Discrete Mathematics 83 (1990) 213–217
North-Holland

A [45, 13] CODE WITH MINIMAL DISTANCE 16

J.H. CONWAY
Mathematics Department, Princeton University, Princeton, New Jersey 08540, USA

S.J. LOMONACO Jr.
Computer Science Department, University of Maryland at Baltimore County, Catonsville, Maryland 21228, USA

N.J.A. SLOANE
Mathematics Sciences Research Center, AT&T Bell Laboratories, Murray Hill, New Jersey 07974, USA

Received 10 February 1988
Revised 6 June 1988

A record binary code of length 45, dimension 13 and minimal distance 16 is constructed in several ways: as an Abelian code (an ideal in the regular representation of $C_3 \times C_{15}$), from a [15, 6, 8] cyclic code over GF(4), and from the $|a + x \mid b + x \mid c + x|$ construction. Its automorphism group has order 360, and its even subcode is a [45, 12, 16] code with only four nonzero weights.

1. Introduction

We describe a remarkable [45, 13, 16] binary linear code $\mathscr{C}$ (compare [7]). Its minimal distance is larger than the estimates provided by the Hartmann–Tzeng and other bounds (see for example [4]), and it therefore appears to have been overlooked by Jensen [3] in his study of Abelian codes of length up to 129.

We give three constructions for $\mathscr{C}$, which has weight distribution:

i	0	16	17	20	21	24	25	28	29	45
A_i	1	405	540	1260	1890	1890	1260	540	405	1

The even subcode $\mathscr{D}$ is a [45, 12, 16] code with only four nonzero weights. Once $\mathscr{D}$ is constructed, we have

$$\mathscr{C} = \mathscr{D} \cup (1 + \mathscr{D}). \tag{1}$$

When discussing codes over GF(4) we follow the notation and conventions of [1].

2. The construction from a cyclic code over GF(4)

We construct GF(16) by adjoining to GF(4) $= \{0, 1, \omega, \bar{\omega}\}$ a root ϵ of $x^2 + \omega x + 1$. Then $\zeta = \epsilon\omega$ is a primitive element of GF(16), with $\zeta^{15} = 1$, $\zeta^2 + \bar{\omega}\zeta + \bar{\omega} = 0$, $\zeta^{10} = \omega$, $\zeta^6 = \epsilon$, $\epsilon^5 = 1$, $\epsilon^4 + \epsilon^3 + \epsilon^2 + \epsilon + 1 = 0$ (cf. [1]).

0012-365X/90/$03.50

Let $\mathscr{C}$ be the [15, 6] cyclic code over GF(4) with generator polynomial

$$\begin{aligned} g(x) &= (x+1)(x+\omega)(x+\bar{\omega})(x^2+\bar{\omega}x+\bar{\omega})(x^2+\bar{\omega}x+1)(x^2+x+\omega) \\ &= 1+x+\omega x^2+\bar{\omega}x^4+\bar{\omega}x^5+\omega x^7+x^8+x^9, \end{aligned} \tag{2}$$

a divisor of $x^{15}+1$. The zeros of the six factors of $g(x)$ are respectively 1; $\omega=\zeta^{10}$; $\bar{\omega}=\zeta^5$; ζ, ζ^4; ζ^3, ζ^{12}; ζ^{11}, ζ^{14}; or in other words g has zeros ζ^i for

$$i \in \{-5, -4, -3, \quad -1, 0, 1, \quad 3, 4, 5\}.$$

Although the Hartmann–Tzeng bound for example gives $d \geqslant 6$, the minimal distance of this code is in fact 8 (see Section 3), and its weight distribution (found by computer) is

i	0	8	10	12	14
A_i	1	405	1260	1890	540

When we map

$$0 \to \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \quad 1 \to \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \quad \omega \to \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \quad \bar{\omega} \to \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \tag{3}$$

$\mathscr{C}$ becomes the [45, 12, 16] binary code $\mathscr{D}$ (see Section 4).

Remark. An [18, 9, 8] self-dual code over GF(4) is described in [1]. By taking the subcode that vanishes on coordinates ∞, 0 and Ω, we obtain a [15, 6, 8] code which we have verified is equivalent to $\mathscr{C}$.

3. From the $|a+x \mid b+x \mid c+x|$ construction

By shortening the well-known [6, 3, 4] hexacode over GF(4) ([2, p.82]), we obtain a [5, 2, 4] code $\mathscr{P}$ over GF(4), which we take to have generator matrix

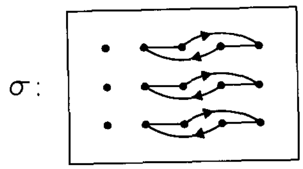
$$\begin{bmatrix} \omega & \bar{\omega} & \bar{\omega} & \omega & 0 \\ 0 & \omega & \bar{\omega} & \bar{\omega} & \omega \end{bmatrix}.$$

Let $\mathscr{F}$ be the [15, 16] code over GF(4) consisting all 3×5 arrays

$$\begin{bmatrix} a+x \\ b+x \\ c+x \end{bmatrix}, \tag{4}$$

where $a, b, c \in \bar{\mathscr{P}}$ (the conjugate of $\mathscr{P}$), $a+b+c=0$, and $x \in \mathscr{P}$ (cf. [2, p. 317], [6, p. 587]). The mapping

$$\begin{bmatrix} c_0 & c_6 & c_{12} & c_3 & c_9 \\ c_{10} & c_1 & c_7 & c_{13} & c_4 \\ c_5 & c_{11} & c_2 & c_8 & c_{14} \end{bmatrix} \leftrightarrow (c_0, c_1, \ldots, c_{14}), \tag{5}$$



THEN CONJUGATE

Fig. 1. The semilinear automorphism σ of order 4.

identifies $\mathscr{F}$ with $\mathscr{E}$. It is now easy to check by hand that $\mathscr{F}$ and therefore $\mathscr{E}$ has minimal distance 8 (compare [6, p. 588]).

The codes $\mathscr{C}, \mathscr{D}, \mathscr{E}, \mathscr{F}$ share the same automorphism group G (using the definition in [1]). Described in terms of $\mathscr{F}$, the group G is generated by scalar multiplication by ω, bodily permutations of the three rows of (4), bodily cyclic shifts of the five columns of (4), and the semilinear automorphism σ of order 4 defined in *Fig. 1.* The permutation σ^2 and the cyclic shifts of the columns of (4) generate a dihedral permutation group of order 10 on the columns, and G has order $3 \cdot 3! \cdot 10 \cdot 2 = 360$.

The group G is (imprimitively) transitive on the 15 coordinates of $\mathscr{F}$. We checked that G is the full automorphism group of $\mathscr{F}$ (and $\mathscr{E}$), and (when acting on the 45 coordinates in the obvious way) of $\mathscr{C}$ and $\mathscr{D}$.

The dual code $\mathscr{D}^\perp$ is a [45, 33, 3] code with weight distribution (in part) $A_0 = 1$, $A_3 = 15$, $A_5 = 189$, $A_6 = 1995$, $A_7 = 11475, \ldots$ $(A_{45-i} = A_i)$, and the 15 words of weight 3 show that the division of the 45 coordinates into 15 blocks of 3 is intrinsic. The dual code $\mathscr{C}^\perp$ is a [45, 32, 6] code, and is the even subcode of $\mathscr{D}^\perp$.

There are four orbits of minimal weight codewords of $\mathscr{F}$ (and therefore of $\mathscr{C}, \mathscr{D}, \mathscr{E}$) under G, namely

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & \bar\omega & \omega & \omega & \bar\omega \\ 0 & \bar\omega & \omega & \omega & \bar\omega \end{bmatrix},$$

$$\begin{bmatrix} 0 & \omega & \bar\omega & \bar\omega & \omega \\ 0 & 0 & \omega & \omega & 0 \\ 0 & 0 & \omega & \omega & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & \bar\omega & 0 & 0 & \bar\omega \\ 0 & 0 & \omega & \omega & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 0 & \omega & \omega & 0 \\ \bar\omega & 0 & 1 & 0 & \omega \\ \bar\omega & \omega & 0 & 1 & 0 \end{bmatrix},$$

with respectively 45, 90, 90 and 180 images, for a total of 405.

4. As an Abelian code

The map (3), when interpreted literally, sends the codewords of $\mathscr{C}$ onto 3×15 binary arrays. The image set may therefore be regarded as an ideal in the group ring $\mathrm{GF}(2) \cdot H$, where $H = C_3 \times C_{15}$ is a product of cyclic groups. In this form $\mathscr{D}$ is an Abelian code, generated as a cyclic submodule of $\mathrm{GF}(2) \cdot H$ by the single vector

$$v = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{6}$$

which is the image of $g(x)$ (see (2)) under the map (3), and similarly $\mathscr{C}$ is generated either by $\mathbf{1}$ and v, or by the single vector $\mathbf{1} + v$.The code $\mathscr{C}$ was originally obtained in this form, while carrying out a computer search for Abelian codes (cf. [5], [6, pp. 677, 733]). A generator matrix for $\mathscr{C}$ is given in *Fig. 2*.

$$\left[\begin{array}{l}
100000000000011100100110010011111011001101111 \\
010000000000010010110101011010000110101011000 \\
001000000000001001011010101101000011010101100 \\
000100000000011000001011000101111010100111001 \\
000010000000010000100011110001000110011110011 \\
000001000000001100010001111000100011001111001 \\
000000100000011110101110101111001010101010011 \\
000000010000010011110001000100011110011000110 \\
000000001000001001111000100010001111001100011 \\
000000000100011100011010000010011100101011110 \\
000000000010010110101011010010110101011000000 \\
000000000001001011010101101001011010101100000 \\
000000000000111001001100100111110110011011111
\end{array}\right]$$

Fig. 2. Generator matrix for [45, 13, 16] binary code $\mathscr{C}$.

Acknowledgements

We should like to thank Ying Cheng for some helpful discussions.

References

[1] Y. Cheng and N.J.A. Sloane, The automorphism group of an [18, 9] quaternary code, *Discrete Math.*, this issue.

[2] J.H. Conway and N.J.A. Sloane, Sphere-Packings, Lattices and Groups (Springer Verlag, New York, 1988).

[3] J.M. Jensen, The concatenated structure of cyclic and Abelian codes, IEEE Trans. Inform. Theory IT-31 (1985) 788–793.

[4] J.H. van Lint and R.M. Wilson, On the minimum distance of cyclic codes, IEEE Trans. Inform. Theory IT-32 (1986) 23–40.

[5] S.J. Lomonaco, Jr., Metacyclic error-correcting codes, Technical Report 5, Computer Science Dept., Univ. of Maryland at Baltimore County, Catonsville, MD, 1987.

[6] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes (North-Holland, Amsterdam, 1979).

[7] T. Voerhoeff, An updated table of minimum-distance bounds for binary linear codes, IEEE Trans. Inform. Theory, IT-33 (1987) 665–680.