# Some results for linear binary codes with minimum distance 5

Iliya Bouyukliev [1]
Institute of Mathematics, Bulgarian Academy of Sciences,
P.O.Box 323, 5000 V. Tarnovo, (e-mail: iliya@moi.math.bas.bg)
Zlatko Varbanov
Department of Mathematics and Informatics, Veliko Tarnovo University, 5000 Veliko Tarnovo, (e-mail:vtgold@yahoo.com)

**Abstract**

We prove that a linear binary code with parameters $[34, 24, 5]$ does not exist. Also, we characterize some codes with minimum distance 5.

## 1 Introduction

Let $F_2^n$ be the $n$-dimensional vector space over the Galois field $F_2 = GF(2)$. The Hamming distance between two vectors of $F_2^n$ is defined to be the number of coordinates in which they differ. A linear binary $[n, k, d]$-code is a $k$-dimensional linear subspace of $F_2^n$ with minimum Hamming distance $d$. The *weight* of the vector $c$ ($wt(c)$) is the number of nonzero entries in $c$.

A central problem in coding theory is that of optimizing one of the parameters $n, k$ and $d$ for given values of the other two. Two versions are:

*Problem 1:* Find $d_2(n, k)$, the largest value of $d$ for which there exists binary $[n, k, d]$-code.

*Problem 2:* Find $k_2(n, d)$, the largest value of $k$ for which there exists binary $[n, k, d]$-code.

Another important problem is

*Problem 3:* Characterize all binary $[n, k_2(n, d), d]$ codes with given values of $n$ and $d$.

Bounds for $d_2(n, k)$ were presented in [2]. The exact values of $k_2(n, d)$ are known for $d \leq 4$ and for $d = 5$, $n \leq 33$.

In this paper, we investigate linear binary codes with minimum distance $d = 5$.

We have two basic results:

1. A linear binary code with parameters $[34, 24, 5]$ does not exist and $k_2(34, 5) = 23$.
2. There are at least four nonequivalent codes with parameters $[33, 23, 5]$.

The bounds for binary codes with minimum distance 5 and 6 are strongly related because of the parity check bits in binary case. Some results for $d = 5$ and $d = 6$ have been presented in [3], [6], [7], [8], [9], etc. A linear binary $[33, 23, 5]$ code was found in [3].

In this research, we use some theoretical and software tools. These tools are discussed in section 2. In section 3 we give an algorithm for constructing of codes with fixed dual distance and some other restrictions. Section 4 contains new results for codes with minimum distance 5.

[1]Partially supported by the Bulgarian National Science Fund under Contract MM1304/2003.

## 2 Preliminaries and tools

Let $(u,v)=\sum_{i=1}^{n} u_i v_i \in F_2$ for $u=(u_1,\ldots,u_n), v=(v_1,\ldots,v_n)\in F_2^n$ be the inner product in $F_2^n$ and $C$ be a linear binary $[n,k,d]$ code.

**Definition 1** The *dual code* $C^\perp$ of the code $C$ is $C^\perp=\{v\in F_q^n \mid (u,v)=0, \text{ for all } u\in C\}$.

It is known that $C^\perp$ is an $[n,n-k,d^\perp]$ code. Also, $d^\perp$ is called *dual distance* of the code.

**Definition 2** Let $G$ be a generator matrix of a linear binary $[n,k,d]$ code $C$. Then the *residual code* $Res(C,c)$ of $C$ with respect to a codeword $c$ is the code generated by the restriction of $G$ to the columns where $c$ has a zero entry. If $w=wt(c)$ we will also use the notation $Res_w(C)$.

A lower bound on the minimum distance of the residual code is given by

**Lemma 2.1** [4]: Suppose $C$ is a binary $[n,k,d]$-code and suppose $c\in C$ has weight $w$, where $d>w/2$. Then $Res(C,c)$ is an $[n-w,k-1,d']$-code with $d'\geq d-w+\lceil w/2\rceil$.

Let $C$ be a binary $[n,k,d]$ code and $B_i$ denote the number of codewords of weight $i$ in its dual code $C^\perp$.

**Lemma 2.2** [5]: For a binary $[n,k,d]$ code $B_i=0$ for each value of $i$ (where $1\leq i\leq k$) such that there does not exist a binary $[n-i,k-i+1,d]$ code.

One of our tools is Q-Extension. The main problem which we solve in some cases with this program is the problem to construct all inequivalent linear codes with length $n$, dimension $k$, and minimum distance $d$.

If we can fix a part of the generator matrix, we will consider less cases. If the fixed part is greater, the number of the considering codes which we will investigate for equivalence in the end will be smaller. This fixed part can be the identity matrix of order $k$, since any code has a generator matrix in systematic form or generator matrix of residual code. More information on this topic can be found in [1]. In our research for some specific cases we use another algorithm for constructing of codes.

## 3 An algorithm for constructing of codes with $d^\perp > 2$

Let $C$ be a linear binary code with parameters $[n,k,d]$ and dual distance $(d^\perp)$ greater than 2. Let $C_r=[n-d,k-1,\geq\lceil d/2\rceil]$ be its residual $Res_d(C)$ code and let a code with parameters $[n-d+1,k-1,d']$ and dual distance $d^\perp$ does not exist. We consider a generator matrix $G$ of the code $C$ in the following form:

$$G=\begin{pmatrix} 0..0 & 1..1 \\ G_r & X \end{pmatrix} \tag{1}$$

Obviously, there are no $d^\perp-1$ columns in $G$ which are linearly dependent. We can obtain $G$ from $G_r$ adding $d$ vectors with length $k$ in the form $(1,a_2,\ldots,a_k)^t$. If we add $1,2,\ldots d$ vectors to $G_r$ then the minimum distance of the code $C$ will be $1,2\ldots d$. The goal is: to find all possibilities for $X$ (all columns from $n-d+1$ to $n$ in $G$). Doing that we check only the dual distance not the minimum distance.

The problem for constructing $G$ if we know $G_r$ can be defined as the following combinatorial problem - to find all vectors of length $k$ in the form $(1, a_2, \ldots, a_k)^t$ such that there are not $d^{\perp} - 1$ vectors which are linearly dependent in the set of these vectors and the first $n - d$ vectors.

We present a back-track search. Let $M$ be a set of vectors of length $k$ such that no $d^{\perp} - 1$ between them are linearly dependent. In the beginning we have the set $M = M_0$ of $n - d$ vectors from the generator matrix of the residual code $C_r$.

In the step $t$ we find the set $S_t$ which consists of all proper vectors for column $n - d + t$ if we have fixed the first $n - d + t - 1$ columns.

Obviously, in the first step, we can take $S_1 := \{v\}$, where $v$ is an arbitrary vector from $V^k$.

We will use the following notations for data variable types:

**S** is an array of set of vectors of length $k$.

**Tree** is an array of integers. This variable defines in step $t < d$ the set $M$ in the following way. $M$ contains $M_0$ and the vector with number tree[1]+1 in set $S_1$, the vector with number tree[2]+1 in set $S_2$, ..., the vector with number tree[t]+1 in set $S_t$. If $t = d$ we have to use all vectors from $S_d$.

In procedure **find_S** we determine the set $S_t$ if we know $S_{t-1}$ and tree[lev] (the set $M$ in step $t - 1$).

```
const    max = d;
var      lev:integer;
         S:array[1..max] of set of vectors;
         tree:array[1..max] of integer;
begin
   lev:=1; tree[1]:=1; fix S[1];
   while (lev>0) do
   begin
      if (tree[lev]>0) and (lev<max) then
      begin
       if ((lev>2) and (S[lev][tree[lev]]<S[lev-1][tree[lev-1]+1])) or (lev ≤ 2) then
         begin
            tree[lev]:=tree[lev]-1;
            lev:=lev+1; find_S;
            if lev= max then printM;
            tree[lev]:=|S[lev]|;
         end
         else tree[lev]:=tree[lev]-1;
      end (* if (tree[lev]>0) and (lev<max) *)
      else
         lev:=lev-1;
   end;
end.
```

In the level $t, t > 2$, we can take only these vectors which are smaller than the vector S[t-1][tree[t-1]+1] (selected in previous level) under the naturally lexicographic ordering - row 7 in the algorithm.

Actually we use this algorithm in more general case.

# 4 Structure of the codes

## 4.1 Nonexistence of linear binary code with parameters $[34, 24, 5]$

Let $C$ be a putative linear binary code with parameters $[34, 24, 5]$. Lemma 2.2 and the table in [2] give us that the dual distance $d^{\perp}$ of the code $C$ is greater than 10. We will consider $C^{\perp}$ which is $[34, 10, 11]$ or $[34, 10, 12]$ code.

In the first case, let $C$ be an $[34, 10, 11]$ code. From Lemma 2.1, the residual code $Res_{11}(C)$ is $[23, 9, d']$ code, where $6 \geq d' \geq 8$ and dual distance 5. It is known that there is a unique binary $[23, 14, 5]$ code [9]. Hence, there exists a unique $[23, 9, d']$ code with dual distance 5. Its minimum distance $d'$ is 8.

After the extension of this unique $[23, 9, 8]$ code we obtain that:

– There are 672 nonequivalent binary $[30, 10, 7]$ codes with $d^{\perp} = 5$.

– Binary codes with parameters $[31, 10, 8]$, $[32, 10, 9]$, $[33, 10, 10]$, $[34, 10, 11]$ and $d^{\perp} = 5$ do not exist.

In the second case we will consider a binary $[34, 10, 12]$ code $C_{34}$. Its residual code $Res_{12}(C_{34})$ is $[22, 9, 6]$, $[22, 9, 7]$ or $[22, 9, 8]$ code with dual distance 5.

To construct these codes we can start from the codes with parameters $[16, 8, \geq 3]$, $[15, 8, 4]$ and $[14, 8, 4]$. It is easy to find that there exist a unique $[16, 8, 5]$ code, six $[15, 8, 4]$ codes, and three $[14, 8, 4]$ codes with dual distance 5.

The extension of these codes give us:

– There exist 101 nonequivalent binary codes with parameters $[22, 9, 6]$ and $d^{\perp} = 5$.

– There exist 21 nonequivalent binary codes with parameters $[22, 9, 7]$ and $d^{\perp} = 5$.

– Binary code with parameters $[22, 9, 8]$ and $d^{\perp} = 5$ does not exist.

In the end, we obtain that:

– There are 2686 nonequivalent binary $[31, 10, 9]$ codes with $d^{\perp} = 5$.

– Binary codes with parameters $[32, 10, 10]$, $[33, 10, 11]$, $[34, 10, 12]$ with $d^{\perp} = 5$ do not exist.

We can conclude:

**Theorem 4.1** Linear binary code with parameters $[34, 24, 5]$ does not exist and $k_2(34, 5) = 23$.

**Proposition 4.2** Linear binary codes with parameters $[33, 10, 10]$ and $[33, 10, 11]$ with $d^{\perp} = 5$ do not exist.

## 4.2 Linear binary codes with parameters $[33, 23, 5]$

Let $C$ be a linear binary code with parameters $[33, 23, 5]$. From Lemma 2.2, Proposition 4.2 and the table in [2] it follows that the dual distance $d^{\perp}$ of the code $C$ is 12. We consider its dual $[33, 10, 12]$ code.

Let $C_{33}$ be a linear binary code with parameters $[33, 10, 12]$ and dual distance 5. Its residual code $Res_{12}(C_{33})$ is $[21, 9, 6]$, $[21, 9, 7]$ or $[21, 9, 8]$ code.

To construct these codes we can start from the codes with parameters $[15, 8, \geq 3]$, $[14, 8, 4]$ and $[13, 8, 4]$. It is easy to find that there exist six $[15, 8, 4]$ codes, three $[14, 8, 4]$ codes and a unique $[13, 8, 4]$ code with dual distance 5.

After the extension of these codes we obtain that:

– There exist 1696 nonequivalent binary $[21, 9, 6]$ codes with $d^{\perp} = 5$.

– Binary codes with parameters $[21, 9, 7]$ and $d^{\perp} = 5$ do not exist.

– There exists a unique binary $[21, 9, 8]$ code with $d^{\perp} = 5$.

The last code cannot be extended to the code $C_{33}$.

After the extension of about a half of the $[21, 9, 6]$ codes, we obtain four nonequivalent codes with parameters $[33, 10, 12]$ and $d^{\perp} = 5$. This calculation took about ten days of CPU time on a 1800 MHz PC.

Therefore, we obtain:

**Proposition 4.3** There exist at least four nonequivalent linear binary codes with parameters $[33, 23, 5]$.

## References


[1] I. Bouyukliev, J. Simonis, Some New Results for Optimal Ternary Linear Codes, IEEE Transactions on Information Theory 48 (4) (2002), 981–985.

[2] A.E.Brouwer, "Bounds on the size of linear codes", in *Handbook of Coding Theory*, Edited by V.Pless and W.C.Huffman, Elsevier, Amsterdam etc., ISBN:0-444-50088-X, 1998.

[3] C.L. Chen, "Construction of some binary linear codes of minimum distance five", IEEE Trans. Inform. Theory 37 (1991), 1429-1432.

[4] S. Dodunekov, "Minimal block length of a $q$-ary code with prescribed dimension and code distance", *Problems of Inform. Transmission*, vol. 20, No. 4, (1984), pp. 239-249.

[5] R. Hill and D. E. Newton, "Optimal ternary linear codes," *Designs, Codes and Cryptography* vol. 2, (1992), pp. 137–157. 1992.

[6] J.Simonis, "Binary even [25,15,6] codes do not exist, IEEE Trans.Inform.Theory 33 (1987), 151-153.

[7] J.Simonis, A Description of the [16,7,6] codes, Lecture Notes in Computer Science, Vol.508, Springer, Berlin, (1991), pp.24-35.

[8] J.Simonis, The [18,9,6] code is unique, Discrete Math. 106/107 (1992), pp. 439-448.

[9] J. Simonis, "The [23,14,5] Wagner code is unique", *Discrete Mathematics*, 213, (2000), pp. 269-282.