CHALMERS | GÖTEBORGS UNIVERSITET

PREPRINT

Error Detection with a Class of Irreducible Binary Cyclic Codes and Their Dual Codes

R. DODUNEKOVA
OLIVIER RABASTE
JOSÉ LEÓN VEGA PÁEZ

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

Preprint 2004:16

Error Detection with a Class of Irreducible Binary Cyclic Codes and Their Dual Codes

R. Dodunekova
Olivier Rabaste
José León Vega Páez

CHALMERS | GÖTEBORGS UNIVERSITET

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

NO 2004:16
ISSN 0347-2809

Matematiska Vetenskaper
Göteborg 2004

Error detection with a class of irreducible binary cyclic codes and their dual codes

R. Dodunekova[*]
Mathematical Sciences
Chalmers University of Technology
and Göteborg University

Olivier Rabaste[**]
Ecole Nationale Supérieure
des Télécommunications de Bretagne
Signal and Communications Department

José León Vega Páez[**]
Michoacan 31, Col. San Jose de los Olvera
Queretaro city, Queretaro State
76901 Mexico

Abstract The irreducible binary cyclic codes of even dimension introduced by Delsarte and Goethals in 1970 constitute a parametric class with three parameters. We determine for these codes whether they are proper for error detection or not, and show the properness of a major part of their dual codes.

Key words: linear code, dual code, error detection, proper code.

1 Introduction

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

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

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

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

[*]Supported by the Swedish Research Council under grant 621-2003-5325.

[**]The work was done during these authors' study in the International Master Program *Digital Communication Systems and Technology* at Chalmers University of Technology in 2003.

The code C is *proper* for error detection if $P_{ue}(C, \varepsilon)$ is an increasing function of $\varepsilon \in [0, 1/2]$, see [16] and [17]. Thus a proper code performs the worst in the worst case channel condition $\varepsilon = 1/2$, and performs better on channels with smaller symbol error probability. Moreover, since the procedure of averaging $P_{ue}(C, \varepsilon)$ over the set of all $[n, k]$ linear binary codes results in an increasing function of ε, see [20], a proper code is sufficiently appropriate for error detection in the sense that it performs like an "average" error detecting code in the class.

Many linear codes known to be optimal or close to optimal in one sense or another, turn out to be proper, see for example the survey [11]. Such are the Perfect codes over finite fields [18] and [16], the Maximum Distance Separable codes [13], see also [8], some Reed-Muller codes [15], some Near Maximum Distance Separable codes [7], [10], the Maximum Minimum Distance codes and their duals [6], [9]. Many cyclic codes are proper as well, see e.g.[2], [3], [4], [14]. It is interesting to mention in this connection that some standardized Cyclic Redundancy-check codes are non-proper, as shown in [14]. Examples of nonlinear binary codes which are proper in the above sense are the Kerdock and the Preparata codes, and codes satisfying or meeting the Grey-Rankin bound, see [12].

In this paper we study the properness of a class of irreducible binary cyclic codes $C(r, t, s)$, introduced by Delsarte and Goethals in [5], see also [19], pp. 228–229, and also the properness of their dual codes. The parameters of the class are positive integers satisfying $r \geq 1, \quad t > 1, \quad s > 1$ and $s | 2^r + 1$. The dimension and the length of the code $C(r, t, s)$ are

$$k = 2rt, \quad n = \frac{2^{2rt} - 1}{s}, \tag{1.3}$$

respectively. The code has two non-zero weights,

$$\tau_1 = \frac{2^{2rt-1} + (-1)^t (s-1) 2^{rt-1}}{s}, \quad \tau_2 = \frac{2^{2rt-1} - (-1)^t 2^{rt-1}}{s}, \tag{1.4}$$

and its weight distribution is given by

$$A_{\tau_1} = n, \qquad A_{\tau_2} = (s-1)n. \tag{1.5}$$

Our study of the codes $C(r, t, s)$ and $C^{\perp}(r, t, s)$ in this note will reveal the following:

- When the parameter t is even, $C(r, t, s)$ and $C^{\perp}(r, t, s)$ are proper for any possible values of r and s.

- When the parameter t is odd and $s = 3$, $C(r, t, 3)$ and $C^{\perp}(r, t, 3)$ are proper for any possible values of r.

- When the parameter t is odd and $s \neq 3$, $C(r, t, s)$ is non-proper.

Thus we fully classify the codes $C(r,t,s)$ regarding properness, and show that a major part of their dual codes are proper. The codes not studied here are $C^{\perp}(r,t,s)$ with t odd and $s \neq 3$. Simulations suggest that these codes are non-proper.

We study the codes $C(r,t,s)$ in Section 2 and the codes $C^{\perp}(r,t,s)$ in Section 3. Section 4 concludes the paper.

The following technical lemma is basic for the proofs.

Lemma [12]. *Let $n, a,$ and b be integers such that $0 < a < \frac{n}{2} \leq b < n$, and let α and β be positive constants. The function*

$$G(\varepsilon) = \alpha\varepsilon^{a}(1-\varepsilon)^{n-a} + \beta\varepsilon^{b}(1-\varepsilon)^{n-b} \tag{1.6}$$

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

$$\alpha(n-2a) \leq \beta(2b-n) \tag{1.7}$$

and if either

$$a+b \leq n \quad \text{and} \quad \frac{ab}{n} \geq \frac{(a+b-1)^2}{4(n-1)} \tag{1.8}$$

or

$$a+b \geq n \quad \text{and} \quad (n-2a)(2b-n) \leq n. \tag{1.9}$$

The proof of the Lemma uses standard analysis and may be found in [12].

Throughout the rest of the work we will use the notation $m = 2^{rt-1}$, and we will also make use of the relationships

$$\tau_1 + (s-1)\tau_2 = \frac{sn+1}{2} = 2m^2, \tag{1.10}$$

$$(s-1)\tau_2(2\tau_2 - n) - \tau_1(n-2\tau_1) = 2m^2, \tag{1.11}$$

which are easily obtained from (1.3) and (1.4).

2 The codes $C(r,t,s)$.

Theorem 1. *When the parameter t is even, the code $C(r,t,s)$ is proper.*

Proof. The probability of undetected error of $C(r,t,s)$ is, by (1.1) and (1.5),

$$P_{ue}(C(r,t,s),\varepsilon) = (s-1)n\varepsilon^{\tau_2}(1-\varepsilon)^{n-\tau_2} + n\varepsilon^{\tau_1}(1-\varepsilon)^{n-\tau_1}, \quad 0 \leq \varepsilon \leq 1/2,$$

where, in accordance with (1.3) and (1.4),

$$n = \frac{4m^2-1}{s}, \quad \tau_1 = \frac{2m^2+(s-1)m}{s} > \frac{n}{2}, \quad \tau_2 = \frac{2m^2-m}{s} < \frac{n}{2}. \tag{2.1}$$

The function $P_{ue}(C(r,t,s),\,\varepsilon)$ is of the form (1.6) with $a = \tau_2,\ b = \tau_1$, and $\alpha = (s-1)n,\ \beta = n$. We will show that this function is increasing for $\varepsilon \in [0, \frac{1}{2}]$ by using the Lemma. The condition (1.7) holds since

$$n(2\tau_1 - n) - (s-1)n(n-2\tau_2) = n[2(\tau_1 + (s-1)\tau_2) - sn] = n,$$

where we have used (1.10). Since

$$\tau_1 + \tau_2 = \frac{4m^2 + (s-2)m}{s} > n$$

and

$$\begin{aligned}(n-2\tau_2)(2\tau_1 - n) &= \frac{2m-1}{s}\cdot\frac{(s-1)2m+1}{s} = \frac{(s-1)4m^2 - (s-2)2m - 1}{s^2}\\ &< \frac{(s-1)4m^2 - (s-2) - 1}{s^2} = \frac{s-1}{s}\cdot\frac{4m^2-1}{s} < n,\end{aligned}$$

(1.9) holds as well. Thus $P_{ue}(C(r,t,s),\,\varepsilon)$ increases for $\varepsilon \in [0, \frac{1}{2}]$ and hence C is proper.

Theorem 2. *When the parameter t is odd and $s = 3$, the code $C(r,t,3)$ is proper.*

Proof. The probability of undetected error of $C(r,t,3)$ is, by (1.1),

$$P_{ue}(C(r,t,s),\varepsilon) = n\varepsilon^{\tau_1}(1-\varepsilon)^{n-\tau_1} + 2n\varepsilon^{\tau_2}(1-\varepsilon)^{n-\tau_2},$$

where

$$n = \frac{4m^2-1}{3}, \quad \tau_1 = \frac{2m^2-2m}{3} < \frac{n}{2} \quad \tau_2 = \frac{2m^2+m}{3} > \frac{n}{2}. \tag{2.2}$$

The condition (1.7) of the Lemma holds for the above function since by (1.10) with $s = 3$ we have

$$2n(2\tau_2 - n) - n(n - 2\tau_1) = n[2(\tau_1 + 2\tau_2) - 3n] = n.$$

The first inequality of (1.8) holds as well, since from (2.2)

$$\tau_1 + \tau_2 = \frac{4m^2 - m}{3} < n.$$

To show the second inequality we consider

$$\begin{aligned}&4(n-1)\tau_1\tau_2 - n(\tau_1+\tau_2-1)^2\\ =&n\big[-(\tau_2-\tau_1)^2 + 2(\tau_1+\tau_2) - 1)\big] - 4\tau_1\tau_2\\ =&n\Big[-m^2 + \frac{8m^2-2m}{3} - 1\Big] - 4\tau_1\tau_2\\ =&\frac{1}{9}\big[(4m^2-1)(5m^2-2m-3) - 4(2m^2-2m)(2m^2+m)\big]\\ =&\frac{1}{9}(4m^4 - 9m^2 + 2m + 3) > \frac{1}{9}\big[4m^2(m^2-16)\big] \geq 0,\end{aligned}$$

where in the last inequality we have used the fact that $m = 2^{rt-1} \geq 4$, since $t > 1$ is odd by assumption and thus $t \geq 3$, and also $r \geq 1$.

By the Lemma, the function $P_{ue}(C(r,t,3),\, \varepsilon)$ is increasing for $\varepsilon \in [0, 1/2]$ and hence C is proper.

Theorem 3. *When the parameter t is odd and $s \neq 3$, the code $C(r,t,s)$ is non-proper.*

Proof. In this case we have

$$n = \frac{4m^2 - 1}{s}, \qquad \tau_1 = \frac{2m^2 - (s-1)m}{s}, \qquad \tau_2 = \frac{2m^2 + m}{s}. \tag{2.3}$$

Put

$$\varepsilon_i = \frac{\tau_i}{n}, \quad i = 1,\ 2.$$

It is obvious from (2.3) that

$$\varepsilon_1 < \frac{1}{2}, \quad \varepsilon_2 > \frac{1}{2}. \tag{2.4}$$

From

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

and (1.1) we have

$$\begin{aligned} &P'_{ue}(C(r,t,s),\, \varepsilon) \\ &= n^2\varepsilon^{\tau_1-1}(1-\varepsilon)^{n-\tau_1-1}(\varepsilon_1 - \varepsilon) + (s-1)n^2\varepsilon^{\tau_2-1}(1-\varepsilon)^{n-\tau_2-1}(\varepsilon_2 - \varepsilon) \\ &= (s-1)n^2\varepsilon^{\tau_2-1}(1-\varepsilon)^{n-\tau_2-1}(\varepsilon_2-\varepsilon)\Big[1 - \frac{1}{s-1}\cdot\frac{\varepsilon - \varepsilon_1}{\varepsilon_2 - \varepsilon}\Big(\frac{1-\varepsilon}{\varepsilon}\Big)^{\tau_2 - \tau_1}\Big]. \end{aligned} \tag{2.5}$$

The relationships (2.4) and (2.5) show that when $\varepsilon \in [0,\, 1/2]$ the sign of $P'_{ue}(C(r,t,s),\, \varepsilon)$ is the same as the sign of the function in the brackets in the right-hand side of (2.5). To prove the theorem we will show that, under the assumptions of the theorem, this function is negative at the point

$$\varepsilon_0 = \frac{1}{s-1}\cdot\varepsilon_1 + \frac{s-2}{s-1}\cdot\frac{1}{2} \in \big(\varepsilon_1, 1/2\big), \tag{2.6}$$

or, that

$$f(\varepsilon_0) = \frac{1}{s-1}\cdot\frac{\varepsilon_0 - \varepsilon_1}{\varepsilon_2 - \varepsilon_0}\Big(\frac{1-\varepsilon_0}{\varepsilon_0}\Big)^{\tau_2 - \tau_1} > 1 \tag{2.7}$$

when t is odd and $s \neq 3$. First we find

$$\frac{1}{s-1} \cdot \frac{\varepsilon_0 - \varepsilon_1}{\varepsilon_2 - \varepsilon_0} = \frac{1}{s-1} \cdot \frac{\frac{s-2}{s-1}(\frac{1}{2} - \varepsilon_1)}{(\varepsilon_2 - \varepsilon_1) - \frac{s-2}{s-1}(\frac{1}{2} - \varepsilon_1)}$$
$$= \frac{s-2}{s-1} \cdot \frac{\frac{1}{2} - \varepsilon_1}{(s-1)(\varepsilon_2 - \varepsilon_1) - (s-2)(\frac{1}{2} - \varepsilon_1)}$$
$$= \frac{s-2}{s-1} \cdot \frac{\frac{1}{2} - \varepsilon_1}{s(\varepsilon_2 - \frac{1}{2}) - (\varepsilon_1 + \varepsilon_2) + 1}$$
$$= \frac{s-2}{s-1} \cdot \frac{n - 2\tau_1}{s(2\tau_2 - n) - 2(\tau_1 + \tau_2) + 2n}.$$

From this and (2.3),

$$\frac{1}{s-1} \cdot \frac{\varepsilon_0 - \varepsilon_1}{\varepsilon_2 - \varepsilon_0} = \frac{s-2}{s-1} \cdot \frac{(s-1)2m - 1}{s(2m+1) + 2[(s-2)m - 1]}$$
$$= \frac{s-2}{s-1} \cdot \frac{(s-1)2m - 1}{(s-1)(4m+1) - 1}$$
$$= \Big(1 - \frac{1}{s-1}\Big)\Big(\frac{2m}{4m+1} - \frac{1 - \frac{2m}{4m+1}}{(s-1)(4m+1) - 1}\Big)$$
$$= \Big(1 - \frac{1}{s-1}\Big)\Big(\frac{1}{2} - \frac{1/2}{4m+1} - \frac{1/2 + \frac{1/2}{4m+1}}{(s-1)(4m+1) - 1}\Big).$$

Obviously, the above expression increases in s and m, and also $m = 2^{rt-1}$ increases in rt. Since $t > 1$ is odd by assumption, we must have $t \geq 3$, and also $r \geq 2$, since if $r = 1$, s would equal 3, while by assumption $s \neq 3$. Also, the minimum possible value of s is 5, since $s | 2^r + 1$ and s thus is odd. Note that either $rt \geq 9$ or $rt = 6$ with $r = 2$ and $t = 3$. We consider these cases separately. In the first case, the minimum value of m is $2^8 = 256$. Put $s = 5$ and $m = 256$ in the expression on line two in the above chain to get the bound

$$\frac{1}{s-1} \cdot \frac{\varepsilon_0 - \varepsilon_1}{\varepsilon_2 - \varepsilon_0} \geq \frac{3}{4} \cdot \frac{8 \cdot 256 - 1}{4(4 \cdot 256 + 1) - 1} > 0.374, \tag{2.8}$$

which as we recall is valid when $s \neq 3$, t odd, and $rt \geq 9$. Under the same assumptions on the parameters, consider now the other factor of $f(\varepsilon_0)$ in (2.7). Using the inequality

$$1 + y > e^{\frac{y}{1+y}}, \quad y > 0,$$

(see [1], chapter 4), we obtain

$$\Big(\frac{1 - \varepsilon_0}{\varepsilon_0}\Big)^{\tau_2 - \tau_1} = \Big(1 + \frac{1 - 2\varepsilon_0}{\varepsilon_0}\Big)^m > e^{\frac{1-2\varepsilon_0}{1-\varepsilon_0} \cdot m}, \tag{2.9}$$

where

$$\begin{aligned}\frac{1-2\varepsilon_0}{1-\varepsilon_0} &= \frac{2\cdot\frac{1}{s-1}(\frac{1}{2}-\varepsilon_1)}{\frac{1}{s-1}(s-1-\varepsilon_1-\frac{1}{2}(s-2))} = \frac{1-2\varepsilon_1}{\frac{s}{2}-\varepsilon_1}\\ &= 2\cdot\frac{n-2\tau_1}{sn-2\tau_1} = 2\cdot\frac{(s-1)2m-1}{s(4m^2-1)-4m^2+(s-1)2m}\\ &= \frac{(s-1)4m-2}{(s-1)(4m^2+2m-1)-1}.\end{aligned}$$

Thus

$$\begin{aligned}\frac{1-2\varepsilon_0}{1-\varepsilon_0}\cdot m &= \frac{(s-1)4m^2-2m}{(s-1)(4m^2+2m-1)-1}\\ &= \frac{4m^2}{4m^2+2m-1}\cdot\frac{s-1-\frac{2m}{4m^2}}{s-1-\frac{1}{4m^2+2m-1}}\\ &= \frac{4m^2}{4m^2+2m-1}\Big(1-\frac{\frac{1}{2m}-\frac{1}{4m^2+2m-1}}{s-1-\frac{1}{4m^2+2m-1}}\Big).\end{aligned}$$

Since the last expression increases in s, and since $s \geq 5$, we obtain from the first line of the above chain

$$\begin{aligned}\frac{1-2\varepsilon_0}{1-\varepsilon_0}\cdot m &\geq \frac{4.4m^2-2m}{4(4m^2+2m-1)-1} = \frac{16m^2-2m}{16m^2+8m-5}\\ &= 1-\frac{\frac{10}{4}(4m-2)}{(4m+1+\sqrt{6})(4m+1-\sqrt{6})}\\ &> 1-\frac{5}{2}\cdot\frac{1}{4m+1+\sqrt{6}} \geq 1-\frac{5}{2}\cdot\frac{1}{4\cdot 256+1+\sqrt{6}} > 0.997,\end{aligned}$$

where in the last line we have used the fact that $m \geq 256$.

We now apply the above bound in (2.9) and use the result together with the bound in (2.8) to get, for $f(\varepsilon_0)$ in (2.7),

$$f(\varepsilon_0) > 0.374\cdot e^{0.997} > 0.37\cdot 2.71 > 1.0027.$$

This proves the inequality (2.7) which together with (2.5) show that

$$P'_{ue}(C(r,t,s),\,\varepsilon_0) < 0.$$

Hence the code $C(r,t,s)$ is non-proper, when t is odd, $s \neq 3$, and $rt \geq 9$.

It now remains to prove the statement in the case t odd, $s \neq 3$, and $rt = 6$, i.e., $r = 2$, $t = 3$, and $s = 5$. Computations show that even for these values of the parameters we have for $f(\varepsilon_0)$ with ε_0 as in (2.6)

$$f(\varepsilon_0) > 1.005,$$

and again by (2.5), the code $C(2,3,5)$ is non-proper.

The codes $C(r,t,s)$ are thus now fully classified regarding properness in error detection.

3 The codes $C^{\perp}(r,t,s)$.

Theorem 4. *When the parameter t is even, the code $C^{\perp}(r,t,s)$ is proper.*

Proof. To show the properness of $C^{\perp}(r,t,s)$ we will use (1.2). In this case τ_1 and τ_2 are as in (2.1) and we have

$$\begin{aligned} P_{ue}(C^{\perp}(r,t,s),\,\varepsilon) =& 2^{-k}[1+n(s-1)(1-2\varepsilon)^{\tau_2} \\ &+n(1-2\varepsilon)^{\tau_1}]-(1-\varepsilon)^n, \quad 0\le\varepsilon\le 1/2, \end{aligned}$$

and also

$$\begin{aligned} P'_{ue}(C^{\perp}(r,t,s),\,\varepsilon) =& -2^{-k+1}[n(s-1)\tau_2(1-2\varepsilon)^{\tau_2-1} \\ &+n\tau_1(1-2\varepsilon)^{\tau_1-1}]+n(1-\varepsilon)^{n-1}, \quad 0\le\varepsilon\le 1/2. \end{aligned}$$

Hence

$$\begin{aligned} \frac{P'_{ue}(C^{\perp}(r,t,s),\,\varepsilon)}{n(1-\varepsilon)^{n-1}} =& 1-2^{-k+1}\cdot\Big[(s-1)\tau_2\Big(\frac{1-2\varepsilon}{1-\varepsilon}\Big)^{\tau_2-1}\Big(\frac{1}{1-\varepsilon}\Big)^{n-\tau_2} \\ &+\tau_1\Big(\frac{1-2\varepsilon}{1-\varepsilon}\Big)^{\tau_1-1}\Big(\frac{1}{1-\varepsilon}\Big)^{n-\tau_1}\Big] \\ =& 1-2^{-k+n}\cdot\Big[[(s-1)\tau_2\Big(1-\frac{1}{2(1-\varepsilon)}\Big)^{\tau_2-1}\Big(\frac{1}{2(1-\varepsilon)}\Big)^{n-\tau_2} \\ &+\tau_1\Big(1-\frac{1}{2(1-\varepsilon)}\Big)^{\tau_1-1}\Big(\frac{1}{2(1-\varepsilon)}\Big)^{n-\tau_1}\Big] \\ =& 1-2^{-k+n}\Big[[(s-1)\tau_2\delta^{\tau_2-1}(1-\delta)^{n-\tau_2}+\tau_1\delta^{\tau_1-1}(1-\delta)^{n-\tau_1}\Big], \end{aligned} \tag{3.1}$$

where we have put

$$\delta = 1-\frac{1}{2(1-\varepsilon)}, \quad 0\le\delta\le 1/2. \tag{3.2}$$

As (3.1) and (3.2) show, in order to establish the properness of $C^{\perp}(r,t,s)$, it suffices to prove that the function

$$G_1(\delta) = (s-1)\tau_2\delta^{\tau_2-1}(1-\delta)^{n-\tau_2}+\tau_1\delta^{\tau_1-1}(1-\delta)^{n-\tau_1} \tag{3.3}$$

satisfies the inequality

$$G_1(\delta)\le 2^{k-n}, \quad 0\le\delta\le 1/2. \tag{3.4}$$

We will first show by using the Lemma that the function $G_1(\delta)$ increases for $\delta\in[0,\,1/2]$. The condition (1.7) holds because of (1.10) and (1.11):

$$\begin{aligned} &\tau_1[2(\tau_1-1)-(n-1)]-(s-1)\tau_2[(n-1)-2(\tau_2-1)] \\ &\quad=(s-1)\tau_2(2\tau_2-n)-\tau_1(n-2\tau_1)-[\tau_1+(s-1)\tau_2]=0. \end{aligned}$$

We will now show that (1.9) holds as well. First,

$$(\tau_2-1)+(\tau_1-1)-(n-1)=\frac{(s-2)m-s+1}{s}=\frac{(s-2)(m-1)-1}{s}\geq 0,$$

since $s\geq 3$ and $m\geq 2$. Thus the first inequality of (1.9) is satisfied. The second inequality follows from

$$\begin{aligned}&(n-1)-[(n-1)-2(\tau_2-1)][2(\tau_1-1)-(n-1)]\\&=\frac{4m^2-1-s}{s}-\frac{2m+s-1}{s}\cdot\frac{(s-1)(2m-1)}{s}\\&=\frac{1}{s^2}\big[4m^2-(s-1)(s-2)2m-3s+1\big]\\&=\frac{1}{s^2}\big[4m^2-(s-1)^2 2m+(s-1)(2m-3)-2\big]\\&\geq\frac{2m}{s^2}\big[2m-(s-1)^2\big]\geq 0\end{aligned}$$

since

$$(s-1)^2\leq 2^{2r}\leq 2^{rt}=2m.$$

By the Lemma, the function in (3.3) is increasing for $\delta\in[0,\,1/2]$. Therefore,

$$\max_{0\leq\delta\leq 1/2}G_1(\delta)=G(1/2)=2^{-n+1}[(s-1)\tau_2+\tau_1]=2^{k-n},$$

where again we have made use of (1.10) and also of (1.3). This shows (3.4) which gives, together with (3.1) and (3.2), that $P_{ue}(C^{\perp}(r,t,s),\,\varepsilon)\geq 0$ for $\varepsilon\in[0,\frac{1}{2}]$, i. e., $C^{\perp}(r,t,s)$ is proper.

Theorem 5. *When the parameter t is odd and $s=3$, the code $C^{\perp}(r,t,3)$ is proper.*

Proof. From (1.2) we obtain

$$P_{ue}(C^{\perp}(r,t,s),\,\varepsilon)=2^{-k}\big[1+n(1-2\varepsilon)^{\tau_1}+2n(1-2\varepsilon)^{\tau_2}\big]-(1-\varepsilon)^n,$$

where τ_1 and τ_2 are as in (2.2). As in (3.1),

$$\frac{P'_{ue}(C^{\perp}(r,t,s),\varepsilon)}{n(1-\varepsilon)^{n-1}}=1-2^{-k+n}\big[\tau_1\delta^{\tau_1-1}(1-\delta)^{n-\tau_1}+2\tau_2\delta^{\tau_2-1}(1-\delta)^{n-\tau_2}\big],\quad(3.5)$$

where

$$\delta=1-\frac{1}{2(1-\varepsilon)},\quad 0\leq\delta\leq 1/2.\qquad(3.6)$$

In order to prove the properness of $C^{\perp}(r,t,s)$ we will establish that the function

$$G_2(\delta)=\tau_1\delta^{\tau_1-1}(1-\delta)^{n-\tau_1}+2\tau_2\delta^{\tau_2-1}(1-\delta)^{n-\tau_2}$$

in the right-hand side of (3.5) satisfies the inequality

$$G_2(\delta) \leq 2^{-n+k}, \quad 0 \leq \delta \leq 1/2. \tag{3.7}$$

We will first show by means of the Lemma that $G_2(\delta)$ is increasing for $\delta \in [0, 1/2]$. The condition (1.7) holds in this case since by (1.10) and (1.11) we have

$$\begin{aligned} &2\tau_2[2(\tau_2 - 1) - (n-1)] - \tau_1[(n-1) - 2(\tau_1 - 1)] \\ &\quad = 2\tau_2(2\tau_2 - n) - \tau_1(n - 2\tau_1) - (2\tau_2 + \tau_1) = 0. \end{aligned}$$

Since

$$(\tau_1 - 1) + (\tau_2 - 1) = \frac{4m^2 - m}{3} - 2 < n - 1,$$

the first inequality of (1.8) holds as well. We show the second by using again the fact that $m = 2^{rt-1} \geq 4$:

$$\begin{aligned} &4(n-2)(\tau_1 - 1)(\tau_2 - 1) - (n-1)\big((\tau_1 - 1) + (\tau_2 - 1) - 1\big)^2 \\ &\quad = (n-1)\big[-(\tau_2 - \tau_1)^2 + 2(\tau_1 + \tau_2 - 2) - 1)\big] - 4(\tau_1 - 1)(\tau_2 - 1) \\ &\quad = (n-1)\Big[-m^2 + \frac{8m^2 - 2m}{3} - 5\Big] - 4(\tau_1 - 1)(\tau_2 - 1) \\ &\quad = \frac{1}{9}\big[(4m^2 - 4)(5m^2 - 2m - 15) - 4(2m^2 - 2m - 3)(2m^2 + m - 3)\big] \\ &\quad = \frac{4}{9}(m^4 - 6m^2 - m + 6) = \frac{4}{9}\big[m^2(m^2 - 16) + m(10m - 1) + 6\big] > 0. \end{aligned}$$

By the lemma, the function $G_2(\delta)$ is increasing for $\delta \in [0, 1/2]$. Therefore

$$\max_{0 \leq \delta \leq 1/2} G_2(\delta) = G_2(1/2) = (\tau_1 + 2\tau_2)2^{-n+1} = 2^{k-n},$$

and the inequality (3.7) thus holds true. Together with (3.5) and (3.6) it implies that $C^{\perp}(r, t, 3)$ is proper.

4 Conclusion

We have shown that the irreducible binary cyclic codes $C(r, t, s)$ introduced by Delsarte and Goethals are proper for error detection when the parameter t is even and when the parameter t is odd and $s = 3$, and that they are non-proper when the parameter t is odd and $s \neq 3$. We have therefore fully classified the codes $C(r, t, s)$ regarding properness.

We have also shown that the dual codes $C^{\perp}(r, t, s)$ are proper for error detection when the parameter t is even and when the parameter t is odd and $s = 3$. To complete the classification of the dual codes regarding properness, it remains to investigate the codes $C^{\perp}(r, t, s)$ with t odd and $s \neq 3$. As mentioned before, we believe that these codes are non-proper.

References

[1] M. Abramovitz and I. A. Stegun, Eds. *Handbook of Mathematical Functions*, National Bureau of Standards, Applied Mathematics Series, 55, 1964.

[2] Ts. Baicheva, S. Dodunekov, P. Kazakov, On the error detection performance of some standardized CRC codes. In *Proc. Telecom 98*, Drujba, Bulgaria, pp. 66–72, 1998.

[3] Ts. Baicheva, S. Dodunekov, P. Kazakov, On the undetected error probability performance of cyclic redundancy-check codes of 16-bit redundancy. *IEEE Trans. Commun.* vol. 147, no. 5, pp. 253–256, 2000.

[4] Ts. Baicheva, S. Dodunekov, R. Kötter, On the performance of the ternary [13, 7, 5] quadratic residue code. *IEEE Trans. Inform. Theory*, vol. 48, no. 2, pp. 562–564, 2002.

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

[6] R. Dodunekova, The duals of the MMD codes are proper for error detection. *IEEE Trans. Inform. Theory*, vol. 49, no. 8, pp. 2034-32038, 2003.

[7] R. Dodunekova, S. M. Dodunekov, On the probability of undetected error for Near MDS codes. Prep. no. 1995–25, Dept. Math. Göteborg University, 1995.

[8] Dodunekova, R. and Dodunekov, S. M. Sufficient conditions for good and proper error detecting codes. *IEEE Trans. Inform. Theory*, vol 43, pp. 2023–2026, 1997.

[9] R. Dodunekova, S. M. Dodunekov, The MMD codes are proper for error detection. *IEEE Trans. Inform. Theory*, vol. 48, no. 12, pp. 3109–3111, 2002.

[10] R. Dodunekova, S. M. Dodunekov, T. Kløve, Almost MDS and Near MDS codes for error detection. *IEEE Trans. Inform. Theory*, vol. 43, no. 1, pp. 285–290, 1997.

[11] R. Dodunekova, S. 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).

[12] R. Dodunekova, S. Dodunekov and E. Nikolova, On the error-detecting performance of some classes of block codes. Prep. no. 2004:13, Dept. Math. Sciences, Chalmers University of Technology and Göteborg University, 2004.

[13] T. Kasami, S. Lin, On the probability of undetected error for the maximum distance separable codes. *IEEE Trans. Commun.*, vol. 32, no. 9, pp. 998–1006, 1984.

[14] P. Kazakov, *Application of Polynomials to CRC and Spherical codes*, PhD Thesis. Technishe Universitet Delft, 2000.

[15] T. Kløve, Reed-Muller codes for error detection: The Good, The Bad, and The Ugly. *IEEE Trans. Inform. Theory*, vol. 42, no. 6, pp. 1615–1622, 1996.

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

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

[18] S. K. Leung-Yan-Cheong, M. E. Hellman, Concerning a bound on undetected error probability. *IEEE Trans. Inform. Theory*, vol. 22, no. 2, pp. 235–237, 1976.

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

[20] J. Massey, Coding techniques for digital data networks. In *Proc.Int. Conf. Inform. Theory and Syst.*, NTG-Fachberichte, vol. 65, Sept. 18–20, 1978, Berlin, Germany.