SUFFICIENT CONDITIONS FOR GOOD AND PROPER LINEAR ERROR DETECTING CODES VIA THEIR DUALS

R. Dodunekova
Department of Mathematics
Chalmers University of Technology
and the University of Gothenburg
412 96 Gothenburg, Sweden

S. M. Dodunekov*
Institute of Mathematics
Bulgarian Academy of Sciences
8 G. Bontchev Street
1113 Sofia, Bulgaria

Abstract

We have found earlier in [1] sufficient conditions for a linear block code to be good or proper for error detection. These conditions are expressed in terms of the weight distribution of the code. However, for codes with small co-dimension or with small number of nonzero weights in their dual codes the conditions would be technically easier to check if they were presented in terms of the dual weight distribution. This alternative representation is the purpose of the present paper.

Index terms: error detecting code, dual code, probability of undetected error.

*Partially supported by grant MM-502/95 from Bulgarian NSF.

1 INTRODUCTION

A linear block code $C = [n, k, d; q]$ with symbols from a finite field of q elements $GF(q)$ is a k-dimensional subspace of the n-dimensional vector space over $GF(q)$, with minimum Hamming distance d. When C is used for error detection only, the decoder proceeds as follows. Let $x \in C$ be the codeword transmitted and let $y \in GF(q)^n$ be the vector received. The error vector is then $e = y - x$. If $y \in C$, the decoder accepts it as the codeword sent. When $y \notin C$, the decoder makes the correct decision for a transmission error. Clearly, all cases of an undetected transmission error will be the cases $y \in C$, but $y \neq x$, that is, $e \in C$ but $e \neq 0$.

Assume now that the transmission channel is a discrete channel without memory with q inputs and q outputs and with symbol error probability ε. In such a channel, every symbol will be correctly received with probability $1 - \varepsilon$ and will be transformed to each of the $(q-1)$ other symbols with probability $\varepsilon/(q-1)$. As usual, we assume that $0 \leq \varepsilon \leq (q-1)/q$, which ensures that every symbol will be more probably transmitted as itself than as some other fixed symbol.

Let $\{A_i, a \leq i \leq n\}$ be the weight distribution of the code C, that is, A_i is the number of codewords of weight i in C, and let C be used for error detection on the q-nary symmetric channel. The probability that a certain vector $e \in C$ of weight $i > 0$ will occur as an error vector is obviously $(\varepsilon/(q-1))^i(1-\varepsilon)^{n-i}$. Then the probability $P_{ud}(C, \varepsilon)$ of an undetected transmission error must be

$$P_{ud}(C, \varepsilon) = \sum_{i=1}^{n} A_i \left(\frac{\varepsilon}{q-1}\right)^i (1-\varepsilon)^{n-i} \tag{1.1}$$

(see [2], p. 66).

In the worst case of symbol error probability $\varepsilon = (q-1)/q$, we get

$$P_{ud}(C, \frac{q-1}{q}) = \sum_{i=1}^{n} A_i q^{-i} q^{-(n-i)} = q^{-n}(q^k - 1) = q^{-(n-k)} - q^{-n}.$$

Assume that $P_{ud}(C, \varepsilon)$ in (1.1) is computable. (This means that the weight distribution of C is known). How shall one decide whether C is suitable for error detection or not? Reasonable criteria based on comparing $P_{ud}(C, \varepsilon)$ to $P_{ud}(C, \frac{q-1}{q})$ have been worked out in a series of papers (see for this the monograph [3]). Namely, C is *good* for error detection if for any $\varepsilon \in [0, (q-1)/q]$,

$$P_{ud}(C, \varepsilon) \leq q^{-(n-k)} - q^{-n}$$

and C is *proper* for error detection if $P_{ud}(C, \varepsilon)$ increases in $\varepsilon \in [0, (q-1)/q]$. Obviously, proper codes are also good codes of some regularity: the smaller symbol error-probability is the better they perform in detecting errors.

Introduce the notations

$$A_0^* = 0, \quad A_\ell^* = \sum_{i=1}^{\ell} \frac{\ell_{(i)}}{n_{(i)}} A_i, \ \ell = 1, \dots n \tag{1.2}$$

where $m_{(i)} = m(m-1)\dots(m-i+1)$ for a positive integer m. Obviously, $A_1^* = A_2^* = \dots = A_{d-1}^* = 0$.

The two theorems below give sufficient conditions for good and proper codes and have been proved in [1].

Theorem 1′. If for $\ell = d, \dots, n$

$$q^{-(n-k)} - q^{-n} \geq q^{-\ell} A_\ell^*, \tag{1.3}$$

then C is good.

Theorem 2′. If for $\ell = d+1, \dots n$

$$A_\ell^* \geq q A_{\ell-1}^*, \tag{1.4}$$

then C is proper.

In Section 2 we give equivalent forms of (1.3) and (1.4) in terms of the weight distribution $\{B_i, 0 \leq i \leq n\}$ of the dual code $C^\perp$. Then, in Section 4, we show some examples where checking the equivalent forms turns to be easier than checking (1.3) and (1.4) themselves.

2 CRITERIA FOR GOOD AND PROPER ERROR DETECTING CODES VIA THEIR DUALS

For a code C with dual weight distribution $\{B_i, 0 \leq i \leq n\}$ we introduce correspondingly

$$B_0^* = 0, \quad B_\ell^* = \sum_{i=1}^{\ell} \frac{\ell_{(i)}}{n_{(i)}} B_i, \ \ell = 1, \dots n \tag{2.1}$$

LEMMA 1. *For $\ell = 0, 1, \dots, n$ the following equalities hold true:*

$$A_\ell^* + 1 = q^{-(n-k-\ell)}[B_{n-\ell}^* + 1], \tag{2.2}$$

$$B_\ell^* + 1 = q^{-(k-\ell)}[A_{n-\ell}^* + 1]. \tag{2.3}$$

Proof. Let $\ell = 0$. Then $A_\ell^* = 0$,

$$B_n^* = \sum_{i=1}^{n} B_i = q^{n-k} - 1$$

and obviously (2.2) is true. Now, let $\ell \geq 1$. Consider

$$\begin{aligned} \binom{n}{\ell}[1 + A_\ell^*] &= \binom{n}{\ell} + \sum_{i=1}^{\ell} \binom{n}{\ell} \frac{\ell_{(i)}}{n_{(i)}} A_i \\ &= \binom{n}{\ell} + \sum_{i=1}^{\ell} \Big[\binom{n}{\ell}\binom{\ell}{i} \Big/ \binom{n}{i}\Big] A_i. \end{aligned}$$

¿From the obvious equality

$$\binom{n}{\ell}\binom{\ell}{i} = \binom{n}{i}\binom{n-i}{\ell-i}$$

we get

$$\binom{n}{\ell}[1 + A_\ell^*] = \binom{n}{\ell} + \sum_{i=1}^{\ell} \binom{n-i}{\ell-i} A_i = \sum_{i=0}^{\ell} \binom{n-i}{\ell-i} A_i \tag{2.4}$$

and similarly

$$\binom{n}{n-\ell}[1 + B_{n-\ell}^*] = \sum_{i=0}^{n-\ell} \binom{n-i}{\ell} B_i. \tag{2.5}$$

By Lemma 2.2 of [4],

$$\sum_{i=0}^{\ell} \binom{n-i}{\ell-i} A_i = q^{-(n-k-\ell)} \sum_{i=0}^{n-\ell} \binom{n-i}{\ell} B_i$$

which together with (2.4) and (2.5) imply (2.2) and correspondingly (2.3).

We are now in the position to formulate (1.3) and (1.4) in terms of $B_i^{*'}s$.

Theorem 1. *If for $\ell = d, \ldots, n$*

$$q^{-k} - q^{-(n+k-\ell)} \geq q^{-(n-\ell)} B_{n-\ell}^*, \tag{2.6}$$

then C is good for error detection.

Proof. Using the Lemma we get

$$\begin{gathered}
q^{-(n-k)} - q^{-n} \geq q^{-\ell} A_\ell^* \\
\Updownarrow \\
q^{-(n-k)} - q^{-n} + q^{-\ell} \geq q^{-\ell}[A_\ell^* + 1] \\
\Updownarrow \\
q^{-(n-k)} - q^{-n} + q^{-\ell} \geq q^{-\ell} q^{-(n-k-\ell)}[B_{n-\ell}^* + 1] \\
\Updownarrow \\
q^{-\ell} - q^{-n} \geq q^{-(n-k)} B_{n-\ell}^* \\
\Updownarrow \\
q^{-k} - q^{-(n+k-\ell)} \geq q^{-(n-\ell)} B_{n-\ell}^*.
\end{gathered}$$

The statement now follows from Theorem 1′.

Theorem 2. *If for* $\ell = d+1, \ldots, n$

$$B_{n-\ell}^* \geq B_{n-\ell+1}^* - q^{n-k-\ell+1} \tag{2.7}$$

then C *is proper for error detection.*

Proof. Using again the Lemma we have

$$\begin{gathered}
A_\ell^* \geq q A_{\ell-1}^* \\
\Updownarrow \\
A_\ell^* + 1 \geq q[A_{\ell-1}^* + 1] - q \\
\Updownarrow \\
q^{-(n-k-\ell)}[B_{n-\ell}^* + 1] \geq q q^{-(n-k-\ell+1)}[B_{n-\ell+1}^* + 1] - q \\
\Updownarrow \\
q^{-(n-k-\ell)}[B_{n-\ell}^* + 1] \geq q^{-(n-k-\ell)}[B_{n-\ell+1}^* + 1] - q \\
\Updownarrow \\
B_{n-\ell}^* \geq B_{n-\ell+1}^* - q^{n-k-\ell+1}.
\end{gathered}$$

The statement now follows from Theorem 2′.

3 EXAMPLES

1. Consider the degenerate binary simplex code $C^\perp$ with parameters

$$n = 2^{2u} - 1,\ \dim C^\perp = u,\ d = 2^{2u-1} + 2^{u-1}$$

and weight distribution

$$B_0 = 1,\ B_d = 2^u - 1.$$

(see [5, Ch.8, Ex. 1 of §7]).

For any $\ell = d+1, \dots, n$

$$n - \ell < n - d = 2^{2u} - 1 - 2^{2u-1} - 2^{u-1} = 2^{2u-1} - 2^{u-1} - 1 < d$$

and hence

$$B^*_{n-\ell+1} = B^*_{n-l} = 0.$$

According to Theorem 2 the code C is proper.

2. Consider the MacDonald codes $C^u_k(q)$ with parameters

$$\left[n = \frac{q^k - q^u}{q-1}, k, d = q^{k-1} - q^{u-1},\ 1 \le u \le k-1\right]$$

and weight distribution

$$B_0 = 1,\ B_d = q^k - q^{k-u},\ B_{q^{k-1}} = q^{k-u} - 1$$

(see [6], [7]).

Let $q > 2$. Then for any $\ell = d+1, \dots, n$

$$n - \ell < n - d = \frac{q^{k-1} - q^{u-1}}{q-1} < d$$

and

$$B^*_{n-\ell+1} = B^*_{n-\ell} = 0.$$

If $q = 2$, then $n = 2d$ and the above equalities hold for $\ell = d+2, \dots, n$. It is easy to check that always

$$B^*_d \le 2^{d-k}$$

except for the [4, 3, 2] and [2, 2, 1] codes. Hence, the dual codes of the MacDonald codes are proper.

3. For a cyclic redundancy check (CRC) code C of length n and with generator polynomial $g(x)$ the dimension of the dual code $C^\perp$ coincides with the degree r of $g(x)$. For all practically interesting CRC codes

$$n - r = \deg C \gg r.$$

Therefore, the use of Theorem 2 instead of Theorem 2′ will reduce the complexity of computations necessary to test a CRC code for properness.

4. Consider the binary codes G_n with parameters $[n, n-12, 8]$, $19 \leq n \leq 23$. It was shown in [8] that G_n is unique up to equivalence and that there exist exactly two nonequivalent $[18, 6, 8]$ codes G_{18}^1 and G_{18}^2. All codes G_n, G_{18}^1 and G_{18}^2 are shortened of the extended binary $[24, 12, 8]$ Golay code. Their weight distributions are listed bellow:

	B_1	B_8	B_{12}	B_{16}
G_{18}^1	1	46	16	1
G_{18}^2	1	45	18	
G_{19}	1	78	48	1
G_{20}	1	130	120	5
G_{21}	1	210	280	21
G_{22}	1	330	616	77
G_{23}	1	506	1288	253

A straightforward application of Theorem 2 shows that the duals of all these codes are proper.

References

1. R. Dodunekova and S. M. Dodunekov, Sufficient conditions for good and proper error detecting codes, *IEEE Trans. Inform. Theory* vol. **43**, No. **06**, 2023-2026,1997.

2. S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications.* Englewood Cliffs, NJ: Prentice-Hall, 1983.

3. T. Kløve and V. Korzhik, *Error Detecting Codes.* Boston: Kluwer Academic Publishers, 1995.

4. F.J.MacWilliams, A theorem on the distribution of weights in a systematic code, *The Bell System Technical Journal*, v. 42, 79-94, 1963.

5. F.J.MacWilliams and N.J.A.Sloane, *The Theory of Error-Correcting Codes.* New York: North-Holland, 1977.

6. J.E.MacDonald, Design methods for maximum distance error-correcting codes, *IBM J. Res. Devel.* v. 4, 43-57, 1960.

7. A.M.Patel, Maximum q-ary linear codes with large minimum distance, *IEEE Trans. Inf. Theory* v. 21, No 1, 106-110, 1975.

8. S.M.Dodunekov, S.B.Encheva, On the uniqueness of some subcodes of the binary extended Golay code, *Prob. Inform. Transmission* vol. 29, No 1, 38-43, 1993.