Teaching Linear Codes*

Tsonka Baicheva, Iliya Bouyukliev, Stefan Dodunekov
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
W. Willems
University of Magdeburg, Germany

Abstract

Because of their practical significance linear block codes are traditionally included in basic Coding Theory courses. In this paper, using a rich set of simple examples, we demonstrate some interesting facts which, as we believe, are useful to get to know for students, and will help them to learn how to solve practical error control problems in modern communications. The work is finished with an answer of research problem 5.1 stated in the book of MacWilliams and Sloane [10].

Index Terms: Linear codes, Error detecting and error correcting performance.

1 Introduction

The basic idea of noisy coding is to add some redundancy symbols to the information symbols in order to be able to detect or correct errors that occur during a transmission over a noisy channel. In this work, we will focus our attention on the most important class among error-correcting block codes - the linear codes. These codes have an accessible mathematical structure which leads to effective coding and decoding methods and allows easy to analyze their performence. A particular class of linear codes - cyclic codes - have properties which make them very easy to implement and have a wide range of applications. On the other hand, linear codes are strongly connected

*Partially supported by the Bulgarian National Science Fund under Contracts MM901/1999 and MM1304/2003.

to many classical mathematical objects like groups, graphs, designs, finite geometries, curves and their study is also of pure theoretical interest.

In the next section definitions and theorems which the reader will need to follow the paper are given. In section 3 questions which are discussed and answered in the paper are formulated. Section 4 is devoted to the investigation of three classes of binary linear codes and we compare their performance according to the different code parameters. In the final section we solve open problem stated in [10].

2 Preliminaries

There are many books devoted to coding theory and its applications, and Werner Heise's home page maintains a long list of such books [11]. Here we will summarize the basic facts on linear block codes in order to make the paper self-contained.

Definition Let F_q^n be an n-dimensional vector space over the finite field with q elements. A *linear code* C is a k-dimensional subspace of F_q^n.

Definition A k-by-n matrix G having as rows the vectors of a basis of C is called a *generator matrix* of C.

Definition Let $x, y \in F_q^n$. The *Hamming distance* $d(x, y)$ between x and y is the number of positions in which x and y differ, i.e.

$$d(x, y) = |\{\, \imath \mid x_i \neq y_i\}|.$$

Definition The *minimum distance* of a linear code C is the minimum Hamming distance between all distinct pairs of codewords in C.

With these notations a linear code with length n, dimension k and minimum distance d over F_q is denoted by $[n, k, d]_q$.

The inner product of two vectors $\mathbf{u} = (u_1, u_2, \ldots u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ from F_q^n is defined by

$$\mathbf{uv} = u_1v_1 + u_2v_2 + \ldots + u_nv_n.$$

Two vectors are said to be *orthogonal* if their inner product is 0. The set of all vectors of F_q^n orthogonal to all codewords from C is called the *dual code* $C^\perp$ to C which is a linear $[n, n-k]_q$ code.

Let C_1 and C_2 be two linear $[n,k]_q$ codes. They are said to be equivalent if the codewords of C_2 can be obtained from the codewords of C_1 via a sequence of transformations of the following types:

(1) permutation of the set of coordinate positions;

(2) multiplication of the elements in a given position by a non-zero element of F_q;

(3) application of a field automorphism to the elements in all coordinate positions.

An automorphism of a linear code C is a finite sequence of transformations of type (1)-(3), which maps each codeword of C onto a codeword of C. All the automorphisms of a code C form a group, which is called the *automorphism group* $Aut(C)$ of the code.

Let A_i denote the number of codewords of C of weight i. Then the numbers $A_0, \dots, A_n$ are called the *weight distribution* of the code C.

If B is a binary code with $v, w \in B$ we define

$$i(v,w) = \textit{the number of } r \textit{ with } v_r = 0 \textit{ and } w_r = 0,$$

$$j(v,w) = \textit{the number of } r \textit{ with } v_r = 0 \textit{ and } w_r = 1,$$

$$k(v,w) = \textit{the number of } r \textit{ with } v_r = 1 \textit{ and } w_r = 0,$$

$$l(v,w) = \textit{the number of } r \textit{ with } v_r = 1 \textit{ and } w_r = 1.$$

The *biweight enumerator* of the code B is given by

$$\mathcal{I}_B(w,x,y,z) = \sum_{v \in B} \sum_{w \in B} w^{i(v,w)} x^{j(v,w)} y^{k(v,w)} z^{(l(v,w)}.$$

A *coset* of the code C defined by the vector $x \in F_q^n$ is the set $x + C = \{x + c \mid c \in C\}$. A *coset leader* of $x + C$ is a vector in $x + C$ of smallest weight. We will denote by α_i for $i = 0, 1, \dots, n$ the number of coset leaders of weight i.

The *covering radius* R of a code is the largest weight in the set of coset leaders and the smallest integer R, such that the spheres of radius R around the codewords completely cover F_q^n.

Cosets in which the minimum weight vector is unique are of special interest. The *Newton radius* ν of a code is the weight of the largest unique coset leader. This parameter determines the weight of a maximal uniquely correctable error (see [7]).

Definition 5 The block code C *detects t errors* if each word a', obtained from a codeword a by pertubation of $1, 2, \ldots, t$ symbols, is not a code word.

Theorem The code C detects t errors iff $d > t$.

Definition The block code C *corrects t errors* if for each code word a and each word a', obtained from a by pertubation of $1, 2, \ldots, t$ symbols, the Hamming distance $d(a, a')$ is strictly smaller then the Hamming distance of any other code word to a'.

.

Theorem The code C corrects t errors iff $d > 2t$.

In other words, a linear $[n, k, d]_q$ code detects up to $d - 1$ errors and corrects up to $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ errors.

A central problem in coding theory is to optimize one of the *basic parameters* n, k or d of a linear code, given the two others. Thus we get the following three optimization problems:

(1) Find $N_q(k, d)$ the smallest value of n for which there exists a $[n, k, d]_q$ code.

(2) Find $K_q(n, d)$ the largest value of k for which there exists a $[n, k, d]_q$ code.

(3) Find $D_q(n, k)$ the largest value of d for which there exists a $[n, k, d]_q$ code.

A code of length $N_q(k, d)$, dimension k and minimum distance d is said to be *optimal* with respect to n. Similarly, codes with parameters $[n, K_q(n, d), d]_q$ and $[n, k, D_q(n, k)]_q$ are called optimal with respect to k and d. Values for $D_q(n, k)$ and small q can be found in [3].

The natural question which arises now is: "Do the basic parameters uniquely determine the error correcting and error detecting properties of the code?". To answer the question we have to consider more precisely the communication system which we use for the data transmission.

There is a transmitter which transmits codewords through a communication channel to the receiver. Suppose that v is the transmitted code word and w is the received word. The channel adds to the code word an *error vector* which is of the same length and has nonzero entries in the positions where errors occur, i.e. $w = v + e$.

A channel model is a description of the probability of receiving a vector y of length n when a vector x of the same length was transmitted. We say that the channel has no memory if the errors in different positions occur independently. The q-ary *symmetric channel without memory* (qSC) is a discrete channel with q-ary input, q-ary output and channel error probability p, where $0 \leq p \leq \dfrac{p}{(q-1)}$. Any symbol has probability $1-p$ of being received correctly and a probability $\dfrac{p}{(q-1)}$ of being transformed into each of the other $q-1$ symbols.

On the receive-site decoding is perfomed to a code word which is nearest to the reveived word in the Hamming distance. We assume that the error vector is always a coset leader. Following this procedure

1. we may find a unique code word v for which the Hamming distance $d(v,w)$ is minimal and decode the reveived word w to v.
We decode correctly in this case. Clearly the probability of correct decoding is given by

$$P_{corr} = \sum_{i=0}^{n} \alpha_i \left(\frac{p}{q-1}\right)^i (1-p)^{n-i}$$

and the probability of error by

$$P_{err} = 1 - P_{corr} = 1 - \sum_{i=0}^{n} \alpha_i \left(\frac{p}{q-1}\right)^i (1-p)^{n-i}.$$

2. We may detect an error if there are more than one codeword with minimal Hamming distance $d(v,w)$.
3. We decode incorrectly if the channel error have changed v in such a way that the closest code word to w is $v' \neq v$; i.e. we have an *undetectable error.*

Since the code is linear, an undetected error occurs (assuming the code is used for error detection) iff the error vector e is a nonzero code word. If i positions of the code word are disturbed, i.e. e has Hamming weight i, then the probability of this error pattern is $\left(\frac{p}{q-1}\right)^i (1-p)^{n-i}$ and the probability of an undetected error is given by

$$P_{ue}(C,p) = \sum_{i=1}^{n} A_i \left(\frac{p}{q-1}\right)^i (1-p)^{n-i}.$$

Let $P_{ue}^{(t)}(C,p)$ denote the probability of an undetected error after t error correction and $P_h(p)$ denote the probability that an undetectable error pattern in a coset of weight h occurs with $0 \leq h \leq t$. Let $Q_{h,l}$ be the number of vectors of weight l in the cosets of minimum weight h, excluding the coset leaders. Then (see [8], [9])

$$P_h(p) = \sum_{l=0}^{n} Q_{h,l} \left(\frac{p}{q-1}\right)^l (1-p)^{n-l}$$

and

$$P_{ue}^{(t)}(C,p) = \sum_{h=0}^{t} P_h(p).$$

In case we want to find an $[n,k]$ code for error detection or correction in some application, the best choice may be a code for which $P_{ue}^{(t)}(C,p)$ is minimal (*optimal code*), provided we know p. Therefore, it is useful to have some criteria which help to decide whether a given code is good for error detection. A code C is called *t-proper* (or *proper* when t=0 and the code is only used for error detection) if $P_{ue}^{(t)}(C,p)$ is monotonous and *t-good* if $P_{ue}^{(t)}(C,p) \leq P_{ue}^{(t)}(C,\frac{q-1}{q})$ for all $p \in [0,\frac{q-1}{q}]$. Clearly, if a code is proper then it is good. Unfortunately, in many cases the weight distribution of a code is extremly complex and we are not able to check these criteria. Discrete sufficient conditions for a linear $[n,k,d]_q$ code to be *t-good* or *t-proper* were derived by Dodunekova and Dodunekov [5].

Let $A_i^{(t)} = \sum_{h=0}^{t} Q_{h,i}$ for $i = t+1,\ldots,n$ be the weight distribution of the vectors in the cosets with coset leaders 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 *If*

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

for $l = t+1,\ldots,n$ then C is t-good for error correction.

Theorem *If*

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

for $l = t+2,\ldots,n$ 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.

3 Questions about error control performance of a linear code

An interesting question for linear codes with the same basic parameters (length, dimension, minimum distance and covering radius) is how precisely these parameters determine the error control performance of the code. To illustrate the problem we investigated 3 classes of binary linear codes and answer the following questions:

1. If a code is optimal according to one of functions $n_q(k,d)$, $K_q(n,d)$ and $D_q(n,k)$ is it also optimal with respect to the other two?
2. Do we get again nonequivalent codes if we extend two nonequivalent codes with a parity-check symbol?
3. Are there codes with the same basic parameters but different weight enumerators. Even more, are there nonequivalent codes with the same basic parameters and the same weight enumerators?
4. Are there codes which have the same weight distribution of coset leaders but different weight distributions?
5. Are the optimal codes in sense of error probability also optimal in sense of undetected error probability after t-error correction?
6. When two codes have the same covering and newton radii what are their numbers of unique coset leaders for cosets with weights greater than t?
7. (Research Problem 5.1 in [10]). To what extend do the numbers α_i of a code determine the equivalent numbers of the dual code?

4 On the performance of binary [15,3,7], [15,3,8] and [16,3,8] codes

To demonstrate how different parameters of linear codes affect their performance we will use three classes of binary codes with parameters $[15,3,7]$, $[15,3,8]$ and $[16,3,8]$. In [6] Fontaine and Peterson showed that there are two $[15,3,7]$ codes, one optimal w.r.t. P_{err} if the channel error probability is small ($p \leq 0.307$), the other if it is large ($p \geq 0.307$). For this reason we decided to investigate the full class of $[15,3,7]$ codes and related to them the $[16,3,8]$ codes which are obtained by adding a parity-check symbol and thirdly the class of $[15,3,8]$ codes (which are distance-optimal).

By [3] and [4] we have $n_2(3,7)=13,\ n_2(3,8)=14,\ D_2(15,3)=D_2(16,3)=8,\ K_2(15,7)=K_2(16,8)=5,\ K_2(15,8)=4$. Hence

(i) the $[15,3,7]$ codes are not optimal for any of the three functions $D_2(n,k), N_2(k,d)$ and $K_2(n,d)$.

(ii) the $[15,3,8]$ and $[16,3,8]$ codes are optimal with respect to $D_2(n,k)$ but not optimal with respect to the other two functions.

Using the computer package Q-EXTENSION [2] all nonequivalent $[15,3,7]$ codes (17 codes), $[16,3,8]$ codes (12 codes) and $[15,3,8]$ codes (3 codes) were found. For all codes the weight distributions, biweight enumerators, coset leader weight distributions, weight distribution of all cosets, automorphism groups, covering and Newton radii were computed. The results are presented in the tables bellow. In order to save space, the columns of the generator matrices of the codes are written as the decimal digits which binary representation is the corresponding column. In the third column we have the automorphism groups and in the fourth column the weight enumerators. In the last column of the first table we stated the numbers of the corresponding codes from the second table obtained by adding a parity-check bit. Note that there are nonequivalent $[15,3,7]$ codes which extend to a unique $[16,3,7]$ code. For example codes with numbers 1, 2 and 16 from Table 1 extend to the code number 1 from Table 2.

It is also seen from the tables that almost all codes with the same n,k,d have different weight enumerators. This means that they may have different values for the undetected error probability $P_{ue}^{(t)}(C,p)$ after t error correction. There are however nonequivalent codes with the same weight enumerators. Such are pairs of codes with numbers 5,6; 8,9; 13,14 from Table 1 and 4,5; 9,10 from Table 2. But for all the codes from the tables the biweight enumerators are different.

Table 1. $[15,3,7]$ codes.

Num	Generator matrix	AUT	Weight enumerator	EQU
1	773333666622124	13824	$3z^7, 2z^8, 1z^{10}, 1z^{13}$	1
2	777333666222124	10368	$2z^7, 3z^8, 1z^9, 1z^{13}$	1
3	773333666224124	3456	$3z^7, 1z^8, 1z^9, 1z^{10}, 1z^{12}$	4
4	773333666624124	9216	$3z^7, 2z^8, 1z^{11}, 1z^{12}$	3
5	777333666224124	10368	$2z^7, 2z^8, 2z^9, 1z^{12}$	6
6	773335666222124	3456	$2z^7, 2z^8, 2z^9, 1z^{12}$	4
7	733335666224124	3456	$3z^7, 1z^8, 2z^{10}, 1z^{11}$	4
8	773331666224124	3456	$2z^7, 2z^8, 1z^9, 1z^{10}, 1z^{11}$	5
9	773335662224124	1152	$2z^7, 2z^8, 1z^9, 1z^{10}, 1z^{11}$	4
10	777331662224124	9216	$2z^7, 3z^8, 2z^{11}$	3
11	773335666224124	1728	$1z^7, 3z^8, 2z^9, 1z^{11}$	4
12	773331662244124	10368	$3z^7, 1z^9, 3z^{10}$	9
13	773335662244124	1728	$2z^7, 1z^8, 2z^9, 2z^{10}$	9
14	773351662224124	3072	$2z^7, 1z^8, 2z^9, 2z^{10}$	10
15	773351666224124	1152	$1z^7, 2z^8, 3z^9, 1z^{10}$	9
16	333311666644124	41472	$3z^7, 2z^8, 1z^9, 1z^{14}$	1
17	777711222444124	497664	$3z^7, 3z^8, 1z^{15}$	12

Table 2. $[16, 3, 8]$ codes.

Num	Generator matrix	AUT	Weight enumerator
1	7773333666622124	82944	$5z^8, 1z^{10}, 1z^{14},$
2	7773335666222124	31104	$3z^8, 3z^9, 1z^{13},$
3	7733331666624124	73728	$5z^8, 2z^{12},$
4	7733335666224124	6912	$4z^8, 2z^{10}, 1z^{12},$
5	7773331666224124	41472	$4z^8, 2z^{10}, 1z^{12},$
6	7773335666224124	20736	$2z^8, 4z^9, 1z^{12},$
7	7733351666224124	3456	$2z^8, 3z^9, 1z^{10}, 1z^{11},$
8	7733355662224124	9216	$3z^8, 2z^9, 2z^{11},$
9	7733351662244124	10368	$3z^8, 4z^{10},$
10	7733551662224124	36864	$3z^8, 4z^{10},$
11	7733551666224124	9216	$1z^8, 4z^9, 2z^{10},$
12	7777111222444124	7962624	$6z^8, 1z^{16},$

Table 3. $[15, 3, 8]$ codes

Num	Generator matrix	AUT	Weight enumerator
1	777333566622124	31104	$6z^8, 1z^{12},$
2	773335166624124	4608	$5z^8, 2z^{10},$
3	773355166224124	9216	$3z^8, 4z^9,$

We compared the codes w.r.t. the undetected error probability after t-error correction. Since the codes have minimum distances 7 or 8 we have $t = 0, 1, 2, 3$. The results are as follows

$[15, 3, 7]_2$ codes:
The best code is N 15 for all $p \in (0, 1/2]$ and $t = 0, 1, 2, 3$.
$[16, 3, 8]_2$ codes:
The best code is N 11 for all $p \in (0, 1/2]$ and $t = 0, 1, 2, 3$.
$[15, 3, 8]_2$ codes:
The best code is N 3 for all $p \in (0, 1/2]$ and $t = 0, 1, 2, 3$.

It is also interesting to compare the codes from the three classes w.r.t. the error probability. To do this we need the weight enumerators of the coset leaders. This information is presented in the table below. As the covering radius of a code is the largest weight in the set of coset leaders we have also determined this parameter. With a star we marked codes which have the smallest covering radius among the codes with a given length and dimension. In the last column the values of the Newton radii are given. We should note that there are codes which have different weight enumerators, but have equal coset leaders weight enumerators. This means that they have different values for $P_{ue}^{(t)}(C, p)$, but the same values for P_{err}.

Results for P_{err} in case of $[15, 3, 7]$ codes are already known from [6] and we only checked them. For $p \leq 0.307$ the best code is N 14. For $p > 0.307$ the best codes are N 12, N 13 and N 15 as they have the same coset leaders weight enumerators.

$[16, 3, 8]_2$ codes
The best code is N 11 for all $p \in (0, 1/2]$.
$[15, 3, 8]_2$ codes
The best code is N 3 for all $p \in (0, 1/2]$.

As it is noted by Slepian [12] in 1956 a $[7, 3, 3]$ code is better than the $[7, 3, 4]$ simplex code w.r.t. the error probability. If we compare the best $[15, 3, 7]$ codes with the best $[15, 3, 8]$ code we obtain that suitable $[15, 3, 7]$ codes are better for $p > 0.307$. So, the code which is superior by minimum distance is i.g. not w.r.t. error probability.

Table 4. Coset leaders weight enumerators and the Newton radii.

Code	α_0	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	ν
$[15,3,7]$										
1*	1	15	105	455	1192	1572	756			6
2*	1	15	105	455	1192	1572	756			6
3*	1	15	105	455	1226	1682	612			6
4	1	15	105	455	1192	1656	600	72		5
5*	1	15	105	455	1225	1647	648			6
6*	1	15	105	455	1226	1682	612			6
7*	1	15	105	455	1226	1682	612			6
8*	1	15	105	455	1225	1647	648			6
9*	1	15	105	455	1226	1682	612			6
10*	1	15	105	455	1192	1656	600	72		5
11*	1	15	105	455	1226	1682	612			6
12*	1	15	105	455	1260	1693	567			6
13*	1	15	105	455	1260	1693	567			6
14	1	15	105	455	1261	1711	500	48		5
15*	1	15	105	455	1260	1693	567			6
16*	1	15	105	455	1192	1572	756			6
17	1	15	105	455	1158	1498	702	162		5
$[16,3,8]$										
1*	1	16	120	560	1647	2764	2328	756		6
2*	1	16	120	560	1716	3079	2430	270		6
3	1	16	120	560	1647	2848	2256	672	72	5
4*	1	16	120	560	1681	2908	2294	612		6
5*	1	16	120	560	1680	2872	2295	648		6
6*	1	16	120	560	1750	3216	2286	243		6
7*	1	16	120	560	1750	3231	2298	216		6
8*	1	16	120	560	1716	3194	2345	240		6
9*	1	16	120	560	1715	2953	2260	567		6
10	1	16	120	560	1716	2972	2211	548	48	5
11*	1	16	120	560	1785	3298	2196	216		6
12	1	16	120	560	1613	2656	2200	864	162	5
$[15,3,8]$										
1	1	15	105	455	1159	1497	783	81		5
2	1	15	105	455	1192	1506	750	72		5
3	1	15	105	455	1261	1711	500	48		5

When we look at the results for the best codes in sense of $P_{ue}^{(t)}(C,p)$ and P_{err} we see that for the three classes of investigated codes the codes which are best according to the first function are also best according to the second. It will be interesting to know whether this is true in general?

It is seen from the above table that there are codes which have the same covering and newton radii. If we compare them by the number of unique coset leaders (UCL) for cosets with weights greater than t we obtain that they differ. The best codes in this sense are those which have the largest number of UCL. The results are as follows

$[15, 3, 7]_2$ codes:
Codes with $R = 6$ and $\nu = 6$. For cosets of weight 4 - code N 12 (1260 UCL), for cosets of weight 5 - code N 5 (1416 UCL), for cosets of weight 6 - code N 16 (324 UCL).
Codes with $R = 7$ and $\nu = 5$. For cosets of weights 4 and 5 - code N 14 (1227 and 1310 UCL respectively).

$[16, 3, 8]_2$ codes:
Codes with $R = 7$ and $\nu = 6$. For cosets of weight 4 and 5 - code N 11 (1750 and 2792 UCL respectively), for cosets of weight 6 - code N 2 (1080 UCL).
Codes with $R = 8$ and $\nu = 5$. For cosets of weights 4 and 5 - code N 10 (1613 and 1848 UCL respectively).

$[15, 3, 8]_2$ codes:
For cosets of weight 4 and 5 - code N 3 (1158 and 1152 UCL respectively).

Another interesting fact mentioned already in [1] can also be seen here. There are codes which have identical weight enumerators but different coset weight enumerators. Such codes are $[15, 3, 7]$ codes with numbers 5,6; 8,9; 13,14 and $[16, 3, 8]$ codes with numbers 4,5; 9,10. The weight enumerator of a particular coset reveals how well each word in that coset is approximated by the set of codewords.

We finish this section with an interesting example, which helped us to solve the research problem 5.1 stated in [10](Chapter 5, p. 132). The problem is the following:

Let C be a linear code. Let α_i be the number of coset leaders of C of weight i and α'_i the corresponding number for the dual code $C^{\perp}$. To what extent do the numbers $\{\alpha_i\}$ determine $\{\alpha'_i\}$?

It turns out that the weight distribution of a code does not determine the weight distribution of the dual code. In the table bellow are listed the enumerators of the coset leaders of the duals of all $[15, 3, 7]$ codes. These are

$[15,12]$ codes. It can be seen that $[15,3,7]$ codes with numbers 1,2 and 16 have the same weight enumerator of coset leaders, but not their duals. More precisely, the dual codes of numbers 1 and 2 have the same enumerator, but code number 16 has adifferent one. This is true also for codes with numbers 3,6,7,9,11 and 12,13,15.

Table 5. Coset leaders weight enumerators of $[15,12]$ codes

Num	α_0	α_1	α_2	Num	α_0	α_1	α_2	Num	α_0	α_1	α_2
1	1	6	1	7	1	7		13	1	7	
2	1	6	1	8	1	6	1	14	1	7	
3	1	6	1	9	1	7		15	1	7	
4	1	6	1	10	1	6	1	16	1	5	2
5	1	6	1	11	1	7		17	1	4	3
6	1	7		12	1	6	1				

5 Conclusion

We investigated to a large extent three classes of binary linear codes and compared their error correcting and error detecting performances. It is shown that codes with the same basic parameters like length, dimension, minimum distance and covering radius may have different error correcting and error detecting performance. As a by-product we solve an open problem from [10].

In order to save space, we included only extracts of the results of the investigations. All numerical data can be found in `http://www.moi.math.bas.bg/~tsonka`.

6 Acknowledgement

This work was initiated during a visit of S. M. Dodunekov in the Institute for Algebra and Geometry of the Otto-von-Gruericke-University Magdeburg. He would like to thank his hosts for the nice working conditions and hospitality.

References

[1] E. R. Berlecamp and L. R. Welch, Weight distributions of the cosets of the (32,6) Reed-Muller code, *IEEE Trans. Inform. Theory*, vol. 18, No. 1, Jan., pp. 203-207, 1972.

[2] I. Bouyukliev, 'Q-EXTENSION' - strategy in algorithms, *Proc. of the International Workshop on Algebraic and Combinatorial Coding Theory*, Bansko, pp. 84-88, 2000.

[3] A. E. Brouwer, Minimum distance bounds for linear codes over GF(q) (q=2,3,4,5,7,8,9), lincodbd server, aeb@cwi.nl, Eindhoven University of Technology, Eindhoven, The Netherlands.

[4] A. E. Brouwer, Bounds on the size of linear codes, In: V. S. Pless and W. C. Huffman, Eds., Handbook of Coding Theory, vol. 1, Chapter 4, pp. 295-461.

[5] 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, Sozopol, Bulgaria, pp. 62-67, 1998.

[6] A. B. Fontaine and W. W. Peterson, Group code equivalence and optimum codes, *IRE Trans.*, IT-5, Special Supplement, pp. 60-70, 1959.

[7] T. Helleseth, T. Kløve and V. Levenshtein, The Newton radius of equidistant codes, *Proc. IEEE Intern. Symp. on Inform. Theory and its Applications*, Victoria, B.C., Canada, Sept. 17-30, pp. 721-722, 1996.

[8] T. Kasami and S. Lin, On the probability of undetected error for the Maximum Distance Separable codes, *IEEE Trans. Communi. 32*, pp. 998-1006, 1984.

[9] F. J. MacWilliams, A theorem on the distribution of weights in a systematic code, *The Bell System Tech. J. 42*, pp. 79-94, 1963.

[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting codes*, North-Holland Publishing Company, Amsterdam, London, New York, Tokyo, Ninth impression, 1996.

[11] http://werner-heise.de/lit_IC.html, Theory of Coding and Information. List of Textbooks.

[12] D. Slepian, A class of binary signaling alphabets, *BSTJ 35*, pp. 203-234, Jan. 1956.