

1978

## **A class of codes generated by circulant weighing matrices**

K Wehrhahn

Jennifer Seberry

*University of Wollongong*, [jennie@uow.edu.au](mailto:jennie@uow.edu.au)

Follow this and additional works at: <https://ro.uow.edu.au/infopapers>



Part of the [Physical Sciences and Mathematics Commons](#)

---

### **Recommended Citation**

Wehrhahn, K and Seberry, Jennifer: A class of codes generated by circulant weighing matrices 1978.  
<https://ro.uow.edu.au/infopapers/989>

---

## A class of codes generated by circulant weighing matrices

### Abstract

Some properties of a new class of codes constructed using circulant matrices over  $GF(3)$  will be discussed. In particular we determine the weight distributions of the  $(14, 7)$  and two inequivalent  $(26, 13)$ -codes arising from the incidence matrices of projective planes of orders 2 and 3.

### Disciplines

Physical Sciences and Mathematics

### Publication Details

Wehrhahn, K and Seberry, J, A class of codes generated by circulant weighing matrices, Combinatorial Mathematics: Proceedings of the international Conference, Canberra, August, 1977, 686, in Lecture Notes in Mathematics, Springer-Verlag, Berlin-Heidelberg-New York, 1978, 282-289.

Jennifer Seberry and K. Wehrhahn

Applied Mathematics Department and  
 Pure Mathematics Department,  
 University of Sydney,  
 N.S.W., 2006

# ABSTRACT.

Some properties of a new class of codes constructed using circulant matrices over  $GF(3)$  will be discussed. In particular we determine the weight distributions of the  $(14, 7)$  and two inequivalent  $(26, 13)$ -codes arising from the incidence matrices of projective planes of orders 2 and 3.

## 1. INTRODUCTION.

In this paper "code" will mean a linear code over  $GF(3)$ . An  $(n, k)$ -code  $C$  has length  $n$ , dimension  $k$ . An  $(n, k, d)$ -code is an  $(n, k)$ -code with minimum non-zero weight  $d$ . Our notation and definitions are consistent with those of Blake and Mullin [2].

Let  $Q$  be the circulant incidence matrix of a projective plane of order  $q$  (See Hall [6]). Then  $Q$ , of order  $q^2 + q + 1$  satisfies

$$QQ^T = qI + J, \quad QJ = (q+1)J$$

where  $J$  is the appropriate all 1's matrix.  $W = Q^2 - J$  is a circulant  $(0, 1, -1)$  matrix of order  $q^2 + q + 1$  satisfying

$$WW^T = q^2I, \quad WJ = qJ$$

i.e.  $W$  is a circulant weighing matrix of weight  $q^2$ . We write  $W = W(q^2+q+1, q^2)$  to denote its order and weight. More details of  $W$  can be found in Hain [5] and Wallis and Whiteman [10].

We call codes with basis

$$[I \ W] \quad \text{for } q \equiv 0 \pmod{3}$$

$$[I \ qW] \quad \text{for } q \equiv 1 \text{ or } 2 \pmod{3}$$

over  $GF(3)$  *weighing codes*. The purpose of this paper is to establish some general properties of weighing codes and to determine the weight distributions

and design properties of the codes corresponding to  $q = 2$  and  $q = 3$ .

Note that if

$$G = [I \ W]$$

is the basis of  $C$  then for  $q \equiv 1$  or  $2 \pmod{3}$

$$G^\perp = [I \ -W]$$

is the basis of the dual code  $C^\perp$ . Hence  $C$  is neither self-dual nor self-orthogonal. However we shall see that  $C$  and  $C^\perp$  always have the same weight distribution and hence the same minimum distance  $d$ . By a well known result, cf. Delsarte [3], weighing codes are orthogonal arrays of strength  $d-1$ . In this sense the weighing codes belong to a family of codes including the self-dual codes, see Mallows, et. al [7] and the symmetry codes, see Pless [8, 9] and Blake [1].

We observe that the one's vector  $\underline{1}$  is in  $C$  for  $q \equiv 1$  or  $2 \pmod{3}$  and is the sum of the basis vectors. The vector  $\underline{k} = (1, 1, \dots, 1, -, \dots, -)$  (where  $-$  represents  $-1$ ) of  $q^2 + q + 1$  ones and  $q^2 + q + 1$  minuses occurs in the dual code for  $q \equiv 1$  or  $2 \pmod{3}$ .

If  $q \equiv 0 \pmod{3}$  then the sum of the basis vectors

$$[I \ W] \text{ is not } \underline{1},$$

and so the code cannot contain  $\underline{1}$ . Moreover, in this case  $\text{rank } W < \text{order of } W$  since  $WW^T \equiv 0 \pmod{3}$ .

## 2. GENERAL PROPERTIES OF THE CODES.

If  $A_i$  is the number of codewords of weight  $i$  in  $C$ , then we call the bivariate polynomial

$$WE(x, y) = \sum_{i=0}^n A_i x^{n-i} y^i$$

the *weight enumerator* of  $C$ . If  $A_{ijk}$  is the number of codewords of weight  $j+k$  in  $C$  containing  $j$  ones and  $k$  twos (minus ones over  $GF(3)$ ) then we call the trivariate polynomial

$$CWE(x, y, z) = \sum_{i=0}^n A_{ijk} x^{n-i} y^j z^k$$

the *complete weight enumerator* of  $C$ .

## THEOREM.

Let  $C$  be the code over  $GF(q)$  with basis  $G = [I \ X]$  where  $X$  is a circulant matrix of order  $k$  and  $I$  is the identity matrix of order  $k$ . Then  $C$  and  $C^\perp$  have the same weight enumerators.

Proof :

First recall that if  $X$  is a circulant matrix and  $R$  the back diagonal permutation matrix then

$$(XR)^T = XR.$$

Now  $C^\perp$  has basis

$$[-X^T \ I]$$

and the basis vectors of  $C^\perp$  may be written as

$$R[-X^T \ I] = [-RX^T \ R] = [-XR^T \ R] = [-XR \ R]$$

since this merely involves rearranging the order of the basis vectors. Hence  $C^\perp$  is equivalent to the code  $D^\perp$  with basis

$[-XR \ I]$  as this just rearranges the columns of  $R$ . Since  $XR$  is symmetric we have that  $(D^\perp)^\perp = D$  has basis  $[I \ XR]$ .

If  $b$  is a  $q$ -ary vector of length  $k$

then  $WE(b[I \ XR]) = WE(b) + WE(bXR)$

whereas  $WE(b[-XR \ I]) = WE(-bXR) + WE(b)$

and hence  $D$  and  $C^\perp$  have the same weight enumerators. But  $D$  is equivalent to  $C$  and hence the theorem holds. ■

In particular  $A_1 = A_1^\perp$  for weighing codes, and so  $C$  and  $C^\perp$  form orthogonal arrays of maximum strength  $d-1$  where  $d$  is the minimum distance of  $C$  (and  $C^\perp$ ).

Any two vectors from the basis of  $C$  can be written as

$$\begin{array}{cccccccc} 100\dots 0 & 1\dots 11\dots 11\dots 1 & \dots\dots\dots & 0\dots 00\dots 00 \\ 010\dots 0 & 1\dots 1\dots\dots 0\dots 0 & 1\dots 1\dots\dots 0\dots 0 & 1\dots 1\dots\dots 0 \\ \hline q^2+q+1 & a & b & c & d & e & f & g & h & 1 \end{array}$$

and we obtain the following equations

$$a + b + c = a + d + g = \frac{1}{2}(q^2 + q) = \text{number of ones.}$$

$$d + e + f = b + e + h = \frac{1}{2}(q^2 - q) = \text{number of minus ones.}$$

$$1 + g + h = c + f + 1 = q + 1 = \text{number of zeros.}$$

$$a + e = b + d \quad (\text{orthogonality}).$$

These equations can be solved for  $c, d, e, f, g, h$  in terms of  $q, a, b$ . The OWE of the sum and difference of two vectors are

$$x \frac{1}{2}(3q^2+q) \quad y \frac{1}{2}(2+q^2+q-3a) \quad z -\frac{1}{2}q^2+\frac{1}{2}q+3a$$

and

$$x \frac{1}{2}(3q^2+q) \quad y \frac{1}{2}(1+q^2-3b) \quad z -\frac{1}{2}q^2+\frac{3}{2}q+3b+1$$

respectively.

Of course the negatives of these vectors are also in  $C$  and hence the weight of every two combination is  $\frac{1}{2}(q^2 + 3q + 4)$  and consequently there are at least  $4\binom{q^2 + q + 1}{2}$  vectors of this weight.

We may observe that

$$\frac{1}{2}(q^2 + 3q + 4) < q^2 + 1 \quad \text{for } q \geq 4$$

and hence  $\frac{1}{2}(q^2 + 3q + 4)$  provides an upper bound on the minimum distance of  $C$  for  $q \geq 4$ .

### 3. THE (14, 7) CODE WITH MINIMUM DISTANCE 5.

This code is generated by  $W$  with first row

$$-110100.$$

In order to ensure the  $\frac{1}{2}$  vector is in  $C$  we use the basis vectors

$$G = [I \quad qW] = [I \quad -W]$$

where  $q = 2$ .

We observe that the linear combinations given by  $XG$  where

$X = I + Q + J$  ( $Q$  as before the incidence matrix of the projective plane of order 2 and  $W = Q^2 - J$ ) are

$$H = [X \quad -XW] = [I+Q+J \quad 2Q+2J] \pmod{3}$$

and  $K = 2H - 3J$  satisfies the equation  $KK^T = 16I - 2J$  over the real numbers.

Since each row of  $K$  has eight +1's and six -1's and each column has four +1's and three -1's we have a  $(7, 14, 8, 4, 4)$ -BIBD. In fact the 16 vectors  $\frac{1}{2}, \frac{2}{2}, H, 2H$  contain a  $(14, 16, 6)$ -block code. The vectors

$$\begin{bmatrix} 1 & 1 & -1 \\ \mathbf{1}^T & \mathbf{1}^T & -\mathbf{H} \end{bmatrix},$$

where  $\mathbf{1}$  is the vector of seven ones, are the first eight rows of an Hadamard matrix of order 16 (See Wallis, et al [11]).

We note that since every vector in the code  $C$  is orthogonal to every vector in  $C^\perp$  the remaining 8 rows of this Hadamard matrix of order 16 (and their negatives) will be obtained from the vectors of full weight in  $C^\perp$ .

We found the weight distribution for this code, which is given in Figure 1, and that of the dual code, given in Figure 2. As expected, we see  $C$  and  $C^\perp$  have the same weight distribution but not the same complete weight enumerator.

The  $(14, 7)$ -code has minimum distance 5 and hence forms an orthogonal array of strength 4.

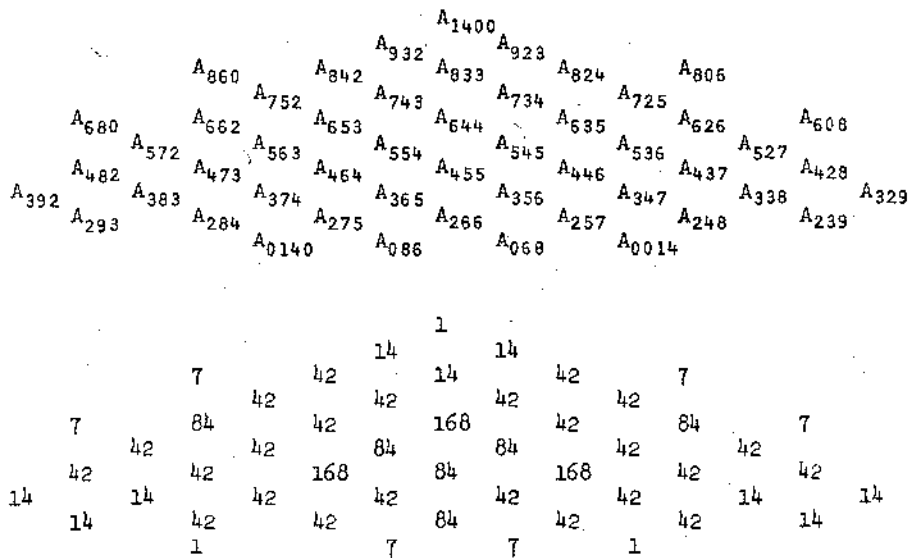


Figure 1.

	A <sub>1400</sub>			1	
	A <sub>941</sub>	A <sub>914</sub>		14	14
A <sub>860</sub>	A <sub>833</sub>	A <sub>806</sub>	7	98	7
	A <sub>752</sub>	A <sub>725</sub>		84	84
A <sub>671</sub>	A <sub>644</sub>	A <sub>617</sub>	42	350	42
	A <sub>563</sub>	A <sub>536</sub>		168	168
A <sub>482</sub>	A <sub>455</sub>	A <sub>428</sub>	84	420	84
	A <sub>374</sub>	A <sub>347</sub>		112	112
A <sub>293</sub>	A <sub>266</sub>	A <sub>239</sub>	56	168	56
	A <sub>077</sub>			16	

Figure 2.

## 4. TWO (26, 13)-CODES WITH DISTANCE 3 AND 4

Richard M. Hain [5] conjectured and Peter Eades [4] verified (by computer) that there are two equivalence classes of circulant  $W(13, 9)$ . They have first rows

0-0-10011-111

and

0101100--11-1 .

Call the circulant matrices with these first rows  $W_1$  and  $W_2$  .

The linear codes  $C_1$ ,  $C_2$  with bases

$$[I W_1], [I W_2]$$

respectively, were studied via the computer at the University of Sydney and their CWE's obtained. We give here their WE's in Figures 3 and 4 respectively.

It is most interesting to note that the codes have different minimum distances 3 and 4 respectively. Also, as expected since  $q = 3 \equiv 0 \pmod{3}$  for these codes, neither  $C_1$  nor  $C_2$  contains  $\underline{1}$  (and neither does  $C_1^\perp$  nor  $C_2^\perp$  as  $\underline{1}$  is not orthogonal to their basis vectors). Also neither contains any full weight vectors.

Since the codes have minimum distance 3 and 4 they are orthogonal arrays of strength 2 and 3 respectively.



$A_0 = 1$   
 $A_1 = 0$   
 $A_2 = 0$   
 $A_3 = 104$   
 $A_4 = 468$   
 $A_5 = 1404$   
 $A_6 = 4056$   
 $A_7 = 8424$   
 $A_8 = 11934$   
 $A_9 = 13442$   
 $A_{10} = 11258$   
 $A_{11} = 5928$   
 $A_{12} = 4264$   
 $A_{13} = 11260$   
 $A_{14} = 39780$   
 $A_{15} = 105768$   
 $A_{16} = 211224$   
 $A_{17} = 317538$   
 $A_{18} = 352638$   
 $A_{19} = 281632$   
 $A_{20} = 154128$   
 $A_{21} = 51168$   
 $A_{22} = 7904$   
 $A_{23} = 0$   
 $A_{24} = 0$   
 $A_{25} = 0$   
 $A_{26} = 0$

---

Weight Distribution of  $C_1$

Figure 3.

$A_0 = 1$   
 $A_1 = 0$   
 $A_2 = 0$   
 $A_3 = 0$   
 $A_4 = 26$   
 $A_5 = 0$   
 $A_6 = 156$   
 $A_7 = 624$   
 $A_8 = 0$   
 $A_9 = 1118$   
 $A_{10} = 3458$   
 $A_{11} = 8736$   
 $A_{12} = 24830$   
 $A_{13} = 54264$   
 $A_{14} = 100152$   
 $A_{15} = 152568$   
 $A_{16} = 212862$   
 $A_{17} = 259974$   
 $A_{18} = 272766$   
 $A_{19} = 222976$   
 $A_{20} = 145002$   
 $A_{21} = 73996$   
 $A_{22} = 37180$   
 $A_{23} = 16848$   
 $A_{24} = 6006$   
 $A_{25} = 780$   
 $A_{26} = 0$

---

Weight Distribution of  $C_2$

Figure 4.

#### REFERENCES.

- (1) Ian F. Blake, "On a generalization of the Pless symmetry codes", *Information and Control*, 27(1975), 369-373.
- (2) Ian F. Blake and Ronald C. Mullin, *An Introduction to Algebraic and Combinatorial Coding theory*, Academic Press, N.Y. -San Francisco-London, 1976.

- (3) P. Delsarte, "Four Fundamental Parameters of a code and Their Combinatorial Significance", *Information and Control*, 23(1973) 407-458.
- (4) P. Eades, *On the Existence of Orthogonal Designs*, Ph.D. Thesis, Australian National University, Canberra, 1977.
- (5) Richard M. Hain, *Circulant Weighing matrices*, M.Sc. Thesis, Australian National University, Canberra, 1977.
- (6) Marshall Hall Jr., *Combinatorial Theory*. Blaisdell, [Ginn Co.], Waltham, Mass, 1967.
- (7) G.L. Mallows, V. Pless and N.J.A. Sloane, "Self-Dual codes over  $GF(3)$ ", *SIAM J. Appl. Math.* Vol 31, (1976), 649-666.
- (8) V. Pless, "On a new family of symmetry codes and related new five designs", *Bull. Amer. Math. Soc.* 75(1969), 1339-1342.
- (9) V. Pless, "Symmetry codes over  $GF(3)$  and new-five designs", *J. Combinatorial Th. Ser. A* 12(1972), 119-142.
- (10) Jennifer Seberry Wallis and Albert Leon Whiteman, "Some results on weighing matrices", *Bull. Austral. Math. Soc.* 12(1975), 433-447.
- (11) W.D. Wallis, Anne Penfold Street, Jennifer Seberry Wallis, *Combinatorial Room Squares, sum-free sets, Hadamard matrices*, Lecture Notes in Mathematics, Vol. 292, Springer-Verlag, Berlin-Heidelberg-New York, 1978.