M. Y. Hsiao
D. C. Bossen
R. T. Chien

Orthogonal Latin Square Codes

Abstract: A new class of multiple-error correcting codes has been developed. Since it belongs to the class of one-step-decodable majority codes, it can be decoded at an exceptionally high speed. This class of codes is derived from a set of mutually orthogonal Latin squares. This mutually orthogonal property provides a class of codes having a unique feature of "modularity." The parity check matrix possesses a uniform pattern and results in a small number of inputs to modulo 2 adders. This class of codes has m^2 data bits, where m is an integer, and $2tm$ check bits for t-error correcting.

Introduction

The paper deals with the class of one-step majoriyt-decodable codes. In general, a t-error correcting majority-decodable code[1–7] works on the principle that $2t + 1$ copies of each information bit are generated from $2t + 1$ independent sources. One copy is the bit itself received from memory or any transmitting device. The other $2t$ copies are generated from $2t$ parity relations involving the bit. By choosing a set of h Latin squares that are pairwise orthogonal, one can construct a parity check matrix such that the number of 1's in each column is $2t = h + 2$. The orthogonality condition ensures that for any bit b_i there exists a set of $2t$ parity check equations orthogonal on b_i, and thus makes the code self-orthogonal and one-step majority decodable. One-step majority decoding is the fastest parallel decoding method.

The only related work we have found in the literature is that of Olderoge[8] of the Soviet Union. He discovered a class of double-error correcting and triple-error detecting codes using a single Latin square to construct a set of row and column parity check equations.

Besides being one-step majority decodable, our codes are constructed in such a way that the decoder can be built in modular form; i.e., each additional module adds a further error correction capability without affecting the existing modules. This feature of modularity results from parity check equations that are constructed in modular form.

The t-error correcting codes generated by the method of this paper have m^2 data bits and $2tm$ check bits per word. The minimum distance between words is $d = h + 3$, where h is the number of orthogonal Latin squares that can be constructed with m elements. The relation between m and h is given by $h = \min (p_i^{e_i} - 1)$, where the $p_i^{e_i}$ are integer powers of the prime factors of the integer m.

Orthogonal Latin squares and error correcting codes

In this section, we shall show how the properties of a set of orthogonal Latin squares can be used to construct the parity check matrix of a t-error correcting majority-decodable code. The method of constructing orthogonal Latin squares is included in the Appendix. The reader may either refer to the Appendix or find the existing orthogonal Latin squares from the table of Fisher and Yates.[9]

We shall first review the properties of the parity check matrix that are related to the requirement that the code be majority decodable.[4]

Consider a parity check matrix of a linear code. A set of parity equations is said to be orthogonal on the digit d_i if, for any two parity equations c_1 and c_2 that contain d_i, d_i is the only common variable involved in c_1 and c_2. Now, if there is a set of $2t + 1$ parity equations orthogonal on d_i, then d_i can be decoded correctly by majority coding in the presence of t errors. This is true since each error can alter at most one vote of the majority gate. The preceding information is specifically stated in the following theorem.

Theorem 1:[4] If, in a linear code, there are at least $d - 1$ check sums orthogonal on each digit, then the code has minimum distance at least d.

This theorem implies that the number of 1's in each column of the data-bit positions of the parity check

M. Y. Hsiao and D. C. Bossen are at the Systems Development Division Laboratory in Poughkeepsie, New York. R. T. Chien is at the Coordinated Science Center, University of Illinois, Urbana, Illinois.

matrix $\mathbf{H}$ should be at least $2t$ for t-error correction. In the codes that we derive, the number of 1's in each column is exactly $2t$. The code is self-orthogonal[4] and noncyclic. This t-error correcting code can be derived from the existing orthogonal Latin squares discussed in the following section.

Definition:[10] A Latin square of order (size) m is an $m \times m$ square array of the digits $0, 1, \cdots, m-1$, with each row and column a permutation of the digits $0, 1, \cdots, m-1$. Two Latin squares are orthogonal if, when one Latin square is superimposed on the other, every ordered pair of elements appears only once.

Let the m^2 data bits be denoted by a vector

$$\mathbf{D} = [d_0, d_1, \cdots, d_{m^2-1}]. \tag{1}$$

Then the $2mt$ check-bit equations for t-error correcting are obtained from the following parity check matrix $\mathbf{H}$:

$$\mathbf{H} = \left[\begin{array}{c|c} \mathbf{M}_1 & \\ \mathbf{M}_2 & \\ \mathbf{M}_3 & \mathbf{I}_{2tm} \\ \vdots & \\ \mathbf{M}_{2t} & \end{array}\right]. \tag{2}$$

$\mathbf{I}_{2tm}$ is an identity matrix of order $2tm$ and $\mathbf{M}_1, \cdots, \mathbf{M}_{2t}$ are submatrices of size $m \times m^2$. These submatrices $\mathbf{M}_1 \cdots \mathbf{M}_{2t}$ have the form

$$\mathbf{M}_1 = \begin{bmatrix} 11\cdots1 & & & \\ & 11\cdots1 & & \\ & & \ddots & \\ & & & 11\cdots1 \end{bmatrix}_{m\times m^2} \tag{3}$$

$$\mathbf{M}_2 = [\mathbf{I}_m \mathbf{I}_m \cdots \mathbf{I}_m]_{m\times m^2}. \tag{4}$$

The matrices $\mathbf{M}_3, \cdots, \mathbf{M}_{2t}$ are derived from the existing set of orthogonal Latin squares $\mathbf{L}_1, \mathbf{L}_2, \cdots, \mathbf{L}_{2t-2}$ of size $m \times m$. Denote the set of Latin squares as

$$\begin{aligned} \mathbf{L}_1 &= [l_{ij}^1]_{m\times m} \\ \mathbf{L}_2 &= [l_{ij}^2]_{m\times m} \\ &\vdots \\ \mathbf{L}_{2t-2} &= [l_{ij}^{2t-2}]_{m\times m}, \end{aligned} \tag{5}$$

where

$$l_{ij} \in \{1, 2, \cdots, m\}.$$

For any given Latin square having m elements, one can associate an incidence matrix defined on one of its elements as follows.

Definition: Let $\mathbf{L} = [l_{ij}]_{m\times m}$ be a Latin square; then an incidence matrix defined with respect to the element $\mu (1 \leq \mu \leq m$, integer), denoted by $\mathbf{Q}_\mu = [q_{ij}^\mu]$, is defined by the rules

$$q_{ij}^\mu = \begin{cases} 1 & \text{if} \quad l_{ij} = \mu \\ 0 & \text{if} \quad l_{ij} \neq \mu. \end{cases} \tag{6}$$

For each Latin square of m elements, there exist m incidence matrices $\mathbf{Q}_1, \mathbf{Q}_2, \cdots, \mathbf{Q}_m$. Each incidence matrix is concatenated into a vector form,

$$\mathbf{V}_\mu = [q_{11}^\mu \cdots q_{1m}^\mu q_{21}^\mu \cdots q_{2m}^\mu \cdots q_{m1}^\mu \cdots q_{mm}^\mu]. \tag{7}$$

If submatrix $\mathbf{M}_i$ is derived from a unique Latin square $\mathbf{L}_j$, then

$$\mathbf{M}_i = \begin{bmatrix} \mathbf{V}_1 \\ \mathbf{V}_2 \\ \vdots \\ \mathbf{V}_m \end{bmatrix}, \tag{8}$$

where $\mathbf{V}_1, \mathbf{V}_2, \cdots, \mathbf{V}_m$ are derived from $\mathbf{L}_j$.

The above procedures lead to the following theorem.

Theorem 2: For an existing set of λ_m $m \times m$ orthogonal Latin squares ($\lambda_m \leq m-1$), there exists a t-error correcting code, where*

$$t = \left\lfloor \frac{\lambda_m}{2} \right\rfloor + 1 \tag{9}$$

under the previously described procedures of constructing the $\mathbf{H}$ matrix.

Proof: We show that the entire set of parity check equations specified by the $\mathbf{H}$ matrix is "pairwise" orthogonal. This is clearly true for the equations in $\mathbf{M}_1$ and $\mathbf{M}_2$. For $\mathbf{M}_3, \mathbf{M}_4, \cdots, \mathbf{M}_{2t}$, no two elements of an $\mathbf{M}_i$ have any intersections. Suppose now that an element of $\mathbf{M}_i$ and an element of $\mathbf{M}_j$ for $i, j = 3, 4, \cdots, 2t$ and $i \neq j$ have more than one intersection. This implies that the superposition of Latin squares $\mathbf{L}_i$ and $\mathbf{L}_j$ has an ordered pair occurring more than once, contrary to their orthogonality. Suppose that some element of $\mathbf{M}_i$ for $i \neq 1, 2$ has more than one intersection with either $\mathbf{M}_1$ or $\mathbf{M}_2$. But this implies that $\mathbf{M}_i$ is not a Latin square.

Illustrative example

A detailed example demonstrates the building concept of modularity.

Example: Given $k = 25$, design a system derived from an orthogonal Latin square code of class (n, k).

Start with single-error correction. Since $k = 25 = 5^2$, there is a (35, 25) single-error correcting code with the

* $\lfloor X \rfloor$ is the greatest integer $\leq X$.

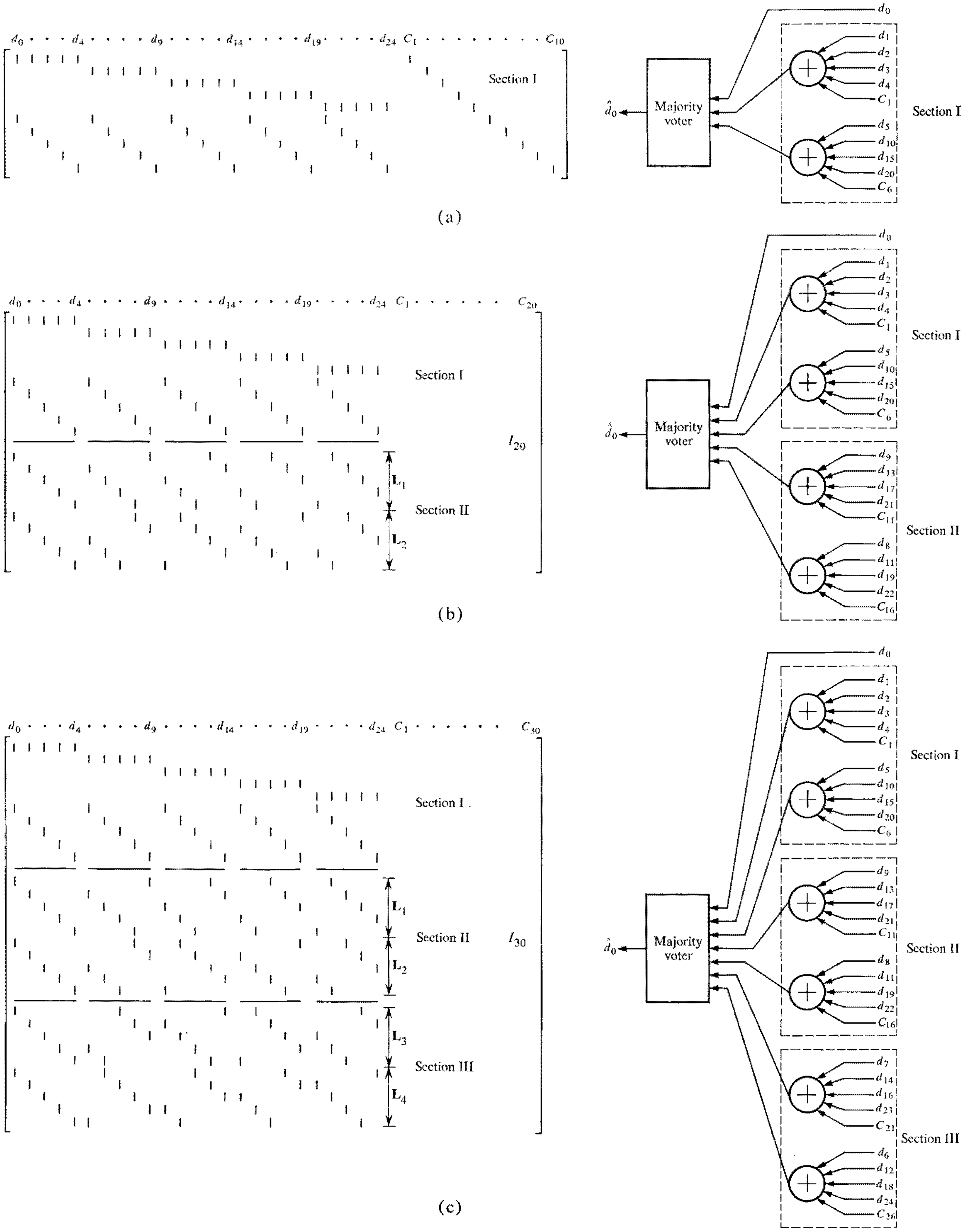

Figure 1 H matrices and decoder circuits for data-bit d_0. (a) Single-error correcting code (35, 25); (b) double-error correcting code (45, 25); and (c) triple-error correcting code (55, 25).

H matrix as shown in Fig. 1(a). Note here that only $\mathbf{M}_1$ and $\mathbf{M}_2$ are used. The decoding circuit for data bit d_0 is also shown in Fig. 1(a).

If there is a need for the system to have the error correcting capability increased, a maximum set of orthogonal Latin squares is sought. Since $25 = 5^2$ and $m = 5$, there exist four possible orthogonal Latin squares:

$$L_1 = \begin{matrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{matrix} \qquad L_2 = \begin{matrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{matrix}$$

$$L_3 = \begin{matrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \end{matrix} \qquad L_4 = \begin{matrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 3 & 4 & 0 & 1 & 2. \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \end{matrix}$$

To generate additional coding for the double-error correcting capability, ten more check bits are necessary since $2tm$ equals 20. These additional ten equations are derived from the Latin squares L_1 and L_2.

Use the procedures described in the previous section for converting the Latin squares into the H matrix as shown in Fig. 1(b). Note that rows 11 to 15 are derived from L_1 and rows 16 to 20 are derived from L_2.

Check bits C_{11} up to C_{20} can be similarly derived. The decoder for data bit d_0 shown in Fig. 1(b) now requires two identical logic boxes instead of the one shown in Fig. 1(a).

The circuitry necessary for correcting the additional error (the second error) can be added to the first error correcting circuit as a modular arrangement (see Section II, Fig. 1(b). It is not necessary to interfere with the mechanization of the original first-error correcting circuit. This arrangement allows for considerable flexibility in circuits that can be built in modular form and easily packaged.

Extending the example to triple-error correction capability, the modularity concept can be further utilized by deriving additional check-bit equations $C_{21}, C_{22}, \cdots, C_{30}$ from Latin squares L_3 and L_4. This results in a (55, 25) triple-error correcting code shown in Fig. 1(c). To decode data bit d_0, simply add a third section [Section III of Fig. 1(c)] to the existing Section I and II modules.

This example demonstrates the modular property. The choice of any section of the H matrix results in single-error correcting codes; the choice of any two sections will result in double-error correcting codes; the choice of all three possible sections results in a triple-error correcting code. Moreover, the circuit for implementing each module is identical. The triple-error correction capability, since there are no additional orthogonal Latin squares, is the maximum capability of this code. Generally, the maximum t is less than or equal to $(m + 1)/2$.

Conclusions

An ideal error correcting code must have a high speed and simple decoder with minimum number of check bits. Unfortunately, speed and redundancy do not go together. Low redundancy usually implies the requirement of a complex and slow decoder. One example is the decoding process of the BCH codes. One way of solving this dilemma is to increase the redundancy so that decoding is fast and inexpensive. Following this line, the class of orthogonal Latin square codes was developed by adding redundancy systematically. Low-density parity check matrices were obtained as a result of high redundancy. The decoder shows simplicity and regularity because only mod 2 adders and $(2t + 1)$-way voting gates are required. Furthermore, modularity was introduced and this further simplified the design of the decoder. At a time when integrated circuits are being developed rapidly, orthogonal Latin square codes should make a strong and timely candidate for competition with linear cyclic codes in the field of error correction for computer applications.

Appendix. Construction of a set of orthogonal Latin squares

The essential result of finding a set of h orthogonal Latin squares of order m is the following theorem from Mann.[10]

Theorem: Let $m = p_1^{e_1} p_2^{e_2}, \cdots, p_s^{e_s}$ be the factorization of m into prime powers. Let

$$g_{i_1}^{(1)}, g_{i_2}^{(2)}, \cdots, g_{i_s}^{(s)}$$

denote the elements of GF $(p_1^{e_1})$, GF $(p_2^{e_2})$, $\cdots$, GF $(p_s^{e_s})$, respectively, where $g_0^{(1)}$ is the 0 element and $g_1^{(i)}$ is the identity element of GF $(p_i^{e_i})$. Form the points

$$\gamma = [g_{i_1}^{(1)}, g_{i_2}^{(2)}, \cdots, g_{i_s}^{(s)}],$$

which are elements of the Cartesian product of GF $(p_1^{e_1})$, GF $(p_2^{e_2})$, $\cdots$, GF $(p_s^{e_s})$. These elements are multiplied and added by multiplying and adding their coordinates. Further, let

$$\gamma_j = [g_j^{(1)}, g_j^{(2)}, \cdots, g_j^{(s)}]$$

$$0 < j \leq h = \min (p_i^{e_1} - 1)$$

and number the remaining γ in any arbitrary way from $h + 1$ to m so that

$$\gamma_m = 0 = [g_0^{(1)}, g_0^{(2)}, \cdots, g_0^{(s)}].$$

Then, the arrays

$$\mathbf{L}_j = \begin{array}{llll} 0 & 1 & \cdots & \gamma_{m-1} \\ \gamma_j & \gamma_j + 1 & \cdots & \gamma_j + \gamma_{m-1} \\ \gamma_j\gamma_2 & \gamma_j\gamma_2 + 1 & \cdots & \gamma_j\gamma_2 + \gamma_{m-1} \\ \vdots & \vdots & & \vdots \\ \gamma_j\gamma_{m-1} & \gamma_j\gamma_{m-1} + 1 & \cdots & \gamma_j\gamma_{m-1} + \gamma_{m-1} \end{array}$$

for $j = 1, 2, \cdots, h$ form a set of h orthogonal Latin squares.

A few special cases are of interest. For example, if $m = p$ is a prime number, then the arrays

$$\mathbf{L}_j = \begin{array}{llll} 0 & 1 & \cdots & m-1 \\ j & 1+j & \cdots & m-1+j \\ 2j & 1+2j & \cdots & m-1+2j \\ \vdots & \vdots & & \vdots \\ (m-1)j & 1+(m-1)j & \cdots & (m-1)+(m-1)j \end{array}$$

for $j = 1, 2, \cdots, m-1$ are written using mod m arithmetic and form the maximal set of orthogonal Latin squares of order m.

The case for $m = p^e$ is also of interest. The construction of $(m-1)$ orthogonal Latin squares is obtained by constructing a GF (p^e) which contains W as a primitive root.[11] The elements of this GF (p^e) are $0, 1, X_3, \cdots, X_m$. Then, the set of orthogonal Latin squares is as follows:

$$\bar{\mathbf{L}}_j = \begin{array}{llll} 0 & 1 & \cdots & X_m \\ W^{0+j} & 1 + W^{0+j} & \cdots & X_m + W^{0+j} \\ W^{1+j} & 1 + W^{1+j} & \cdots & X_m + W^{1+j} \\ \vdots & \vdots & & \vdots \\ W^{m-2+j} & 1 + W^{m-2+j} & \cdots & X_m + W^{m-2+j} \end{array}$$

for $j = 0, 1, \cdots, m-2$.

It should be observed that $\bar{\mathbf{L}}_{j+1}$ is obtained from $\bar{\mathbf{L}}_j$ by cyclically permuting the last $m - 1$ rows.

Example: Let $m = 4$. We have GF (2^2) and the elements are $0, 1, X, 1 + X$ with X as a primitive root. Its addition table is as shown:

$+$	0	1	X	$1+X$
0	0	1	X	$1+X$
1	1	0	$1+X$	X
X	X	$1+X$	0	1
$1+X$	$1+X$	X	1	0

We shall, however, replace X by 2 and $X + 1$ by 3. Then, cyclically permuting the last three rows of the first square yields the following three orthogonal Latin squares.

$$\begin{array}{cccc} 0&1&2&3\\ 1&0&3&2\\ 2&3&0&1\\ 3&2&1&0 \end{array} \qquad \begin{array}{cccc} 0&1&2&3\\ 2&3&0&1\\ 3&2&1&0\\ 1&0&3&2 \end{array} \qquad \begin{array}{cccc} 0&1&2&3\\ 3&2&1&0\\ 1&0&3&2\\ 2&3&0&1. \end{array}$$

References

1. R. G. Gallager, "Low-density Parity Check Codes," *IRE Trans. Info. Theory* **IT-8,** 21 (1962).
2. S. L. Hakimi and J. G. Bredeson, "Graph Theoretic Error-correcting Codes," *IEEE Trans. Info. Theory* **IT-14,** No. 4, 584 (1968).
3. T. Kasami, S. Lin and W. W. Peterson, "Some Results on Cyclic Codes Which Are Invariant Under the Affine Group," Scientific Report, AFCRL-66-622, Air Force Cambridge Research Laboratory, Bedford, Mass., 1966.
4. J. L. Massey, *Threshold Decoding,* MIT Press, Cambridge, 1963.
5. L. D. Rudolph, "Geometric Configuration and Majority Logic Decodable Codes," MEE Thesis, University of Oklahoma, Norman, Oklahoma, 1964.
6. E. J. Weldon, Jr., "Difference-Set Cyclic Codes," *Bell System Tech. J.* **45,** 1045 (1966).
7. E. J. Weldon, Jr., "Some Results on Majority-Logic Decoding," Technical Report NASA Grant NGR-12-001-046, April 1968.
8. G. B. Olderoge, "Some Special Matrix-type Error-correcting Codes," *Radiotekhno* **18,** No. 7, 14 (1963); *Trans. Part 2,* No. 7, 12–18 (1963).
9. R. A. Fisher and F. Yates, *Statistical Tables for Biological Agricultural and Medical Research,* Hafner Publishing Co., 1957.
10. H. B. Mann, *Analysis and Design of Experiments,* Dover Publications, New York, 1949.
11. R. C. Bose, "On the Application of the Properties of Galois Fields to the Problem of Construction of Hyper-Graeco-Latin Squares," *Sankhya* **3,** Part 4, 323 (1938).

Received August 18, 1969