FAMILIES OF CODES FROM ORTHOGONAL (0,1,-1)-MATRICES

by

Jennifer Seberry Wallis

I.A.S., A.N.U., Canberra, A.C.T., Australia

Abstract

Sloane and Seidel have constructed $(n,2n,\frac{1}{2}(n-2))$ and $(n-1,2n,\frac{1}{2}(n-2))$ codes whenever $n = 1 + a^2 + b^2 \equiv 2 \pmod 4$, a,b integer, is the order of a conference matrix. We give constructions for $(n,2n,\frac{1}{2}(n-2))$ and $(n-1,2n,\frac{1}{2}(n-4))$ codes when $n \equiv 2 \pmod 4$ and conference matrices cannot exist.

In particular we give results for $n = 22, 34, 66, 70, 106, 130, 154, 162, 202, 210, \ldots$,"210,..., but our codes are not as "good" as those from Hadamard matrices or of Sloane and Seidel".

~~~~~~~~~~~~~~~~~~~~

This paper was written while the author was visiting Queen's University, Kingston, Ontario, Canada.

PROC. THIRD MANITOBA CONFERENCE ON NUMERICAL MATH., 1973, pp. 419-426.
~~~~~~~~~~~~~~~~~~~~

1. Introduction

We use I for the identity matrix and J for the matrix of all 1's. The orders of matrices should be determined from the context.

We shall call an $M \times n$ (0,1) matrix, any pair of whose row vectors differ in at least d coordinates, an (n,M,d) code. We refer the reader to [2] for a recent survey.

A square (1,-1) matrix, H, of order h, which satisfies $HH^T = hI_h$ will be called an Hadamard matrix. If $H = I+S$ where $S^T = -S$ then H is called a skew-Hadamard matrix. For more details see [4].

A symmetric conference matrix $I + N$ is a square (1,-1) matrix of order $c \equiv 2 \pmod 4$ for which $NN^T = (c-1)I_c$, $N^T = N$. Necessarily $n = 1 + a^2 + b^2$, where a,b are integers (see [4]).

Suppose A is a (1,-1)-matrix of size $M \times n$. Suppose x is the maximum inner product between distinct rows of A. Then

$$C = \frac{1}{2}(J+A) \quad ,$$

where J is the appropriate matrix of all 1's, is an

$$(n,M,d) \text{ code with } x = n-2d \quad .$$

Thus if H is an Hadamard matrix of order n and

$$A = \begin{bmatrix} H \\ -H \end{bmatrix} \quad ,$$

$x = 0$ and $C = \frac{1}{2}(J+A)$ is an $(n,2n,\frac{1}{2}n)$ code.

Let N be a symmetric conference matrix of order $n = 2 \pmod 4$. Now

$$A = \begin{bmatrix} I+N \\ I-N \end{bmatrix} ,$$

has $x = 2$ and C is an $(n,2n,\frac{1}{2}(n-2))$ code. Sloane and Seidel [3] observed that this code is especially good as removing the first column does not effect the distance and an $(n-1,2n,\frac{1}{2}(n-2))$ code is obtained.

The codes we obtain below are not as good as those of Sloane and Seidel in that our $(n,2n,\frac{1}{2}(n-2))$ codes only give $(n-1,2n,\frac{1}{2}(n-4))$ codes but our codes exist for n for which the Sloane-Seidel codes **cannot exist as conference matrices** cannot exist for those n. Some orders for which conference matrices cannot exist are

22, 34, 58, 70, 78, 94, 106, 130, 134, 142, 162, 166, 178, 190, 202, 210, 214,...,342,...

and for which conference matrices can exist but are note known are

46, 66, 86, 118, 146, 154, 186, 206, 222, 246, 262, 266,... .

We give some results for $n = 22, 34, 66, 70, 106, 130, 154, 162, 202, 210, 266,...,342,...$.

2. A Construction

Suppose

$$\begin{bmatrix} 1 & 1 \ldots 1 \\ 1 & \\ \vdots & B \\ 1 & \end{bmatrix}$$

is an Hadamard matrix of order $h = c \pm 2$ where $c \equiv 2 \pmod 4$ is the order of a symmetric conference matrix $I + N$. Then

$$BJ = -J \quad \text{and} \quad BB^T = hI - J \ .$$

Now consider

$$A = \begin{bmatrix} I \times J & + & N \times B \\ -I \times J & - & N \times B \end{bmatrix} \ , \qquad (1)$$

which is a $(1,-1)$ matrix with maximum inner product $+2$. Hence $\frac{1}{2}(J+A)$ is an $(m, 2m, \frac{1}{2}m-1)$code, where $m = c(c+1)$ or $c(c-3)$.

So we have

Theorem 1: Suppose c is the order of a symmetric conference matrix and there exists an Hadamard matrix of order $c+2$ or $c-2$. Then there exist

$$(m, 2m, \tfrac{1}{2}m-1)$$

codes with $m = c(c+1)$ or $c(c-3)$ respectively.

Hence we have

(70, 140, 34) , (154, 308, 76) and (210, 420, 104)

codes.

We note that the matrix J in (1) may be replaced by $J - 2I$ when $B = I+S$ with $S^T = -S$, $SJ = 0$ and we have:

Theorem 2: Suppose c is the order of a symmetric conference matrix and there exists a skew-Hadamard matrix of order $c+2$ or $c+6$. Then there exist $(m, 2m, \frac{1}{2}m-1)$ codes with $m = c(c+1)$ or $c(c+5)$ respectively.

Hence we have

(66, 132, 32) and (266, 532, 132) codes.

3. Another Construction

Suppose I, X, Y are $(0,1,-1)$-matrices of order m which satisfy

(i) I, X, Y are all circulant;

(ii) $I \pm X \pm Y$, $I \pm X \pm X^T$ and $I \pm Y \pm Y^T$ are $(1,-1)$-matrices;

(iii) $I + XX^T + YY^T = mI_m$.

Then the maximum inner product of distinct rows of

$$C = \begin{bmatrix} I+X+Y & I+X-Y \\ I+X^T-Y^T & -I-X^T-Y^T \\ -I-X-Y & -I-X+Y \\ -I-X^T+Y^T & I+X^T+Y^T \end{bmatrix}$$

is $+2$ and so $\frac{1}{2}(J+C)$ is a $(2m, 4m, m-1)$ code.

Now such matrices I, X, Y are known to exist for

$$m = 1 + 2^a 10^b 26^c \quad , \quad a,b,c \text{ positive integers,}$$

and hence we have

(22, 44, 10), (34, 68, 16), (66, 132, 32), (106, 212, 52), (130, 260, 64), (162, 324, 80), (202, 404, 100) etc. codes.

We note that for the orders $n = 22, 34, 106, 130, 162, 202$ the Sloane-Seidel codes cannot exist. Summarizing

Theorem 3: There exist $(n,2n,\frac{1}{2}n-1)$ codes when $n = 2(1+2^a10^b26^c)$, a,b,c positive integers.

4. Final Comment

We have used M for the number of codewords. In [1] Goethals states that for a complementary code (i.e. a code having the property that, for any vector in the code, its binary complement is also in the code), the maximal number of code words. A(n,d) of an (n,M,d) code is given by

$$A(n,d) \leq 8d(n-d)/(n-(n-2d)^2) \text{ , for } n-\sqrt{n} < 2d \leq n \text{ .}$$

Now for $(n,2n,\frac{1}{2}(n-2))$ codes

$$2n < A(n,d) \leq 2(n-2)(n+2)/(n-4) \text{ , for } n > 2 \text{ .}$$

But as $n \to$ large , $A(n,d) \to 2n$ and these codes are more nearly optimal. For $(n-1,2n,\frac{1}{2}(n-4))$ codes

$$2n < A(n,d) \leq 2(n-4)(n+2)/(n-10) \text{ , for } n > 10 \text{ .}$$

But as $n \to$ large, $A(n,d) \to 2n-4$ and we have the seeming contradiction that for large n our codes have more codewords than the bound given by Grey.

Finally we note that if $h = n+2$ is the order of an Hadamard matrix there exist

$$(n,2n+4,\tfrac{1}{2}(n-2)) \text{ and } (n-1,2n+4,\tfrac{1}{2}(n-4))$$

codes and our

$$(n,2n,\tfrac{1}{2}(n-2)) \text{ and } (n-1,2n,\tfrac{1}{2}(n-4))$$

codes always have slightly greater redundancy.

References

[1] J.M. Goethals, Some Combinatorial Aspects of Coding Theory, M.B.L.E. Research Report, R149, Brussels, 1971.

[2] N.J.A. Sloane, A survey of constructive coding theory, and a table of binary codes of highest known rate, Discrete Math. 3 (1972), 265-294.

[3] N.J.A. Sloane and J.J. Seidel, A new family of nonlinear codes obtained from conference matrices, Annals. of the New York Academy of Sciences, 175, New York, 1970, 363-365.

[4] W.D. Wallis, Anne Penfold Street, Jennifer Seberry Wallis, Combinatorics: Room squares, Sum-free Sets, Hadamard Matrices, Lecture Notes in Mathematics, Vol. 292, Springer-Verlag, Berlin, Heidelberg, New York, 1972.