Serdica

Bulgariacae mathematicae publicationes

Сердика

Българско математическо списание

SERDICA — Bulgaricae
mathematicae publicationes
18 (1992) 224-231

BINARY LINEAR BLOCK CODES WITH IMPROVED MINIMUM DISTANCE BOUNDS

R. N. DASKALOV

ABSTRACT. The nonexistence of binary linear $[n,k,d]$-codes having parameters $[60,18,22]$,$[64,18,24]$,$[72,18,28]$, $[93,19,38]$,$[72,29,22]$, $[76,29,24]$,$[85,30,28]$,$[105,30,38]$, $[104,48,28]$ and $[101,53,24]$ is proven and as a consequence 194 minimum distance upper bounds in Verhoeff's table [8] have been improved.

1. Introduction.

Let $GF(2)$ denote the Galois field of two elements, and let $V(n,2)$ denote the vector space of all ordered n-tuples over $GF(2)$. A linear code C of length n and dimension k over $GF(2)$ is a k-dimensional subspace of $V(n,2)$; it is denoted by $[n,k]$-code.

A linear $k \times n$ matrix whose rows form a basis of a linear code C is called a generator matrix of the code. Elements of the subspace are called codewords.

For an $[n,k]$-code C we define its dual code, denoted by $C^{\perp}$, as the set of vectors of $V(n,2)$ which are orthogonal to every codeword of C. The generator matrix of $C^{\perp}$ is called parity check matrix of C.

A binary linear code of length n, dimension k, and minimum distance at least d is called an $[n,k,d]$-code. Define $d(n,k)$ as the maximum value of d for which there exists a binary linear $[n,k,d]$-code.

T.Verhoeff [8] has recently provided an updated table of bounds on $d(n,k)$ for $1 \le k \le n \le 127$. We improve on some of the upper bounds given in that table by proving the nonexistence of codes with certain parameters.

In Section 2 we state the necessary preliminary definitions and results.

In Section 3 we improve the best known upper bounds on $d(n,k)$ in ten essentially different cases. The results give rise to upper bounds on $d(n,k)$ for 194 values of (n,k).

Our method aims at assuming the existence of a certain code and obtaining a contradiction to MacWilliams' identities, similarly as in [1], [3], [4], [5], [7].

2. Preliminary results.

The Hamming weight of a vector x, denoted by $wt(x)$, is the number of nonzero entries in x. For a linear code the minimum distance is equal to the smallest of the weights of the nonzero codewords.

Let G be the generator matrix of an $[n, k, d]$-code C.

Definition. *The residual code of C with respect to $c \in C$ is the code generated by the restriction of G to the columns where c has a zero. The residual code of C with respect to $c \in C$ is denoted by $Res(C, c)$ or $Res(C, w)$ if the Hamming weight of c is w.*

Lemma 2.1. (the MacWilliams identities) [6, p.129] *Let C be an $[n, k, d]$-code and A_i and B_i denote the number of codewords of weight i in the code C and in its dual code $C^\perp$ respectively. Then*

$$\sum_{i=0}^{n} K_t(i) A_i = 2^k B_t, \quad \text{for } 0 \le t \le n,$$

where

$$K_t(i) = \sum_{j=0}^{t} (-1)^j \binom{n-i}{t-j} \binom{i}{j}.$$

Lemma 2.2. [6, p.592] *Suppose C is an $[n, k, d]$-code whose dual code has minimum distance $d^\perp$. Then there exists an $[n - d^\perp, k - d^\perp + 1, d]$-code.*

Lemma 2.3. [7] *Let C be an $[n, k, d]$-code and $x \in C$, $wt(x) = w$ and $w < 2d$. Then $Res(c; w)$ has parameters $[n - w, k - 1, d^\circ]$, where $d^\circ \ge d - \lfloor w/2 \rfloor$. (By $\lfloor x \rfloor$ the greatest integer $\le x$ is denoted.)*

The following lemmas 2.4-2.7 are well known.

Lemma 2.4. *Suppose that an $[n, k, d]$-code does not exist. Then an $[n+2d, k+1, 2d]$-code C does not exist.*

Proof. By Lemma 2.3, $Res(C, 2d) = [n, k, d]$-code.

Lemma 2.5. *If there exists an $[n, k, d]$-code C with d even, then there exists an $[n, k, d]$-code whose codewords have even weights (just puncture C and then add an overall parity check).*

Lemma 2.6.

(a) If $d(n, k) \le d$, where d is odd, then $d(n - 1, k) \le d - 1$;

(b) $d(n + 1, k + 1) \le d(n, k)$.

Lemma 2.7. *If x and y are distinct codewords in an $[n,k,d]$-code, then $wt(x)+wt(y)\le 2n-d$.*

Proof. The $3\times n$ matrix consisting of rows x, y and $x+y$ has at most two 1's in each column, and so

$$wt(x)+wt(y)+wt(x+y)\le 2n.$$

Since $wt(x+y)\ge d$, the result follows.

Theorem 2.1. $d(67,14)\le 27$.

Proof. Suppose that there exists a $[67,14,28]$-code C. By [3] a $[61,9,28]$-code does not exist and by Lemma 2.2 the dual code $C^{\perp}$ is a $[67,53,7]$-code. By [8] a $[67,53,7]$-code does not exist which is a contradiction. □

Corollary 2.1. $d(66,14)\le 26$.

3. New Upper Bounds on $d(n,k)$

In each of the theorems of this section, we shall assume that a certain $[n,k,d]$-code with d even exists. By Lemma 2.5, there is no loss in assuming that the code is an even-weight one, i.e. that all the codewords are of an even weight.

We shall denote MacWilliams' identities for $t=0,1,2,\dots$ by e_t (see Lemma 2.1).

Theorem 3.1. $d(60,18)\le 21$.

Proof. Suppose that there exists an even-weight $[60,18,22]$-code C. By [8] a $[54,13,22]$-code does not exist and by Lemma 2.2, $d^{\perp}\ge 7$. By [8] $Res(C,26)=[34,17,9]$-code and $Res(C,34)=[26,17,5]$-code do not exist and so $A_{26}=A_{34}=0$. □

Although only the first six MacWilliams' identities are free of B_1, B_2, B_3, B_4, B_5 and B_6, the first seven identities seem to be useful. Hence the MacWilliams identities (Lemma 2.1) for $t=0,1,2,3,4,5,6,7$ give the following equations:

$$\begin{aligned}
e_0: &\quad A_{22}+A_{24}+A_{28}+A_{30}+A_{32}+A_{36}+A_{38}+A_{40}+A_{42}+A_{44}\\
+&\quad A_{46}+A_{48}+A_{50}+A_{52}+A_{54}+A_{56}+A_{58}+A_{60}=262143
\end{aligned}$$

$$\begin{aligned}
e_1: &\quad 16.A_{22}+12.A_{24}+4.A_{28}-4.A_{32}-12.A_{36}-16.A_{38}-20.A_{40}\\
-&\quad 24.A_{42}-28.A_{44}-32.A_{46}-36.A_{48}-40.A_{50}-44.A_{52}-48.A_{54}\\
-&\quad 52.A_{56}-56.A_{58}-60.A_{60}=-60
\end{aligned}$$

$$\begin{aligned}
e_2: &\quad 98.A_{22}+42.A_{24}-22.A_{28}-30.A_{30}-22.A_{32}+42.A_{36}+98.A_{38}\\
+&\quad 170.A_{40}+258.A_{42}+362.A_{44}+482.A_{46}+618.A_{48}+770.A_{50}\\
+&\quad 938.A_{52}+1122.A_{54}+1322.A_{56}+1538.A_{58}+1770.A_{60}=-1770
\end{aligned}$$

$$\begin{aligned}
e_3: \quad & 208.A_{22} - 68.A_{24} - 108.A_{28} + 108.A_{32} + 68.A_{36} - 208.A_{38} \\
- \quad & 740.A_{40} - 1592.A_{42} - 2828.A_{44} - 4512.A_{46} - 6708.A_{48} - 9480.A_{50} \\
- \quad & 12892.A_{52} - 17008.A_{54} - 21892.A_{56} - 27608.A_{58} - 34220.A_{60} = -34220
\end{aligned}$$

$$\begin{aligned}
e_4: \quad - \quad & 589.A_{22} - 813.A_{24} + 211.A_{28} + 435.A_{30} + 211.A_{32} - 813.A_{36} \\
- \quad & 589.A_{38} + 1235.A_{40} + 5811.A_{42} + 14547.A_{44} + 29107.A_{46} \\
+ \quad & 51411.A_{48} + 83635.A_{50} + 128211.A_{52} + 187827.A_{54} + 265427.A_{56} \\
+ \quad & 364211.A_{58} + 487635.A_{60} = -487635
\end{aligned}$$

$$\begin{aligned}
e_5: \quad - \quad & 4256.A_{22} - 1176.A_{24} + 1400.A_{28} - 1400.A_{32} + 1176.A_{36} \\
+ \quad & 4256.A_{38} + 3496.A_{40} - 9744.A_{42} - 49224.A_{44} - 134848.A_{46} \\
- \quad & 293688.A_{48} - 561008.A_{50} - 981288.A_{52} - 1609248.A_{54} \\
- \quad & 2510872.A_{56} - 3764432.A_{58} - 5461512.A_{60} = -5461512
\end{aligned}$$

$$\begin{aligned}
e_6: \quad - \quad & 5852.A_{22} + 5236.A_{24} - 1036.A_{28} - 4060.A_{30} - 1036.A_{32} \\
+ \quad & 5236.A_{36} - 5852.A_{38} - 23180.A_{40} - 15260.A_{42} + 93940.A_{44} \\
+ \quad & 447524.A_{46} + 1282292.A_{48} + 2959460.A_{50} + 5999476.A_{52} \\
+ \quad & 11120932.A_{54} + 19283572.A_{56} + 31735396.A_{58} + 50063860.A_{60} \\
= \quad & -50063860
\end{aligned}$$

$$\begin{aligned}
e_7: \quad & 20064.A_{22} + 18216.A_{24} - 11592.A_{28} + 11592.A_{32} - 18216.A_{36} \\
- \quad & 20064.A_{38} + 38760.A_{40} + 128880.A_{42} + 11000.A_{44} - 986304.A_{46} \\
- \quad & 4287096.A_{48} - 12503280.A_{50} - 30000872.A_{52} - 63613728.A_{54} \\
- \quad & 123521112.A_{56} - 224305488.A_{58} - 386206920.A_{60} - 262144.B_7 \\
= \quad & -386206920
\end{aligned}$$

The equation

$$(-2417.e_0 - 2289.e_1/2 - 347.e_2 - 315.e_3/2 - 37.e_4 - 129.e_5/8 - 5.e_6/2 - 7.e_7/8)/512$$

gives

$$\begin{aligned}
& 4.A_{30} + 105.A_{42} + 704.A_{44} + 2772.A_{46} + 8320.A_{48} + 21021.A_{50} \\
+ \quad & 47040.A_{52} + 96096.A_{54} + 182784.A_{56} + 328185.A_{58} \\
+ \quad & 561792.A_{60} + 448.B_7 = -113920,
\end{aligned}$$

a contradiction.

Corollary 3.1.

$$d(59+i,18+i) \le 20 \quad \textit{for } 0 \le i \le 3$$

$$d(61+i,19+i) \le 21 \quad \textit{for } 0 \le i \le 2.$$

By Lemma 2.4 and Lemma 2.6 we have

$$d(100+i,19+i) \le 40 \quad \text{for } 0 \le i \le 1$$

$$d(101+i,19+i) \le 41 \quad \text{for } 0 \le i \le 1.$$

Theorem 3.2. $d(64,18) \le 23$.

Proof. Suppose that there exists an even-weight $[64,18,24]$-code C. By [5] a $[58,13,24]$-code does not exist and by Lemma 2.2, $d^{\perp} \ge 7$. (i.e. $B_1 = B_2 = B_3 = B_4 = B_5 = B_6 = 0$.) By [8] $Res(C,30) = [34,17,9]$-code and $Res(C,38) = [26,17,5]$-code do not exist and so $A_{30} = A_{38} = 0$. Although only the first six MacWilliams' identities are free of B_i terms, it turns out to be useful here to row reduce the first seven identities. The equation

$$\begin{aligned}(& - 7951.e_0 - 4639.e_1 - 1831.e_2 - 983.e_3 \\ & - 303.e_4 - 127.e_5 - 23.e_6 - 7.e_7)\,/\,8192\end{aligned}$$

gives

$$\begin{aligned} & 7.A_{18} + 21.A_{34} + 160.A_{36} + 693.A_{38} + 2240.A_{40} + 6006.A_{42} \\ + & \ 14112.A_{44} + 30030.A_{46} + 112.B_7 = -10736,\end{aligned}$$

a contradiction.

Corollary 3.2.

$$d(46+i,17+i) \le 14 \quad \textit{for } 0 \le i \le 3$$

$$d(48+i,18+i) \le 15 \quad \textit{for } 0 \le i \le 2.$$

By Lemma 2.4 and Lemma 2.6 we have

$$d(75+i,18+i) \le 28 \quad \text{for } 0 \le i \le 1$$

$$d(76+i,18+i) \le 29 \quad \text{for } 0 \le i \le 1.$$

Theorem 3.3. $d(72, 18) \leq 27$.

Proof. Let us assume that there exists an even-weight $[72, 18, 28]$-code C. By Theorem 2.1 a $[67, 14, 28]$-code does not exist and by Lemma 2.2 $d^{\perp} \geq 6$. By [2] $Res(C, 30) = [42, 17, 13]$-code does not exist and so $A_{30} = 0$. By Lemma 2.3 and [8] $A_{38} = A_{46} = 0$.

The equation

$$\begin{aligned}(& - 62496.e_0 - 110075.e_1/4 - 9506.e_2 - 12471.e_3/4 \\ & - 784.e_4 - 793.e_5/4 - 30.e_6 - 21.e_7/4)/1024\end{aligned}$$

gives

$$\begin{aligned} & 64.A_{32} + 616.A_{50} + 3456.A_{52} + 12285.A_{54} + 34496.A_{56} + 83160.A_{58} \\ + & 179712.A_{60} + 357357.A_{62} + 665280.A_{64} + 1173744.A_{66} \\ + & 1980160.A_{68} + 3216213.A_{70} + 5056128.A_{72} + 7680.B_6 + 1344.B_7 \\ = & -165312, \end{aligned}$$

a contradiction.

Corollary 3.3.

$$d(71 + i, 18 + i) \leq 26 \quad \textit{for } 0 \leq i \leq 7$$

$$d(73 + i, 19 + i) \leq 27 \quad \textit{for } 0 \leq i \leq 6.$$

Theorem 3.4.

$$d(93, 19) \leq 37, \ d(72, 29) \leq 21, \ d(76, 29) \leq 23,$$

$$d(85, 30) \leq 27, \ d(105, 30) \leq 37, \ d(104, 48) \leq 27.$$

Proof. The proof of Theorem 3.4 is similar to that of Theorem 3.1.

Theorem 3.5. $d(101, 53) \leq 23$.

Proof. Suppose that there exists an even-weight $[101, 53, 24]$-code C. By Lemma 2.2 and Theorem 3.6, $d^{\perp} \geq 26$. By Lemma 2.3 and [8] $A_i = 0$ for $i = 26, 28, 30$ and 34. Two of the first twenty six row-reduced MacWilliams' identities become:

$$
\begin{aligned}
a) \qquad & 28.A_{80} - 8970.A_{84} - 160425.A_{86} - 1674400.A_{88} - 12876435.A_{90} \\
- \quad & 80057250.A_{92} - 423361575.A_{94} - 1966582800.A_{96} - 8205150525.A_{98} \\
- \quad & 31256180280.A_{100} = -783933116521200,
\end{aligned}
$$

$$
\begin{aligned}
b) \qquad & 145.A_{82} + 3744.A_{84} + 50220.A_{86} + 465920.A_{88} + 3359070.A_{90} \\
+ \quad & 20049120.A_{92} + 103079340.A_{94} + 469048320.A_{96} + 1926426645.A_{98} \\
+ \quad & 7247809920.A_{100} = 157331114940160.
\end{aligned}
$$

By Lemma 2.7 follows that $A_i = 0$ or 1 for $i = 90, 92, 94, 98$ and 100.

If $A_{100} = 1$, then $A_i = 0$ for $80 \leq i \leq 98$. a) now gives a contradiction. So $A_{100} = 0$.

If $A_{98} = 1$, then $A_i = 0$ for $82 \leq i \leq 96$. a) now gives a contradiction. So $A_{98} = 0$.

If $A_{96} = 1$, then $A_i = 0$ for $84 \leq i \leq 94$. a) now gives a contradiction. So $A_{96} = 0$.

If $A_{94} = 1$, then $A_i = 0$ for $86 \leq i \leq 92$. a)+4.b) now gives a contradiction. So $A_{94} = 0$.

The equation a)+4.b) gives a contradiction, because its left-hand side is positive but its right-hand side is negative and thus the result is obtained.

Corollary 3.4.

$$d(100+i, 53+i) \leq 22 \quad for\ 0 \leq i \leq 11$$

$$d(102+i, 54+i) \leq 23 \quad for\ 0 \leq i \leq 10.$$

REFERENCES

[1] DASKALOV, R.N. Certain binary linear codes with improved minimum distance upper bounds. *Mathematics and Education in Mathematics*, (1992) 285-290.

[2] DASKALOV, R.N., S. N. KAPRALOV. New minimum distance bounds for certain binary linear codes. *IEEE Trans. Inform. Theory*, (to appear).

[3] DODUNEKOV, S.M., S.B.ENCHEVA. New bounds on binary linear codes of dimension nine, in Proc. Fourth Joint Swedish-Soviet International Workshop on Information Theory, Gotland, Sweden, August 27-September 1, (1989) 280-282.

[4] DODUNEKOV, S.M., T. HELLESETH, N. MANEV, O. YTREHUS. New bounds on binary linear codes of dimension eight. *IEEE Trans. Inform. Theory*, **IT-33** (1987) 917-919.

[5] HILL, R., K. TRAYNOR, The nonexistence of certain binary linear codes. *IEEE Trans. Inform. Theory*, **36** (1990) 917-922.

[6] MACWILLIAMS, F.J., N. J. A. SLOANE. The Theory of Error-Correcting Codes, Amsterdam, North-Holland, 1977.

[7] TILBORG, H.C.A. VAN. The smallest length of binary 7-dimensional linear codes with prescribed minimum distance. *Discr. Math.*, **33** (1981) 197-207.

[8] VERHOEFF, T. An updated table of minimum-distance bounds for binary linear codes, (revised), Preprint, January, 1989.

Department of Mathematics
Technical University
5300 Gabrovo
BULGARIA

Received 04.02.1992
Revised 26.10.1992