A NOTE ON NON-BINARY ORTHOGONAL CODES

Sze-Hou Chang
Northeastern University
Boston, Massachusetts

ABSTRACT

This paper presents three methods of constructing orthogonal signals whose amplitude levels are discrete, but not limited to binary: (1) method using M-sequence, (2) method by inspection, and (3) recursive method.

A NOTE ON NON-BINARY ORTHOGONAL CODES*

Sze-Hou Chang
Northeastern University
360 Huntington Avenue
Boston, Massachusetts 02115
Area Code 617, CO 2-1100, Ext. 433

An effective set of signals for use in a channel with additive white Gaussian noise is the orthogonal set. Methods of constructing orthogonal continuous waveforms are widely studied. The construction of binary orthogonal codes is based primarily on Hadamard matrices. A Hadamard matrix is an orthogonal matrix whose elements are the integers +1 and -1. Hadamard matrices of various orders have been constructed[1,2,3] through the generation of pseudo-random sequences of the types (1) maximum length sequences (m-sequences), (2) quadratic residue sequence (or Legender sequence), (3) twin prime sequence, and (4) Hall sequence. It seems that no such study has been made for the construction of orthogonal matrices using integers (or rational numbers) as elements, although their uses in non-binary coding can be anticipated. Furthermore, it is felt that such study may bring the two areas of endeavor, discrete coding and waveform design, closer to each other.

---

*This research work was supported by Air Force Cambridge Research Labs, under Contract No. AF19(628)-3312 and by Electronic Research Center, NASA under Grant No. NGR-22-011-013.

Three methods are explored. They are summarized as follows.

(1) <u>M-Sequences Over GF(p), p = 3, 5, 7, 11</u>

To illustrate this method by an example, consider $p = 5$ and an irreducible primitive polynomial of degree $m = 2$ over GF(5)

$$f(x) = x^2 + 3x + 3.$$

With the aid of the shift register circuit shown in Fig. 1, it is easy to see that a typical sequence generated by the polynomial is

$$1\ 0\ 2\ {-1}\ 2\ 2\ {-2}\ 0\ 1\ 2\ 1\ 1\ {-1}\ 0\ {-2}\ 1\ {-2}\ {-2}\ 2\ 0\ {-1}\ {-2}\ {-1}\ {-1},$$

with period $r = 5^2-1 = 24$. By listing the above sequence and 11 successive cyclic shifts of the sequence in 12 rows, and retaining only the first 12 columns, then a 12×12 orthogonal matrix using elements $0, \pm1, \pm2$ is obtained.

$$\begin{matrix}
1 & 0 & 2 & -1 & 2 & 2 & -2 & 0 & 1 & 2 & 1 & 1 \\
0 & 2 & -1 & 2 & 2 & -2 & 0 & 1 & 2 & 1 & 1 & -1 \\
2 & -1 & 2 & 2 & -2 & 0 & 1 & 2 & 1 & 1 & -1 & 0 \\
-1 & 2 & 2 & -2 & 0 & 1 & 2 & 1 & 1 & -1 & 0 & -2 \\
2 & 2 & -2 & 0 & 1 & 2 & 1 & 1 & -1 & 0 & -2 & 1 \\
2 & -2 & 0 & 1 & 2 & 1 & 1 & -1 & 0 & -2 & 1 & -2 \\
-2 & 0 & 1 & 2 & 1 & 1 & -1 & 0 & -2 & 1 & -2 & -2 \\
0 & 1 & 2 & 1 & 1 & -1 & 0 & -2 & 1 & -2 & -2 & 2 \\
1 & 2 & 1 & 1 & -1 & 0 & -2 & 1 & -2 & -2 & 2 & 0 \\
2 & 1 & 1 & -1 & 0 & -2 & 1 & -2 & -2 & 2 & 0 & -1 \\
1 & 1 & -1 & 0 & -2 & 1 & -2 & -2 & 2 & 0 & -1 & -2 \\
1 & -1 & 0 & -2 & 1 & -2 & -2 & 2 & 0 & -1 & -2 & -1
\end{matrix}$$

This method is easily extended to generate $n \times n$ orthogonal matrices, $n = \frac{r}{2} = \frac{5^m-1}{2}$. Similar procedures, with proper mapping of the elements in the field of GF(p) onto elements of integers, or rational numbers (see table) can be used to obtain n $\times$ n orthogonal matrices with 3, 7 and 11 elements with $n = \frac{r}{2} = \frac{p^m-1}{2}$, $p > 2$.

<u>Table of Mapping Elements of GF(p) to Integers or Rationals for the Construction of Orthogonal Matrices from the M-Sequences</u>

p	Elem of GF(p)	Integ	p	Elem of GF(p)	Ratnl	Integ	p	Elem of GF(p)	Ratnl	Integ
2	0	1	7	0	0	0	11	0	0	0
	1	-1		1	1	3		1	1	2
3	0	0		2	2	6		2	2	4
	1	1		3	2/3	2		3	3	6
	2	-1		4	-2/3	-2		4	4	8
5	0	0		5	-2	-6		5	-1/2	-1
	1	1		6	-1	-3		6	1/2	1
	2	-1						7	-4	-8
	3	-2						8	-3	-6
	4	-1						9	-2	-4
								10	-1	-2

The construction is based upon the properties[1] of the autocorrelation function $\phi(\tau)$ of the m-sequences of p elements ($p = 3, 5, 7, 11$) relative to certain mapping η. The autocorrelation function has the same period as the m-sequence, namely, $r = p^m-1$. Under symmetrical mapping, as adopted here, the values of $\phi(\tau)$ at $\tau = 0$ and $\tau = r/2$ differ in signs but equal in magnitude. Therefore, unlike the case for $p = 2$, a segment equal to the half period of the sequence is used for construction of the orthogonal matrices. Furthermore, for cases $p = 7$ and 11, $\phi(\tau)$ assumes non-zero values under ordinary mapping for τ smaller than a half period. These are restored to zero by suitable remapping the elements of GF(7) and GF(11) onto specially chosen sets of rationals or integers. Similar procedures applied to the cases for $p > 11$

result in solutions in mapping of elements of GF(13), etc onto elements of irrational or complex field.

(2) Construction by Inspection

The following orthogonal matrices are obtained by inspection.

(1) 2×2 (3 level or less)

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

(2) 4×4 (7 level or less)

$$\begin{bmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{bmatrix}$$

(3) 8×8 (15 level or less)

$$\begin{bmatrix} a & b & -c & d & e & f & g & h \\ -b & a & d & c & -f & e & -h & g \\ c & -d & a & b & -g & h & e & -f \\ -d & -c & -b & a & -h & -g & f & e \\ -e & f & g & h & a & -b & c & -d \\ -f & -e & -h & g & b & a & -d & -c \\ -g & h & -e & -f & -c & d & a & -b \\ -h & -g & f & -e & d & c & b & a \end{bmatrix}.$$

By assigning suitable values to the letters, some of which may have the same value, orthogonal matrices of various elements can be constructed.

(3) Recursive Methods

Let A and B be two orthogonal matrices of size $n \times n$. Then the following recursive methods may be used to obtain new orthogonal matrices.

(a) $C = A \cdot B$ size $n \times n$, different elements from A or B.

(b) $C = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \otimes A$ size $2n \times 2n$, same elements as A. where $\otimes$ denotes the Knonecker or tensor product.

(c) $C = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \otimes A$ size $2n \times 2n$, different elements as A.

(d) $C = \begin{bmatrix} A & B \\ -B^T & D \end{bmatrix}$ size $2n \times 2n$, same elements as A and B combined provided AB = BA.

In the last method, the matrix D is computed from:

$$D^T = B^{-1} AB.$$

However, if AB = BA, then

$$D^T = B^{-1} BA = A$$

and

$$D = A^T.$$

References

1. N. Zierler, "Linear Recurring Sequences", J. Soc. Indust. Appl. Math., 7, 31-48, 1959, also in W. H. Kautz (editor), Linear Sequential Switching Circuits, Holden-Day, 1965.

2. E. F. Beckenbach (editor), Applied Combinatorial Mathematics, Chapter 13, Block Designs by M. Hall, Jr., John Wiley and Sons, 1964.

3. S. W. Golomb (editor), Digital Communications with Space Applications, Chapter 4, Codes with Special Correlation by L. D. Baumert, Prentice-Hall, 1964.

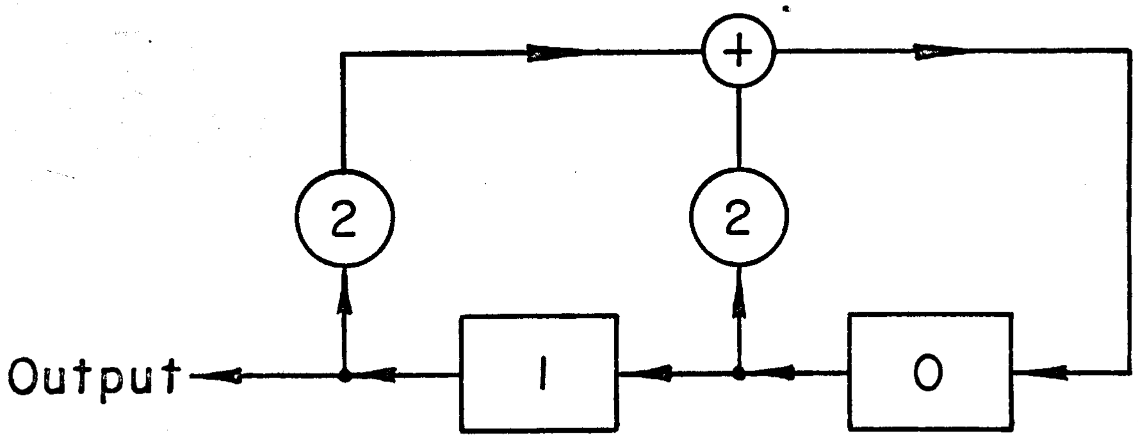

Fig. 1. Shift Register Circuit used to Generate M-Sequence Over GF(5).

Recursion Polynomial: $f(x)=x^2+3x+3$.