CHALMERS | GÖTEBORG UNIVERSITY

PREPRINT 2005:24

Error Detection with a Class of Cyclic Codes

ROSSITZA DODUNEKOVA
STEFAN DODUNEKOV

Department of Mathematical Sciences
Division of Mathematical Statistics
CHALMERS UNIVERSITY OF TECHNOLOGY
GÖTEBORG UNIVERSITY
Göteborg Sweden 2005

Preprint 2005:24

Error Detection with a Class of Cyclic Codes

Rossitza Dodunekova
Stefan Dodunekov

CHALMERS | GÖTEBORG UNIVERSITY

Department of Mathematical Sciences
Division of Mathematical Statistics
Chalmers University of Technology and Göteborg University
SE-412 96 Göteborg, Sweden
Göteborg, June 2005

Preprint 2005:24
ISSN 1652-9715

Matematiskt centrum
Göteborg 2005

Error detection with a class of cyclic codes *

Rossitza Dodunekova[†]
Mathematical Sciences
Chalmers University of Technology
and Göteborg University
412 96 Göteborg, Sweden

Stefan Dodunekov[‡]
Institute of Mathematics and
Informatics
Bulgarian Academy of Sciences
1113 Sofia, Bulgaria

Abstract. We study a parametric class of q-ary two-weight cyclic codes and their dual codes, with regard to properness or goodness in detecting errors on a q-ary symmetric memoryless channel. We prove that for some parameters the codes and their duals are proper, while the remaining codes and their duals are not good.

1 Introduction

Baumert and McEliece [1], and also Wolfmann [14], consider a parametric class of q-ary irreducible cyclic codes $C(q, r, t, s)$ with positive integer parameters such that q is a prime power, $r \geq 1, \quad t > 1, \quad s > 1, \quad$ and $\quad s \,|\, q^r + 1$. The dimension k and the length n of the code $C(q, r, t, s)$ are

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

and its non-zero weights and the weight distribution are

$$\begin{aligned} \tau_1 &= (q-1) \cdot \frac{q^{2rt-1} + (-1)^t (s-1) q^{rt-1}}{s}, & A_{\tau_1} &= n, \\ \tau_2 &= (q-1) \cdot \frac{q^{2rt-1} - (-1)^t q^{rt-1}}{s}, & A_{\tau_2} &= n(s-1) \end{aligned} \tag{1.2}$$

(semiprimitive case). When $q = 2$, (1.1) and (1.2) describe the parameters and the weight distribution of the Delsarte and Goethals irreducible binary cyclic codes introduced in [2].

*Partially supported by the European Community under project MTKD-CT-2004-003006.
[†]Partially supported by the Swedish Research Council under grant 621-2003-5325.
[‡]Partially supported by the Bulgarian NSF under Contract MM1405/2004.

The error-detection performance of the binary codes and their duals has been studied in [10], where a complete classification has been given by showing that $C(2,r,t,s)$ and $C^{\perp}(2,r,t,s)$ are both either proper for error detection or not good. A similar study of $C(q,r,t,s)$ with $q>2$ carried out in [6] revealed that the codes are not good for a large set of parameter values, and for the remaining values it was determined whether $C(q,r,t,s)$ is proper or not.

In this work we give a complete classification of the codes $C(q,r,t,s)$ and $C^{\perp}(q,r,t,s)$ with $q>2$ regarding properness and goodness in error detection. It turns out, like in the binary case, that $C(q,r,t,s)$ and $C^{\perp}(q,r,t,s)$ are both either proper for error detection or not good. The results have been partially presented in [6] and [7].

We recall that when a q-ary linear $[\,n,\,k,\,d\,]$ code C is used to detect errors on a symmetric memoryless channel with symbol error probability ε, the probability of undetected error is given by

$$P_{ue}(C,\,\varepsilon)=\sum_{i=d}^{n}A_i\Big(\frac{\varepsilon}{q-1}\Big)^{i}(1-\varepsilon)^{n-i},\quad \varepsilon\in\Big[0,\,\frac{q-1}{q}\Big],\tag{1.3}$$

where $\{A_0,\,A_1,\,\ldots,\,A_n\}$ is the Hamming weight distribution of the code. In terms of the dual weight distribution $\{B_0,\,B_1,\,\ldots,\,B_n\}$,

$$P_{ue}(C,\,\varepsilon)=q^{-(n-k)}\sum_{i=0}^{n}B_i\Big(1-\frac{\varepsilon}{q-1}\Big)^{i}-(1-\varepsilon)^{n},\quad \varepsilon\in\Big[0,\,\frac{q-1}{q}\Big].\tag{1.4}$$

C is *proper* for error detection if $P_{ue}(C,\,\varepsilon)$ is increasing in $\varepsilon\in[0,\,(q-1)/q]$, and it is *good* if $P_{ue}(C,\,\varepsilon)$ is bounded by its value at the biggest possible ε (the worst case channel condition), i.e., if

$$P_{ue}(C,\,\varepsilon)\le P_{ue}\Big(C,\,\frac{q-1}{q}\Big)=q^{-n}(q^{k}-1),\quad \varepsilon\in[0,\,(q-1)/q],\tag{1.5}$$

see [12] and [13].

Thus a proper error-detecting code is also good, but a proper code performs certainly better on better channels, i.e., channels with smaller symbol error probability.

Often the symbol error probability of the channel is not known exactly and it would then be natural to prefer a proper error-detecting code to a good one, or a good error-detecting code to one that is not good.

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, some Griesmer codes and their duals, as well as many cyclic codes. More examples may be found in the survey [8]. The concept of properness has been extended to non-linear block codes, and examples of proper non-linear codes are the Kerdock and the Preparata codes, as well as non-linear codes which satisfy or achieve the Grey-Rankin bound, see [9].

2 Main results

Our study regarding goodness or properness of the non-binary codes $C(q,r,t,s)$ and their duals will show the following.

Theorem.

(i) The codes $C(3,r,t,2)$, $C(3,1,2,4)$, *and their duals are proper.*
(ii) The remaining codes $C(q,r,t,s)$ *with* $q \geq 3$ *and their duals are not good.*

In the binary case, the codes and their duals are proper when t is even or when t is odd and $s=3$, and not good in the remaining cases, as shown in [10].

3 Proofs

Throughout the proofs we will use the notation $m = q^{rt}$.

Proof of part (i) of the Theorem. Consider first the codes $C(3,r,t,2)$. From (1.1)–(1.3) we obtain

$$P_{ue}(C\,(3,\,r,\,t,\,2\,),\,\varepsilon\,) = n\,\Big[\,\Big(\frac{\varepsilon}{2}\Big)^{\tau_1}(1-\varepsilon)^{n-\tau_1} + \Big(\frac{\varepsilon}{2}\Big)^{\tau_2}(1-\varepsilon)^{n-\tau_2}\,\Big],\ 0 \leq \varepsilon \leq 2/3,$$

where $n = (3^{rt}-1)/2$ and τ_1 and τ_2 are

$$\tau_1 = \frac{m^2-m}{3}, \qquad \tau_2 = \frac{m^2+m}{3}$$

when t is odd, while for t even their values are interchanged. Hence without loss of generality we can assume that τ_1 and τ_2 are as above. With

$$\varepsilon_1 = \frac{\tau_1}{n} < \frac{2}{3}, \quad \varepsilon_2 = \frac{\tau_2}{n} > \frac{2}{3},$$

the properness of $C(3,r,t,2)$ follows from

$$\frac{2^{\tau_2}\,P'_{ue}(C\,(3,\,r,\,t,\,2\,),\,\varepsilon\,)}{n^2\,(\varepsilon_2-\varepsilon)\,\varepsilon^{\,\tau_2-1}\,(1-\varepsilon)^{\,n-\tau_2-1}} = 1 - 2^{\tau_2-\tau_1}\,g(\varepsilon) \geq 1 - 2^{\tau_2-\tau_1}\,g(2/3) = \frac{2}{m+1},$$

where the function

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

is increasing for $\varepsilon \in (0,\, 2/3]$ since

$$g'(\varepsilon) = \frac{n-1}{\varepsilon^2}\,\frac{\varepsilon_2-\varepsilon_1}{(\varepsilon_2-\varepsilon)^2}\left(\frac{1-\varepsilon}{\varepsilon}\right)^{\tau_2-\tau_1-1}\left(\frac{2}{3}-\varepsilon\right)\left(\frac{2n+1}{3(n-1)}-\varepsilon\right).$$

To show the properness of $C^{\perp}(\,3,\, r,\, t,\, 2\,)$ we use (1.4). Differentiating and using the substitution

$$\delta = 1 - \frac{1}{q\,(1-\varepsilon)} \tag{3.2}$$

we easily obtain

$$\frac{P'_{ue}(C^{\perp}\,(3,\, r,\, t,\, 2\,),\, \varepsilon\,)}{n(1-\varepsilon)^{n-1}} = 1 - 3^{n-k}\,H(\delta) \tag{3.3}$$

with

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

The term $x^a(1-x)^b$ with $a>0$ and $b>0$ increases for $0 \le x \le a/(a+b)$ and decreases for $a/(a+b) \le x \le 1$, which implies that $P_{ue}(C,\,\varepsilon)$ in (1.3) increases for $0 \le \varepsilon \le d/n$. Applied in (3.3) this gives

$$1 - 3^{n-k}H(\delta) \ge 0, \quad 2/3 \ge \delta \ge \delta_0 = (2n-9)/(3n-9) = \frac{2}{3}\cdot\frac{m^2-10}{m^2-7}, \tag{3.4}$$

since the minimum code distance of $C^{\perp}\,(3,\, r,\, t,\, 2\,)$ equals 3.

It is clear from (3.3) and (3.4) that the result will follow if we show that $H'(\delta) \ge 0$ for $0 < \delta \le \delta_0$. We do this below. Denoting

$$\delta_1 = (\tau_1-1)/(n-1) < 2/3, \quad \delta_2 = (\tau_2-1)/(n-1) > 2/3,$$

we have for $0 < \delta \le \delta_0$

$$\frac{2^{\tau_2}\,H'(\delta)}{\tau_2\,(n-1)(\delta_2-\delta)\delta^{\tau_2-2}(1-\delta)^{n-\tau_2-1}} = 1 - h(\delta) \ge 1 - h(\delta_0), \tag{3.5}$$

since the function

$$h(\delta) = \frac{\tau_1\,2^{\tau_2-\tau_1}}{\tau_2}\,\frac{\delta-\delta_1}{\delta_2-\delta}\left(\frac{1-\delta}{\delta}\right)^{\tau_2-\tau_1}$$

is increasing for $0 < \delta \le \delta_0$. Indeed, we have

$$h'(\delta) = \frac{\tau_1}{\tau_2}\,2^{\tau_2-\tau_1}\,\frac{\delta_2-\delta_1}{(\delta_2-\delta)^2}\frac{1}{\delta^2}\left(\frac{1-\delta}{\delta}\right)^{\tau_2-\tau_1-1}h_1(\delta),$$

where

$$h_1(\delta) = (n-2)\delta^2 - (\tau_1+\tau_2-3)\delta + \frac{(\tau_1-1)(\tau_2-1)}{n-1}.$$

Simple algebraic computations show that $h_1(\delta)$ achieves its minimum at a point larger than 2/3 and also that

$$h_1(\delta_0) = 2 + \frac{36}{(m^2-7)^2} - \frac{3}{m^2-3} - \frac{4}{9}\Big(1 - \frac{3}{m^2-7}\Big)^2 > 0 \quad \text{for} \quad m = 3^{rt} \geq 3^2,$$

implying $h'(\delta) > 0$ for $0 < \delta \leq \delta_0$. Evaluation of $h(\delta_0)$ in (3.5) with δ_0 as in (3.4) gives the function

$$h(\delta_0) = f(m) = \Big(\frac{m-1}{m+1}\Big)^2 \cdot \frac{m^2-2m-9}{m^2+2m-9} \cdot \Big(\frac{m^2-1}{m^2-10}\Big)^{2m/3},$$

which increases for $m \geq 9$, hence $h(\delta_0) = f(m) < \lim_{m\to\infty} f(m) = 1$ and consequently, $H'(\delta) \geq 0$ for $0 < \delta \leq \delta_0$. The fact that $f(m)$ increases can be established by considering

$$\begin{aligned}\big(\ln f(m)\big)' &= \frac{4}{m^2-1} + \frac{4(m^2+9)}{(m^2-9)^2-4m^2} \\ &+ \frac{2}{3}\ln\Big(1 + \frac{9}{m^2-10}\Big) - \frac{12m^2}{(m^2-1)(m^2-10)} \\ &> \frac{4}{m^2-1} + \frac{4(m^2+9)}{(m^2-10)^2} + \frac{2}{3}\ln\Big(1+\frac{9}{m^2-10}\Big) - \frac{12m^2}{(m^2-1)(m^2-10)}.\end{aligned}$$

Since the logarithmic function above is bounded below by the first two terms of its Taylor series we obtain

$$\begin{aligned}\big(\ln f(m)\big)' &> \frac{4}{m^2-1} + 4\left[\frac{1}{m^2-10} + \frac{19}{(m^2-10)^2}\right] \\ &+ \frac{6}{m^2-10} - \frac{27}{(m^2-10)^2} - 12\left[\frac{1}{m^2-10} + \frac{1}{(m^2-1)(m^2-10)}\right] \\ &> \frac{4}{m^2-1} - \frac{2}{m^2-10} - \frac{12}{(m^2-1)(m^2-10)} > 0.\end{aligned}$$

This completes the proof for the codes $C^{\perp}(\,3,\, r,\, t,\, 2\,)$.

We prove the properness of $C(\,3,\,1,\,2,\,4)$ and $C^{\perp}(\,3,\,1,\,2,\,4)$ by using the sufficient conditions for properness derived in [4] and [5], see also [3]. According to these conditions, if the extended binomial moments

$$A^*_\ell = \sum_{i=d}^{\ell} \frac{\ell(\ell-1)\ldots(\ell-i+1)}{n(n-1)\ldots(n-i+1)}\, A_i, \quad \ell = d, \cdots, n,$$

of a q-ary linear $[\,n,\,k,\,d\,]$ code with weight distribution $\{\,A_1,\,A_2,\,\ldots,A_n\,\}$ and dual code distance $d^{\perp}$ satisfy

$$A^*_\ell \geq q\,A^*_{\ell-1} \quad \text{for} \quad \ell = d+1, \ldots n - d^{\perp} + 1,$$

then the code is proper, and if

$$A^*_{n-\ell} \geq q\, A^*_{n-\ell+1} - q^{k-\ell}(q-1) \quad \text{for} \quad \ell = d^\perp + 1, \ldots n - d + 1,$$

then the dual code is proper. It is straightforward to check that the extended binomial moments of $C(\,3,\, 1,\, 2,\, 4\,)$ satisfy both the above conditions. ■

To prove part (ii) of the Theorem we treat separately the cases t odd and t even. The main idea of the proof is to show that at a certain point, defined by the code parameters, the probability of undetected error of the code exceeds the upper bound in (1.5). Basic for the proofs is the following Lemma, which extends part 1 of Theorem 3.4.2 in [12] to non-binary linear codes.

Lemma. *Let C be a q-ary linear $[\,n,\, k,\, d\,]$ code. If for some $\delta_0 \in \big(0,\, (q-1)/q\,\big)$ holds*

$$q^{n-k} P_{ue}(C,\, \delta_0\,) \geq 1, \tag{3.6}$$

then $C^\perp$ is not good.

Proof. Applying the substitution (3.2) in (1.4) we obtain the inequality

$$\frac{P_{ue}(C^\perp,\, \varepsilon)}{q^{-k} - q^{-n}} > 1 + \frac{1}{(q^{n-k}-1)\,(1-\delta)^n}\Big[q^{n-k}\, P_{ue}(C,\, \delta) - 1\Big]$$

which implies

$$P_{ue}(C^\perp,\, \varepsilon_0) > q^{-k} - q^{-n} \quad \text{for} \quad \varepsilon_0 = 1 - \frac{1}{q\,(1-\delta_0)},$$

i.e., $C^\perp$ is not good. ■

Note that a code for which (3.6) holds is not good. Such codes are called ugly [11]. Thus the Lemma says that if a code is ugly then its dual is not good.

We will now modify the Lemma to be suitable for application to the codes $C(q, r, t, s)$. From (1.1)–(1.3) we get

$$P_{ue}(C\,(q,\, r,\, t,\, s\,),\, \varepsilon\,) = (q^k - 1)\, G(\varepsilon), \tag{3.7}$$

where

$$G(\varepsilon) = \frac{1}{s}\left[\,\Big(\frac{\varepsilon}{q-1}\Big)^{\tau_1} (1-\varepsilon)^{\,n-\tau_1} + (s-1)\,\Big(\frac{\varepsilon}{q-1}\Big)^{\tau_2} \big(1-\varepsilon\big)^{\,n-\tau_2}\,\right]. \tag{3.8}$$

Corollary. *Consider $C(q,r,t,s)$ with $q \geq 3$ and the corresponding function $G(\varepsilon)$, defined by (3.7)–(3.8). If for some $\delta_0 \in \big(0,\, (q-1)/q\big)$ we have*

$$\big(1 - 1/q^k\big)\, q^n\, G(\delta_0) \geq 1 \tag{3.9}$$

or

$$q^n\, G(\delta_0) \geq 1.013, \tag{3.10}$$

then $C\,(q,\, r,\, t,\, s\,)$ and $C^\perp(q,\, r,\, t,\, s\,)$ are not good.

Proof. We have

$$q^{n-k} P_{ue}(C\,(q,\, r,\, t,\, s\,),\, \varepsilon,\,) = \big(1 - 1/q^k\big)\, q^n\, G(\varepsilon) \geq 1$$

when (3.9) holds and

$$\big(1 - 1/q^k\big)\, q^n\, G(\varepsilon) \geq \big(1 - 1/3^4\big) \cdot 1.013 > 1,\ q \geq 3,$$

when (3.10) does. The statement thus follows by the Lemma. ■

We will also make use of the well known fact that the functions $(1 + \frac{1}{x})^x$ and $(1 - \frac{1}{x})^x$ are increasing for $x > 1$ and

$$\Big(1 + \frac{1}{x}\Big)^x \to e, \quad \Big(1 - \frac{1}{x}\Big)^x \to e^{-1}, \quad \text{when} \quad x \to \infty, \tag{3.11}$$

as well as of the Bernoulli inequality

$$(1 + x)^\beta > 1 + \beta x \quad \text{for} \quad |x| < 1 \quad \text{and} \quad \beta \geq 1. \tag{3.12}$$

Proof of part (ii) of the Theorem for t odd. The two non-zero weights of the code $C(q, r, t, s)$ are

$$\tau_1 = \frac{q-1}{q} \cdot \frac{m^2 - (s-1)m}{s}, \quad \tau_2 = \frac{q-1}{q} \cdot \frac{m^2 + m}{s}. \tag{3.13}$$

Define $\delta_s \in (\,0,\, (q-1)/q)$ as

$$\delta_s = \frac{q-1}{q}(1 - z_s), \quad \text{where} \quad z_s = \frac{s}{(q-1)\, m}. \tag{3.14}$$

A substitution from (3.13) and (3.14) in (3.8) gives

$$\begin{aligned} q^n\, G(\delta_s) = {} & \frac{1}{s}\Big[(1 - z_s)^{\,q-1}\big(1 + (q-1)\, z_s\big)\Big]^{\frac{m^2}{qs}} \\ & \times (1 - z_s)^{\frac{(q-1)\, m}{s} \cdot \frac{1}{q}} \big(1 + (q-1)\, z_s\big)^{-(\frac{q-1}{q} + \frac{1}{m})\, \frac{m}{s}} \\ & \times \Bigg[\Big(\frac{1 + (q-1)\, z_s}{1 - z_s}\Big)^{\frac{(q-1)\, m}{q}} + (s-1)\Bigg]. \end{aligned} \tag{3.15}$$

Assume that q_0, c_1, c_2, and c_3, are constants such that

$$q \geq q_0, \quad \frac{m}{s} \geq c_1, \quad \frac{(q-1)\, m}{s} \geq c_2, \quad \frac{q-1}{q} + \frac{1}{m} \leq c_3. \tag{3.16}$$

Using these constants and the monotonicity of the convergence in (3.11) we obtain lower bounds for the power factors in (3.15). First we apply the Bernoulli inequality (3.12) to get

$$\begin{aligned} \Big[(1-z_s)^{\,q-1}\big(1+(q-1)\,z_s\big)\Big]^{\frac{m^2}{qs}} &> \Big(1-(q-1)^2\,z_s^2\Big)^{\frac{m^2}{qs}} \\ &= \Big(1-\frac{s^2}{m^2}\Big)^{\frac{m^2}{qs}} \geq \Big(1-\frac{1}{c_1^2}\Big)^{\frac{c_1^2}{q_0}\cdot s}. \end{aligned} \tag{3.17}$$

Next we have

$$(1-z_s)^{\frac{(q-1)\,m}{s}\cdot\frac{1}{q}} = \Big(1-\frac{s}{(q-1)\,m}\Big)^{\frac{(q-1)\,m}{s}\cdot\frac{1}{q}} \geq \Big(1-\frac{1}{c_2}\Big)^{\frac{c_2}{q_0}}, \tag{3.18}$$

$$\big(1+(q-1)\,z_s\,\big)^{-(\frac{q-1}{q}+\frac{1}{m})\,\frac{m}{s}} = \Big(1+\frac{s}{m}\Big)^{-(\frac{q-1}{q}+\frac{1}{m})\,\frac{m}{s}} > e^{-c_3}. \tag{3.19}$$

Finally, from

$$(1-z_s\,)^{-\frac{(q-1)\,m}{q}} = \Big(1-\frac{s}{(q-1)\,m}\Big)^{-\frac{(q-1)\,m}{q}} > e^{\frac{s}{q}}$$

and

$$\big(1+(q-1)\,z_s\,\big)^{\frac{(q-1)\,m}{q}} = \Big(1+\frac{s}{m}\Big)^{\frac{(q-1)\,m}{q}} > \Big(1+\frac{1}{c_1}\Big)^{c_1\,s}\,e^{-\frac{s}{q}}$$

we obtain

$$\Big(\frac{1+(q-1)\,z_s}{1-z_s}\Big)^{\frac{(q-1)\,m}{q}} > \Big(1+\frac{1}{c_1}\Big)^{c_1\,s}. \tag{3.20}$$

Applying in (3.15) the lower bounds obtained in (3.17)–(3.20), with q_0, c_1, c_2, and c_3 as in (3.16), we obtain

$$q^n\,G(\delta_s) > \frac{1}{s}\Big(1-\frac{1}{c_1^2}\Big)^{\frac{c_1^2}{q_0}\cdot s}\cdot\Big(1-\frac{1}{c_2}\Big)^{\frac{c_2}{q_0}}\cdot e^{-c_3}\cdot\left[\Big(1+\frac{1}{c_1}\Big)^{c_1\,s}+s-1\right]. \tag{3.21}$$

We now treat separately seven different cases of possible values of the parameters of $C(q,r,t,s)$. In each case we choose constants q_0, c_1, c_2, and c_3, and replace them in (3.21) to compute a lower bound for $q^n\,G(\delta_s)$. As we will see, either the obtained lower bound exceeds 1.013 or $\big(1-1/q^k\big)\,q^n\,G(\delta_0) > 1$, then by the Corollary $C(q,r,t,s)$ and its dual are not good.

Case $\mathbf{q} > \mathbf{3}$, $\mathbf{s} > \mathbf{3}$. With $q_0 = 4$, $c_1 = 12.8$, $c_2 = 38.4$, $c_3 = 1$, where c_1 is computed from

$$\frac{m}{s} \geq \frac{q^{rt}}{q^r+1} \geq \frac{q^t}{q+1} \geq \frac{4^3}{5} = 12.8,$$

we obtain from (3.21)

$$q^n\, G(\delta_s) > \frac{1}{s}\cdot 0.77^s\cdot 0.77\cdot 0.36[\,2.6^s+s-1\,] > 0.27\left[\frac{2^s}{s}+\frac{s-1}{s}\cdot 0.77^{\,s}\right] = 0.27\, f(s).$$

It is easy to see that $f'(s) > 0$ for positive s and then, since $s > 3$, we have

$$q^n G(\delta_s) \geq 0.27\, f(4) > 1.15.$$

Case $\mathbf{q = 3}$, $\mathbf{s > 3}$. In this case we compute the right hand side of (3.21) with the constants $q_0 = 3$, $c_1 = 6.75$, $c_2 = 13.5$, $c_3 = 0.704$, and obtain

$$\begin{aligned} q^n G(\delta_s) &> \frac{1}{s}\cdot 0.7138^s\cdot 0.7072\cdot 0.4946\left[2.5408^s + s - 1\right] \\ &> 0.3497\left[\frac{1.8136^s}{s} + \frac{s-1}{s}\cdot 0.7138^{\,s}\right] = 0.3498\, f_1(s). \end{aligned}$$

Since the function $f_1(s)$ is increasing for $s > 3$ we have

$$q^n G(\delta_s) \geq 0.3498\, f_1(4) > 1.014.$$

The results of the evaluation of the right hand side of (3.21) in the remaining cases are presented in the table below, where in the last column we have used the notation

$$T(\delta_s) = \left(1 - 1/q^k\right) q^n\, G(\delta_s).$$

Case	q_0	c_1	c_2	c_3	$q^n\, G(\delta_s)$	$T(\delta_s)$
$\mathbf{q \geq 5}$, $\mathbf{s = 3}$.	5	141.66	166.66	1	> 1.2	–
$\mathbf{q = 4}$, $\mathbf{s = 3}$.	4	21.33	2.64	0.77	> 1.1	–
$\mathbf{q = 5}$, $\mathbf{s = 2}$.	5	62.5	250	0.81	> 1.009	> 1.008
$\mathbf{q = 7}$, $\mathbf{s = 2}$.	7	171.5	1029	0.861	> 1.1	–
$\mathbf{q \geq 9}$, $\mathbf{s = 2}$.	9	364.5	2916	1	> 1.1	–

■

Proof of part (ii) of the Theorem for t even. We follow the ideas of the previous proof. The two non-zero weights of the code $C(q,r,t,s)$ are in this case

$$\tau_1 = \frac{q-1}{q}\cdot\frac{m^2+(s-1)m}{s}, \quad \tau_2 = \frac{q-1}{q}\cdot\frac{m^2-m}{s}.$$

Now the point under consideration is

$$\delta_0 = \frac{q-1}{q}(1-z_0) \quad \text{with} \quad z_0 = \frac{1}{(q-1)(m-1)}.$$

A substitution in (3.8) gives

$$\begin{aligned}
&\Big(q^n\, G(\delta_0)\Big)^s = \Big[(1-z_0)^{\,q-1}\big(1+(q-1)\,z_0\big)\Big]^{\frac{m^2}{q}} \\
&\times \Big(\frac{1+(q-1)\,z_0}{1-z_0}\Big)^{\frac{(q-1)\,m}{q}} \big(1+(q-1)\,z_0\big)^{-1} \\
&\times \left[1-\frac{1}{s}\left(1-\Big(\frac{1-z_0}{1+(q-1)\,z_0}\Big)^{\frac{(q-1)\,m}{q}}\right)\right]^s . \qquad (3.22)
\end{aligned}$$

With

$$s_0 \le s, \quad q_0 \le q, \quad c_1 \le m-1, \quad c_2 \le \frac{(q-1)\,m}{q} - 1, \quad c_3 = \Big(\frac{c_2}{c_2+1}\Big)^{c_2+1} \qquad (3.23)$$

we obtain lower bounds for the factors in the right hand side of (3.22).

$$\begin{aligned}
&\Big[(1-z_0)^{\,q-1}\big(1+(q-1)\,z_0\big)\Big]^{\frac{m^2}{q}} > \Big(1-(q-1)^2\,z_0^2\,\Big)^{\frac{m^2}{q}} \\
&= \Big(1-\frac{1}{(m-1)^2}\Big)^{(m-1)^2\cdot\frac{m^2}{q(m-1)^2}} \ge \Big(1-\frac{1}{c_1^2}\,\Big)^{q_0^3}, \qquad (3.24)
\end{aligned}$$

$$\begin{aligned}
&\Big(\frac{1+(q-1)\,z_0}{1-z_0}\Big)^{\frac{(q-1)\,m}{q}} \\
&= \Big(1+\frac{q}{(q-1)\,m-q}\Big)^{\frac{(q-1)\,m}{q}} > \Big(1+\frac{1}{c_2}\Big)^{c_2}, \qquad (3.25)
\end{aligned}$$

$$\big(1+(q-1)\,z_0\,\big)^{-1} = \frac{m-1}{m} \ge \frac{c_1}{c_1+1}, \qquad (3.26)$$

$$\begin{aligned}
&\left[1-\frac{1}{s}\left(1-\Big(\frac{1-z_0}{1+(q-1)\,z_0}\Big)^{\frac{(q-1)\,m}{q}}\right)\right]^s \\
=&\left[1-\frac{1}{s}\left(1-\Big(1-\frac{q}{(q-1)\,m}\Big)^{\frac{(q-1)\,m}{q}}\right)\right]^s \\
\ge&\left[1-\frac{1}{s}\left(1-\Big(1-\frac{1}{c_2+1}\Big)^{c_2+1}\right)\right]^s \ge \Big(1-\frac{1-c_3}{s_0}\Big)^{s_0}. \qquad (3.27)
\end{aligned}$$

From (3.22) and (3.24)–(3.27) with s_0, q_0, c_1, c_2, and c_3 as in (3.23) we obtain

$$\left(q^n\, G(\delta_0)\right)^s > \left(1-\frac{1}{c_1^2}\right)^{q_0^3}\cdot\left(1+\frac{1}{c_2}\right)^{c_2}\cdot\frac{c_1}{c_1+1}\cdot\left(1-\frac{1-c_3}{s_0}\right)^{s_0}. \tag{3.28}$$

In the same manner we treat different cases of possible values of the parameters of $C(q,r,t,s)$ separately. In each case we determine constants s_0, q_0, c_1, c_2, and c_3, and insert them into (3.28) to evaluate a lower bound for $\left(q^n\, G(\delta_0)\right)^s$. It turns out that either $q^n\, G(\delta_0) > 1.013$ or $\left(1-1/q^k\right)^s \left(q^n\, G(\delta_0)\right)^s > 1$, thus $C(q,r,t,s)$ and its dual are not good, by the Corollary.

We present the results of the evaluation in two tables below. In the cases marked by * we have derived better lower bounds for the term in the left hand side of (3.24) than the one obtained there, and in the evaluation of the right hand side of (3.28) we have replaces the first power factor by these bounds. We show the improved lower bounds immediately after the table with the cases to which these bounds are related. In the case $q = 4$, $s = 5$, $r = 1$, $t = 2$, the lower bound of $q^n\, G(\delta_0)$ has been computed from (3.22). In the last column of the tables we have denoted

$$T_1(\delta_0) = \left(1-1/q^k\right)^s \left(q^n\, G(\delta_0)\right)^s.$$

To compute lower bounds for $T_1(\delta_0)$ in the cases where s is not fixed we have used that $s \leq q^r + 1$ to obtain

$$\left(1-1/q^k\right)^s \geq \left(1-1/q_0^4\right)^{q_0+1}.$$

The first table presents all possible cases with $q > 3$, $s > 3$.

Case	s_0	q_0	c_1	c_2	c_3	$\left(q^n\, G(\delta_0)\right)^s$	$q^n\, G(\delta_0)$	$T_1(\delta_0)$
$\mathbf{q > 4,\ s \geq 4.}$	4	5	24	19	0.358	> 1.01	–	> 1.0003
$\mathbf{q = 4,\ s \geq 7.}^*$	7	4	15	11	0.358	> 1.02	–	> 1.0002
$\mathbf{q = 4,\ s = 5,}$ $\mathbf{r \geq 3.}^*$	5	4	4095	3071	0.3678	> 1.07	> 1.013	–
$\mathbf{q = 4,\ s = 5,}$ $\mathbf{r = 1,\ t \geq 4.}^*$	5	4	224	191	0.36	> 1.04	> 1.007	> 1.03
$\mathbf{q = 4,\ s = 5,}$ $\mathbf{r = 1,\ t = 2.}$						> 1.1	> 1.019	–

The improved lower bounds used above are as follows.

$\mathbf{q = 4},\ \mathbf{s \geq 7}$. From $(1-z_0)^3(1+3z_0) > 1-6z_0^2$ we obtain

$$[(1-z_0)^3(1+3z_0]^{\frac{m^2}{4}} > (1-6z_0^2)^{\frac{m^2}{4}} = \left(1-\frac{2}{3(m-1)^2}\right)^{\frac{m^2}{4}}$$

$$> \left(1-\frac{2}{3\cdot 15^2}\right)^{\frac{16^2}{4}} > 0.827.$$

$\mathbf{q = 4},\ \mathbf{s = 5},\ \mathbf{r \geq 3}$. We have

$$\left(1-\frac{1}{c_1^2}\right)^{c_1^2\cdot\frac{m^2}{q(m-1)^2}} \geq \left(1-\frac{1}{c_1^2}\right)^{c_1^2\cdot\frac{4^{12}}{4(4^6-1)^2}} > 0.7787.$$

$\mathbf{q = 4},\ \mathbf{s = 5},\ \mathbf{r = 1},\ \mathbf{t \geq 4}$.

$$\left(1-\frac{1}{c_1^2}\right)^{c_1^2\cdot\frac{m^2}{q(m-1)^2}} \geq \left(1-\frac{1}{c_1^2}\right)^{c_1^2\cdot\frac{4^{8}}{4(4^4-1)^2}} > 0.77.$$

The computations in the remaining cases, $q > 3$ and $s = 2$ or 3 and $q = 3,\ s \geq 4$, give the following.

Case	s_0	q_0	c_1	c_2	c_3	$\left(q^n\, G(\delta_0)\right)^s$	$q^n\, G(\delta_0)$	$T(\delta_0)$
$\mathbf{q \geq 7},\ \mathbf{s = 2}$.	2	7	48	41	0.363	> 1.05	> 1.02	–
$\mathbf{q \geq 7},\ \mathbf{s = 3}$.	3	7	48	41	0.363	> 1.1	> 1.03	–
$\mathbf{q = 5},\ \mathbf{s = 2}$.*	2	5	24	19	0.358	> 1.02	> 1.009	> 1.01
$\mathbf{q = 5},\ \mathbf{s = 3}$.*	3	5	24	19	0.358	> 1.07	> 1.02	–
$\mathbf{q = 3},\ \mathbf{s \geq 4}$, $\mathbf{rt \geq 4}$.*	4	3	80	53	0.364	> 1.03	–	> 1.02

Below we give the improved lower bounds used in the cases marked by *.

$\mathbf{q = 5},\ \mathbf{s = 2}$.

$$[(1-z_0)^4(1+4z_0]^{\frac{m^2}{5}} > (1-10z_0^2)^{\frac{m^2}{5}} = \left(1-\frac{5}{8(m-1)^2}\right)^{\frac{m^2}{5}}$$

$$> \left(1-\frac{5}{8\,c_1^2}\right)^{(c_1+1)^2/5} > 0.873.$$

$\mathbf{q=5},\ \mathbf{s=3}$. The improved lower bound is as above.

$\mathbf{q=3},\ \mathbf{s\geq 4}$. We have $rt \geq 4$, since when $rt < 4$ we obtain the code $C(3,1,2,4)$ from part (i). Thus

$$[(1-z_0)^2(1+2z_0]^{\frac{m^2}{3}} > (1-3z_0^2)^{\frac{m^2}{3}} = \Big(1-\frac{3}{4(m-1)^2}\Big)^{\frac{m^2}{3}}$$
$$> \Big(1-\frac{3}{4\,c_1^2}\Big)^{\frac{(c_1+1)^2}{3}} > 0.773.$$

The proof of the Theorem is now complete. ■

References

[1] L. D. Baumert and R. J. McEliece, Weights of irreducible cyclic codes. *Information and Control* **20**, 158–175, 1972.

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

[3] R. Dodunekova, Extended binomial moments of a linear code and the undetected error probability. *Problemy Peredachi Informatsii* **39**, no. 3, 28–39, 2003, English translation in *Problems Inform. Transmission* **39**, no. 3, 255–265, 2003.

[4] R. Dodunekova, S. Dodunekov, Sufficient conditions for good and proper error detecting codes. *IEEE Trans. Inform. Theory* **43**, no. 6, 2023–2026, 1997.

[5] R. Dodunekova, S. Dodunekov, Sufficient conditions for good and proper error detecting codes via their duals. *Math. Balkanica (N.S.)* **11**, no 3-4, 375–381, 1997.

[6] R. Dodunekova, S. Dodunekov, Error detection with a class of q-ary two-weight codes. *Proc. IEEE International Symposium on Information Theory,* Adelaide, September 2005, to appear.

[7] R. Dodunekova, S. Dodunekov, Error detection with a class of cyclic codes. *Proc. Fourth International Workshop on Optimal Codes and Related topics*, Pamporovo, June 2005, to appear.

[8] R. Dodunekova, S. Dodunekov, E. Nikolova, A survey on proper codes. In: *General Theory of Information Transfer and Combinatorics*, a special issue of *Discrete Applied Mathematics*, to appear.

[9] R. Dodunekova, S. Dodunekov, E. Nikolova, On the error-detecting performance of some classes of block codes. *Problemy Peredachi Informatsii* **40**, no. 4, 68–78, 2004, English translation in *Problems Inform. Transmision* **40**, no. 4, 356–364, 2004.

[10] R. Dodunekova, O. Rabaste, J. L. Vega Páez, Error detection with a class of irreducible binary cyclic codes and their dual codes. *IEEE Trans. Inform. Theory* **51**, no. 3, 1206–1209, 2005.

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

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

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

[14] J. Wolfmann, Formes quadratiqies et codes à deux poids. C.R.A.S. **281**, 533–535, 1975.