Binary and ternary linear codes which are good and proper for error correction

Tsonka Baicheva
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
P.O. Box 323, 5000 Veliko Tarnovo, Bulgaria
lpmivt@vt.bia-bg.com

Abstract

All binary cyclic codes of lengths up to 31 and ternary cyclic and negacyclic codes of lengths up to 20 have been tested and those of them which satisfy the sufficient conditions to be good and proper for error correction have been determined. The same way some binary distance optimal linear codes of lengths up to 33 have been tested. Tables with the results have been prepared.

I Introduction

Suppose a q-ary $[n, k, d]$ code C is used for simultaneous error correction and detection. We shall consinder the performance of C when it is used to correct up to $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ errors on a q-ary symmetric channel (qSC) without memory, i.e. any symbol has a probability $1 - p$ of being received correctly and a probability $\frac{p}{q-1}$ of being transformed into each of the $q - 1$ other symbols. We assume that $0 \leq p \leq \frac{q-1}{q}$. Denote by $P_{ue}^{(t)}(C, p)$ the probability of an undetected error after a t-error correction. Since $p = \frac{1}{q}$ is the biggest value of the error bit probability we can expect that $P_{ue}^{(t)}(C,p) \leq P_{ue}^{(t)}\left(C, \frac{1}{p}\right)$ for all $p \in \left[0, \frac{q-1}{q}\right]$. However, there are examples of codes for which this inequality does not hold (see [8, p.46]). A code C is called *t-proper* if $P_{ue}^{(t)}(C,p)$ is monotonous and *t-good* if $P_{ue}^{(t)}(C,p) \leq P_{ue}^{(t)}\left(C, \frac{q-1}{q}\right)$ for all $p \in \left[0, \frac{q-1}{q}\right]$. It is clear that we can check these criteria only for a finite set of points of p. The same problem concerns sufficient conditions for *t-good* codes from [7]. Discrete sufficient conditions for a linear $[n,k,d;q]$ code to be *t-good* and *t-proper* were derived by Dodunekova and Dodunekov [4].

Let $Q_{h,l}$ be the number of vectors of weight l in the cosets of minimum weight h, excluding the coset leaders and let $A_i^{(t)} = \sum_{h=0}^{t} Q_{h,i}$, $i = t+1, \ldots, n$ be the weight distribution of the vectors in the cosets of weight at most t, excluding the leaders. Denote by $V_q(t)$ the volume of the q-ary sphere of radius t in the n-dimensional vector space over $GF(q)$ and $m_{(i)} = m(m-1)\ldots(m-i+1)$.

Theorem 1. [4] *If for* $l = t+1, \ldots, n$

$$(q^{-(n-k)} - q^{-n})V_q(t) \geq q^{-l} \sum_{i=t+1}^{l} \frac{l_{(i)}}{n_{(i)}} A_i^{(t)}$$

then C is t-good for error correction.

Theorem 2. [4] *If for* $l = t+2, \ldots, n$

$$\sum_{i=t+1}^{l} \frac{l_{(i)}}{n_{(i)}} A_i^{(t)} \geq q \sum_{i=t+1}^{l-1} \frac{(l-1)_{(i)}}{n_{(i)}} A_i^{(t)}$$

then C is t-proper for error correction.

Remark. For $t = 0$ these conditions must be sufficient for the code C to be *good* and *proper* for error detection.

There are many known examples of classes of codes which are *good* and *proper* but only one example of a class of codes (MDS codes) which are *t-good* and *t-proper* [8, pp. 104-115]. The aim of this work is to find other examples of codes which are good and proper for error correction checking the sufficient conditions from Theorems 1 and 2.

II Complexity of checking the sufficient conditions for good and proper linear error correcting codes

It is known [3] that the following problem is NP complete: given a $k \times n$ (binary) generator matrix G and an integer w, decide if the code C generated by G contains a code word of weight w. In particular, this implies that the problem of finding the weight distribution of C is NP hard. To check if the code is good and proper for error correction using Theorems 1 and 2 we have to find the weight distributions of the code and of all its cosets. We have done this using programms written on C. Then we check the conditions in linear time using the Maple package.

III Results

Binary cyclic codes of lengths up to 31 have been investigated by Downie and Sloane [5]. All such codes are classified and their weight spectra and covering radii are determined. The same investigation for ternary cyclic codes of lengths up to 25 and ternary negacyclic codes of length up to 26 has been made by Baicheva [1], [2]. Using these classifications we have checked the sufficient conditions for *t-good* and *t-proper* linear codes for all binary cyclic codes of lengths up to 31 and for all ternary cyclic and negacyclic codes of lengths up to 20. The results for the ternary codes are presented in the tables below. Only codes which are good and/or proper for error correction are included in the Tables and their length, dimension, minimum distance, generator polynomial and values of t for which the code is good and proper are given. The generator polynomials are given as sequences of coefficients with the leading coefficient in the first place.

Table 1. Ternary cyclic codes.

No	[n,k,d]	generator polynomial	good and proper
1.	[8,5,3]	1011	t=0,1 g&p
2.	[8,4,4]	11012	t=0,1 g&p
3.	[8,3,5]	102111	t=0,1,2 g&p
4.	[8,3,4]	120012	t=0,1 g
5.	[8,2,6]	1120221	t=0,1,2 g&p
6.	[8,2,4]	1020102	t=0,1 g
7.	[10,5,4]	112122	t=0,1 g&p
8 .	[11,6,5]	102122	t=0,1,2 g&p

Table 1. (Continued)

No	[n,k,d]	generator polynomial	good and proper
9.	[11,5,6]	1222101	t=0,1,2 g&p
10.	[13,10,3]	1112	t=0,1 g&p
11.	[13,9,3]	10011	t=0,1 g&p
12.	[13,7,5]	1022201	t=0,1,2 g&p
13.	[13,7,4]	1222121	t=0,1 g&p
14.	[13,6,6]	12200112	t=0,1,2 g&p
15.	[13,6,6]	11002122	t=0,1,2 g&p
16.	[13,4,7]	1120102201	t=0,1,2,3 g&p
17.	[13,3,9]	10111220121	t=0,1,2,3,4 g&p
18.	[16,10,4]	1101121	t=0,1 g&p
19.	[16,9,5]	10210122	t=0,1,2 g&p
20.	[16,8,5]	111210221	t=0,1,2 g&p
21.	[16,7,6]	1001222022	t=0,1,2 g&p
22.	[16,6,6]	11010112212	t=0,1,2 g&p
23.	[16,3,10]	10211100102111	t=0,1,2,3,4 g&p
24.	[16,2,12]	112022101120221	t=0,1,2,3,4,5 g&p
25.	[20,15,4]	102222	t=0,1 g&p
26.	[20,14,4]	1121112	t=0,1 g&p
27.	[20,14,4]	1221221	t=0,1 g&p
28.	[20,13,4]	10021122	t=0,1 g
29.	[20,12,4]	100222211	t=0,1 g&p
30.	[20,11,5]	1202000202	t=0,1,2 g&p
31.	[20,9,6]	121102020102	t=0,1,2 g&p
32.	[20,8,8]	1002122221122	t=0,1,2,3 g&p
33.	[20,7,8]	10022121211122	t=0,1,2,3 g
34.	[20,6,10]	112100101002221	t=0,1,2,3,4 g&p
35.	[20,6,8]	122110102022112	t=0,1,2,3 g&p
36.	[20,5,11]	1012201212020022	t=0,1,2,3,4,5 g&p
37.	[20,4,12]	11101210002220212	t=2,3,4,5 g

Table 2. Ternary Negacyclic Codes.

No	[n,k,d]	generator polynomial	good and proper
1.	[6,2,3]	10201	t=0,1 g
2.	[10,6,4]	11021	t=0,1 g&p
3.	[10,4,6]	1110121	t=0,1,2 g&p
4.	[12,8,3]	12211	t=0,1 g&p

Table 2. (Continued)

No	[n,k,d]	generator polynomial	good and proper
5.	[12,4,6]	122122211	t=0,1,2 g&p
6.	[12,2,9]	12202110122	t=0,1,2,3,4 g&p
7.	[14,8,5]	1101011	t=0,1,2 g&t=0,1 p
8.	[14,6,6]	111202111	t=0,1,2 g&t=0,1 p
9.	[20,16,3]	10111	t=0,1 g&p
10.	[20,14,4]	1100222	t=0,1 g&p
11.	[20,12,5]	112212211	t=0,1,2 g&p
12.	[20,10,7]	12201101002	t=0,1,2,3 g&t=0 p
13.	[20,10,6]	11121011012	t=0,1,2 g&t=0 p
14.	[20,8,8]	1122201022211	t=0,1,2,3 g&t=0,1 p
15.	[20,6,9]	101212021220212	t=3,4 g
16.	[20,6,9]	120121010211212	t=0,1,2,3,4 g&t=0,1 p
17.	[20,4,12]	11021100212101201	t=0,1,2,3,4,5 g&t=0,1,2 p
18.	[20,2,15]	1120221011202210112	t=0,1,2,3,4,5,6,7 g&t=0,1,2,3,4,5 p

Finally many examples of binary linear codes of lengths up to 33 which satisfy the conditions of Theorems 1 and 2 were found among the distance optimal codes. Their generator matrices were taken from [6]. In addition their covering radii were determined.

The tables with the results for the binary cyclic and distance optimal codes are not included in the paper but can be received from the author on response.

References

[1] T. Baicheva, The Covering Radius of Ternary Cyclic Codes with Length up to 25, *Designs, Codes and Cryptography*, vol.13, pp. 223-227, 1998.

[2] T. Baicheva, On the Covering Radius of Ternary Negacyclic Codes with Length up to 26, *Proc. 2000 IEEE Intern. Symposium of Inform. Theory*, to appear.

[3] E. R. Berlekamp, R. J. McEliece, H. C. A. van Tilborg, On the inherent intractability of certain coding problems, *IEEE Trans. Inform. Theory*, vol. 24, 1978, pp. 384-386.

[4] R. Dodunekova, S. Dodunekov, Sufficient conditions for good and proper linear error correcting codes, *Proc. Second International Workshop on Optimal Codes and Related Topics*, June 9-15, 1998, Sozopol, Bulgaria, pp. 62-67.

[5] D. Downie, N. J. A. Sloane, The covering radius of cyclic codes of length up to 31, *IEEE Trans. Inf. Theory*, vol. 31, 1985, pp. 446-447.

[6] D. Jaffe, Binary Linear Codes: New Results on Noneistence, Draft (Version 0.4), Department of Mathematics and Statistics, University of Nebraska, April 14, 1997.

[7] T. Klöve, Using codes for error correction and detection, *IEEE Trans. Inforom. Theory*, vol. 30, 1984, pp. 868-870.

[8] T. Klöve and V. Korzhik, *Error Detecting Codes*, Kluwer Academic Publishers, Boston, 1995.