A NEW FAMILY OF NONLINEAR CODES
OBTAINED FROM CONFERENCE MATRICES

by
N. J. A. Sloane
Bell Telephone Laboratories, Incorporated
Murray Hill, New Jersey

and
J. J. Seidel
Technological University of Eindhoven
Eindhoven, The Netherlands

ABSTRACT

Conference matrices are used to construct a new infinite family of nonlinear error correcting codes with high minimum distance.

CONFERENCE MATRICES ([1])

Let $I_n$ denote the nxn unit matrix, $F_n$ the matrix of all ones, $f_n$ the row vector of n ones, and let a prime (') denote the transpose of a matrix.

A real $(q+1)x(q+1)$ conference matrix $T_{q+1} = (t_{ij})$ satisfies $t_{ii} = 0$, $t_{ij} = +1$ or $-1$ ($i \neq j$), and $T_{q+1}'T_{q+1} = qI_{q+1}$.

By multiplying rows and columns by $-1$, $T_{q+1}$ can be put in the form

$$T_{q+1} = \begin{pmatrix} 0 & f_q \\ f_q' & J_q \end{pmatrix}$$

(1)

where $J_q^q = qI_q - F_q$ and $F_qJ_q = J_qF_q = 0$.

Theorem 1 ([1]): Necessary conditions for a real symmetric $T_{q+1}$ to exist are $q \equiv 1 \pmod{4}$ and $q = a^2 + b^2$, $a$ and $b$ integers.

CODES

An $(n,M,d)$ code is a set of $M$ binary vectors of length $n$, any two of which differ in at least $d$ places, i.e., have distance at least $d$.

If the sum (mod 2) of two code vectors is also in the code, the code is said to be linear. It is thought ([5]) that the best codes may not be linear, but few examples of good nonlinear codes are known (see [6]).
Theorem 2: Let $T_{q+1}$, $q = 4k + 1$, be a real symmetric conference matrix, and let $J_q$ be defined by (1). Then the rows of $A = \frac{1}{2}(I_q + F_q + J_q)$ and of $B = \frac{1}{2}(I_q + F_q - J_q)$ together with the zero vector and the all-ones vector form a binary nonlinear code.

Proof: We must show that any two of these $2q + 2 = 8k + 4$ binary vectors differ in at least $2k$ places. The distances between the zero vector and the rows of $A$ are the elements of $Aq' = (2k+1)q'$ and are all $2k + 1$. To find the distances between rows of $A$, we convert $A$ to a (+1,-1) matrix by defining $A^* = F_q - 2A = -(I_q + F_q)$. Then the minimum distance between distinct rows of $A$ is $\frac{1}{2}(q - \text{largest dot product of distinct rows of } A^*)$, which is found to be $2k$. The other verifications are similar, and are omitted.

EXAMPLES

For $q = p^h \equiv 1 \pmod{4}$, $p$ prime, real symmetric conference matrices $T_{q+1}$ have been constructed (see [1]). Thus the codes (2) exist for lengths $4k + 1 = 5, 9, 13, 17, 25, 29, 37, 41$. 21 and 33 do not exist by Theorem 1, and 45 is the first undecided case.

The $(9,20,4)$ code has been constructed by different methods in [2] and [6], and in [4] has been used to give a dense sphere packing in nine dimensional Euclidean space. The $(9,20,4)$ code was shown in [7] to be optimal, but it is not known whether any of the longer codes are optimal.

REMARKS

Theorem 2 generalized a construction of Sloane and Whitehead ([6]), which gave the codes (2) for the case $q = \text{prime} \equiv 1 \pmod{4}$.

The following coincidence, pointed out to us by S. M. Johnson, is worth mentioning. Grey ([3]) has given an upper bound for the number of codewords in codes which are closed under complementation. Although the codes (2) do not have this property, they do meet the bound.

REFERENCES


