CHALMERS | GÖTEBORGS UNIVERSITET

PREPRINT

On the Error-Detecting Performance of the Delsarte-Goethals Irreducible Binary Cyclic Codes and Their Duals

R. DODUNEKOVA

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

Preprint 2004:17

On the Error-Detecting Performace of the Delsarte-Goethals Irreducible Binary Cyclic Codes and Their Duals

R. Dodunekova

CHALMERS | GÖTEBORGS UNIVERSITET

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

Göteborg, April 2004

NO 2004:17
ISSN 0347-2809

Matematiska Vetenskaper
Göteborg 2004

On the error-detecting performance of the Delsarte-Goethals irreducible binary cyclic codes and their duals

*Rossitza Dodunekova**

Mathematical Sciences

Chalmers University of Technology

and Göteborg University

412 96 Göteborg, Sweden

Abstract In this note we complete the classification with respect to properness carried out in [4] for the Delsarte-Goethals irreducible binary cyclic codes and for some of their duals, by proving that the dual codes not considered there are in fact non-proper. We also prove that the Delsarte-Goethals irreducible binary cyclic codes, shown in [4] to be non-proper, are actually not even good for error detection.

Key words: cyclic code, dual code, error detection, good code, proper code.

1 Introduction

The irreducible binary cyclic codes $C(r,t,s)$ introduced in 1970 by Delsarte and Goethals [1], see also [8], pp. 228–229, depend on three parameters r, t, and s, which are positive integers satisfying $r \geq 1$, $t > 1$, $s > 1$, and $s|2^r+1$. The dimension k and the length n of the code $C(r,t,s)$ are

$$k = 2rt, \qquad n = \frac{2^{2rt}-1}{s}. \tag{1.1}$$

The code has two non-zero weights,

$$\tau_1 = \frac{2^{2rt-1}+(-1)^t(s-1)2^{rt-1}}{s}, \quad \tau_2 = \frac{2^{2rt-1}-(-1)^t 2^{rt-1}}{s}, \tag{1.2}$$

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

and its weight distribution is given by

$$A_{\tau_1} = n, \qquad A_{\tau_2} = (s-1)n. \tag{1.3}$$

The error detecting performance of the codes $C(r,t,s)$ and of some of their dual codes $C^{\perp}(r,t,s)$ has been studied in [4]. It was shown there that $C(r,t,s)$ and $C^{\perp}(r,t,s)$ are proper when t is even, and also when t is odd and $s=3$, and that $C(r,t,s)$ is non-proper when t is odd and $s \neq 3$.

While in [4] the classification with respect to properness was complete for the codes $C(r,t,s)$, it was not for the dual codes, since the codes $C^{\perp}(r,t,s)$ with t odd and $s \neq 3$ still remained not studied. However, it was conjectured in [4] that these codes are non-proper. We give a proof of this conjecture in Theorem 1 of Section 3. We also give a better insight into the codes $C(r,t,s)$ with t odd and $s \neq 3$, shown in [4] to be non-roper. It turns out, that these codes are in fact not even good for error detection, which we prove in Theorem 2 of Section 3. In Section 2 we present a technical lemma, which is basic for the proofs of the theorems.

For completeness, we first recall the concepts of a proper and a good linear error detecting code, restricting ourselves to the binary case.

When a linear binary $[n,k,d]$ code C 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

$$P_{ue}(C,\,\varepsilon) = \sum_{i=d}^{n} A_i \varepsilon^i (1-\varepsilon)^{n-i}, \quad 0 \le \varepsilon \le \frac{1}{2}, \tag{1.4}$$

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

$$P_{ue}(C,\,\varepsilon) = 2^{-(n-k)} \sum_{i=0}^{n} B_i (1-2\varepsilon)^i - (1-\varepsilon)^n, \quad 0 \le \varepsilon \le \frac{1}{2}. \tag{1.5}$$

The code C is *proper* for error detection if $P_{ue}(C,\,\varepsilon)$ is an increasing function of $\varepsilon \in [0, 1/2]$, and *good* if $P_{ue}(C,\,\varepsilon)$ takes its largest value in the worst case channel condition $\varepsilon = 1/2$, see [6] and [7]. Thus a proper code is also a good code, but a proper code has the advantage of performing better on better channels, i.e., on channels with smaller symbol error probability. Another way of looking at a proper $[n,k,d]$ binary linear code is to say that its behavior in error detection is similar to the behavior of an "average" code in the set of all $[n,k]$ binary linear codes since, as shown in [9], the procedure of averaging $P_{ue}(C,\,\varepsilon)$ over this set results in an increasing function of ε.

Some 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, and the Maximum Minimum Distance codes and their duals, see also the survey [2] on proper codes. Many cyclic codes are proper, and there are non-proper standardized Cyclic Redundancy-check codes, see [5]. The Kerdock and the Preparata codes, and codes satisfying the Grey-Rankin bound are examples of non-linear binary codes which are proper in the above sense, see [3].

2 A basic technical Lemma

Let r, t, and s be the parameters of the binary cyclic code $C(r,t,s)$ with t odd and $s \neq 3$. Setting $m = 2^{rt-1}$, the length and the non-zero weights of the code are, cf. (1.1) and (1.2),

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

The parameter s is odd, since $s|2^r+1$, and thus $s = 5,\ 7\ \ldots$. Define $\delta_s \in (0,1/2)$ as

$$\delta_s = \frac{1}{2} - \frac{\alpha_s}{2}, \qquad \alpha_s = \begin{cases} \dfrac{5}{3m}, & \text{if } \ s=5, \\ \dfrac{s}{2m}, & \text{if } \ s \geq 7, \end{cases} \tag{2.2}$$

and with n, τ_1, and τ_2 as in (2.1),

$$G(\delta) = \frac{1}{s}\big[\delta^{\tau_1}(1-\delta)^{n-\tau_1} + (s-1)\delta^{\tau_2}(1-\delta)^{n-\tau_2}\big]. \tag{2.3}$$

Lemma. It holds

$$2^n G(\delta_s) > 1.021. \tag{2.4}$$

Proof. We have $t \geq 3$, because t is odd and $t > 1$, and $r \geq 2$, because $s|2^r+1$ and $s \geq 5$. Therefore

$$m \geq 32, \qquad \frac{m}{s} \geq \frac{2^{3r-1}}{2^r+1} \geq \frac{2^5}{5} = 6.4 = c. \tag{2.5}$$

From (2.1), (2.2) and (2.3) we have

$$\begin{aligned} 2^n G(\delta_s) &= \frac{1}{s}\big[(2\delta_s)^{\tau_1}(2(1-\delta_s))^{n-\tau_1} + (s-1)(2\delta_s)^{\tau_2}(2(1-\delta_s))^{n-\tau_2}\big] \\ &= \frac{1}{s}\big[(1-\alpha_s)^{\tau_1}(1+\alpha_s)^{n-\tau_1} + (s-1)(1-\alpha_s)^{\tau_2}(1+\alpha_s)^{n-\tau_2}\big] \\ &= \frac{1}{s}(1-\alpha_s)^{\tau_2}(1+\alpha_s)^{n-\tau_2}\big[(1-\alpha_s)^{\tau_1-\tau_2}(1+\alpha_s)^{\tau_2-\tau_1} + s - 1\big] \\ &= \frac{1}{s}(1-\alpha_s^2)^{\frac{2m^2}{s}}(1-\alpha_s)^{\frac{m}{s}}(1+\alpha_s)^{-\frac{m+1}{s}}\big[(1-\alpha_s)^{-m}(1+\alpha_s)^{m} + s - 1\big]. \end{aligned} \tag{2.6}$$

Consider first $s \geq 7$, in which case $\alpha_s = s/(2m)$. Since the functions $\left(1+\frac{1}{x}\right)^x$ and $\left(1-\frac{1}{x}\right)^x$ are increasing for $x > 1$ and

$$\left(1+\frac{1}{x}\right)^x \to e, \quad \left(1-\frac{1}{x}\right)^x \to e^{-1}, \quad x \to \infty, \tag{2.7}$$

we obtain using (2.5), for the factors in the last line of (2.6),

$$\begin{aligned}
&\left(1-\frac{s^2}{4m^2}\right)^{\frac{2m^2}{s}} \geq \left(1-\frac{1}{4c^2}\right)^{2c^2 s} > (0.605)^s,\\
&\left(1-\frac{s}{2m}\right)^{\frac{m}{s}} \geq \left(1-\frac{1}{2c}\right)^{c} > 0.59,\\
&\left(1+\frac{s}{2m}\right)^{-\frac{m+1}{s}} > e^{-\frac{m+1}{2m}} = e^{-1/2-1/2m} > e^{-1/2-1/64} > 0.59,\\
&\left(1-\frac{s}{2m}\right)^{-m} > e^{s/2},\\
&\left(1+\frac{s}{2m}\right)^{m} \geq \left(1+\frac{1}{2c}\right)^{cs} > 1.618^s.
\end{aligned}$$

Substituting the above bounds into (2.6) we get

$$\begin{aligned}
2^n G(\delta_s) &> \frac{(0.59)^2}{s}\Big[(0.605 \cdot e^{1/2} \cdot 1.618)^s + (s-1)(0.605)^s\Big]\\
&> 0.3\Big[\frac{(1.6)^s}{s} + \frac{(s-1)(0.6)^s}{s}\Big].
\end{aligned} \tag{2.8}$$

The function

$$f(s) = \frac{a^s}{s} + \frac{(s-1)b^s}{s}, \qquad a = 1.6, \qquad b = 0.6,$$

is increasing for $s \geq 7$, since

$$\begin{aligned}
f'(s) &= \frac{1}{s}\Big[a^s(\ln a - 1/s) + b^s((s-1)\ln b + 1/s)\Big]\\
&> \frac{1}{s}\Big[a^s(\ln a - 1/7) + b^s s \ln b\Big] > \frac{b^s}{s}\Big[\left(\frac{a}{b}\right)^s \cdot 0.3 - s \cdot 0.6\Big]\\
&> \frac{0.3b^s}{s}(2^s - 2s) > 0.
\end{aligned}$$

Therefore we have for $s \geq 7$ that $f(s) \geq f(7) > 3.8$, which gives in (2.8),

$$2^n G(\delta_s) > 0.3 \cdot 3.8 > 1.1, \quad s \geq 7. \tag{2.9}$$

Consider now $s=5$. We have $\alpha_5 = 5/(3m)$ and by (2.5) and the monotonicity of the functions in (2.7) we obtain, for the factors in the last line of (2.6),

$$\Big(1-\frac{25}{9m^2}\Big)^{\frac{2m^2}{5}} \geq \Big(1-\frac{1}{9c^2}\Big)^{10c^2} > 0.3286,$$
$$\Big(1-\frac{5}{3m}\Big)^{\frac{m}{5}} \geq \Big(1-\frac{1}{3c}\Big)^{c} > 0.7101,$$
$$\Big(1+\frac{5}{3m}\Big)^{-\frac{m+1}{5}} > e^{-\frac{m+1}{3m}} = e^{-1/3-1/3m} > e^{-1/3-1/3\cdot 2^5} > 0.7091,$$
$$\Big(1-\frac{5}{3m}\Big)^{-m} > e^{5/3} > 5.2944,$$
$$\Big(1+\frac{5}{3m}\Big)^{m} \geq \Big(1+\frac{1}{3c}\Big)^{5c} > 5.0769.$$

Substituting the above bounds in (2.6) gives

$$2^n G(\delta_5) > \frac{1}{5}\cdot 0.3286\cdot 0.7101\cdot 0.7091\cdot(5.2944\cdot 5.0769+4) > 1.021,$$

which together with (2.9) proves the Lemma.

3 Main results

We consider the codes $C(r,t,s)$ and $C^{\perp}(r,t,s)$ with t odd and $s\neq 3$. For these t and s the non-zero weights τ_1 and τ_2 are as in (2.1), and also the Lemma holds true.

Theorem 1. *The code $C^{\perp}(r,t,s)$ is non-proper when the parameter t is odd and $s\neq 3$.*

Proof. The probability of undetected error of $C^{\perp}(r,t,s)$ is, by (1.3) and (1.5),

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

and hence

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

Therefore

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

where we have put

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

Consider (3.1) at $\varepsilon_s = 1 - \frac{1}{2(1-\delta_s)} \in (0, 1/2)$, where δ_s is as in (2.2). From $\tau_1 < \tau_2$, cf. (2.1), and $2^{-k} = 4m^2$, cf. (1.1), we get

$$\frac{P'_{ue}(C^{\perp}(r,t,s),\, \varepsilon_s))}{n(1-\varepsilon_s)^{n-1}} < 1 - \frac{s\tau_1}{4m^2\delta_s} 2^n G(\delta_s). \tag{3.3}$$

When $s \ge 7$, (2.1) and (2.2) give

$$\frac{s\tau_1}{4m^2\delta_s} = \frac{2m^2 - (s-1)m}{4m^2(1/2 - s/4m)} = \frac{2m^2 - (s-1)m}{2m^2 - sm} > 1, \tag{3.4}$$

and when $s = 5$,

$$\frac{s\tau_1}{4m^2\delta_5} = \frac{2m^2 - 4m}{4m^2(1/2 - 5/6m)} = 1 - \frac{2}{6m - 10} \ge 1 - \frac{2}{6 \cdot 32 - 10} > 0.989, \tag{3.5}$$

since $m \ge 32$, according to (2.5). Applying (3.4) and (3.5) in (3.3) and using (2.4) we obtain

$$\frac{P'_{ue}(C^{\perp}(r,t,s),\, \varepsilon_s))}{n(1-\varepsilon_s)^{n-1}} < 1 - 0.989 \cdot 2^n G(\delta_s) < 1 - 0.989 \cdot 1.021 < -0.009,$$

showing that the function $P_{ue}(C^{\perp}(r,t,s),\, \varepsilon)$ is decreasing at ε_s and thus that the code $C^{\perp}(r,t,s)$ is non-proper.

Theorem 2. *The code $C(r,t,s)$ is not good when the parameter t is odd and $s \ne 3$.*

Proof. The probability of undetected error of $C(r,t,s)$ is, by (1.3) and (1.5),

$$P_{ue}(C(r,t,s),\varepsilon) = n\varepsilon^{\tau_1}(1-\varepsilon)^{n-\tau_1} + n(s-1)\,\varepsilon^{\tau_2}(1-\varepsilon)^{n-\tau_2} = nsG(\varepsilon), \tag{3.6}$$

and in the worst-case channel condition $\varepsilon = 1/2$ we have

$$P_{ue}(C(r,t,s), 1/2) = ns2^{-n}. \tag{3.7}$$

From the Lemma,

$$\frac{P_{ue}(C(r,t,s),\delta_s)}{ns2^{-n}} = 2^n G(\delta_s) > 1.021, \tag{3.8}$$

and thus the code $C(r,t,s)$ is not good.

References

[1] 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.

[2] 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).

[3] 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.

[4] R. Dodunekova, O. Rabaste, Jose Jose Leon Vega Paez, Error detection with a class of irreducible binary cyclic codes and their dual codes. Prep. no. 2004:16, Dept. Math. Sciences, Chalmers University of Technology and Göteborg University, 2004.

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

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

[7] 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.

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

[9] 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.