but if the burst syndrome is in H_2 it is not in H_2' and if it is in H_3 it is not in H_3', and if in H_4 it is not in H_4', where H_2', H_3', and H_4' are given by

$$H_2' = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \quad H_3' = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \\ 0 & 0 \end{bmatrix} \quad H_4' = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Thus by using the null spaces of H_i and H_i' one can test for a block-zero burst. For example, the null space of H_3 is G_3 where $H_3G_3^T = 0$, and the null space of H_3' is G_3' where $H_3'G_3'^T = 0$.

$$G_3 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad G_3' = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

For a block-zero syndrome to be in the space of H_3 it is necessary and sufficient that $S^TG_3 = 0$ and $S^TG_3' \neq 0$, where S is the syndrome. From H_3, it is seen that $e_0^{(3)} = s_1$, $e_0^{(4)} = s_0 + s_1$, $e_1^{(1)} = s_5$, and $e_1^{(2)} = s_2$ where s_i $(0 \leq i \leq 7)$ are the syndrome bits. This method requires less logic than testing the syndrome against every possible block-zero burst [3], especially as the rate increases (if higher rate codes are discovered).

An optimal type-$B1$ code of rate $\frac{2}{5}$ has also been discovered. It is given by

$$B_0 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & & & \\ 0 & 0 & & & \\ 0 & 1 & & & \\ 0 & 0 & & & \\ 1 & 0 & & & \\ 0 & 1 & & & \\ 1 & 0 & & & \end{bmatrix}.$$

An optimal type-$B1$ code of rate $1/n_0$ is given by

$$B_0(1/n_0) = \begin{bmatrix} 0 & \\ 0 & I_{n_0-1} \\ \vdots & \\ 0 & \\ \hline 1 & \\ 0 & \\ \vdots & \\ 0 & \\ 1 & \end{bmatrix},$$

where $I_{(n_0-1)}$ is the identity matrix of order $n_0 - 1$. In [3], $B_0(1/3)$ was given as an optimal type-$B2$ code.

References

[1] E. R. Berlekamp, "Note on recurrent codes," *IEEE Trans. Inform. Theory* (Corresp.), vol. IT-10, pp. 257–258, July 1964.

[2] J. L. Massey, "Implementation of burst-correcting convolutional codes," *IEEE Trans. Inform. Theory*, vol. IT-11, pp. 416–422, July 1965.

[3] R. W. Lucky, J. Salz, and E. J. Weldon, Jr., *Principles of Data Communication*. New York: McGraw-Hill, 1968, pp. 398–404.

[4] A. D. Wyner and R. B. Ash, "Analysis of recurrent codes," *IEEE Trans. Inform. Theory*, vol. IT-9, pp. 143–156, July 1963.

Is There a (72,36) $d = 16$ Self-Dual Code?

N. J. A. SLOANE

We wish to draw the attention of the readers of this TRANSACTIONS to an unsolved problem in coding theory. According to a theorem of Gleason [1], [2], [3], the greatest possible minimum distance d of a binary self-dual code in which the length n is a multiple of 24, and all weights are divisible by 4, is $d = \frac{1}{6}n + 4$. (A self-dual code is a linear code of rate $\frac{1}{2}$ which coincides with its dual code.)

For the first two values of n such codes exist and have this greatest minimum distance: these are the $(n,k) = (24,12)$, $d = 8$ Golay code, and the $(48,24)$, $d = 12$, quadratic residue code. The next case is undecided, and it is this problem that we wish the reader to consider: does there exist a (72,36), $d = 16$, binary self-dual code in which all weights are divisible by 4?

The weight distribution of any code in this family is given in [4]. In particular, the (72,36) code would have the following weight distribution

i		A_i
0	72	1
16	56	249,849
20	52	18,106,704
24	48	462,962,955
28	44	4,397,342,400
32	40	16,602,715,899
36		25,756,721,120

A $t - (v,k,\lambda)$ design is a collection of k-subsets, called blocks, of a given v-set S such that every t-subset of S is contained in exactly λ blocks. (An x-set is a set of cardinality x.) Whenever a code of length n in the above family exists, it follows from the theorem of Assmus and Mattson [5, Theorem 4.2] that the codewords of any fixed weight i form the blocks of a $5 - (n,i,\lambda)$ design with $\lambda = A_i \binom{i}{5} \Big/ \binom{n}{5}$. For example, the codewords of weight 16 in the (72,36) code would form a $5 - (72,16,78)$ design.

References

[1] A. M. Gleason, "Weight polynomials of self-dual codes and the MacWilliams identities," *Act. Congr. Int. Math.*, vol. 3, pp. 211–215, 1970. Paris: Gauthier-Villars, 1971.

[2] E. R. Berlekamp, F. J. MacWilliams, and N. J. A. Sloane, "Gleason's theorem on self-dual codes," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 409–414, May 1972.

[3] F. J. MacWilliams, C. L. Mallows, and N. J. A. Sloane, "Generalizations of Gleason's theorem on weight enumerators of self-dual codes," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 794–805, Nov. 1972.

[4] C. L. Mallows and N. J. A. Sloane, "An upper bound for self-dual codes," *Inform. Contr.*, to be published.

[5] E. F. Assmus, Jr., and H. F. Mattson, Jr., "New 5-designs," *J. Comb Theory*, vol. 6, pp. 122–151, Mar. 1969.

Manuscript received August 25, 1972.
The author is with the Bell Laboratories, Murray Hill, N.J.