A new description of the Nadler code

Reprinted by permission from IEEE TRANSACTIONS ON INFORMATION THEORY
Vol. IT-18, No. 6, November 1972, pp. 825-826

A New Description of the Nadler Code

J. H. VAN LINT

Abstract—**A binary code of length 12 and minimum distance 5 with 32 words was discovered by Nadler in 1961. Systematic descriptions of this code given later use larger codes. This correspondence gives a direct construction of Nadler's code.**

If we consider binary codes of block length 12 with minimum distance 5 then it is known [1] that these codes have at most 35 words. The best code presently known of this length with $d = 5$ was discovered by Nadler [2]. His description of the code showed no structure. Since then this code and extensions of this code, e.g., the Nordstrom–Robinson quadratic code [3], have been found to be shortened subcodes of the binary Golay code [4]. Using this knowledge the structure of the Nadler code can be studied, e.g., by showing that it is systematic. The purpose of this correspondence is to present a direct construction of the Nadler code from which the minimum distance is easily proved to be 5 and from which we show the automorphism group of the code to be a transitive group of order 72, namely the even part of $(S_3 \times S_4)$.

Notation: We shall use the following (0,1)-matrices: I_n denotes the identity matrix of order n. If no index is given the order is 3. J always denotes a matrix in which all entries are 1. If no size is given it is 3 by 3 or obvious from the context. E_i is a matrix in which all entries in row i are 1 and all other entries 0. We define

$$P = \begin{pmatrix} 010 \\ 001 \\ 100 \end{pmatrix}.$$

Note that $P^T = P^2$ and $I + P + P^2 = J$. In the following a number of matrices of order 12 will occur that have the form

$$M(R,S) = \begin{pmatrix} RSSS \\ SRSS \\ SSRS \\ SSSR \end{pmatrix},$$

where R and S are of order 3. We use the symbol $M(R,S)$ for such matrices.

For the construction of the code we need four matrices A, B, C, and D defined as follows:

$$A \triangleq M(J - I, I).$$

Using block multiplication we find that $AA^T = M(4I + J, 2J)$, which shows us the following.

1) Every row of A is a word of weight 5 (since all diagonal elements of AA^T are 5).

2) Any two distinct rows of A have distance 6 or 8 (since the distance between two vectors is the sum of their weights minus twice their inner product, and here the inner products are the off-diagonal elements of AA^T, which are one or two). It is in-

Manuscript received November 3, 1971.
The author is with the Bell Telephone Laboratories, Inc., Murray Hill, N.J.

teresting to remark that

$$\begin{pmatrix} J_4 - I_4 & E_1 & E_2 & E_3 & E_4 \\ E_1^T & & & & \\ E_2^T & & A & & \\ E_3^T & & & & \\ E_4^T & & & & \end{pmatrix}$$

is a (16,6,2) block design with a symmetric incidence matrix, namely the symmetric Hadamard design.

$$B \triangleq \begin{pmatrix} J & P & I & P^2 \\ P & J & P^2 & I \\ I & P^2 & J & P \\ P^2 & I & P & J \end{pmatrix}.$$

Using block multiplication we find $BB^T = M(3I + 3J, 3J - I)$.

3) Every row of B is a word of weight 6.

4) Any two distinct rows of B have distance 6 or 8. Again B is part of a block design, namely the (15,7,3) design

$$\begin{pmatrix} J & I & I & I & I \\ I & & & & \\ I & & B & & \\ I & & & & \\ I & & & & \end{pmatrix}.$$

C is of size 3 by 12 and given by

$$C \triangleq (J - I, J - I, J - I, J - I).$$

5) Clearly the three rows of C are words of weight 8 with mutual distances all equal to 8.

D is of size 4 by 12 and given by

$$D \triangleq (J - E_1, J - E_2, J - E_3, J - E_4),$$

where J and E_i are of size 4 by 3.

6) The rows of D are words of weight 9 with all distances equal to 6.

We now claim that $\mathbf{o}$ and the rows of A, B, C, and D form a code with minimum distance 5. The weight enumerator of this code is $1 + 12Z^5 + 12Z^6 + 3Z^8 + 4Z^9$ and the number of words is 32. To prove that the minimum distance is indeed 5 all we have to do, besides referring to (1) to (6), is to calculate the following matrix products

$$AB^T = M(5J,3J) - 2B^T,$$

a matrix in which all entries are 3 or 1 showing that

7) each row of A has distance 5 or 9 from the rows of B

$$CA^T = (4J - 2I, 4J - 2I, 4J - 2I, 4J - 2I)$$

showing that

8) each row of A has distance 5 or 9 from the rows of C

$$CB^T = (4J,4J,4J,4J),$$

showing that

9) each row of B has distance 6 from each row of C

$$DA^T = 3J + D,$$

a matrix in which all entries are 3 or 4, showing that

10) each row of A has distance 8 or 6 from the rows of D. $DB^T = 3J + 2D$, a matrix in which all entries are 3 or 5, showing that

11) each row of B has distance 9 or 5 from the rows of D. Finally $DC^T = 6J$, showing that

12) each row of C has distance 5 from each row of D. This completes the proof.

Furthermore the matrix products that yield 1)–12) give the complete distance structure of the code.

We now turn to the problem of finding permutations that leave the code invariant. First, we consider the words of weight 6 (rows of B), which we rewrite as 3-by-4 matrices in which the four columns are the four 3-tuples that form the corresponding row of B. (This representation was suggested by Conway.) We find

$$\begin{pmatrix}1010\\1100\\1001\end{pmatrix}, \begin{pmatrix}1001\\1010\\1100\end{pmatrix}, \begin{pmatrix}1100\\1001\\1010\end{pmatrix}; \begin{pmatrix}0101\\1100\\0110\end{pmatrix}, \begin{pmatrix}0110\\0101\\1100\end{pmatrix}, \begin{pmatrix}1100\\0110\\0101\end{pmatrix};$$
$$\begin{pmatrix}1010\\0011\\0110\end{pmatrix}, \begin{pmatrix}0110\\1010\\0011\end{pmatrix}, \begin{pmatrix}0011\\0110\\1010\end{pmatrix}; \begin{pmatrix}0101\\0011\\1001\end{pmatrix}, \begin{pmatrix}1001\\0101\\0011\end{pmatrix}, \begin{pmatrix}0011\\1001\\0101\end{pmatrix}.$$

A simple inspection of these matrices shows that we can combine any permutation of the columns with any permutation of the rows that has the same parity. These form a subgroup of index 2 in $S_3 \times S_4$. The matrices A, C, and D have greater symmetry than B. From their form it is obvious that each of the permutations that leave the set of words of weight 6 invariant also leaves the remaining part of the code invariant. Furthermore, from C and D it is clear that no other permutations leave the code invariant. Hence, the subgroup of index 2 in $S_3 \times S_4$ named above is the automorphism group of the Nadler code.

Remarks

i) By combinatorial arguments we can show that a code with minimum distance 5 and block length 12 that has the rows of A as codewords can contain no codewords of weight 7 and at most 12 words of weight 6. If we take these 12 words to be the rows of B then we can add at most 3 words of weight 8 and at most 4 words of weight ≥ 9 as was done above. The rows of B exclude the inclusion of words of weight 4. It seems unlikely that a better code of this length exists.

ii) If we consider only the 12 rows of A and try to add words of weight 4 keeping the minimum distance at 5 then it is possible to add 6 words, namely the rows of

$$E: = \left(\begin{array}{c|c|c|c} 000 & 000 & 011 & 011 \\ 000 & 101 & 000 & 101 \\ 000 & 110 & 110 & 000 \\ \hline 110 & 000 & 000 & 110 \\ 101 & 000 & 101 & 000 \\ 011 & 011 & 000 & 000 \end{array}\right)$$

in which each of the eight submatrices is obtained from $J - I$ by replacing rows by (000). If we take the rows of A and E and extend to length 13 by adding an anticheck, the resulting set has 18 words of length 12, weight 5, and minimum distance 6, which is known to be the maximum number of such words.

iii) It is not hard to check that the code as described in this correspondence is systematic, e.g., on positions 1, 4, 7, 10, and 2.

References

[1] S. M. Johnson, "On upper bounds for unrestricted binary error-correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-17, pp. 466–478, July 1971.
[2] M. Nadler, "A 32-point $n = 12$, $d = 5$ code," *IRE Trans. Inform. Theory* (Corresp.), vol. IT-8, p. 58, Jan. 1962.
[3] A. W. Nordstrom and J. P. Robinson, "An optimum nonlinear code," *Inform. Contr.*, vol. 11, pp. 613–616, 1968.
[4] J. M. Goethals, "On the Golay perfect binary code," *J. Comb. Theory*, vol. 11, pp. 178–186, 1971.