Mathematica
Balkanica

New Series Vol. 21, 2007, Fasc. 3-4

Sufficient Conditions for Interval Properness of Linear Error Detecting Codes

Rossitza Dodunekova[1,a] *and Li Weng*[2,a]

Presented in part at the MASSEE International Congress on Mathematics MICOM - 2006, Cyprus

Properness of a linear error detecting code is a property which in a certain sense makes the code more appropriate for error detection over a symmetric memoryless channel than a non-proper one. This property is related to the undetected error probability of the code, which is a function of the channel symbol error probability, involving the code weight distribution. However, relatively few codes are known with their weight distribution. It is therefore useful to have criteria for properness which do not depend on the code weight distribution. Here we give sufficient conditions for interval properness of a q-ary linear error detecting code, which only involve the code length and the dual code distance. In case of binary codes our criterion reduces to a criterion known earlier. We also give examples, mostly on parametric classes of Griesmer codes, where intervals of properness have been found by help of the new criterion. It turns out that when the dimension of the Griesmer codes under consideration increases the intervals of properness converge to $(0,\ (q-1)/q]$, i.e., the codes are asymptotically proper.

1. Introduction

Consider the q-ary linear codes of length n and dimension k, and let C be such a code of minimum code distance d and weight distribution A_0, A_1, A_2, …, A_n. An important characteristic of the error detecting performance of C over a

[1] Partially supported by Research Platform MP2 of Göteborg University.

[2] Part of the work has been done during the author's master studies at Chalmers University of Technology

symmetric memoryless channel with symbol error probability ε is the probability of undetected error

$$(1.1) \qquad P_{ue}(C,\varepsilon) = \sum_{i=1}^{n} A_i \Big(\frac{\varepsilon}{q-1}\Big)^i (1-\varepsilon)^{n-i}, \quad \varepsilon \in \left[0, \frac{q-1}{q}\right].$$

If the undetected error probability of C is the smallest possible in the set of all q-ary codes of length n and dimension k, C would, of course, be best for error detection in this set. To find such a code is difficult, since in general one has to use exhaustive search. Moreover, even if such a code were found, this might not solve the problem, because usually ε is not known exactly, and a code which is optimal for ε may not be optimal for the true symbol error probability. In such a situation, the properties of goodness and properness appear to be reasonable criteria for estimating the code behavior in error detection. The code C is *good* for error detection if it cannot perform worse than it does in the worst channel, i.e., the channel with $\varepsilon = (q-1)/q$, or if

$$(1.2) \qquad P_{ue}(C,\varepsilon) \le P_{ue}\left(C, \frac{q-1}{q}\right) = q^{-n}(q^k-1) \quad \text{for} \quad \varepsilon \in \left[0, \frac{q-1}{q}\right].$$

Earlier it was supposed that (1.2) must be true for all linear error detecting codes, i.e., the codes must be good, which however has been disproved, cf, e.g. [12].

The code C is *proper* for error detection if $P_{ue}(C,\varepsilon)$ is monotonously increasing in ε. A proper error detecting code performs better on better channels and it is also good.

To classify codes as proper, non proper but good, or not good, often turns out to be complicated, and such a classification has been done so far for relatively few codes. It is worth mentioning that many codes which are known to be optimal or close to optimal in one sense or other, turn out to be proper, such as Maximum Distance Separable (MDS) codes, the Hamming codes, some Griesmer codes, the Maximum Minimum Distance codes and their duals, and some near MDS codes. Some Cyclic Redundancy-Check (CRC) codes and their duals are proper, while other CRC codes, including some standardized, are not even good. For relevant information in this regard we refer to the overview [7].

Sometimes, even if a code C is not good, it might be still interesting to know if its undetected error probability is an increasing function in some sub-interval of $[0,\ (q-1)/q]$. We call such a code proper in this sub-interval. Here we are concerned with intervals of properness of the form $[a, (q-1)/q]$, since in this case the undetected error probability of C obeys the natural upper bound in (1.2) for all ε in the interval of properness.

There are a number of works presenting sufficient conditions for properness and goodness which are expressed in terms of the basic parameters of the code and its weight distribution, see for example [4], [5], and [7]. However, the weight distribution is known for relatively few codes (its computation is an NP-hard problem, see [2]), and it is therefore desirable to have criteria for properness which do not depend on it. One such criterion for interval properness of binary linear codes, found earlier in [8], is the following.

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

$$\left\lceil \frac{n}{3} \right\rceil + 1 \le d^{\perp} \le \left\lfloor \frac{n}{2} \right\rfloor, \tag{1.3}$$

then C is proper for error detection in the interval

$$\left[\frac{n+1-2d^{\perp}}{n-d^{\perp}},\ \frac{1}{2} \right]. \tag{1.4}$$

In the present work we extend the above criterion to the case of q-ary linear codes by proving in Theorem 2 a sufficient condition for properness in intervals of the type $[a,\ (q-1)/q]$, involving only the code length and the dual code distance. If $q = 2$ our criterion coincides with that of Theorem 1 above. We also provide examples where intervals of properness for q-ary linear codes have been obtained by applying our criterion. Examples 1–4 deal with parametric families of Griesmer codes and give intervals of properness for their dual codes. As we will see the intervals of properness approach the interval $(0,\ (q-1)/q]$ when the dimension k of the considered Griesmer codes increases. Thus their dual codes are asymptotically proper. Note that the duals of the Griesmer codes have small redundancy which is usually the case with codes used in error detection. In Example 5 we consider a parametric family of binary cyclic codes, which are known to be not good, and show that they however are asymptotically proper.

The proof of Theorem 2 is given in Section 2 and the examples in Section 3. The proof makes use of the well known formula

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

which expresses the probability of undetected error of an $[n,\, k]_q$ linear code C through its dual weight distribution $B_0,\, B_1,\, \ldots,\, B_n$. We will also make use of the first order *Pless Power Moment* of C [15, p. 130],

$$\sum_{i=d}^{n} iA_i = q^{k-1}[n(q-1) - B_1]. \tag{1.6}$$

2. Main result

Let C be a linear $[n,\, k]_q$ code with dual code distance $d^\perp$. It has been shown in [14] that when

$$d^\perp \geq \frac{n(q-1)+1}{q}$$

the code is proper. We will show below that when the above condition is not satisfied but $d^\perp$ is still sufficiently large, C is proper in $[a,\, (q-1)/q]$, where a is defined through n, q, and $d^\perp$.

Let $A_0,\, A_1,\, \ldots,\, A_n$ be the weight distribution of C and $B_0,\, B_1,\, \ldots,\, B_n$ be the dual weight distribution with $B_1 = 0$. Using (1.1), (1.6), and

$$\left[\varepsilon^i(1-\varepsilon)^{n-i}\right]' = n\,\varepsilon^{i-1}(1-\varepsilon)^{n-i-1}\left(i/n - \varepsilon\right), \tag{2.1}$$

we easily obtain

$$P'_{ue}\left(C,\, \frac{q-1}{q}\right) = q^{-n+2}\left(\frac{1}{q-1}\sum_{i=d}^{n} iA_i - \frac{n}{q}\sum_{i=d}^{n} A_i\right) = nq^{-n+1} > 0,$$

and hence there are intervals of properness for C of the form $[a,\, (q-1)/q]$.

Theorem 2. *Let the q-ary linear code C have length n and dual code distance $d^\perp$. If*

$$\frac{n(q-1)+2}{q+1} < d^\perp < \frac{n(q-1)+1}{q}, \tag{2.2}$$

then C is proper in the interval

$$\left[\frac{n(q-1) - d^\perp q + 1}{n(q-1) - d^\perp q + 1 + \frac{d^\perp - 1}{q-1}},\; \frac{q-1}{q}\right]. \tag{2.3}$$

Proof. We shall show that the derivative of the undetected error probability of C is a non-negative function of ε in the interval given by (2.3). Using the dual formula (1.5) and also (1.6) for the dual code we obtain

$$\begin{aligned} P'_{ue}(C,\varepsilon) &= n(1-\varepsilon)^{n-1} - \frac{q^{k-n+1}}{q-1}\sum_{i=d^\perp}^{n} iB_i\Big(1-\frac{q\varepsilon}{q-1}\Big)^{i-1} \\ &\geq n(1-\varepsilon)^{n-1} - \frac{q^{k-n+1}}{q-1}\Big(1-\frac{q\varepsilon}{q-1}\Big)^{d^\perp-1}\sum_{i=d^\perp}^{n} iB_i \\ &= n(1-\varepsilon)^{n-1} - n\Big(1-\frac{q\varepsilon}{q-1}\Big)^{d^\perp-1} \\ &= n(1-\varepsilon)^{n-1}\Big[1-G(\varepsilon)\Big], \end{aligned} \tag{2.4}$$

where we have denoted

$$G(\varepsilon) = \left(\frac{1-\frac{q\varepsilon}{q-1}}{1-\varepsilon}\right)^{d^\perp-1}\left(\frac{1}{1-\varepsilon}\right)^{n-d^\perp}.$$

We will now show that $G(\varepsilon) \leq 1$ for ε in the interval (2.3). For this we use the substitution

$$\alpha = \frac{\varepsilon}{(q-1)(1-\varepsilon)} \tag{2.5}$$

which gives

$$G(\varepsilon) = (1-\alpha)^{d^\perp-1}\big(1+(q-1)\,\alpha\big)^{n-d^\perp} = G_1(\alpha). \tag{2.6}$$

By using the Bernoulli inequality

$$(1+x)^\beta \geq 1+\beta x \quad \text{for} \quad |x|<1 \quad \text{and} \quad \beta \geq 1,$$

and also the inequalities

$$\Big(1+\frac{1}{x}\Big)^x < e \quad \text{and} \quad \Big(1-\frac{1}{x}\Big)^x < e^{-1} \quad \text{for} \quad x>1$$

we get

$$\begin{aligned} G_1(\alpha) &\leq (1-\alpha)^{d^\perp-1}(1+\alpha)^{(n-d^\perp)(q-1)} \\ &= (1-\alpha^2)^{d^\perp-1}(1+\alpha)^{n(q-1)-d^\perp q+1} \\ &\leq \exp\{-\alpha^2(d^\perp-1)\}\cdot\exp\{\alpha[n(q-1)-d^\perp q+1]\} \\ &= \exp\{\alpha(d^\perp-1)(\alpha_0-\alpha)\}, \end{aligned}$$

where

$$\alpha_0 = \frac{n(q-1) - d^{\perp} q + 1}{d^{\perp} - 1}.$$

Note that we have $d^{\perp} - 1 > 0$ above, which is easily seen from the left hand side of the condition (2.2). Moreover, we have $0 < \alpha_0 < 1$ since, as one can verify, the right hand side of (2.2) is equivalent to $\alpha_0 > 0$ and the left hand side to $\alpha_0 < 1$. Therefore we have

$$(2.7) \qquad G_1(\alpha) \le 1 \qquad \text{for} \qquad \alpha_0 \le \alpha \le 1.$$

One can easily see from the substitution in (2.5) that the above inequalities for α are equivalent to

$$(2.8) \quad \varepsilon_0 \le \varepsilon \le \frac{q-1}{q} \qquad \text{with} \qquad \varepsilon_0 = \frac{n(q-1) - d^{\perp} q + 1}{n(q-1) - d^{\perp} q + 1 + \frac{d^{\perp}-1}{q-1}}.$$

Using (2.7) in (2.6) gives $G(\varepsilon) \le 1$ for ε as in (2.8). Applying this in (2.4) we conclude that the code C is proper in the interval (2.3). ■

Corollary. *If (2.2) holds and in addition*

$$(2.9) \qquad \frac{n(q-1) - d^{\perp} q + 1}{n(q-1) - d^{\perp} q + 1 + \frac{d^{\perp}-1}{q-1}} \le \frac{d}{n},$$

then C is proper.

Proof. The statement follows from Theorem 2 and the fact that C is proper in $[0,\, d/n]$, as seen from (1.1) and (2.1). ■

Remark 1. It is easily seen that when $q = 2$, (2.2) and (2.3) become (1.3) and (1.4), respectively, and the above theorem reduces to Theorem 1.

Remark 2. Let C be a linear $[n,\, k]_q$ code with $d^{\perp} > 1$. The third line in (2.4) shows that $P'_{ue}(C,\, \varepsilon) \ge 0$ if

$$(2.10) \qquad J(\varepsilon) = (1-\varepsilon)^{\frac{n-1}{d^{\perp}-1}} + \frac{q\varepsilon}{q-1} - 1 \ge 0.$$

The function $J(\varepsilon)$ is convex and $J(0) = 0$, $J\left((q-1)/q\right) > 0$. Thus either $J(\varepsilon) > 0$ for $0 < \varepsilon < (q-1)/q$ or $J(\varepsilon) < 0$ for $0 < \varepsilon < \overline{\varepsilon}$ and $J(\varepsilon) > 0$ for $\overline{\varepsilon} < \varepsilon < (q-1)/q$, where $\overline{\varepsilon}$ is the unique solution of the equation $J(\varepsilon) = 0$ in $(0, (q-1)/q)$. The first case takes place when $J'(0) = q/(q-1) - (n-1)/(d^{\perp} - 1) \ge 0$, i.e., when

$$d^{\perp} \ge \frac{n(q-1)+1}{q},$$

and clearly the code is then proper. As mentioned above this condition was shown to be sufficient for properness earlier in [14]. The second case takes place when $d^{\perp} < [n(q-1)+1]/q$, and the code is then proper in the interval $[\overline{\varepsilon},\ (q-1)/q]$, where $\overline{\varepsilon}$ can be computed by using numerical methods, when the values of q, n, and $d^{\perp}$ are fixed.

3. Examples

We now use our results to find intervals of properness for some parametric classes of linear error detecting codes. As usual, we call a q-ary linear code C of length n, dimension k, and minimum distance d, an $[n,\ k,\ d]_q$ code. Since our examples involve Griesmer codes we recall here that an $[n,\ k,\ d]_q$ Griesmer code satisfies the Griesmer bound

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

with equality [13, p. 546]. Given the minimum distance d and the dimension k, the Griesmer codes have the smallest possible length n, which makes them more likely to fit the condition of Theorem 2. Indeed, this is the case in Examples 1–4 below, where we give intervals of properness for codes dual to parametric Griesmer codes. As we will see, these intervals approach $(0,\ (q-1)/q]$, when the dimension k of the Griesmer codes increases, i.e., the dual Griesmer codes are asymptotically proper. This and the fact that the dual Griesmer codes have small redundancy, which is often the case with codes used for error detection, make our results appear of possible interest for applications.

Example 1. In [3], a family of $[n,\ k,\ d]_q$ Griesmer codes has been constructed with parameters

$$n = \sum_{i=1}^{r} a_i \, \frac{q^k - q^{u_i}}{q-1}, \ k, \ d = \sum_{i=1}^{r} a_i \left(q^{k-1} - q^{u_i - 1}\right) ,$$

where

$$1 \leq a_i \leq q-1 \quad \text{and} \quad 1 \leq u_r < u_{r-1} < \ldots < u_1 \leq k-1 \ .$$

Using that $n = d\,q/(q-1)$ we compute

$$d - \frac{n(q-1)+2}{q+1} = \frac{d-2}{q+1} > 0$$

and

$$\frac{n(q-1)+1}{q} - d = \frac{1}{q}.$$

This shows, by Theorem 2, that the duals of the Griesmer codes with $d > 2$ are proper in the interval

$$\left[\frac{1}{1+\dfrac{d-1}{q-1}},\ \frac{q-1}{q}\right].$$

Moreover, the binary dual codes are proper, by the Corollary. Indeed, one can easily see that since the dual code distance of the Griesmer codes under consideration equals 2, the condition (2.9) is satisfied in the binary case.

Note that the above interval of properness tends to $(0,\ (q-1)/q]$, when the dimension k of the Griesmer code increases. Thus if we know a lower bound of the symbol error probability of a particular channel, we can find a dual code which is practically proper for this channel by choosing a sufficiently large k.

Example 2. The existence of $\left[q^4+q^2-q,\ 5,\ q^4-q^3+q^2-2q\right]_q$ Griesmer codes for any prime power $q \geq 3$ has been shown in [11]. Because

$$d - \frac{n(q-1)+2}{q+1} = \frac{q^3(q-1)q(q-3)-2}{q+1} > 0$$

and

$$\frac{n(q-1)+1}{q} - d = \frac{q+1}{q},$$

Theorem 2 implies that the dual codes are proper in the interval

$$\left[\frac{1}{2+\dfrac{q^4-q^3-2q}{q^2-1}},\ \frac{q-1}{q}\right].$$

These codes are also asymptotically proper, since the left hand end-point of the interval approaches zero when q increases. Some numerical results follow below.

Example 2: Numerical results

Code parameters	Interval of properness for the dual code
$[87, 5, 57]_3$	[0.125000, 0.666667]
$[268, 5, 200]_4$	[0.070093, 0.750000]
$[645, 5, 515]_5$	[0.044610, 0.800000]
$[2443, 5, 2093]_7$	[0.022430, 0.857143]
$[4152, 5, 3632]_8$	[0.017055, 0.875000]
$[6633, 5, 5895]_9$	[0.013391, 0.888889]
$[14751, 5, 13409]_{11}$	[0.008870, 0.909091]
$[28717, 5, 26507]_{13}$	[0.006298, 0.923077]
$[65776, 5, 61664]_{16}$	[0.004118, 0.937500]
$[83793, 5, 78863]_{17}$	[0.003639, 0.941176]
$[130663, 5, 123785]_{19}$	[0.002900, 0.947368]
$[280347, 5, 268157]_{23}$	[0.001965, 0.956522]

Example 3. Ternary Griesmer codes with parameters

$$n = (3^k - 1)/2 - 30, \ \ k \geq 4, \ \ d = 3^{k-1} - 21$$

have been characterized in [9]. The parameters satisfy the condition of Theorem 2, since

$$d - \frac{n(q-1)+2}{q+1} \quad = \quad \frac{3^{k-1}}{4} - 6.25 > 0$$

and

$$\frac{n(q-1)+1}{q} - d = 1.$$

The dual codes are then proper in the interval

$$\left[\frac{1}{1 + \dfrac{3^{k-1} - 22}{6}}, \ \ \frac{2}{3} \right],$$

and also asymptotically proper, when $k \to \infty$.

Example 4. In [10] has been shown the existence of q-ary Griesmer codes with parameters

$$\left[n = v_k - 3v_{\mu+1}, \ k, \ d = q^{k-1} - 3q^{\mu} \right],$$

where $\frac{k-2}{2} \geq \mu \geq 1, \quad q \geq 5, \quad$ and $\quad v_\ell = \frac{q^\ell - 1}{q-1}$ for any integer $\quad \ell \geq 0.$

Because

$$d - \frac{n(q-1)+2}{q+1} = \frac{q^\mu(q^{k-1-\mu-3}) + 4}{q+1} > 0$$

and

$$\frac{n(q-1)+1}{q} - d = \frac{3}{q},$$

the dual codes are proper in the interval

$$\left[\frac{1}{1 + \dfrac{q^{k-1} - 3q^\mu - 1}{3(q-1)}}, \quad \frac{q-1}{q}\right]$$

and they are also asymptotically proper.

Example 5. [1] and [16] 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, $r \geq 1,\ t > 1,\ s > 1$, and $s|q^r + 1$. The dimension k and the length n of the code $C(q,r,t,s)$ are

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

and its non-zero weights and the weight distribution are

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

These codes and their duals have been studied in [6], where the following has been proved:

- $C(3,r,t,2),\ C(3,1,2,4)$, and their duals are proper.
- The remaining codes and their duals are not good.

Below we make use of Theorem 2 to give intervals of properness for the non-good dual codes $C^\perp(q,r,t,s)$. When t is even, the minimum code distance of $C(q,r,t,s)$ is τ_2. The inequalities in (2.2) hold in this case, because

$$\begin{aligned} d - \frac{n(q-1)+2}{q+1} &= \frac{(q-1)q^{rt-1}(q^{rt}-q-1)-2s+q-1}{(q+1)s} \\ &\geq \frac{(q-1)q^{rt-1}(q^{rt}-q-1)-2(q^r+1)+q-1}{(q+1)s} \\ &> \frac{(q-1)q^{rt-1}(q^{rt}-q-1)-(q^{rt}-q-1)-4}{(q+1)s} \\ &= \frac{((q-1)q^{rt-1}-1)(q^{rt}-q-1)-4}{(q+1)s} > 0 \end{aligned}$$

and

$$\frac{n(q-1)+1}{q} - d = \frac{(q-1)(q^{rt}-1)+s}{qs} > 0.$$

By Theorem 2, the non-good codes $C^{\perp}(q,r,t,s)$ with t even are proper in the interval

$$\left[\frac{1}{1+\dfrac{q^{2rt-1}-q^{rt-1}-\dfrac{s}{q-1}}{q^{rt+1}-q^{rt}-q+s+1}}, \quad \frac{q-1}{q} \right].$$

When t is odd, the minimum code distance of $C(q,r,t,s)$ is τ_1. In the same manner as above we can show that even in this case

$$d - \frac{n(q-1)+2}{q+1} > \frac{((q-1)q^{r(t+1)-1}-1)(q^{r(t-1)}-q-1)-4}{(q+1)s} > 0$$

and

$$\frac{n(q-1)+1}{q} - d = \frac{(q-1)[q^{rt}(s-1)-1]+s}{qs} > 0.$$

Thus the non-good codes $C^{\perp}(q,r,t,s)$ with t odd are proper in the interval

$$\left[\frac{1}{1+\dfrac{q^{2rt-1}-q^{rt-1}(s-1)-s/(q-1)}{q^{rt+1}(s-1)-q^{rt}(s-1)-q+s+1}}, \ \frac{q-1}{q} \right].$$

4. Conclusions

Goodness and properness are properties characterizing the behavior of linear codes in error detection. These properties are related to the code probability of undetected error, thus to the weight distribution of the code. However, the weight distribution is only known for relatively few codes, and therefore criteria for goodness and properness which do not depend on it are highly appreciated. Such a criterion for a binary linear code to be proper on sub-intervals has been found earlier in [8]. In the present work we extend this to the case of q-ary linear codes. Our criterion is expressed in terms of the length and the minimum distance of the dual code. It reduces to the binary criterion when $q = 2$. We have applied our criterion to parametric classes of codes and have found intervals of properness for their dual codes. For some classes the intervals of properness increase when some parameters become larger, which makes the codes practically proper. Even for some non-good codes we have found sufficiently large intervals of properness, which might make these codes of practical interest.

References

[1] L. D. Baumert, R. J. McEliece. Weights of Irreducible Cyclic Codes, *Information and Control*, **20** (1972), 158–175.

[2] E. R. Berlekamp, R. J. McEliece, H. C. A. van Tilborg. On the Inherent Intractability of Certain Coding Problems, *IEEE Trans. Inform. Theory*, **24** (1978), 384–386.

[3] S. Dodunekov. Minimal Block Length a Linear q-ary Code with Specified Dimension and Code Distance, *Problems Inform. Transmission*, **20** (1984), no. 4, 239–249.

[4] R. Dodunekova, S. Dodunekov. Sufficient Conditions for Good and Proper Error Detecting Codes, *IEEE Trans. Inform. Theory*, **43** (1997), no. 6, 2023–2026.

[5] R. Dodunekova, S. Dodunekov. Sufficient Conditions for Good and Proper Error Detecting Codes via Their Dual Codes, *Math. Balkanica (N.S.)*, **11**(1997), no. 3–4, 375–381.

[6] R. Dodunekova, S. Dodunekov. Error Detection with a Class of Cyclic Codes, *Math. Balkanica (NS)*, **21**(2007), no. 3–4, 361–376.

[7] R. Dodunekova, S. Dodunekov, E. Nikolova. A Survey on Proper Codes, *General Theory of Information Transfer and Combinatorics*, a special issue of *Discrete Applied Mathematics*, to appear.

[8] R. Dodunekova, E. Nikolova. Sufficient Conditions for the Monotonicity of the Undetected Error Probability for Large Channel Error Probabilities, *Problems Inform. Transmission* **41** (2005), no. 3, 3–16 (Russian.) English translation in *Problems Inform. Transmission* **41**(2005), no. 3, 187–198.

[9] N. Hamada, T. Helleseth. Construction of Some Optimal Ternary Linear Codes and the Uniqueness of $[294, 6, 195; 3]$-Codes Meeting the Griesmer Bound, *Finite Fields and Their Applications*, **1** (1995), no. 4, 458–468.

[10] N. Hamada, T. Helleseth. A Characterization of Some $\{3v_{\mu+1}, 3v_{\mu}; k-1, q\}$-Minihypers and Some $(n, k, q^{k-1} - 3q^{\mu}; q)$-Codes ($k \geq 3$, $q \geq 5$, $1 \leq \mu < k-1$) Meeting the Griesmer Bound, *Discrete Mathematics*, **146** (1995), 59–67.

[11] N. Hamada, T. Helleseth, Ø. Ytrehus. On the Construction of $[q^4 + q^2 - q, 5, q^4 - q^3 + q^2 - 2q; q]$-Codes Meeting the Griesmer Bound, *Designs, Codes and Cryptography*, **2** (1992), no. 3, 225–229.

[12] T. Kløve and V. Korzhik, *Error Detecting Codes: General Theory and Their Application in Feedback Communication Systems*, Philip Drive: Kluwer Academic Publishers, 1995.

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

[14] E. Nikolova. A Sufficient Condition for Properness of a Linear Error-Detecting Code and Its Dual, *Mathematics and Mathematical Education*, Proc. 34th Spring Conf. of the Union of Bulgarian Mathematicians, April 2005, 136–139

[15] Vera Pless, *Introduction to the Theory of Error-Correcting Codes*, 3rd ed., New York: John Wiley & Sons, 1998.

[16] J. Wolfmann. Formes Quadratiqies et Codes à Deux Poids, *C. R. Acad. Sci. Paris Ser A-B*, **281** (1975), 533–535.

[a] *Department of Mathematical Sciences*
Chalmers University of Technology
Department of Mathematical Sciences
Göteborg University
412 96 Göteborg, SWEDEN
E-mail: rossitza@math.chalmers.se

[b] *Department of Electrical Engineering*
Katholieke Universitet of Leuven
3001 Leuven-Heverlee, BELGIUM
E-mail: li.weng@esat.kuleuven.be