CHALMERS | GÖTEBORGS UNIVERSITET

PREPRINT

Intervals of Properness for Binary Linear Error-Detecting Codes

R. DODUNEKOVA
E. NIKOLOVA

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

Preprint 2004:42

Intervals of Properness for Binary Linear Error-Detecting Codes

R. Dodunekova
E. Nikolova

CHALMERS | GÖTEBORGS UNIVERSITET

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

NO 2004:42
ISSN 0347-2809

Matematiska Vetenskaper
Göteborg 2004

Intervals of properness for binary linear error-detecting codes

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

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

Abstract We show that a binary linear code C of length n, and the dual code $C^\perp$ of minimum code distance $d^\perp$, are proper for error detection if $d^\perp \geq \lfloor \frac{n}{2} \rfloor + 1$, and C is proper in the interval $\left[\frac{n+1-2d^\perp}{n-d^\perp}, \frac{1}{2}\right]$, if $\lceil \frac{n}{3} \rceil + 1 \leq d^\perp \leq \lfloor \frac{n}{2} \rfloor$. We also provide examples, mostly on Griesmer codes and their duals, which satisfy the above conditions.

Key words: linear code, error detection, proper code, interval properness.

1 Introduction

The probability of undetected error of a linear binary code $C = [n, k, d]$, used to detect errors on a symmetric memoryless channel with symbol error probability ε, is expressed in terms of the code weight distribution $\{A_0, A_1, \ldots, A_n\}$ as

$$P_{ue}(C, \varepsilon) = \sum_{i=d}^{n} A_i \varepsilon^i (1-\varepsilon)^{n-i}, \quad \varepsilon \in [0, 1/2], \tag{1.1}$$

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

$$P_{ue}(C, \varepsilon) = 2^{-(n-k)} \sum_{i=0}^{n} B_i (1-2\varepsilon)^i - (1-\varepsilon)^n, \quad \varepsilon \in [0, 1/2]. \tag{1.2}$$

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

The code C is *proper* for error detection if $P_{ue}(C,\, \varepsilon)$ is an increasing function of ε in $[0, 1/2]$, and it is *good* if $P_{ue}(C,\, \varepsilon)$ has its absolute maximum at $\varepsilon = 1/2$, the worst case channel condition, i.e., if

$$P_{ue}(C,\, \varepsilon) \leq P_{ue}(C,\, 1/2) = 2^{-n}(2^k - 1), \quad \varepsilon \in [0,\, 1/2], \tag{1.3}$$

see [1] and [2]. Thus a proper error-detecting code is also good, but it has the advantage of performing better on better channels, i.e., channels with smaller symbol error probability. A proper binary linear code with parameters $[n, k, d]$ performs like an "average" error-detecting code, since the procedure of averaging $P_{ue}(C,\, \varepsilon)$ over all $[n, k]$ binary linear codes results in an increasing function of ε, see [3].

Examples of proper codes are the Perfect codes over finite fields, the Maximum Distance Separable codes, some Reed-Muller codes, some Near Maximum Distance Separable codes, the Maximum Minimum Distance codes and their duals, as well as many cyclic codes. For more examples see the survey [4]. The concept of properness may be extended to non-linear block codes. Examples of proper non-linear codes are the Kerdock and the Preparata codes, and codes satisfying or achieving the Grey-Rankin bound, see [5].

Even if a code C is not good, for some applications it might be sufficient to know that its probability of undetected error satisfies the upper bound in (1.3) for ε in some subinterval $[a, b]$ of $[0,\, 1/2]$. It then seems reasonable to call C *good in* $[a,\, b]$. We call C *proper in* $[a, b]$, if its probability of undetected error increases for ε in $[a,\, b]$. Note that if a code is proper in $[a,\, 1/2]$ it is also good in this interval.

So far most studies on properness and goodness of error-detecting codes involve the code weight distribution, in one form or another. However, the code weight distribution is known for relatively few codes, since its computation is an NP-hard problem, see [6]. It should therefore be useful to have criteria for properness and goodness which do not involve the code weight distribution. In this work we give two such criteria. In Section 3 we prove that a binary linear code C of length n, and the dual code $C^\perp$ with minimum code distance $d^\perp$, are proper for error detection if (Theorem 1)

$$d^\perp \geq \left\lfloor \frac{n}{2} \right\rfloor + 1,$$

and C is proper in the interval

$$\left[\frac{n + 1 - 2d^\perp}{n - d^\perp},\, \frac{1}{2}\right],$$

if (Theorem 2)

$$\left\lceil \frac{n}{3} \right\rceil + 1 \leq d^\perp \leq \left\lfloor \frac{n}{2} \right\rfloor.$$

As we see, the larger the dual code distance, the larger the above interval of properness of C (and goodness as well, since the interval ends at the point $1/2$). In fact, this is in agreement with a bound on $P_{ue}(C,\,\varepsilon)$ derived in [7], which suggests that codes with large dual code distance might be more appropriate for error detection, see Remark 2 and (3.11) in Section 3. In Section 4 we provide examples using Theorem 1 of families of Griesmer codes which are proper, together with their dual codes, and apply Theorem 2 to give intervals of properness of codes dual to Griesmer codes. As we will see, the interval of properness of the dual code converges to $(0,\,1/2]$ when the dimension k of the Griesmer code increases. For instance, in Example 4 the dual code is proper in the interval $[9.8\cdot 10^{-4},\,1/2]$ when $k \geq 13$. Thus, in practice, for channels with $\varepsilon \geq 9.8\cdot 10^{-4}$ the dual code is essentially proper. We begin in Section 2 with some preliminary material.

2 Preliminaries

Consider a binary linear code $C = [n,k,d]$ and its dual code $C^{\perp} = [n,k,d]$, with weight distribution $\{A_0, A_1, \ldots, A_n\}$ and $\{B_0, B_1, \ldots, B_n\}$, respectively. For brevity, we denote

$$\varepsilon_i = \frac{i}{n}, \quad i = 1,\,2,\,\ldots,n. \tag{2.1}$$

As is easily seen the derivative of $\varepsilon^i(1-\varepsilon)^{n-i}$ is

$$\big(\varepsilon^i(1-\varepsilon)^{n-i}\big)' = n\varepsilon^{i-1}(1-\varepsilon)^{n-i-1}(\varepsilon_i - \varepsilon), \quad i = 1,\,2,\,\ldots,n. \tag{2.2}$$

Remark 1. (2.2) shows that the function $P_{ue}(C,\,\varepsilon)$ of (1.1) increases for ε in $[0,\,\varepsilon_d]$, and C is thus proper in this interval. In particular, C is proper if $\frac{d}{n} \geq \frac{1}{2}$.

We will further need the first order Pless Power Moment of C,

$$\sum_{i=d}^{n} iA_i = 2^{k-1}(n - B_1), \tag{2.3}$$

(see [8], p. 133), and the average non-zero Hamming weight $\overline{d}_C$ of C,

$$\overline{d}_C = \frac{1}{2^k - 1}\sum_{i=d}^{n} iA_i = \frac{2^{k-1}}{2^k - 1}(n - B_1). \tag{2.4}$$

Recall that C is of full length if its generating matrix does not contain any column of zeros [9]. Clearly, for such a code the minimum dual code distance is greater than one.

3 Main results

As above, we let $\{A_0, A_1, \ldots, A_n\}$ denote the weight distribution of $C = [n, k, d]$ and $\{B_0, B_1, \ldots, B_n\}$ the weight distributions of the dual code $C^\perp$. Noticing that (1.2) gives

$$P'_{ue}(C,\, \varepsilon) = -2^{-n+k+1} \sum_{i=d^\perp}^{n} iB_i(1-2\varepsilon)^{i-1} + n(1-\varepsilon)^{n-1}, \quad \varepsilon \in [0,\, 1/2],$$

we have

$$\begin{aligned} \frac{P'_{ue}(C,\varepsilon)}{n(1-\varepsilon)^{n-1}} &= 1 - \frac{2^k}{n} \sum_{i=d^\perp}^{n} iB_i \Big(\frac{1-2\varepsilon}{2(1-\varepsilon)}\Big)^{i-1} \Big(\frac{1}{2(1-\varepsilon)}\Big)^{n-i} \\ &= 1 - \frac{2^k}{n} \sum_{i=d^\perp}^{n} iB_i \delta^{i-1}(1-\delta)^{n-i}, \end{aligned} \tag{3.2}$$

where we have put

$$\delta = 1 - \frac{1}{2(1-\varepsilon)}, \quad \delta \in [0,\, 1/2]. \tag{3.3}$$

Theorem 1. *Let the binary linear code C of length n have minimum dual code distance $d^\perp$. If*

$$d^\perp \geq \left\lfloor \frac{n}{2} \right\rfloor + 1, \tag{3.4}$$

then both C and the dual code $C^\perp$ are proper.

Proof. That $C^\perp$ is proper follows from Remark 1 since (3.4) implies

$$\frac{d^\perp}{n} > \frac{1}{2}.$$

To show the properness of C we use (3.2) and (3.3). For $\delta_i = \dfrac{i-1}{n-1}$ we have by (3.4)

$$\delta_i \geq \frac{d^\perp - 1}{n-1} \geq \frac{1}{2}, \quad d^\perp \leq i \leq n,$$

and again by Remark 1, the second term in the second line of (3.2) is an increasing function of δ in $[0,\, 1/2]$. From this and (2.3) applied to $C^\perp$ we obtain by (3.2)

$$\begin{aligned} \frac{P'_{ue}(C,\varepsilon)}{n(1-\varepsilon)^{n-1}} &\geq 1 - \max_{0 \leq \delta \leq 1/2} \frac{2^k}{n} \sum_{i=d^\perp}^{n} iB_i \delta^{i-1}(1-\delta)^{n-i} \\ &= 1 - \frac{2^k \cdot 2^{-n+1}}{n} \sum_{i=d^\perp}^{n} iB_i \\ &\geq 1 - \frac{2^{k-n+1}}{n} \cdot n2^{n-k-1} = 0, \quad \varepsilon \in [0,\, 1/2], \end{aligned}$$

which shows that C is proper. ■

Assume $C = [n,\, k,\, d]$ is a binary linear code with minimum dual code distance $d^{\perp} > 1$. By (1.1), (2.2), and (2.3) we have

$$\begin{aligned} P'_{ue}(C,\, 1/2) &= n2^{-n+2} \sum_{i=d}^{n} A_i(\varepsilon_i - 1/2) \\ &= 2^{-n+2} \Big[\sum_{i=d}^{n} iA_i - (n/2) \sum_{i=d}^{n} A_i \Big] = n2^{-n+1}, \end{aligned}$$

and C is thus proper and also good in intervals of the form $[a,\, 1/2]$. Below we give one such interval, where a is determined by the length of the code and the minimum dual code distance.

Theorem 2. *Let the binary linear code C of length n have minimum dual code distance $d^{\perp}$. If*

$$\left\lceil \frac{n}{3} \right\rceil + 1 \le d^{\perp} \le \left\lfloor \frac{n}{2} \right\rfloor, \tag{3.5}$$

then C is proper in the interval

$$\left[\frac{n+1-2d^{\perp}}{n-d^{\perp}},\ \frac{1}{2} \right]. \tag{3.6}$$

Proof. From (3.2), (3.3), and (2.3), we obtain

$$\begin{aligned} \frac{P'_{ue}(C, \varepsilon)}{n(1-\varepsilon)^{n-1}} &= 1 - \delta^{d^{\perp}-1}(1-\delta)^{n-d^{\perp}} \frac{2^k}{n} \sum_{i=d^{\perp}}^{n} iB_i \left(\frac{\delta}{1-\delta} \right)^{i-d^{\perp}} \\ &\ge 1 - \delta^{d^{\perp}-1}(1-\delta)^{n-d^{\perp}} \frac{2^k}{n} \sum_{i=d^{\perp}}^{n} iB_i \\ &\ge 1 - 2^{n-1}\delta^{d^{\perp}-1}(1-\delta)^{n-d^{\perp}}, \quad \delta \in [0,\, 1/2]. \end{aligned} \tag{3.7}$$

Noting from (3.5) that for

$$\alpha_0 = \frac{n+1-2d^{\perp}}{d^{\perp}-1}$$

we have $0 < \alpha_0 < 1$, we set

$$\delta = \frac{1}{2} - \frac{\alpha}{2}, \quad \alpha_0 \le \alpha \le 1, \tag{3.8}$$

and write the second term in the last line of (3.7) as

$$\begin{aligned} & 2^{n-1}\delta^{d^{\perp}-1}(1-\delta)^{n-d^{\perp}} = (1-\alpha)^{d^{\perp}-1}(1+\alpha)^{n-d^{\perp}} \\ & = (1-\alpha^2)^{d^{\perp}-1}(1+\alpha)^{n+1-2d^{\perp}}. \end{aligned} \tag{3.9}$$

Since the functions $\left(1+\frac{1}{x}\right)^x$ and $\left(1-\frac{1}{x}\right)^x$ are increasing for $x > 1$ and

$$\left(1+\frac{1}{x}\right)^x \to e, \quad \left(1-\frac{1}{x}\right)^x \to e^{-1}, \quad \text{as} \quad x \to \infty,$$

we have

$$\begin{aligned}&(1-\alpha^2)^{d^\perp-1}(1+\alpha)^{n+1-2d^\perp} < \exp\{-\alpha^2(d^\perp-1)\}\cdot\exp\{\alpha(n+1-2d^\perp)\}\\ &= \exp\big\{-\alpha(d^\perp-1)(\alpha-\alpha_0)\big\} \le 1, \quad \alpha_0 \le \alpha \le 1.\end{aligned}$$

This inequality, (3.8), and (3.9) give

$$2^{n-1}\delta^{d^\perp-1}(1-\delta)^{n-d^\perp} \le 1, \qquad 0 \le \delta \le \frac{1}{2}-\frac{\alpha_0}{2},$$

which implies, by (3.3) and (3.7),

$$P'_{ue}(C,\,\varepsilon) \ge 0, \qquad \frac{1}{2} \ge \varepsilon \ge 1-\frac{1}{1+\alpha_0} = \frac{n+1-2d^\perp}{n-d^\perp},$$

and the statement follows. ■

Corollary 1. When (3.5) is satisfied and in addition

$$(n-d)(n-d^\perp) \le n(d^\perp-1), \tag{3.10}$$

then C is proper.

Proof. It is easily seen that (3.10) is equivalent to

$$\frac{n+1-2d^\perp}{n-d^\perp} \le \frac{d}{n}$$

and from Remark 1 and Theorem 2, it follows that C is proper. ■

Corollary 2. Assume $C^\perp$ is of full length and $d^\perp = n/2, \quad n > 4$. Then C and $C^\perp$ are proper.

Proof. The properness of $C^\perp$ follows from Remark 1. Clearly, $d^\perp$ and n satisfy (3.5). Because $C^\perp$ is of full length, we have $d \ge 2$ and hence (3.10) is also satisfied, since

$$(n-d)(n-d^\perp) \le (n-2)n/2 = n(d^\perp-1).$$

C is thus proper by Corollary 1.

Remark 2. A binary linear code $C = [n, k, d]$ satisfies the Singleton bound

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

The defect s of C is defined as

$$s = n - k + 1 - d.$$

Recall that when the defect of C equals zero, the defect $s^{\perp}$ of the dual code $C^{\perp}$ equals zero as well, and C and of $C^{\perp}$ are Maximum Distance Separable (MDS) codes. For non-MDS codes s and $s^{\perp}$ are positive. It has been shown in [7] for non-MDS codes that

$$\begin{aligned} P_{ue}(C, \varepsilon) < (2^{s^{\perp}} - 1) \sum_{i=d}^{n-d^{\perp}} \binom{n}{i} \varepsilon^i (1 - 2\varepsilon)^{n-i} \\ + \sum_{i=n-d^{\perp}+1}^{n} (2^{-n+k-i} - 1) \binom{n}{i} \varepsilon^i (1 - 2\varepsilon)^{n-i}. \end{aligned} \tag{3.11}$$

The above upper bound suggests that codes with a small dual defect, or large dual code distance, might be more appropriate for error detection. Note that this is in agreement with the results in Theorems 1 and 2. In fact, the interval of properness (3.6) is larger for larger minimum dual code distance.

4 Examples

The Hamming codes and their duals, the Simplex codes (see [10], p. 30), are known to be proper for error detection. In fact, their properness follows from Theorem 1 as well, since (3.4) holds for the Simplex code $C^{\perp} = [2^m - 1, \, m, \, 2^{m-1}]$. The parameters of the Simplex code achieve the Griesmer bound ([10], p. 546),

$$n \geq \sum_{i=0}^{k^{\perp}-1} \left\lceil \frac{d^{\perp}}{2^i} \right\rceil.$$

The first three examples below give other families of codes meeting the Griesmer bound with equality, which satisfy (3.4) and thus are proper, together with their duals, by Theorem 1. The examples are based on the observation that when (3.4) holds true for $C^{\perp} = [n, k^{\perp}, d^{\perp}]$ then

$$d^{\perp} \geq 2^{k^{\perp}-1}. \tag{4.12}$$

Indeed, (3.4) and the Griesmer bound give for $C^{\perp}$

$$2d^{\perp} - 1 \geq n \geq d^{\perp}\Big(1 + \frac{1}{2} + \ldots + \frac{1}{2^{k^{\perp}-1}}\Big) = 2d^{\perp} - \frac{d^{\perp}}{2^{k^{\perp}-1}},$$

which implies (4.12). Another way to derive (4.12) is by noting that (3.4) implies for the average non-zero Hamming weight $\overline{d}_{C^\perp}$ of $C^\perp$

$$\overline{d}_{C^\perp} \geq \frac{n+1}{2}, \tag{4.13}$$

which together with (2.4) and (3.4) gives (4.12).

Example 1. N. L. Manev [11] has shown the uniqueness of the binary Griesmer codes with parameters

$$\left[s2^k - 2^{a+1} - s + 1,\ k,\ s2^{k-1} - 2^a\right], \quad k-1 > a \geq 0. \tag{4.14}$$

Clearly, when $s \geq 2$ the condition (3.4) is satisfied and the codes and their duals are proper, by Theorem 1. When $s = 1$, (4.14) describes the binary MacDonald codes, known to be proper together with their duals [12–13].

Example 2. T. Helleseth [14] considered binary codes meeting the Griesmer bound with equality. These codes have parameters

$$\left[s(2^k-1) - \sum_{i=1}^{p}(2^{u_i}-1),\ k,\ s2^{k-1} - \sum_{i=1}^{p} 2^{u_i-1}\right],\ k > u_i > \ldots > u_p \geq 1. \tag{4.15}$$

The codes have been characterized when $p = 2$ (for this case see also [15]), and with the additional condition $u_{i-1} - u_i \geq 2,\ 2 \leq i \leq p$, when $p > 2$. If $s \geq p+1$, the codes and their duals are proper by Theorem 1, since

$$\begin{aligned} 2d^\perp - n - 1 &= 2\left[s2^{k-1} - \sum_{i=1}^{p} 2^{u_i-1}\right] - \left[s(2^k-1) - \sum_{i=1}^{p}(2^{u_i}-1)\right] - 1 \\ &= s - p - 1 \geq 0, \end{aligned}$$

which easily implies (3.4). If $s = p$ we have

$$d^\perp = n/2, \quad n = p2^k - \sum_{i=1}^{p} 2^{u_i} \geq 2^{k+1} - \sum_{i=1}^{k-1} 2^i = 2^k + 2 > 4,$$

and since a Griesmer code is of full length, the codes and their duals are proper, by Corollary 2. Consider now the case $s < p$. We have

$$\begin{aligned} 3d^\perp - n - 2 &= s2^{k-1} - \sum_{i=1}^{p} 2^{u_i-1} + s - p - 2 \\ &\geq 2^{k-1} - \sum_{i=1}^{p} 2^{u_i-1} - p - 1 > 0, \quad k \geq 5, \end{aligned} \tag{4.16}$$

since, when $k = 2m+1$,

$$2^{k-1} - \sum_{i=1}^{p} 2^{u_i-1} - p - 1 \geq 2^{2m} - \frac{1}{2}\Big[2^{2m} + 2^{2m-2} + \ldots + 2^2\Big] - m - 1$$
$$= 2^{2m} - \frac{2}{3}\Big[2^{2m} - 1\Big] - m - 1 = \frac{2^{2m} - 3m - 1}{3} > 0, \quad m \geq 2,$$

and, when $k = 2m$,

$$2^{k-1} - \sum_{i=1}^{p} 2^{u_i-1} - p - 1 \geq 2^{2m-1} - \frac{1}{2}\Big[2^{2m-1} + 2^{2m-3} + \ldots + 2\Big] - m - 1$$
$$= 2^{2m-1} - \frac{2^{2m} - 1}{3} - m - 1 = \frac{2^{2m-1} - 3m - 2}{3} > 0, \quad m \geq 3.$$

As is easily seen, (4.16) implies the first inequality of (3.5) for $k \geq 5$. Since $n + 1 - 2d^{\perp} = p - s + 1 > 0$, the second inequality of (3.5) is satisfied as well. Thus when $s < p$ and $k \geq 5$, Theorem 2 shows that the dual codes are proper in the interval

$$\Big[\frac{p-s+1}{s2^{k-1} - \sum_{i=1}^{p} 2^{u_i-1} + p - s}, \ \ \frac{1}{2}\Big]. \tag{4.17}$$

When $s < p$ and $k = 4$ we necessarily have $p = 2, \ \ s = 1$, and since the condition (3.5) is satisfied for codes with $u_1 = 1$, their duals are proper in the interval (4.17).

The intervals of properness obviously converge to $(0, 1/2]$ when k tends to ∞. In particular, when $p = 2, \ \ s = 1$, and $k \geq 14$, the interval in (4.17) contains $[9.8 \cdot 10^{-4}, 1/2]$ and the dual codes are thus proper in this interval.

Example 3. H. C. A. van Tilborg [16] has shown the uniqueness of the binary Griesmer codes with parameter

$$[2^{k-1} + k, \ k, \ 2^{k-2} + 2], \quad k \geq 3, \quad k \neq 5. \tag{4.18}$$

When $k = 3$, the code and its dual are proper by Theorem 1, since the condition (3.4) holds true. When $k = 4$ the code and its dual are proper by Corollary 2. When $k \geq 6$, the code parameters (4.18) satisfy (3.5) and by Theorem 2, their dual codes are proper in

$$\Big[\frac{k-3}{2^{k-2} + k - 2}, \ \ \frac{1}{2}\Big].$$

When $k \geq 16$, the dual codes are proper in $[9.8 \cdot 10^{-4}, 1/2]$.

Example 4. The binary Griesmer codes

$$[2^k - 2^{k-i} - 3, \ k, \ 2^{k-1} - 2^{k-i-1} - 2], \quad 2 \leq i \leq k-1, \quad i \neq k-2,$$

have been studied by S. M. Dodunekov and N. L. Manev [17]. For $k \geq 4$, the codes satisfy (3.5) and, by Theorem 2, their dual codes are proper in the interval

$$\left[\frac{2}{2^{k-1} - 2^{k-i-1} - 1}, \quad \frac{1}{2}\right],$$

which contains $[9.8 \cdot 10^{-4},\ 1/2]$, when $k \geq 13$.

Example 5. T. Helleseth and H. C. A. van Tilborg [18] constructed an infinite sequence of k-dimensional binary linear codes with parameters

$$\left[2^k + 2^{k-2} - 15,\ k,\ 2^{k-1} + 2^{k-3} - 8\right], \quad k \geq 7, \tag{4.19}$$

meeting the Griesmer bound with equality. For $k \geq 8$ these codes are unique, while there are five non-isomorphic codes for $k = 7$. By Theorem 2, the dual codes are proper in

$$\left[\frac{2}{2^{k-1} + 2^{k-3} - 7}, \quad \frac{1}{2}\right].$$

When $k \geq 12$ the dual codes are proper in the interval $[9.8 \cdot 10^{-4},\ 1/2]$.

By shortening the codes with parameters given by (4.19), other Griesmer codes have been obtained in [18] with

$$2^{k-1} + 2^{k-3} - 15 \leq d^{\perp} < 2^{k-1} + 2^{k-3} - 8, \quad k \geq 7.$$

It can be shown for these new codes that they also satisfy (3.5), and intervals of properness can be given, in accordance with Theorem 2.

Example 6. The irreducible binary cyclic codes $C(r,t,s)$, introduced by Delsarte and Goethals in [19], depend on three parameters satisfying $r \geq 1$, $t > 1$, $s > 1$ and $s | 2^r + 1$. The code $C(r,t,s)$ is of length

$$n = \frac{2^{2rt} - 1}{s},$$

and it has two non-zero weights,

$$\tau_1 = \frac{2^{2rt-1} + (-1)^t (s-1) 2^{rt-1}}{s}, \quad \tau_2 = \frac{2^{2rt-1} - (-1)^t 2^{rt-1}}{s}.$$

In [20–21] the codes $C(r,t,s)$ and their duals $C^{\perp}(r,t,s)$ have been completely classified with respect to properness. In particular, it has been shown in [21], that a code $C^{\perp}(r,t,s)$ with $s > 3$ and t odd is not proper. Since in this case the length and the minimum code distance of $C(r,t,s)$,

$$d = \tau_1 = \frac{2^{2rt-1} - (s-1) 2^{rt-1}}{s},$$

turn out to satisfy (3.5), $C^{\perp}(r,t,s)$ is proper in the interval

$$\left[\frac{(s-1)(2^{rt}+1)}{2^{2rt-1}-1+(s-1)2^{rt-1}},\ \frac{1}{2}\right], \tag{4.20}$$

by Theorem 2. Indeed, since $t \geq 3$ and $r \geq 2$ (because $s > 3$), the first inequality of (3.5) follows for $C(r,t,s)$, from

$$\begin{aligned} s(3d-n-2) &= 3\cdot 2^{2rt-1} - 3(s-1)2^{rt-1} - 2^{2rt} + 1 - 2s \\ &= 2^{2rt-1} - 3(s-1)2^{rt-1} + 1 - 2s \\ &\geq 2^{2rt-1} - 3\cdot 2^{r}\cdot 2^{rt-1} - 2^{r+1} - 1 \\ &> 2^{2rt-1} - 3\cdot 2^{r(t+1)-1} - 2^{r(t+1)-1} \\ &= 2^{2rt-1} - 2^{r(t+1)+1} \\ &= 2^{r(t+1)+1}(2^{r(t-1)-2}-1) \geq 0, \end{aligned}$$

where in the fourth line we have used the obvious fact that

$$2^{r+1}+1 < 2^{r(t+1)-1},$$

and the second inequality in (3.5) follows from

$$s(n+1-2d) = (s-1)2^{rt} + s - 1 = (s-1)(2^{rt}+1) > 0.$$

Remark 3. In [21], the non-properness of the codes $C^{\perp}(r,t,s)$ with $s > 3$ and t odd was shown by choosing the point

$$\varepsilon_s = \begin{cases} \dfrac{5}{5+3\cdot 2^{rt-1}}, & \text{if } s = 5, \\ \dfrac{s}{s+2^{rt}}, & \text{if } s \geq 7, \end{cases}$$

for which $P'_{ue}(C^{\perp}(r,t,s),\ \varepsilon_s) < 0$. The point ε_s lies, of course, outside the interval of properness (4.20), which can be easily checked.

Acknowledgment. This work has been partially carried out while the first author visited the Technical University of Delft in May 2004, and she gratefully acknowledges the hospitality of prof. Jan van Zanten during her visit.

References

[1] *Kløve T., Korzhik V.* Error detecting codes, General Theory and their Application in Feedback Communication Systems. Boston: Kluwer, 1995.

[2] *Leung-Yan-Cheong S. K., Barnes E. R., Friedman D. U.* On some properties of the undetected error probability of linear codes // IEEE Trans. Inform. Theory 1979. Vol. 25. No. 1. P. 110–112.

[3] *Massey J.* Coding techniques for digital data networks // Proc. Int. Conf. Inform. Theory and Syst., Berlin, Germany, 1978. NTG-Fachberichte, Vol. 65.

[4] *Dodunekova R., Dodunekov S., Nikolova E.* A survey on proper codes // Proc. General Theory of Information Transfer and Combinatorics, ZiF Research Year, Bielefeld 2002. To appear.

[5] *Dodunekova, R., Dodunekov S., Nikolova E.* On the error-detecting performance of some classes of block codes // Problems Inform. Transmission. To appear.

[6] *Berlekamp E. R., McEliece R. J., van Tilborg H. C. A.* On the inherent intractability of certain coding problems // IEEE Trans. Inform. Theory 1978. Vol. 24. P. 384–386.

[7] *Dodunekova R.* Extended binomial moments of a linear code and the undetected error probability // Problems Inform. Transmission 2003. Vol. 39. No. 3. P. 255–265.

[8] *Pless V.* Introduction to the Theory of Error-Correcting Codes. New York: Wiley, 1998.

[9] *Dodunekov, S. M., Simonis J.* Codes and projective multisets // The Electronic J. Combin. 1998. Vol. 5. No. 1.

[10] *MacWilliams F.J., Sloane N. J. A.* The theory of error-correcting codes. Amsterdam: North-Holland Publishing Company, 1977.

[11] *Manev N. L.* On the uniqueness of certain codes meeting the Griesmer bound // PLISKA Studia Mathematica bulgarica 1986. Vol. 8. P. 47–53.

[12] *Dodunekova R., Dodunekov S. M.* Linear block codes for error detection. (Preprint 1996-07). Chalmers University of Technology and Göteborg University, 1996.

[13] *Dodunekova R., Dodunekov S. M.* Sufficient conditions for good and proper error detecting codes via their duals // Math. Balkanica (N.S.) 1997. Vol. 11. No 3–4. P. 375–381.

[14] *Helleseth T.* Further classification of codes meeting the Griesmer bound // IEEE Trans. Inf. Theory 1984. IT-30. No. 3. P. 395–403.

[15] *Manev N. L.* A characterization up to isomorphism of some classes of codes meeting the Griesmer bound // C. R. Acad. Bulg. Sci. 1984. Vol. 37. No. 4. P. 481–483.

[16] *van Tilborg H. C. A.* On the uniqueness resp. nonexistence of certain codes meeting the Griesmer bound // Inform. Control 1980. Vol. 44. No. 1. P. 16–35.

[17] *Dodunekov S. M., Manev N. L.* Characterization of two classes of codes meeting the Griesmar bound // Problems of Inform. Transmission 1983. Vol. 19. No. 4. P. 253–259.

[18] *Helleseth T., van Tilborg H. C. A.* A new class of codes meeting the Griesmer bound // IEEE Trans. Inform. Theory 1981. Vol. IT-27. No. 5. P. 548–555.

[19] *Delsarte, P. Goethals, J.-M.* Irreducible binary cyclic codes of even dimension // Combinatorial Mathematics and its applications, Proc. Second Chapel Hill conference, Univ. of N. Carolina, Chapel Hill, N. C., 1970. P. 100–113.

[20] *Dodunekova R., Rabaste O., Vega Páez J. L.* Error detection with a class of irreducible binary cyclic codes and their dual codes (Preprint 2004-16). Chalmers University of Technology and Göteborg University, 2004.

[21] *Dodunekova R.* On the error-detecting performance of the Delsarte-Goethals irreducible binary cyclic codes and their duals (Preprint. 2004-17). Chalmers University of Technology and Göteborg University, 2004.