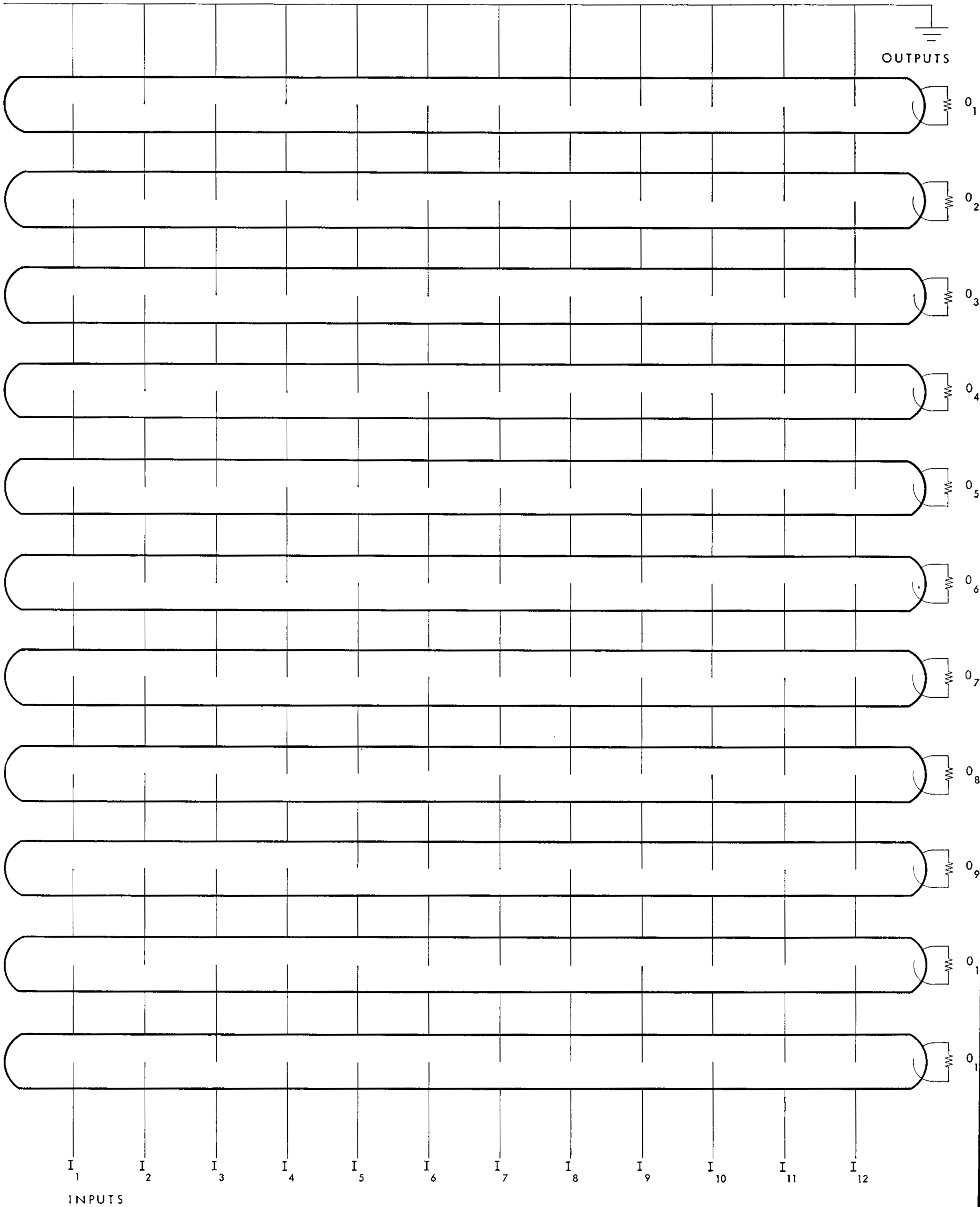

Figure 1 **A noiseless load-sharing matrix switch.**

R. T. Chien

A Class of Optimal Noiseless Load-Sharing Matrix Switches

A load-sharing matrix switch with noise-cancelling features was proposed recently.[1] Another paper[2] suggests that for some cases the number of input wires may be reduced with an improved scheme. The purpose of this note is to report a further improvement over the schemes mentioned. The method to be described requires a minimum number of input wires.

The main body of the paper consists of a mathematical interpretation of the functions of a load-sharing matrix switch in terms of a winding matrix and its identification with a special class of orthogonal matrices. The results obtained by Paley[3] on the construction of orthogonal matrices are then used to advantage in the logical design. It is also shown that the method discussed requires a minimum number of input drivers.

The winding matrix and orthogonality

The features that we wish to incorporate into a noiseless load-sharing matrix switch such as the one shown in Fig. 1 may be summarized in the following conditions:

(1) Half of the input drivers are excited each time for any input pattern.

(2) For each excitation only one output wire is excited, and the excitation should utilize all input power. In all other output wires the net excitation is zero.

If we restrict our attention to the core switches, these requirements may be translated to the requirement on the winding patterns, since the logical structure of a core switch is fixed by the winding patterns of the cores.

The winding pattern of the magnetic cores may be represented by a winding matrix. Each row gives the winding pattern for a core, each column gives the winding pattern for an input driver. The entries are either ONES or MINUS ONES. The matrix entry is ONE if the input wire passes through the core in the reference direction; it is MINUS ONE if the wire passes through the core in the reverse direction. Conditions (1) and (2) can then be restated in terms of the winding matrix as:

(1w) Each row must have as many ONES as MINUS ONES.[4]

(2w) Take any two rows i and k from the matrix, the sum of the values of the entries of row k must be zero for the columns where row i has entry ONE. Same must be true for the columns where row i has MINUS ONE entries.

1	−1	1	−1	1	1	1	−1	−1	−1	1	−1
1	−1	−1	1	−1	1	1	1	−1	−1	−1	1
1	1	−1	−1	1	−1	1	1	1	−1	−1	−1
1	−1	1	−1	−1	1	−1	1	1	1	−1	−1
1	−1	−1	1	−1	−1	1	−1	1	1	1	−1
1	−1	−1	−1	1	−1	−1	1	−1	1	1	1
1	1	−1	−1	−1	1	−1	−1	1	−1	1	1
1	1	1	−1	−1	−1	1	−1	−1	1	−1	1
1	1	1	1	−1	−1	−1	1	−1	−1	1	−1
1	−1	1	1	1	−1	−1	−1	1	−1	−1	1
1	1	−1	1	1	1	−1	−1	−1	1	−1	−1

Figure 2 **Winding matrix of the switch shown in Fig. 1.**

For instance, the winding matrix of the switch in Fig. 1 is shown in Fig. 2. It is seen that the winding matrix satisfies conditions (1w) and (2w). The computation of the matrix of Fig. 2 is illustrated in the two sections that follow.

If one compares the conditions above with the definitions of an orthogonal matrix, it is seen that the rows of the winding matrix satisfy the orthogonality conditions, namely,

$$\sum_{j=0}^{n-1} a_{ij}a_{kj} = \begin{cases} n & i=k \\ 0 & i\neq k \end{cases} .$$

However, an orthogonal matrix does not necessarily satisfy (1w) and (2w).

Given an orthogonal matrix of m rows, it is always possible to construct a winding matrix of $m-1$ rows. To accomplish this, a number of columns in the given matrix are complemented to make the first row consist of ONE entries exclusively.[5] The remaining $m-1$ rows will then satisfy condition (1w) and (2w).

Construction of orthogonal matrices

Methods for constructing orthogonal matrices have been studied by mathematicians as long ago as 1867 by Sylvester.[6] But the results obtained by Paley seem to be more complete. The Paley theory is summarized here without proof. In the following lemmas, m denotes the number of columns in the matrix.

Lemma 0. If $m \neq 1$, 2, then m is divisible by 4.

Lemma 1. If we have a U-matrix[7] of order m_1 and a U-matrix of order m_2 then we may construct a U-matrix of order $m_1 m_2$. The construction is accomplished by substituting U_{m_2} for each "+1" in U_{m_1} and the complement of U_{m_2} for each "−1" in U_m.

Lemma 2. Let m be of the form $p+1$, where p, $\equiv 3 \pmod 4$, is prime.[8] Then we can construct a U-matrix of order m. Let $L(n)$ denote the Legendre symbol (n/p). We write

$$a_{ij} = +1 \qquad (i=0 \text{ or } j=0)$$

$$a_{i,j} = L(j-i) \qquad (1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant p,\ i \neq j),$$

$$a_{i,i} = -1 \qquad (1 \leqslant i \leqslant p).$$

Lemma 3. Let m be divisible by 4 and of the form $2^k(p+1)$, where p is prime. Then we can construct a U-matrix of order m. If $p=2$, or if $p \equiv 3 \pmod 4$, the result follows at once from Lemmas 1 and 2. We may thus assume that $p \equiv 1 \pmod 4$, $k=1$.

We write

$$a_{2i,0} = a_{2i,1} = a_{2i+1,0} = -a_{2i+1,1} = 1 \qquad (1 \leqslant i \leqslant p),$$

$$a_{0,2i} = a_{0,2i+1} = a_{1,2i} = -a_{1,2i+1} = 1 \qquad (1 \leqslant i \leqslant p),$$

$$a_{2i,2j} = a_{2i,2j+1} = a_{2i+1,2j} = a_{2i+1,2j+1} = (j-i) \qquad (1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant p,\ i \neq j),$$

$$a_{2i,2i} = a_{2i,2i+1} = -a_{2i+1,2i} = -a_{2i+1,2i+1} = 1 \qquad (0 \leqslant i \leqslant p).$$

Lemma 4. Let m be divisible by 4 and of the form $2^k(p^h+1)$ where p is an odd prime. Then we can construct a U-matrix of order m.

We may repeat the argument of the last two lemmas instead of quadratic residues (mod p) we consider quadratic residues in the Galois field[9] of polynomials (mod p, mod P) where $P(x)$ is an irreducible polynomial of degree h.

Table 1 **Computation of Legendre functions for $p=11$.**

n	1	2	3	4	5	6	7	8	9	10
n^2	1	4	9	16	25	36	49	64	81	100
$n^2 \pmod p$	1	4	9	5	3	3	5	9	4	1
$L(n)$	1	−1	1	1	1	−1	−1	−1	1	−1

Thus, for instance, if $p^h \equiv 3 \pmod 4$, $k=0$, we write

$$a_{i,j} = +1 \qquad (i=0 \text{ or } j=0)$$

$$a_{i,j} = L(E_j - E_i) \qquad (1 \leqslant i \leqslant p^h,\ 1 \leqslant j \leqslant p^h,\ i \neq j),$$

$$a_{i,i} = -1 \qquad (1 \leqslant i \leqslant p^h),$$

where $E_1, E_2, \ldots, E_{p^h}$ denote the members of the field arranged in any order.

Evaluation of the Legendre functions

The Legendre symbols $(n)/p$ denoted by $L(n)$ is defined as one (minus one) is n is a quadratic residue (nonresidue) of prime p. It is easiest to evaluate all $L(n)$ for $n<p$ at the same time.

We shall use an example to illustrate this: Take $p=11$. First list all integers less than p as in row 1 of Table 1. Then list the squares of these numbers in row 2. Divide the numbers in row 2 by p and list the remainders in row 3. The 4th row exhibits the Legendre function. The entry is ONE if the number at the top of this column appears somewhere in row 3, MINUS ONE otherwise.

In general, there will be $(p-1)/2$ quadratic residues for each prime, so half the numbers will have a value ONE for the Legendre function. This serves as a nice check on the result. The process for any prime p is the same as is shown in the example.

To evaluate the Legendre functions in Galois fields, the same process may be used with a slight modification. In Galois fields of p^m the numbers used are the totality of all polynomials of order less than m with coefficients consisting of integers less than p. For instance, for $GF(3^2)$ there are eight nonzero members, namely, the members in the first row of Table 2. The second row contains the squares of the first row entries. They are reduced

Table 2 **Computation of Legendre functions for $GF(3^2)$.**

g	1	2	x	$2x$	$x+1$	$2x+1$	$x+2$	$2x+2$
g^2	1	4	x^2	$4x^2$	x^2+2x+1	$4x^2+4x+1$	x^2+4x+4	$4x^2+8x+4$
$g^2 \pmod P$	1	4	$x+1$	$x+4$	$3x+2$	$8x+5$	$5x+5$	$12x+8$
$g^2 \pmod P \pmod p$	1	1	$x+1$	$x+1$	2	$2x+2$	$2x+2$	2
$L(g)$	1	1	−1	−1	1	−1	−1	1

to polynomials of order less than m by employing the defining identity P of $GF(3^2)$

$X^2=x+1$. (See Footnote 12)

Then the fourth row is obtained by reducing the coefficient to numbers less than p by dividing the numbers by p and keeping the remainder.

Discussion

Using the different lemmas in combination, Paley has obtained most orthogonal matrices of order 200 or less. The design schemes are summarized in the Appendix. This range seems to be sufficient for most applications in the design of matrix switches.

The fact that there exist no better design methods can be seen from the connection between the orthogonal matrices and the theory of error-correcting codes. For any orthogonal matrix each row may be considered as a sequence of binary variables. Together with their complement sequences we have a code of size $8k$ for $4k$ bits with a distance of $2k$. Plotkin[13] has proved that

$$A(4k, 2k) \leqslant 8k ,$$

which means there can be at most $4k$ orthogonal sequences of $4k$ bits. Thus, for any number of outputs desired, the best one can do is to go to the next multiple of 4 where an orthogonal matrix is possible.

As an illustration, the number of inputs required, using the present approach, are calculated for several cases of interest and compared with what is required if other known methods are used in the design. The results of comparison are shown in Table 3.

Table 3 **A comparison of the methods known.**

	Number of Inputs Required		
Number of Outputs Required	*Constantine*	*Marcus*	*Method Using Orthogonal Matrix*
5	16	8	8
8	16	16	12
16	32	32	20
32	64	64	36
36	128	64	40
64	128	128	68
72	256	128	76

Acknowledgment

The author is indebted to Dr. John W. Gibson for suggestion of the problem and to G. Constantine and R. Ward for discussions on matrix switches.

Appendix: Decomposition of orthogonal matrices of order up to 200

$m=4=2^2$	$m=104=2^2(5^2+1)$
$m=8=2^3$	$m=108=107+1$
$m=12=11+1$	$m=112=2^2(3^3+1)$
$m=16=2^4$	$m=116$
$m=20=19+1$	$m=120=2(59+1)$
$m=24=2(11+1)$	$m=124=2(61+1)$
$m=28=3^3+1$	$m=128=2^7$
$m=32=2^5$	$m=132=131+1$
$m=36=2(17+1)$	$m=136=2(67+1)$
$m=40=2(19+1)$	$m=140=139+1$
$m=44=43+1$	$m=144=2^3(17+1)$
$m=48=2^2(11+1)$	$m=148=2(73+1)$
$m=52=2(5^2+1)$	$m=152=2^2(37+1)$
$m=56=2(3^3+1)$	$m=156$
$m=60=59+1$	$m=160=2^3(19+1)$
$m=64=2^6$	$m=164=163+1$
$m=68=67+1$	$m=168=2(83+1)$
$m=72=2^2(17+1)$	$m=172$
$m=76=2(37+1)$	$m=176=2^2(43+1)$
$m=80=2^2(19+1)$	$m=180=2(89+1)$
$m=84=83+1$	$m=184$
$m=88=2(43+1)$	$m=188$
$m=92$	$m=192=2^4(11+1)$
$m=96=2^3(11+1)$	$m=196=2(97+1)$
$m=100=2(7^2+1)$	$m=200=2^2(7^2+1)$

References and footnotes

1. Constantine, G., *IBM Journal,* **2,** 204-211 (July, 1958).
2. Marcus, M., *IBM Journal,* **3,** 194-196 (April, 1959).
3. Paley, R. E. A., *J. Math. and Phys.,* **12,** 311-320 (1933).
4. Actually this condition may be replaced by a weaker condition, namely, the statement "there exists a row which has as many ONES as ZEROES." It can be shown that this weaker condition and (2w) implies (1w).
5. Substitute ONE for MINUS ONE and vice versa for complementation.
6. Sylvester, J. J., *Phil. Mag.,* (4) **34,** 461-475 (1867).
7. "U-matrix" is short for "orthogonal matrix."
8. $a\equiv b(\text{mod } c)$ means $a=kc+b$ when k is any integer.
9. For definition of Galois fields see Reference 10 or 11.
10. Birkhoff, G. and MacLane, S., *Survey of Modern Algebra,* Macmillan, New York, Revised Edition, 1953.
11. Van Der Waerden, B. L., *Modern Algebra,* vol. 1, Frederick Ungar Publishing Company, N. Y., 1953.
12. This is derived from the irreducible polynomial
$x^2-x-1=0$.
Other irreducible polynomials that are needed for switches up to 199 outputs are
$GF(3^3)X^3-X-2=0$
$GF(5^2)X^2-2X-2=0$
$GF(7^2)X^2-X-4=0$.
13. Plotkin, M., "Binary Codes with Specified Minimum Distance," Research Division, University of Pennsylvania, Philadelphia, Report No. 51-20; January, 1951.

Received January 28, 1960