INFORMATION AND CONTROL 27, 369–373 (1975)

On a Generalization of the Pless Symmetry Codes*

IAN F. BLAKE

Department of Electrical Engineering, University of Waterloo, Waterloo, Ontario

A class of matrices which are orthogonal over the reals and contain only the elements, 0, ± 1, is constructed. For certain parameters, these matrices are used to construct a class of self dual codes over GF(3). This class is shown to contain the class of symmetry codes and possesses many of their properties.

1. INTRODUCTION

In a recent paper Pless (1972) defined the class of symmetry codes over GF(3). The codes are self dual and are of combinatorial interest as new five-designs were found among the incidence vectors of codewords of certain constant weights. The purpose of this note is to show that there is a simple generalization of the symmetry codes which possesses many of their properties. Unfortunately the smallest code in the generalization, which is not a symmetry code, is too large for its weight enumerator to be determined by the methods given in Pless (1972). Thus it is not yet known whether new five-designs will be forthcoming. In the next section a class of matrices orthogonal over the reals and containing only the elements 0, ± 1 is defined. In Section 3 these matrices are used to construct and analyze the generalized symmetry (GS) codes. The Pless symmetry codes are established as a subclass of the GS Codes.

2. A CLASS OF ORTHOGONAL MATRICES

In this section a class of matrices, orthogonal over both GF(3) and the reals, is constructed. This class will be a generalization of the class used by Pless (1972) in her construction of self dual codes. We first give the construction of the matrices used in Pless (1972).

* This work supported by the National Research Council of Canada, Grant No. A-7382.

Let $a(\cdot)$ be a one-to-one mapping of the integers 0, 1,..., $(q-1)$ onto the elements of GF(q) such that $a(0) = 0$, $a(1) = 1$. Define the function

$$\chi\colon \mathrm{GF}(q) \to \{0, 1, -1\}$$

by $\chi(0) = 0$, χ(a square) $= 1$ and χ(a nonsquare) $= -1$. If q is the power of an odd prime then GF(q) contains $(q-1)/2$ squares and the same number of nonsquares. Define the $(q+1) \times (q+1)$ matrix $S(q) = (s_{ij})$ in the following manner: label the rows and columns of the matrix by the elements ∞, 0, 1,..., $(q-1)$ and let

$$s_{\infty,\infty} = 0, \qquad s_{i,\infty} = \chi(-1), \qquad s_{\infty,i} = 1, \qquad s_{ij} = \chi(a(j) - a(i))$$

$$i, j = 0, 1, \ldots, (q-1).$$

It can be shown that $S(q)$ has the property $S(q)\,S(q)^T = -I_{q+1}$ when $q \equiv -1(3)$. In this case the matrix $[I_{q+1}, S(q)]$ is the generator matrix of a self dual code with many interesting properties.

We now give the construction of an orthogonal matrix $S(q^{k-1})$ which, in the case $k = 2$, will be shown to be equivalent to the matrix $S(q)$ defined above. Thus, although the construction methods are quite different, there is no abuse of terminology.

Let G be a $k \times (q^k - 1)$ matrix whose columns contain all the distinct nonzero k-tuples over the finite field GF(q). In coding terms the row space of G, denoted by $\mathscr{C}$, is equivalent to a maximum length cyclic code. It is known (Stiffler, 1971) that the weight of every nonzero codeword in $\mathscr{C}$ is $(q-1)\,q^{k-1}$. If G^1 is the $k \times (q^k - 1)$ matrix whose rows are any set of k linearly independent codewords of $\mathscr{C}$, then every nonzero k-tuple over GF(q) appears as a column of G^1.

Let H be a $k \times n$ submatrix of G, $n = (q^k - 1)/(q-1)$ with the property that any two of its columns are linearly independent. We assume that H is normalized in the sense that the first nonzero element in each column is unity. Let A be an $n \times n$ matrix whose rows are chosen from the nonzero vectors of the row space of H and have the property that any two distinct rows are linearly independent. Assume for convenience that the first k rows of A are rows of H. It follows readily from observations on G that every row of A has weight q^{k-1}. It is not difficult to show that if H^1 is the (0, 1) matrix obtained from H by replacing each nonzero element by unity, then the rows of H^1 are the incidence vectors of the complements of the hyperplanes of the projective geometry PG($k-1, q$).

Let x_1 and x_2 be two distinct rows of A. Since they are independent, they can be extended to a basis x_i, $i = 1,..., k$, each vector of which is a row of A. Let B be the $k \times n$ matrix whose ith row is x_i, $i = 1,..., k$. Assume B has been normalized by multiplying each column so that the first nonzero element in each column is unity. Let B' be the $k \times q^{k-1}$ submatrix of B consisting of those columns with unity in the first row. Every $(k-1)$-tuple over GF(q), including the all-zeros $(k-1)$-tuple, appears in the columns of B in rows 2 through k. Each element of GF(q) appears q^{k-2} times in the second row of B. This fact will be important in the following.

Let q be the power of an odd prime. In the matrix A replace $\alpha \in \mathrm{GF}(q)$ by $\chi(\alpha)$ and call the resulting matrix $S(q^{k-1})$

LEMMA 1. *Over the real numbers*

$$S(q^{k-1})\, S(q^{k-1})^T = q^{k-1} I_n .$$

Proof. Since every row of A is of weight q^{k-1} and each nonzero element of GF(q) is either a square or a nonsquare, the inner product over the reals of any row of $S(q^{k-1})$ with itself is q^{k-1}. Let $x_1 = (\alpha_1 ,..., \alpha_n)$, $x_2 = (\beta_1 ,..., \beta_n)$ be two distinct rows of A. If $y_1 = (\chi(\alpha_1),..., \chi(\alpha_n))$ and $y_2 = (\chi(\beta_1),..., \chi(\beta_n))$ are the corresponding rows of $S(q^{k-1})$ then the inner product of y_1 and y_2 over the reals is the number of nonzero co-ordinate positions for which $\chi(\alpha_i) = \chi(\beta_i)$ less the number of nonzero co-ordinate positions for which $\chi(\alpha_i) \neq \chi(\beta_i)$. Since χ is a multiplicative function in the sense that $\chi(\alpha)\,\chi(\beta) = \chi(\alpha\beta)$, multiplication of a co-ordinate position by a nonzero element of GF(q) does not change the agreement or disagreement between coordinate positions of y_1 and y_2. As before, assume that x_1 and x_2 are the first two rows of the matrix B, which is assumed in normalized form. In the nonzero positions of x_1, each element of GF(q) appears in x_2 q^{k-2} times. Thus the inner product of the corresponding vectors y_1 and y_2 is zero, which completes the lemma.

We now show that, for $k = 2$, the matrices $S(q)$ used in Pless (1972) can be constructed in the above manner. Label the rows and columns of a matrix with $\infty, 0, 1,..., (q-1)$. Using the mapping $a(\cdot)$ introduced previously place the elements $0, -1$ in the first and second rows of column ∞ and 1, $a(j)$ in column j. Denote these first two row vectors by x_1 and x_2 labeled by ∞ and 0, respectively. In the row labeled i place the row vector $-a(i) \cdot x_1 + x_2$. Clearly any two rows are linearly independent and this is a particular construction for the matrix A of the previous section for $k = 2$.

3. Generalized Symmetry Codes

In this section we take the matrices $S(q^{k-1})$ as being matrices over GF(3). If q and k are such that $q^{k-1} \equiv -1(3)$ then, over GF(3) we have

$$S(q^{k-1})\, S(q^{k-1})^T = -I.$$

This occurs iff $q \equiv -1(3)$ and k is even. Using an extension of the notation of Pless (1972), denote the GS code generated by the matrix $[I, S(q^{k-1})]$ by $C(q^{k-1})$, $q \equiv -1(3)$ and k even. The GS code $C(q^{k-1})$ is, by definition, self dual and the weight of every codeword is divisible by 3. The following lemma is the image of Lemma 3.1 in Pless (1972) and we merely adapt her proof to the present case.

Lemma 2 (Pless, 1972).

(a) *The weight of every vector in the basis* $[I, S(q^{k-1})]$ *is* $q^{k-1} + 1$.

(b) *The weight of any linear combination of two vectors in the basis* $[I, S(q^{k-1})]$ *is* $2q^{k-2} + q^{k-2}(q-1)/2 + 2$.

(c) *The weight of any linear combination of three vectors in the basis* $[I, S(q^{k-1})]$ *is* $\geqslant q^{k-2}(q-3)/2 + 5$.

Proof. Part (a) follows from the definition of $S(q^{k-1})$. For part (b), let y_1 and y_2 be two rows of $S(q^{k-1})$. Since their inner product is 0 over GF(3) and the reals, the number of co-ordinate positions in which both y_1 and y_2 are nonzero and agree is equal to the number in which they are both nonzero and disagree. Thus the weight of the sum of any two rows of $S(q^{k-1})$ is precisely $2q^{k-2} + (q^{k-1} - q^{k-2})/2$ and part (b) follows. For part (c) we lower bound the weight of the sum of any three distinct rows of $S(q^{k-1})$ by observing that the sum of a vector of weight q^{k-1} and a vector of weight $2q^{k-2} + (q^{k-1} - q^{k-2})/2$ is at least $q^{k-1} - [2q^{k-2} + (q^{k-1} - q^{k-2})/2] = q^{k-2}(q-3)/2$. Since this quantity must be divisible by 3 it follows that it can be increased to $q^{k-2}(q-3)/2 + 2$. The result of part (c) follows.

From the comments of the previous section and the definition of a GS code, when $k = 2$ and $q \equiv -1(3)$ a GS code reduces to a code equivalent to a Pless symmetry code.

4. Comments

A class of codes, more general than the symmetry codes of Pless, has been constructed. Unfortunately, the smallest such code is of length 312 ($q = 5$,

$k = 4$), which is too long to be analyzed by techniques known at present. The class of $\{0, +1, -1\}$ matrices, orthogonal over the reals, constructed in Section 2 have applications to other areas of combinatorics. Indeed, the class constructed here provides a solution to a problem mentioned in Geramita *et al.* (1973) concerning weighing matrices and orthogonal designs.

The reviewer of this paper raised the interesting question as to which constructions of the matrix A yield $S(q^{k-1})$ symmetric. When $S(q^{k-1})$ is symmetric then both $[I: S(q^{k-1})]$ and $[-S(q^{k-1}): I]$ are bases for the code and this fact can be useful in the analysis of the code. In fact $S(q^{k-1})$ can always be made symmetric by the following argument. By reordering columns of the $k \times n$ matrix H of Section 2, we can assume that the first k columns comprise the $k \times k$ identity matrix. Label each of the n columns of H by the projective k-tuple which it contains. Form an $n \times n$ matrix A with rows and columns labeled with these k-tuples in an identical manner and use H as the first k rows. Label these first k rows by $\mathbf{x}_i$, $i = 1,..., k$. In the row labeled $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_k)$ place the row vector $\sum_{i=1}^{k} \alpha_i \mathbf{x}_i$. This construction satisfies the properties required of the matrix A and has the additional property that it is symmetric. Consider the element placed in row $\boldsymbol{\alpha}$ and column $\boldsymbol{\beta} = (\beta_1, \beta_2, ..., \beta_k)$. By the construction this will be $\sum_{i=1}^{k} \alpha_i \beta_i$ which is also the element placed in row $\boldsymbol{\beta}$ and column $\boldsymbol{\alpha}$. The matrix $S(q^{k-1})$ obtained from A will also be symmetric.

Acknowledgment

The author would like to thank the reviewer for pointing out the significance of constructing $S(q^{k-1})$ to be symmetric.

Received: June 7, 1974

References

Pless, V. (1972), Symmetry codes over GF(3) and new five designs, *J. Combinatorial Theory, Ser. A*, **12**, 119–142.

Stiffler, J. J. (1971), "Theory of Synchronous Communications," Prentice-Hall, Englewood Cliffs, NJ.

Geramita, A. V., Geramita, J. M., and Wallis, J. S. (1973), Orthogonal Designs, Queen's Mathematical Preprint No. 1973-37, Department of Mathematics, Queen's University, Kingston, Canada.