On the minimum distance of combinatorial codes

Citation for published version (APA):
Tolhuizen, L. M. G. M., & van Lint, J. H. (1990). On the minimum distance of combinatorial codes. *IEEE Transactions on Information Theory*, *36*(4), 922-923. https://doi.org/10.1109/18.53759

DOI:
10.1109/18.53759

Document status and date:
Published: 01/01/1990

Document Version:
Publisher’s PDF, also known as Version of Record (includes final page, issue and volume numbers)

$[39,28,6]$-code C. Let D be the dual code $C^{\perp}$. By Corollary 2.1, D is a $[39,11,15]$-code, which contains the all-one vector $\mathbf{1}$ (since C is even-weight). The dual code of D is just C and so has minimum weight 6. Let A_i be the number of codewords of weight i in D. Then $A_i = A_{39-i}$, for each i (since $\mathbf{1} \in D$) and $A_{18} = A_{21} = 0$ (by Lemma 2.4, the residual of D with respect to a codeword of weight 21 is an $[18,10,5]$-code, which does not exist by Table I).

The MacWilliams' identities (2.1) with $t = 0$, 2, 4, and 6 now give

$$\begin{aligned} A_{15}+A_{16}+A_{17}+A_{19}&=1023,\\ 21A_{15}+5A_{16}-7A_{17}-19A_{19}&=-741,\\ -309A_{15}-181A_{16}-29A_{17}+171A_{19}&=-82251,\\ 1519A_{15}+1407A_{16}+595A_{17}-969A_{19}&=-3262623+1024B_6,\end{aligned}$$

which lead to

a) $A_{15}=(5388-9A_{19})/14$,
b) $A_{16}=(-726+5A_{19})/2$,
c) $A_{17}=(7008-20A_{19})/7$,
d) $A_{19}=30720-8B_6$.

From a), d), b) and c), we get respectively

$$A_{19}\equiv 6 \pmod 7,\ A_{19}\equiv 0 \pmod 8,\ A_{19}\geq 146, \text{ and } A_{19}\leq 350,$$

which imply that A_{19} is one of 160, 216, 272, or 328. There are just the following four possible weight distributions for D.

	A_0	A_{15}	A_{16}	A_{17}	A_{19}	A_{20}	A_{22}	A_{23}	A_{24}	A_{39}
W_1:	1	282	37	544	160	160	544	37	282	1
W_2:	1	246	177	384	216	216	384	177	246	1
W_3:	1	210	317	224	272	272	224	317	210	1
W_4:	1	174	457	64	328	328	64	457	174	1

For each of the four cases, the B_i's were calculated (with the aid of a computer program) from the MacWilliams' identities (2.1) in order to check whether they were all integer-valued. Indeed they were, but in each case exactly one B_i was negative. It is easily confirmed by hand calculation that

$$\begin{aligned} &\text{for } W_1,\ B_{38}=-5,\\ &\text{for } W_2,\ B_{38}=-3,\\ &\text{for } W_3,\ B_{38}=-1,\\ &\text{for } W_4,\ B_{36}=-6.\end{aligned}$$

So we have a contradiction in each case. □

Corollary 3.15: $d(39+i,28+i)\leq 5$ and $d(38+i,28+i)\leq 4$, for $0\leq i\leq 4$.

Acknowledgment

We are grateful to P. P. Greenough for computer verification of calculations involved in this work.

We thank the referees for their very helpful comments and in particular for observations which considerably shortened the proofs of Theorems 3.6 and 3.8.

References

[1] S. M. Dodunekov, T. Helleseth, N. Manev and Ø. Ytrehus, "New bounds on binary linear codes of dimension eight," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 917–919, Nov. 1987.

[2] S. M. Dodunekov and N. L. Manev, "An improvement of the Griesmer bound for some small minimum distances," *Discrete Appl. Math.*, vol. 12, pp. 103–114, 1985.

[3] H. J. Helgert and R. D. Stinaff, "Minimum distance bounds for binary linear codes," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 344–356, 1973.

[4] T. Helleseth and Ø. Ytrehus, "New bounds on the minimum length of binary linear block codes of dimension 8," Report in Informatics, no. 21, Dept. of Informatics, Univ. of Bergen, Norway, 1986.

[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.

[6] J. Simonis, "Binary even [25,15,6]-codes do not exist," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 151–153, Jan. 1987.

[7] H. C. A. van Tilborg, "The smallest length of binary 7-dimensional linear codes with prescribed minimum distance," *Discr. Math.*, vol. 33, pp. 197–207, 1981.

[8] T. Verhoeff, "An updated table of minimum-distance bounds for binary linear codes," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 665–680, Sept. 1987.

On the Minimum Distance of Combinatorial Codes

L. TOLHUIZEN AND J. H. VAN LINT

***Abstract*—A conjecture of Da Rocha concerning the minimum distance of a class of combinatorial codes is proven.**

I. Introduction

The generator matrix of the first-order Reed–Muller code $\boldsymbol{R}(1,m)$ of length $n=2^m$ consists of all possible column-vectors from $(\mathbb{F}_2)^m$. The *combinatorial code* $C(m,s)$ has as generator matrix the matrix $A(m,s)$ of length $\binom{m}{s}$, that has all possible column-vectors of weight s as columns.

These codes were introduced by V. C. Da Rocha [2]. It is an easy exercise to show that the weight of the sum of any j rows of $A(m,s)$ only depends on j, m and s. If we denote this weight by $F(m,j,s)$, then we have for $1\leq j\leq m$

$$F(m,j,s)=\frac{1}{2}\left[\binom{m}{s}-P_s(j;m)\right]$$

where $P_s(x;m)$ is a Krawtchouk polynomial (cf. [1], p. 130, [2], Th. 2). Note that $F(m,1,s)=\binom{m-1}{s-1}$.

In [2], Da Rocha conjectures that the minimum weight of $C(m,s)$ is $\binom{m-1}{s-1}$ for $s<m/2$. We shall prove this conjecture and, in fact, we shall prove the following theorem.

Theorem 1: For $m\geq 1$, $2s<m$ and $1\leq j\leq m-1$ we have

$$\binom{m-1}{s-1}\leq F(m,j,s)\leq\binom{m-1}{s}.$$

II. Relations for $F(m,j,s)$

By adding all the rows of $A(m,s)$, or by replacing all 0's by 1's and vice versa, one obtains the following two trivial relations ([2], Theorems 3, 4)

$$F(m,m-j,s)=\begin{cases}F(m,j,s), & \text{if } s \text{ is even},\\ \binom{m}{s}-F(m,j,s), & \text{if } s \text{ is odd},\end{cases} \tag{2.1}$$

$$F(m,j,m-s)=\begin{cases}F(m,j,s), & \text{if } j \text{ is even},\\ \binom{m}{s}-F(m,j,s), & \text{if } j \text{ is odd}.\end{cases} \tag{2.2}$$

Manuscript received May 17, 1989.
The authors are with Philips Research Laboratories, P.O. Box 80,000, 5600 JA, Eindhoven, The Netherlands.
IEEE Log Number 8933971.

0018-9448/90/0700-0922$01.00 ©1990 IEEE

From these we obtain

$$F(2s,j,s)=\frac{1}{2}\binom{2s}{s}=\binom{2s-1}{s-1},\qquad \text{if } j \text{ is odd.} \qquad (2.3)$$

Note that by a permutation of columns, we can give $A(m+1, s+1)$ the form

$$A(m+1,s+1)=\begin{pmatrix} 1\ 1\cdots 1 & 0\ 0\cdots 0 \\ A(m,s) & A(m,s+1)\end{pmatrix}.$$

From this we immediately find two more relations:

$$F(m+1,j,s+1)=F(m,j,s)+F(m,j,s+1), \qquad (2.4)$$

$$F(m+1,j,s+1)=\binom{m}{s}-F(m,j-1,s)+F(m,j-1,s+1). \qquad (2.5)$$

III. Proof of Theorem 1

We prove the theorem by induction on m. For small values of m the theorem is easily checked by hand. Assume the theorem is true for $m \leq k$. Let $2s < k+1$, $1 \leq j \leq k$. We distinguish three cases.

Case a) $j=k$. We have by (2.1)

$$F(k+1,k,s)$$
$$=\begin{cases} F(k+1,1,s)=\binom{k}{s-1}, & \text{if } s \text{ is even,}\\ \binom{k+1}{s}-F(k+1,1,s)=\binom{k+1}{s}-\binom{k}{s-1}=\binom{k}{s}, & \text{if } s \text{ is odd.}\end{cases}$$

Case b) $1 \leq j \leq k-1$ and $2s<k$. Now we use (2.4)

$$F(k+1,j,s)=F(k,j,s-1)+F(k,j,s),$$

so by the induction hypothesis

$$F(k+1,j,s)\leq\binom{k-1}{s-1}+\binom{k-1}{s}=\binom{k}{s}$$

and

$$F(k+1,j,s)\geq\binom{k-1}{s-2}+\binom{k-1}{s-1}=\binom{k}{s-1}.$$

Case c) $1 \leq j \leq k-1$ and $2s=k$. We must now distinguish between odd and even values of j. Let j be odd. By (2.4) and (2.3) we have

$$F(2s+1,j,s)=F(2s,j,s)+F(2s,j,s-1)$$
$$=\binom{2s-1}{s-1}+F(2s,j,s-1),$$

and then the induction hypothesis yields

$$F(2s+1,j,s)\leq\binom{2s-1}{s-1}+\binom{2s-1}{s-1}=\binom{2s}{s},$$

$$F(2s+1,j,s)\geq\binom{2s-1}{s-1}+\binom{2s-1}{s-2}=\binom{2s}{s-1}.$$

Let j be even. By (2.5) and (2.3) we have

$$F(2s+1,j,s)=\binom{2s}{s-1}-F(2s,j-1,s-1)+F(2s,j-1,s)$$
$$=\binom{2s}{s-1}+\binom{2s-1}{s-1}-F(2s,j-1,s-1),$$

and now the induction hypothesis yields

$$F(2s+1,j,s)\leq\binom{2s}{s-1}+\binom{2s-1}{s-1}-\binom{2s-1}{s-2}$$
$$=2\binom{2s-1}{s-1}=\binom{2s}{s},$$

$$F(2s+1,j,s)\geq\binom{2s}{s-1}+\binom{2s-1}{s-1}-\binom{2s-1}{s-1}=\binom{2s}{s-1}.$$

Cases a), b), c) show that the theorem is also true for $m=k+1$ and the proof is complete. □

Note that the theorem has some combinatorial interest. It is nice to know that codewords cannot have weight less than the rows of the generator, but one should also realize that these codes are not good. Also as anticodes they do not seem to be very promising.

For the sake of completeness we mention the following facts concerning $C(m,s)$, (cf. [2])

$$C(m,s) \text{ has dimension } \begin{cases} m, & \text{if } s \text{ is odd,}\\ m-1, & \text{if } s \text{ is even.}\end{cases}$$

By adding the all-one vector of the code $C(m,s)$ if s is even, a code with dimension m is obtained with minimum weight $d(m,s)$ where

$$d(m,s)=\begin{cases} \binom{m-1}{s-1}, & \text{if } 2s<m,\\ \binom{m-1}{s}, & \text{if } 2s>m,\\ 2\binom{2s-1}{s-2}, & \text{if } 2s=m.\end{cases}$$

For $2s>m$, the assertion about the minimum distance is a consequence of the following obvious extension of Theorem 1.

Theorem 1':

a) For $m \geq 1$, $2s>m$ and $1 \leq j \leq m-1$ we have

$$\binom{m-1}{s}\leq F(m,j,s)\leq\binom{m-1}{s-1}.$$

b) For $s \geq 1$ and $1 \leq j \leq 2s-1$ we have

$$F(2s,j,s)=\binom{2s-1}{s-1},\qquad s \text{ odd,}$$

and

$$2\binom{2s-2}{s-2}\leq F(2s,j,s)\leq 2\binom{2s-2}{s-1},\qquad s \text{ even.}$$

Proof:

a) Combination of Theorem 1 and (2.2).
b) Combination of Theorem 1, (2.3), (2.4) and a). □

References

[1] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North Holland, 1977.

[2] V. C. Da Rocha, "Combinatorial codes," *Electron. Lett.*, vol. 21, no. 21, Oct. 1985.