There is no Binary Linear [66,13,28]-Code

Rumen N. Daşkalov

Department of Mathematics
Technical University
5300 Gabrovo
Bulgaria

Abstract. A binary linear code of length n, dimension k, and minimum distance at least d is called an $[n,k,d]$-code. Let $d(n,k) = \max\ \{d :$ there exists an $[n,k,d]$-code$\}$. It is curently known by [6] that $26 \leq d(66,13) \leq 28$. The nonexistence of a linary linear $[66,13,28]$-code is proven.

I. Introduction

Let an $[n,k,d]$-code denote a binary linear code of length n, dimension k, and minimum distance at least d. The Hamming weight of a vector x denoted $\mathrm{wt}\,x$, 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 $\mathrm{Res}\,(C,c)$ or $\mathrm{Res}\,(C,w)$ if the Hamming weight of c is w.

Lemma 1.1. The MacWilliams identities) [4,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*

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

where

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

The weight enumerator of a code C is the polynomial $\sum_{i=0}^{n} A_i z^i$.

Lemma 1.2. [4,p.592]: *Let C be an $[n,k,d]$-code. If $B_i \neq 0$ for some $i \leq k$ then there exists an $[n-i, k-i+1, d]$-code.*

Lemma 1.3. [5, Lemma 2.1]: *Let C be an $[n,k,d]$-code and $x \in C$, $\mathrm{wt}(x) = w$ and $w < 2d$. Then $\mathrm{Res}\,(C,w)$ has parameters $[n-w, k-1, d^\circ]$, where $d^\circ \geq d - \lfloor w/2 \rfloor$. ($\lfloor x \rfloor$ denotes the greatest integer $\leq x$).*

The next Lemmas 1.4–1.8 are well known.

ARS COMBINATORIA 39(1995), pp. 281-285

Lemma 1.4. *If there exists an* $[n, k, d]$ *-code* C *with* d *even, then there exists an* $[n, k, d]$ *-code all of whose codewords have even weight.*

Lemma 1.5. *If* x *and* y *are distinct codewords in an* $[n, k, d]$ *-code, then* $\mathrm{wt}(x) + \mathrm{wt}(y) \leq 2n - d$.

If $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ then by definition $x * y = (x_1 \cdot y_1, x_2 \cdot y_2, \ldots, x_n \cdot y_n)$.

Lemma 1.6. *If* C *is an* $[n, k, d]$ *-code and* $x, y \in C$, *the*

$$\mathrm{wt}(x + y) = \mathrm{wt}(x) + \mathrm{wt}(y) - 2\,\mathrm{wt}(x * y),$$
$$\mathrm{wt}(x * y) \geq \mathrm{wt}(x) + \mathrm{wt}(y) - n.$$

Lemma 1.7. *Suppose there does not exists an* $[n, k, d]$ *-code. Then there does not exist an* $[n + 2d, k + 1, 2d]$ *-code.*

Lemma 1.8.

(a) *If* $d(n, k) \leq d$, *where* d *is odd, then* $d(n - 1, k) \leq d - 1$;
(b) $d(n + 1, k + 1) \leq d(n, k)$.

Our method is to assume the existence of a $[66, 13, 28]$-code and to obtain a contradiction, similarly to [1], [2], [3].

II. The New Result

In the next theorem of this section, we shall assume the existence of a $[66, 13, 28]$-code, all of whose codewords have even weight. By Lemma 1.4, there is no loss in assuming the code to be an even-weight code.

Theorem 2.1. *A binary linear* $[66, 13, 28]$ *-code does not exist.*

Proof: We shall show that there does not exist a $[66, 13, 28]$-code C via Lemmas 2.1.1–2.1.4.

Lemma 2.1.1. *In a* $[66, 13, 28]$ *-code:*

i) $B_1 = B_2 = B_3 = B_4 = B_5 = 0$,
ii) $A_{30} = A_{34} = A_{38} = A_{46} = A_{50} = 0$.

Proof: i) By [2] a $[61, 9, 28]$-code does not exist and by Lemma 1.2 and [6] the result follows. ii) By Lemma 1.3 $\mathrm{Res}(C, 30 = [36, 12, 13]$, $\mathrm{Res}(C, 34) = [32, 12, 11]$, $\mathrm{Res}(C, 38) = [28, 12, 9]$, $\mathrm{Res}(C, 46) = [20, 12, 5]$, $\mathrm{Res}(C, 50) = [16, 12, 3]$. By [6] and [3, Corollary 3.6] none of these residual codes exist and the result follows.

Lemma 2.1.2. *The weight enumerator of a* $[66, 13, 28]$*-code satisfies:*

$$
\begin{aligned}
e_0 :& + A_{28} + A_{32} + A_{36} + A_{40} + A_{42} + A_{44} + A_{48} + A_{52} + A_{54} + A_{56} \\
& + A_{58} + A_{60} + A_{62} + A_{64} + A_{66} = 8191 \\
e_1 :& + 10.A_{28} - 2.A_{32} - 6.A_{36} - 14.A_{40} - 18.A_{42} - 22.A_{44} - 30.A_{48} \\
& - 38.A_{52} - 42.A_{54} - 46.A_{56} - 50.A_{58} - 54.A_{60} - 58.A_{62} - 62.A_{64} \\
& - 66.A_{66} = -66 \\
e_2 :& + 17.A_{28} - 31.A_{32} - 15.A_{36} + 65.A_{40} + 129.A_{42} + 209.A_{44} + 417.A_{48} \\
& + 689.A_{52} + 849.A_{54} + 1025.A_{56} + 1217.A_{58} + 1425.A_{60} + 1649.A_{62} \\
& + 1889.A_{64} + 2145.A_{66} = -2145 \\
e_3 :& - 160.A_{28} - 64.A_{32} + 160.A_{36} - 384.A_{42} - 1056.A_{44} - 3520.A_{48} \\
& - 7904.A_{52} - 10976.A_{54} - 14720.A_{56} - 19200.A_{58} - 24480.A_{60} \\
& - 30624.A_{62} - 37696.A_{64} - 45760.A_{66} = -45760 \\
e_4 :& - 672.A_{28} + 464.A_{32} - 1040.A_{40} - 336.A_{42} + 2464.A_{44} + 19728.A_{48} \\
& + 64064.A_{52} + 101664.A_{54} + 152880.A_{56} + 220528.A_{58} + 307680.A_{60} \\
& + 417664.A_{62} + 554064.A_{64} + 720720.A_{66} = -720720 \\
e_5 :& + 672.A_{28} + 992.A_{32} - 2016.A_{36} + 2912.A_{40} + 6048.A_{42} + 2464.A_{44} \\
& - 74016.A_{48} - 387296 A_{52} - 715680.A_{54} - 1221024.A_{56} - 1963360.A_{58} \\
& - 3014496.A_{60} - 4459040.A_{62} - 6395424.A_{64} \\
& - 8936928.A_{66} = -8936928 \\
e_6 :& + 8064.A_{28} - 4464.A_{32} + 2016.A_{36} + 3952.A_{40} - 14672.A_{42} \\
& - 34496.A_{44} + 166224.A_{48} + 1790880 A_{52} + 3959232.A_{54} \\
& + 7781424.A_{56} + 14082544.A_{58} + 23951104.A_{60} + 38788192.A_{62} \\
& + 60360720 A_{64} + 90858768.A_{66} - 8192.B_6 = -90858768
\end{aligned}
$$

Proof: These are just the MacWilliams' identities for $t = 0, 1, 2, 3, 4, 5, 6$.

It follows from Lemma 1.5 that $A_{66,64,62,60,58,56,54} = 0$ or 1.

Lemma 2.1.3. *In a* $[66, 13, 28]$*-code* $A_{66} = A_{64} = A_{62} = A_{60} = A_{58} = A_{56} = A_{54} = 0$ *and* $A_{52} \geq 3$.

Proof: The equation $(-4191.e_0 - 1416.e_1 - 369.e_2 - 93.e_3 - 17.e_4 - 5.e_5/2)/128$ gives $16.A_{40} + 480.A_{48} + 3200.A_{52} + 6435.A_{54} + 11760.A_{56} + 20020.A_{58} + 32256.A_{60} + 49725.A_{62} + 73920.A_{64} + 106590.A_{66} = 42240$. It is clear now that $A_{66} = A_{64} = A_{62} = 0$. If now $A_{54} = 1$ then reducing modulo 2 we have a contradiction. So $A_{54} = 0$.

Calculating the linear combination $(-891.e_0 - 488.e_1 - 149.e_2 - 33.e_3 - 5.e_4 - e_5/2)512$ we have $4.A_{32} + 12.A_{48} + 96.A_{52} + 392.A_{56} + 693.A_{58} +$

$1152.A_{60} = 5148$. If $A_{58} = 1$ then reducing modulo 2 we have a contradiction. So $A_{58} = 0$.

The equations $(781.e_0+248.e_1+67.e_2+17.e_3+3.e_4+e_5/2)64$ and $(-3435.e_0-1160.e_1-293.e_2-81.e_3-13.e_4-5.e_5/2)/8192$ now gives respectively

a) $7.A_{42} - 256.A_{48} - 1536.A_{52} - 5376.A_{56} - 14336.A_{60} = -18304$, and
b) $A_{44} + 15.A_{48} + 75.A_{52} + 245.A_{56} + 630.A_{60} = 975$.

If $A_{60} = 1$ then by Lemma 1.5 $A_{48,52,56} = 0$ and equation a) gives a contradiction. So $A_{60} = 0$. If $A_{56} = 1$ then $A_{52} = 0$ and now the equation a) $+166$. b)$/10$ gives a contradiction. So $A_{56} = 0$.

After this information, if $A_{52} = 0$ or 1 or 2 then the equation a) $+18$. b) gives now a contradiction and so $A_{52} \geq 3$.

Lemma 2.1.4. *Let* $x, y \in C = [66, 13, 28]$*-code and* $\mathrm{wt}(x) = \mathrm{wt}(y) = 52$, *then* $\mathrm{wt}(x * y) = 38$.

Proof: It follows from Lemma 1.6 that

$$\mathrm{wt}(x) + \mathrm{wt}(y) - 66 \leq \mathrm{wt}(x * y) \leq (\mathrm{wt}(x) + \mathrm{wt}(y) - 28)/2.$$

So $38 \leq \mathrm{wt}(x * y) \leq 38$ and the result follows.

After Lemmas 2.1.1–2.1.3 we have $A_{52} \geq 3$ and after Lemma 2.1.4 without loss of generality we have the following

	⟵ 52 ⟶	⟵ 14 ⟶
x	111111 11	000000 00
y	....	111111 11
z	....	111111 11

Here $\mathrm{wt}(x) = \mathrm{wt}(y) = \mathrm{wt}(z) = 52$. But now it follows that $\mathrm{wt}(x + y + z) = 52 - 28 = 24$, a contradiction. This completes the proof.

By Lemma 1.8, Lemma 1.7, and Verhoeff's propagation rule ([6,B-upper]) we have:

Corollary 2.1.

$$d(62+i, 13+i) \leq 26 \text{ for } 0 \leq i \leq 1$$
$$d(63+i, 13+i) \leq 27 \text{ for } 0 \leq i \leq 1$$
$$d(118+i, 14+i) \leq 52 \text{ for } 0 \leq i \leq 1$$
$$d(119+i, 14+i) \leq 53 \text{ for } 0 \leq i \leq 1$$
$$d(73+i, 20+i) \leq 26 \text{ for } 0 \leq i \leq 5$$
$$d(74+i, 20+i) \leq 27 \text{ for } 0 \leq i \leq 5$$

References

1. R.N. Daskalov and S.N. Kapralov, *New Minimum Distance Bounds for Certain Binary Linear Codes*, IEEE Trans. Inform. Theory 38 (1992), 1795–1796.
2. S.M. Dodunekov, S.B. Encheva, A.I. Ivanov, *New bounds on the minimum length of binary linear block codes*, Report LiTH-ISY-I-1283, Dept. of Elec. Eng., Linkoping Univ., Sweden (1991).
3. R. Hill and K. Traynor, *The nonexistence of certain binary linear codes*, IEEE Trans. Inform. Theory 36 (1990), 917–922.
4. F.J. MacWilliams and N.J.A. Sloane, "The Theory of Error-Correcting Codes", North-Holland, Amsterdam, 1977.
5. H.C.A. van Tilborg, *The smallest length of binary 7-dimensional linear codes with prescribed minimum distance*, Discrete Math. 33 (1981), 197–207.
6. T. Verhoeff, *An Updated Table of Minimum-Distance Bounds for Binary Linear Codes*, IEEE Trans. Inform. Theory 33 (1987), 665–680.