\Big] < 0. \end{aligned}$$

Thus $f(x)$ is a decreasing function for $x \geq 8$ and hence

$$f(x) > \lim_{x \to \infty} f(x) = 0,$$

which implies (4.14) for $n \geq 64$. This proves the Proposition.

To end the proof of the theorem we just notice that the function $S(\delta)$ increases in $[0, \delta_0]$, since the sum of the first and the third terms does, according to the Proposition, and also the second and the fourth terms do. Then (4.11) holds even in this case and the code $\mathcal{P}(m)$ is thus proper.

References

[1] A. E. Brouwer, Some new two-weight codes and strongly regular graphs. Discrete Appl. Math. vol. 10, no. 4 (1985), pp. 455–461.

[2] R. Dodunekova, S. M. Dodunekov and E. Nikolova, A survey on proper codes. In: *Proc. General theory of information transfer and combinatorics.* ZiF research Year, Nov. 4–9 2002, Bielefeld, to appear.

[3] L. D. Grey, Some bounds for error-correcting codes. IEEE Trans. Inform. Theory vol. IT-8 (1962), pp. 200-202.

[4] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, The Z4-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans. Inform. Theory vol. 40, no. 2 (1994), pp. 301–319.

[5] D. Jungnickel and V. D. Tonchev, Exponential number of quasi-symetric SDP designs and codes meeting the Grey-Rankin bound. Designs, Codes, Cryptography vol. 1, no. 3 (1991), pp. 247–253.

[6] A. M. Kerdock, A class of low-rate nonlinear binary codes. Inform. Control vol. 20 (1970), pp. 182–187.

[7] T. Kløve and V. Korzhik, *Error detecting codes*. Boston, MA: Kluwer, 1995.

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

[9] G. McGuire, Quasi-symmetric designs and codes meeting the Grey-Rankin bound. J. Combin. Theory, Ser. A v. 78 (1997), 280-291.

[10] MacWilliams, F. J. and Sloane, N. J. A., *The theory of error-correcting codes*. New York: North Holland, 1977.

[11] F. P. Preparata, A class of optimum nonlinear double error correcting codes. Inform. and Control vol. 13 (1968), pp. 378–400.

[12] R. A. Rankin, The closest packing of spherical caps in n-dimensions. In: *Proc. Glasgow Math. Assoc.* 1955, vol. 2, pp.139–144.

[13] R. A. Rankin, On the minimal points of positive definite quadratic forms. Mathematika vol. 3 (1956), pp. 15–24.

[14] N. V. Semakov and V. A. Zinoviev, Balanced codes and tactical configurations. Problems Inform. Transmission vol. 5, no. 3 (1969), pp. 22–28.