МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2005
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2005
Proceedings of the Thirty Fourth Spring Conference of
the Union of Bulgarian Mathematicians
Borovets, April 6–9, 2005

A SUFFICIENT CONDITION FOR PROPERNESS OF A LINEAR ERROR-DETECTING CODE AND ITS DUAL

Evgeniya P. Nikolova[*]

A sufficient condition for properness of a q-ary linear error-detecting code and its dual code is given in terms of the code length, the minimum code distance, and the dual minimum code distance. Examples of codes satisfying the condition are provided.

1. Introduction. A linear code $C = [n, k, d]$ is *proper* for error detection on a q-ary symmetric memoryless channel with symbol error probability ε, if the probability of undetected error of C is an increasing function of $\varepsilon \in \left[0, \frac{q-1}{q}\right]$, see [11] and [12]. In terms of the code weight distribution $\{A_0, A_1, \ldots, A_n\}$, this probability is given by

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

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

$$(1.2) \qquad P_{ue}(C, \varepsilon) = q^{-(n-k)} \sum_{i=0}^{n} B_i \Big(1 - \frac{q\varepsilon}{q-1}\Big)^i - (1-\varepsilon)^n, \quad \varepsilon \in \Big[0, \frac{q-1}{q}\Big].$$

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, and many cyclic codes. More examples can be found in the survey [8]. The concept of properness may be extended to non-linear block codes. Examples of proper non-linear binary codes are the Kerdock and the Preparata codes, and codes satisfying or achieving the Grey-Rankin bound, see [9].

Most studies on properness of error-detecting codes involve the code weight distribution, see for example, [4–9] and [11]. However, since the computation of the code weight distribution is an NP-hard problem [1], relatively few codes are known with their weight distribution. Therefore, it is important to find criteria for properness which do not use the code weight distribution. For binary linear codes such criteria have been found in [10]. In this note we extend Theorem 1 from [10] to any prime power q by showing in

[*] Partially supported by the Bulgarian NSF under Contract MM1405/2004.

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

Section 2 that if the length n, the minimum code distance d, and the dual code distance $d^{\perp}$ of a q-ary linear code C satisfy

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

then the code and its dual are proper for error detection. In Section 3 we give examples of q-ary codes which satisfy the Theorem and thus are proper, together with their dual codes.

2. Main result. Consider a linear code $C=[n,k,d]_q$ with code weight distribution $\{A_0, A_1, \ldots, A_n\}$. Denoting $\varepsilon_i = \dfrac{i}{n}$, $i=1,\ldots,n$, we can write the derivative of the function $\varepsilon^i(1-\varepsilon)^{n-i}$ as

$$(\varepsilon^i(1-\varepsilon)^{n-i})' = n\varepsilon^{i-1}(1-\varepsilon)^{n-i-1}(\varepsilon_i - \varepsilon), \quad i=1,\ldots,n. \tag{2.1}$$

As noticed yearlier ([5], [11]), the above shows that when

$$\frac{d}{n} \geq \frac{q-1}{q} \tag{2.2}$$

the function in (1.1) increases for $\varepsilon \in \left[0, \dfrac{q-1}{q}\right]$, and C is then proper.

Recall also that the first order Pless Power Moment of C is given by

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

where B_1 is the number of codewords of weight one in the dual code, see [13], p. 133.

Theorem. *Suppose C is a q-ary linear code of length n, minimum code distance d, and dual minimum code distance $d^{\perp}$. If*

$$\max\{\, d,\, d^{\perp}\,\} \geq \frac{(q-1)n+1}{q}, \tag{2.4}$$

then C and its dual are proper for error detection.

Proof. Suppose for definitness that $d \geq \dfrac{(q-1)n+1}{q}$. Then the properness of C follows from (2.2), since $\dfrac{d}{n} > \dfrac{d-1}{n-1} \geq \dfrac{q-1}{q}$. From (1.2), for the derivative of $P_{ue}(C^{\perp},\varepsilon)$ we obtain

$$P'_{ue}(C^{\perp},\varepsilon) = -\frac{q^{-(k-1)}}{q-1}\sum_{i=d}^{n} iA_i\Big(1-\frac{q\varepsilon}{q-1}\Big)^{i-1} + n(1-\varepsilon)^{n-1}, \quad 0 \leq \varepsilon \leq \frac{q-1}{q}.$$

Put $\delta = 1 - \dfrac{1}{q(1-\varepsilon)}$, $0 \leq \delta \leq \dfrac{q-1}{q}$, to get from the above equation

$$\begin{aligned}\frac{P'_{ue}(C^{\perp},\varepsilon)}{n(1-\varepsilon)^{n-1}} &= 1 - \frac{q^{-(k-1)}}{n(q-1)}\sum_{i=d}^{n} iA_i\Big(\frac{q}{q-1}\,\delta\Big)^{i-1}\big(q(1-\delta)\big)^{n-i} \\ &= 1 - \frac{q^{n-k}}{n(q-1)}\sum_{i=d}^{n} iA_i\Big(\frac{1}{q-1}\Big)^{i-1}\delta^{i-1}(1-\delta)^{n-i}.\end{aligned} \tag{2.5}$$

For $\delta_i = \dfrac{i-1}{n-1}$ the condition of the Theorem implies

$$\delta_i \geq \frac{d-1}{n-1} \geq \frac{q-1}{q}, \quad d \leq i \leq n,$$

and, thus, we have from (2.1) that the sum in the right hand side of (2.5) is an increasing function for $0 \leq \delta \leq \dfrac{q-1}{q}$. From this and (2.3) we obtain in (2.5)

$$\begin{aligned}\frac{P'_{ue}(C^{\perp},\varepsilon)}{n(1-\varepsilon)^{n-1}} &\geq 1 - \max_{0\leq\delta\leq\frac{q-1}{q}} \frac{q^{n-k}}{n(q-1)} \sum_{i=d}^{n} iA_i \Big(\frac{1}{q-1}\Big)^{i-1} \delta^{i-1}(1-\delta)^{n-i} \\ &= 1 - \frac{q^{-(k-1)}}{n(q-1)} \sum_{i=d}^{n} iA_i \geq 1 - \frac{q^{-(k-1)}}{n(q-1)}\, n\,(q-1)\, q^{k-1} = 0,\end{aligned}$$

and the Theorem follows. □

3. Examples. We give below two examples of families of codes meeting the Griesmer bound

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

which are proper, together with their dual codes, by the Theorem.

1. Consider the Griesmer codes with parameters

$$\Big[n = s(q^k-1) - \sum_{i=1}^{m} a_i \frac{q^{u_i}-1}{q-1}, \quad k, \quad d = s(q-1)q^{k-1} - \sum_{i=1}^{m} a_i\, q^{u_i-1} \Big],$$

see [2–3]. Here $s \geq 2$ is an arbitrary integer and u_i and a_i for $i = 1, \ldots, m,$ are integers, such that $1 \leq a_i \leq q-1$ and $k = u_0 > u_1 > \ldots > u_m \geq 1$. When $s > m$, the codes and their duals are proper by the Theorem, since

$$qd - (q-1)n - 1 = s(q-1) - \sum_{i=1}^{m} a_i - 1 \geq (q-1)(s-m) - 1 > 0.$$

2. Solomon and Stiffler introduced in [14] Griesmer codes with parameters

$$n = \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil + t\,\frac{q^k-1}{q-1}, \quad k, \quad d' = d + t\,q^{k-1},$$

where t is an arbitrary positive integer. From

$$qd' - (q-1)n - 1 = t + qd - (q-1)\sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil - 1$$

and the Theorem we obtain that if

$$t \geq (q-1)\sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil - qd + 1,$$

the properness of the codes follows as well from Theorem 3.7.3 of [11]

Acknowledgment. The author gratefully acknowledges the many helpful suggestions of Rossitza Dodunekova during the preparation of the paper.

REFERENCES

[1] 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), No. 3, 384–386.

[2] S. M. Dodunekov. Optimal linear codes. Doctor of Math. Sci. Thesis, Institute of Math., BAS, Sofia, 1986.

[3] S. M. Dodunekov. Minimum Block Length of a Linear q-ary Code with Specified Dimension and Code Distance. *Problems Inform. Transmission*, **20** (1984), No. 4, 39–249.

[4] R. Dodunekova. Extended binomial moments of a linear code and the undetected error probability. *Problems Inform. Transmission*, **39** (2003), No. 3, 255–265.

[5] R. Dodunekova, S. M. Dodunekov. Linear block codes for error detection. No 1996-07/ISSN 0347-2809, Dep. of Mathematics, Chalmers University of Technology and Göteborg University, 1996, 11 p.

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

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

[8] R. Dodunekova, S. Dodunekov, E. Nikolova. A survey on proper codes. Proc. General Theory of Information Transfer and Combinatorics, ZiF Research Year, Bielefeld 2002. Preprint No 2003-5, Chalmers University of Technology and Göteborg University.

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

[10] R. Dodunekova, E. Nikolova. Intervals of properness for binary linear error-detecting codes. Preprint No 2004-42, Chalmers University of Technology and Göteborg University.

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

[12] 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*, **25** (1979), No 1, 110–112.

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

[14] G. Solomon, J. J. Stiffler Algebraically punctured cyclic codes. *Inform. Control*, **8** (1965), No 2, 70–179.

Bourgas Free University
Faculty for Computer Science
Engineering and Natural Studies
101, Aleksandrovska Str.
8000 Bourgas, Bulgaria
e-mail: e_nikolova@bfu.bg

ДОСТАТЪЧНО УСЛОВИЕ ЛИНЕЕН КОД И НЕГОВИЯТ ДУАЛЕН ДА СА ПОДХОДЯЩИ ЗА ОТКРИВАНЕ НА ГРЕШКА

Евгения П. Николова

В термините на кодовата дължина и минималното дуално розстояние на кода е дадено достатъчно условие q-ичен линеен код и неговият дуален да са подходящи за откриване на грешка. Представени са примери, удовлетворяващи това условие.