On the Synthesis of Two-Dimensional Arrays with Desirable Correlation Properties*

DOMENICK CALABRO

Sonar Systems Department, Sperry Gyroscope Division,
Great Neck, New York 11020

AND

JACK K. WOLF

Department of Electrical Engineering, Polytechnic Institute of Brooklyn,
Brooklyn, New York 11201

Considerable effort has been devoted in the literature to the synthesis of one-dimensional, periodic, binary and nonbinary sequences having small values for their out-of-phase autocorrelation functions. This paper considers the synthesis of two-dimensional, periodic, binary and nonbinary sequences (arrays) which exhibit similar properties for their two-dimensional autocorrelation functions. These arrays may have future application in the areas of optical signal processing, pattern recognition, etc.

Various procedures are presented for the synthesis of such arrays. Two perfect binary arrays and an infinite class of perfect nonbinary arrays are given. A class of binary arrays is presented which are the two-dimensional analog of the quadratic residue sequences and are shown to have out-of-phase autocorrelation of \(-1\), or to alternate between \(+1\) and \(-3\). The perfect maps of Gordon are shown to have all values of out-of-phase autocorrelation equal to \(-1\). Other methods of constructing arrays based upon good one-dimensional sequences are also discussed.

Synthesis procedures are given for constructing pairs of arrays such that their cross-correlation is identically zero for all shifts and, in addition, individually have good autocorrelation functions. Examples are given for the various synthesis procedures.

* This research was partially supported by the Air Force Office of Scientific Research under Contract AF 49(638)-1600.
1. INTRODUCTION

Considerable effort has been devoted in the literature to the synthesis of one-dimensional binary and nonbinary sequences. In particular, these studies have been concerned with sequences that exhibit small values for their out-of-phase autocorrelation (e.g., Golomb, 1955; Zierler, 1959).

Two different situations have been considered. In the first case, the sequences were assumed to be periodic and infinite in extent. The resultant autocorrelations were calculated over a full period of the sequences and thus were also periodic. Such periodic sequences have found application in wide-band digital communication systems. In the second case, the sequences were nonperiodic and assumed to extend only over some finite interval and to be identically zero outside that interval. The autocorrelation function was then nonperiodic and nonzero over, at most, a range of the shift variable equal to twice the sequence length. These nonperiodic sequences have been used in radar applications.

This paper extends the concept of periodic sequences and their resultant periodic autocorrelation to the two-dimensional case. A doubly periodic array is formed by considering a basic $p$ by $q$ block of elements repeated on all sides until the entire plane is covered. Such a two-dimensional periodic structure has been termed a matrix on a torus by Reed and Stewart (1962) and Gordon (1966). Both binary and non-binary two-dimensional arrays will be considered. These two-dimensional arrays may have future application in the areas of optical signal processing, map matching, and pattern recognition.

Various synthesis procedures are presented for two-dimensional arrays which possess small values for their out-of-phase autocorrelation. Two perfect binary arrays (arrays exhibiting zero out-of-phase autocorrelation for all two-dimensional cyclic shifts) and an infinite class of perfect nonbinary arrays are presented. Another class of binary arrays which exhibit out-of-phase autocorrelation of $-1$, or alternate from $+1$ to $-3$, are derived as an extension of the one-dimensional quadratic residue sequences. The perfect maps of Gordon (1966) are shown to have all out-of-phase autocorrelation values equal to $-1$, analogous to the one-dimensional $m$-sequences (maximal-length linear shift register sequences). Methods of constructing two-dimensional arrays based upon good one-dimensional sequences are also discussed.

Finally, a synthesis procedure is given for constructing pairs of arrays which exhibit perfect cross-correlation functions (zero cross-correlation for all two-dimensional cyclic shifts) and good autocorrelation functions.
These arrays are constructed from a class of cyclically-orthogonal binary sequences.

A previous paper by Spann (1965) treats two-dimensional arrays formed in a different fashion than those discussed in the paper. The differences between the two-dimensional sequences formed by Spann and the sequences discussed in this paper lie in the manner in which the basic \((p \times q)\) blocks are repeated and also in the definition of the correlation function. Spann is concerned with the cross-correlation between the basic \((p \times q)\) block and the mosaic pattern shown in Fig. 1a. We are concerned with the two-dimensional autocorrelation (to be defined) of the checkerboard pattern shown in Fig. 1b.

2. DEFINITIONS

If \(A\) is a \(p \times q\) basic block of binary or nonbinary elements, a doubly-periodic array is formed by repeating this basic block on each of its sides and continuing the process until the entire plane is covered. The elements of this doubly-periodic array can be written as \(A(x, y)\) in the usual manner of describing an array of symbols. Then the \(x\) and the \(y\) period of the array, \(p\) and \(q\), are defined as the least positive integers such that

\[
A(x + p, y) = A(x, y)
\]
\[
A(x, y + q) = A(x, y)
\]
\[
A(x - p, y - q) = A(x, y).
\]

The area of the array is defined as the product of the \(x\) and \(y\) periods, \((pq)\).

The periodic cross-correlation of two doubly-periodic arrays \(A(x, y), B(x, y)\) with areas \((pq)\) and \((p'q')\), respectively, is given by the following double sum:

\[
R_{AB}(i, j) = \sum_{x=0}^{p'-1} \sum_{y=0}^{q'-1} A(x, y)B^*(x + i, y + j),
\]

where \(p''\) is the least common multiple of \(p\) and \(p'\) (and similarly for \(q''\)). The asterisk (*) denotes complex conjugate. If

\[
A(x, y) = B(x, y),
\]

one defines

\[
R_A(i, j) = \sum_{x=0}^{p-1} \sum_{y=0}^{q-1} A(x, y)A^*(x + i, y + j)
\]

as the periodic autocorrelation of the array \(A(x, y)\).
In this paper the elements of the array $A(x, y)$ will be considered as the complex $N$th roots of unity. Thus, in the binary case the elements are $+1$ or $-1$.

The imbalance ($D_A$) of an array $A(x, y)$ is defined as
SYNTHESIS OF TWO-DIMENSIONAL ARRAYS

\[ D_A = \sum_{x=0}^{p-1} \sum_{y=0}^{q-1} A(x, y). \]

Note that in the binary case the minimum of the absolute value of the imbalance is given as

\[ \min |D_A| = +1 \text{ if } pq \text{ odd} \]
\[ = 0 \text{ if } pq \text{ even}. \]

Binary arrays exhibiting a minimum imbalance will be referred to as balanced arrays.

In this paper the emphasis is placed on binary arrays, although many of the concepts generalize easily to the nonbinary case. An example of this extension to the nonbinary case is given in Section 6.

3. PROPERTIES OF THE PERIODIC AUTOCORRELATION FUNCTION OF BINARY ARRAYS

Some basic properties of the periodic autocorrelation of binary arrays will be presented in this section. These properties are derived directly from the definition of the autocorrelation function and are analogous to the one-dimensional case (see Titsworth, 1963 for proofs in one-dimension). From these properties, optimal binary arrays will be defined in the next section.

**Property 1.** The periodic autocorrelation function can be shown to have the following symmetry properties:

\[ R_A(p - i, j) = R_A(-i, j) \]
\[ = R_A(i, q - j) = R_A(i, -j) \]
\[ R_A(p - i, q - j) = R_A(i, j) = R_A(-i, -j). \]

From this property it is seen that one need only consider the autocorrelation function for shifts in one quadrant of the entire plane.

**Property 2.** The sum of the autocorrelation values per block of area \((pq)\) is equal to the square of the imbalance. That is

\[ \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} R_A(i, j) = D_A^2. \]

**Property 3.** The autocorrelation values of the array \(A(x, y)\) are congruent to \((pq)\) modulo \((4)\).

**Property 4.** The maximum (not in absolute value) out-of-phase value of the autocorrelation of \(A(x, y)\) is bounded as
Based upon Property 4 of the previous section, it is convenient to define the following binary arrays:

**Definition 1.** A **minimax array** is a binary array for which the maximum out-of-phase autocorrelation values attain the lower bound $R_m$ specified in Property 4.

**Definition 2.** An **optimal array** is a minimax array for which the autocorrelation function $R_A(i, j)$ takes on the value $R_m$ the minimum number of times per block (as compared to other minimax arrays having the same $x$ and $y$ periods).

**Definition 3.** An **absolute optimal array** is a minimax array for which the out-of-phase autocorrelation values do not differ from $R_m$ by more than 4 and for which the maximum of the absolute value of the out-of-phase autocorrelation function is taken on a minimum number of times.

**Definition 4.** A **perfect array** is one for which all out-of-phase autocorrelation values are equal to zero. It should be noted that the area of such an array is restricted to be congruent to zero mod 4.

The theorem to follow plays a fundamental role in the search for arrays with desirable autocorrelation properties. The proof of this theorem is analogous to Titsworth's proof for one-dimension (Titsworth, 1963).

**Theorem 1.** If $A(x, y)$ is a balanced binary array with three-level autocorrelation for which the two out-of-phase correlation values differ by 4, then $A(x, y)$ is both minimax and optimal.

Note, a two-level autocorrelation function can be considered a special case of a three-level autocorrelation function for which one level occurs zero times. In particular, if the area of $A(x, y)$ is congruent to 3 mod (4) then the arrays satisfying the conditions of this theorem have all out-of-phase correlation values equal to $-1$. In addition, if $pq = 2 \mod (4)$, the two out-of-phase values are $\pm 2$. Finally, if $pq = 1 \mod (4)$, the two out-of-phase values are $+1$ and $-3$. Hence the arrays satisfying these conditions will also be useful in applications where it is desirable to keep the absolute value of the out-of-phase correlations as small as possible.
5. SYNTHESIS OF BINARY ARRAYS

In this section techniques will be presented for synthesizing binary arrays. Although most of the techniques also are applicable to non-binary arrays, the consideration here is restricted to the binary case. It will be shown that two perfect binary arrays exist and that minimax and optimal arrays can be synthesized. The first technique considered is included merely for purposes of illustration.

5.1. Arrays Formed From Cyclic Permutations of a Basic One-Dimensional Sequence

An array of area $p^2$, $A(x, y)$ can be constructed by considering a one-dimensional sequence $A(x)$ of period $p$ as the first row and all $p - 1$ cyclic permutations of this sequence as successive rows. It is easily shown that the autocorrelation of this array $A(x, y)$ can be written in terms of the autocorrelation of the sequence $A(x)$ in the following manner:

$$R_A(i, j) = pR_A(|i - j|).$$

The autocorrelation function $R_A(i, j)$ takes on an interesting form if the sequence $A(x)$ is chosen as a pseudo-noise sequence. For this case

$$R_A(i, j) = \begin{cases} p^2 & \text{if } i \equiv j \text{ mod } (p) \\ -p & \text{if } i \not\equiv j \text{ mod } (p). \end{cases}$$

The correlation function for arrays formed in this manner exhibit a ridge along the diagonal.

5.2. Hadamard Arrays

For this application a Hadamard matrix (see Golomb, 1964) can be considered as a $p$ by $p$ matrix whose rows (and columns) are pairwise orthogonal. When considered as an array, this will insure that the autocorrelation function of a Hadamard array will exhibit zero values along its major axes. As an example, the Hadamard matrix of order 4, given by

$$A = \begin{bmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{bmatrix},$$

In this paper we used the term pseudo-noise sequence to indicate a periodic one-dimensional sequence with all out-of-phase autocorrelation values equal to $-1$. A special case of a pseudo-noise sequence is then a maximal-length linear shift register sequence.
possesses the following autocorrelation function:

\[ R_A = \begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & -4 & 0 & +4 \\ 0 & 0 & 0 & 0 \\ 0 & +4 & 0 & -4 \end{bmatrix}. \]

In order for a Hadamard array also to possess zero autocorrelation values for all off-axis shifts, the cross-correlation functions of the rows must be complementary for all shifts. That is, if

\[ r_{i,j}(t) = \text{the periodic cross-correlation of the } i\text{th and } j\text{th rows for a shift } (t), \]

the required condition is that

\[ \sum_{t=0}^{p-1} r_{i,j}(t) = 0 \quad \text{for all } j = i + k \]

\[ 0 < k < p \]

\[ 0 \leq t < p. \]

The Hadamard matrix of order 2, given by

\[ A = \begin{bmatrix} + & + \\ + & - \end{bmatrix}, \]

is the only Hadamard matrix known to the authors which satisfies this condition. This array has the following autocorrelation function,

\[ R_A = \begin{bmatrix} 4 & 0 \\ 0 & 0 \end{bmatrix}, \]

and will be referred to as the perfect array of area 4. It will be seen in a later section that this array is a degenerate case of a general class of perfect \((N \times N)\) arrays with elements which are \(N\)th complex roots of unity.

5.3. Term-by-Term Products of Binary Sequence

If the array \(A(x, y)\) is formed by taking the term-by-term product of two sequences \(C(x)\) and \(B(y)\) with periods \(p\) and \(q\), respectively,

\[ A(x, y) = C(x)B(y), \]
then the resultant array \( A(x, y) \) [of area \( pq \)] has a two-dimensional auto-
correlation equal to the product of the autocorrelations of the respective
sequences. That is,

\[
R_A(i, j) = R_C(i)R_B(j).
\]

If the sequences \( C(x) \) and \( B(y) \) are each taken to be the perfect
sequence of period 4 (i.e., \( C(x) = B(y) = (\ldots \ldots) \)), then \( A(x, y) \),
given as

\[
A(x, y) = \begin{bmatrix}
+ & + & + & - \\
+ & + & + & - \\
+ & + & + & - \\
- & - & - & +
\end{bmatrix},
\]

is a perfect array of area 16:

\[
R_A(i, j) = 16 \quad (i, j) \equiv (0, 0) \mod (4, 4)
\]

\[
= 0 \quad (i, j) \not\equiv (0, 0) \mod (4, 4).
\]

If \( C(x) \) is the perfect sequence and \( B(y) \) is any pseudo-noise sequence of
period \( q \), \( A(x, y) \) has three-level autocorrelation:

\[
R_A(i, j) = 4q \quad (i, j) \equiv (0, 0) \mod (4, q)
\]

\[
= -4 \quad i \equiv 0 \mod (4); j \not\equiv 0 \mod (q)
\]

\[
= 0 \quad i \not\equiv 0 \mod (4); j \equiv 0 \mod (q)
\]

and imbalance 2. These arrays are minimax, and since the 0 out-of-phase
level occurs \( 3q \) times per block and the \( -4 \) level occurs \( q - 1 \) times per
block, these arrays are termed near-absolute optimal arrays.

Balanced, minimax, three-level arrays of area \( pq \equiv 1 \mod (4) \) can be
formed as term-by-term products of two pseudo-noise sequences of
periods \( p \) and \( q \) respectively. It is readily seen that the resultant arrays
have correlation functions given by

\[
R_A(i, j) = pq \quad (i, j) \equiv (0, 0) \mod (p, q)
\]

\[
= -p \quad i \equiv 0 \mod (p); j \not\equiv 0 \mod (q).
\]

\[
= -q \quad i \not\equiv 0 \mod (p); j \equiv 0 \mod (q)
\]

\[
= +1 \quad i \not\equiv 0 \mod (p); j \not\equiv 0 \mod (q).
\]
5.4. Quadratic Residue Arrays

The optimal and minimax arrays to be presented in this section are derived as an extension of the one-dimensional quadratic residue sequences. It will be shown that arrays of area \( pq \) attaining the values of \(-1\) for all out-of-phase correlations can be synthesized for all prime integers \( p, q \) such that \( q - p = 2 \). (Such arrays are called pseudo-noise arrays.)

The basis of these arrays is the algebraic structure of the Legendre operator \((x/p)\), defined below, where \( p \) is always considered a prime:

\[
(x/p) = \begin{cases} 
0 & \text{if } x \equiv 0 \mod (p); \\
1 & \text{if } x \text{ is a square mod } (p) \\
-1 & \text{if } x \text{ is a non-square mod } (p).
\end{cases}
\]

Those values of \( x \) for which \((x/p) = 1\) are called quadratic residues. Certain properties of this operator and the proof of the correlation property of the arrays as given in Theorem 2 are included in Appendix A-1.

**Theorem 2.** If \( A(x, y) \) has area \((pq)\) where \( p \) and \( q \) are primes and has elements

\[
A(x, y) = \begin{cases} 
(x/p)(y/q) & x \not\equiv 0 \mod (p); y \not\equiv 0 \mod (q) \\
-1 & x \not\equiv 0 \mod (p); y \equiv 0 \mod (q) \\
+1 & x \equiv 0 \mod (p); y \not\equiv 0 \mod (q) \\
-1 & (x, y) \equiv (0, 0) \mod (p, q),
\end{cases}
\]

then the two-dimensional autocorrelation function of \( A(x, y) \) is as follows:

(a) If \( q - p = 0 \), \( A(x, y) \) is a balanced minimax array with autocorrelation

\[
R_A(i, j) = \begin{cases} 
pq & (i, j) \equiv (0, 0) \mod (p, q) \\
+1 & i \not\equiv 0 \mod (p); j \equiv 0 \mod (q) \\
-3 & i \equiv 0 \mod (p); j \not\equiv 0 \mod (q) \\
-2(i/p)(j/q) - 1 & i \not\equiv 0 \mod (p); j \not\equiv 0 \mod (q)
\end{cases}
\]

where the quantity

\[-2(i/p)(j/q) - 1\]

takes on the values \(+1\) and \(-3\). These arrays are optimal.
(b) If $q - p = 2$, $A(x, y)$ is a balanced minimax array such that

$$R_A(i, j) = pq \quad (i, j) \equiv (0, 0) \mod (p, q)$$

$$= -1 \quad (i, j) \not\equiv (0, 0) \mod (p, q)$$

Such arrays are also optimal and will be referred to as pseudo-noise arrays.

(c) If $q - p = 4$, $A(x, y)$ is a minimax array with imbalance 3 such that

$$R_A(i, j) = pq \quad (i, j) \equiv (0, 0) \mod (p, q)$$

$$= -3 \quad i \not\equiv 0 \mod (p); \quad j \equiv 0 \mod (q)$$

$$= +1 \quad i \equiv 0 \mod (p); \quad j \not\equiv 0 \mod (q)$$

$$= -2(i/p)(j/q) - 1 \quad i \not\equiv 0 \mod (p); \quad j \not\equiv 0 \mod (q).$$

(d) If $q - p = 6$, $A(x, y)$ is an array with imbalance 5 such that

$$R_A(i, j) = pq \quad (i, j) \equiv (0, 0) \mod (p, q)$$

$$= -5 \quad i \not\equiv 0 \mod (p); \quad j \equiv 0 \mod (q)$$

$$= +3 \quad i \equiv 0 \mod (p); \quad j \not\equiv 0 \mod (q)$$

$$= -1 \quad (i, j) \not\equiv (0, 0) \mod (p, q).$$

This is a minimax array if no pseudo-noise array of area $pq$, $q - p = 6$, exists.

If $q - p > 6$, then the maximum out-of-phase value of $R_A(i, j)$ is always greater than the minimax value and this correlation value will always occur along one of the axes $j \equiv 0$ or $i \equiv 0$. Also, no matter what the separation between the primes $p$ and $q$, the off-axis correlations will always alternate between the values $+1$ and $-3$ if $pq \equiv 1 \mod (4)$, and will always be $-1$ if $pq \equiv 3 \mod (4)$.

The general expression for the correlation function and the imbalance of the arrays constructed in this manner are given by,

$$R_A(i, j) = \begin{cases} 
    pq & (i, j) \equiv (0, 0) \mod (p, q) \\
    p - q + 1 & i \not\equiv 0 \mod (p); j \equiv 0 \mod (q) \\
    q - p - 3 & i \equiv 0 \mod (p); j \not\equiv 0 \mod (q) \\
    -2(i/p)(j/q) - 1 & i \not\equiv 0 \mod (p); j \not\equiv 0 \mod (q) \text{ and } pq \equiv 1 \mod (4) \\
    -1 & i \not\equiv 0 \mod (p); j \not\equiv 0 \mod (q) \text{ and } pq \equiv 3 \mod (4) 
\end{cases}$$
and

\[ D_A = q - p - 1. \]

As examples, optimal arrays of area 25 and 15 are given below, together with their autocorrelation functions.

(1) \( pq = 25 = 1 \mod (4) \); quadratic residues are 1, 4

\[
A(x, y) = \begin{bmatrix}
- & - & - & - \\
+ & + & - & - \\
+ & - & + & + \\
+ & - & + & - \\
+ & + & - & - \\
\end{bmatrix},
\]

\[
R_A(i, j) = \begin{bmatrix}
25 & +1 & +1 & +1 & +1 \\
-3 & -3 & +1 & +1 & -3 \\
-3 & +1 & -3 & -3 & +1 \\
-3 & -3 & +1 & +1 & -3 \\
\end{bmatrix}.
\]

(2) \( pq = 15 = 3 \mod (4) \); quadratic residues \( \begin{cases} 1 & \text{for } p = 3 \\ 1, 4 & q = 5 \end{cases} \)

\[
A(x, y) = \begin{bmatrix}
- & - & - \\
+ & + & - \\
+ & - & + \\
+ & + & - \\
\end{bmatrix},
\]

\[
R_A(i, j) = \begin{bmatrix}
15 & -1 & -1 \\
-1 & -1 & -1 \\
-1 & -1 & -1 \\
-1 & -1 & -1 \\
\end{bmatrix}.
\]
5.5. Gordon Arrays

Gordon (1966) gave a construction procedure for two-dimensional binary arrays which are perfect maps. (For a definition of the term "perfect map," see Reed and Stewart, 1962 or Gordon, 1966). It is shown in Appendix A-2 that these arrays have an autocorrelation function given as

\[ R(i, j) = \begin{cases} \frac{pq}{(i, j) \equiv (0, 0) \mod (p, q)} \\ -1 & (i, j) \not\equiv (0, 0) \mod (p, q) \end{cases} \]

In our notation, one construction procedure for these arrays is as follows:

1. Find a prime \( p_1 \) such that \( p_1 \mid 2^N - 1 \).
2. Define the parameter \( a \) such that \( p_1 a \mid 2^N - 1 \) but \( p_1^{a+1} \nmid 2^N - 1 \).
3. Let the \( x \) period of the array be given as \( p = p_1^a \) and let the \( y \) period of the array be given as

\[ q = \frac{2^N - 1}{p_1^a}. \]

(Thus the area of the array is \( 2^N - 1 \).)

4. Let \( \gamma \) be a primitive element of \( GF(2^N) \) and let \( L(\ ) \) be a linear operator which maps all elements of \( GF(2^N) \) into elements of \( GF(2) \). (Assume that \( L \) does not map all elements of \( GF(2^N) \) into the element 0.)

5. Then the desired array \( A(x, y) \) is given as

\[ A(x, y) = 1 - 2L(\gamma^{xy+yp}) \quad \text{for} \quad (x, y) \mod (p, q). \]

The proof of the autocorrelation function of this array in Appendix A-2 first shows that the array \( \tilde{A}(x, y) \) [with elements 0 and 1] defined as

\[ \tilde{A}(x, y) = L(\gamma^{xy+yp}), \quad (x, y) \mod (p, q) \]

has the "shift and add property" (see Birdsall, and Ristenbatt, 1958) with respect to \( \mod (2) \) addition for all two-dimensional shifts. Then it is shown that the array \( A(x, y) \) has imbalance \( D_A = -1 \). The autocorrelation follows immediately from these two factors.

As an example of this construction procedure, consider \( N = 4, 2^N - 1 = 15 \). Let \( p_1 = 3 \) and \( a = 1 \) so that \( p = 3 \) and \( q = 5 \). Then the nonzero elements of \( GF(2^N) \), as well as the result of operating on these elements by the operator \( L \), are given in Table I.
TABLE I

<table>
<thead>
<tr>
<th>$\gamma^i$</th>
<th>$\gamma^i = a_6z^3 + a_5z^2 + a_4z + a_0$</th>
<th>$(a_i \in GF(2))$</th>
<th>$L(\gamma^i) = a_6$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\gamma^0$</td>
<td>$0z^3 + 0z^2 + 0z + 1$</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>$\gamma^1$</td>
<td>$0z^3 + 0z^2 + 1z + 0$</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>$\gamma^2$</td>
<td>$0z^3 + 1z^2 + 0z + 0$</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>$\gamma^3$</td>
<td>$1z^3 + 0z^2 + 0z + 0$</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>$\gamma^4$</td>
<td>$0z^3 + 0z^2 + 1z + 1$</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>$\gamma^6$</td>
<td>$0z^3 + 1z^2 + 1z + 0$</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>$\gamma^7$</td>
<td>$1z^3 + 0z^2 + 1z + 1$</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>$\gamma^8$</td>
<td>$0z^3 + 1z^2 + 0z + 1$</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>$\gamma^9$</td>
<td>$1z^3 + 0z^2 + 1z + 0$</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>$\gamma^{10}$</td>
<td>$0z^3 + 1z^2 + 1z + 1$</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>$\gamma^{11}$</td>
<td>$1z^3 + 1z^2 + 1z + 0$</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>$\gamma^{12}$</td>
<td>$1z^3 + 1z^2 + 1z + 1$</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>$\gamma^{13}$</td>
<td>$1z^3 + 1z^2 + 0z + 1$</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>$\gamma^{14}$</td>
<td>$1z^3 + 0z^2 + 0z + 1$</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

The corresponding arrays $\bar{A}(x, y)$ and $A(x, y)$ are given as

$$
\bar{A}(x, y) = \begin{bmatrix}
L(\gamma^0) & L(\gamma^5) & L(\gamma^{10}) \\
L(\gamma^3) & L(\gamma^8) & L(\gamma^{13}) \\
L(\gamma^7) & L(\gamma^{11}) & L(\gamma^4) \\
L(\gamma^9) & L(\gamma^{14}) & L(\gamma^7)
\end{bmatrix} = \begin{bmatrix}
1 & 0 & 1 \\
0 & 1 & 1 \\
0 & 0 & 0 \\
0 & 1 & 1
\end{bmatrix}
$$

and

$$
A(x, y) = \begin{bmatrix}
- & + & - \\
+ & - & - \\
+ & + & + \\
- & - & -
\end{bmatrix}.
$$

6. SYNTHESIS OF NONBINARY ARRAYS WITH PERFECT AUTOCORRELATION PROPERTIES

Heimiller (1961), and Frank and Zadoff (1962) have synthesized sequences with perfect autocorrelation functions from a consideration of the Nth complex roots of unity. In these papers the following array is
SYNTHESIS OF TWO-DIMENSIONAL ARRAYS

presented:

\[
\begin{array}{cccc}
1 & 1 & 1 & \cdots & 1 \\
1 & a_1 & a_1^2 & \cdots & a_1^{N-1} \\
1 & a_2 & a_2^2 & \cdots & a_2^{N-1} \\
\vdots \\
1 & a_{N-1} & a_{N-1}^2 & \cdots & a_{N-1}^{N-1}
\end{array}
\]

where \(1, a_1, a_2, \ldots, a_{N-1}\) are then the \(N\)th complex roots of unity. By adjoining the columns of this array the authors have shown that the resulting sequence

\[
1, 1, 1, 1, 1, a_1, a_2, a_{N-1}, 1, a_{N-1}, \ldots, a_{N-1}
\]

of length \(N^2\) has perfect periodic autocorrelation function.

If the \(N\)th roots of unity in the complex number field are represented in exponent notation, the two-dimensional array as presented by these authors can be expressed as

\[
A(x, y) = \exp \left( i(xy) \left( \frac{2\pi}{N} \right) \right).
\]

Then, it is shown in Appendix A-3 that this array of area \(N^2\) has all out-of-phase autocorrelation values equal to zero (a perfect array). As an example, consider the binary case \((N = 2)\); the roots of unity are then \(+1\) and \(-1\). Hence,

\[
A(x, y) = \begin{bmatrix} + & + \\ + & - \end{bmatrix}.
\]

This array is seen to be the Hadamard matrix of order 2 discussed in Section 5.2.

The term-by-term product technique and the resultant product autocorrelation function applies as well to the nonbinary case. Thus, if one forms \(A(x, y) = B(x)B(y)\) where \(B(x)\) is the perfect one-dimensional \(N\)-ary sequence of length \(N^2\), the resultant two-dimensional array of area \(N^4\) will be a perfect array. The perfect binary array of area 16 can be formed in this manner by choosing \(B(x)\) as \((+++-)\).

7. SYNTHESIS OF ARRAYS WITH PERFECT CROSS-CORRELATION PROPERTIES

In an application where more than one array is utilized, mutual interference between arrays may present a problem. Thus, it is desirable to
find arrays which exhibit cross-correlation functions which are zero for all cyclic shifts. Furthermore, it would be desirable for the autocorrelation functions of these arrays to possess low out-of-phase values. A technique for synthesizing such arrays is given below.

7.1. Term-by-Term Product of Sequences

It is readily shown that the cross-correlation function of two arrays formed as the term-by-term product of two sequences factors into the product of the respective cross-correlation functions of the sequences. That is, if

\[ A(x, y) = C(x)D(y) \]
\[ B(x, y) = E(x)F(y), \]

where the period of \( C(x) \) and \( E(x) \) is \( p \) and the period of \( D(y) \) and \( F(y) \) is \( q \), then

\[ R_{AB}(i, j) = R_{CE}(i)R_{DF}(j). \]

Hence, the problem of synthesizing arrays which cross-correlate to zero for all cyclic shifts (cyclically-orthogonal arrays) reduces to the problem of finding one-dimensional sequences which possess this property.

A set of cyclically-orthogonal \( N \)-ary sequences of the same least period \( N^kL \) has been synthesized by Wolf and Levitt (1965), (1966) for all \( L, k \) and \( N > 2 \). These sequences are derived from a consideration of the \( N \)th roots of unity. Pairs of cyclically-orthogonal binary sequences of the same least period \( 2^k \) have been synthesized by D. Calabro and J. Paolillo (to appear) for any integer \( k \) and nonprime odd integer \( r \). These sequences were derived as Kronecker products of certain subsequences. The following two cyclically-orthogonal binary sequences of the same least period 18 can be obtained in this manner and will be used in a later illustration:

\[ C(x) = + - + + - + + - + - + - + + - + \]
\[ E(x) = - + + + - - + + - + + + + - - . \]

It is interesting to note that one need only restrict one pair of sequences, say \( C(x) \) and \( E(x) \) to cross-correlate to zero for all cyclic shifts in order to force \( R_{AB}(i,j) = 0 \) for all \( (i,j) \). In this manner one can choose the sequences \( D(y) \) and \( F(y) \) to achieve good autocorrelation functions for the arrays \( A(x, y) \) and \( B(x, y) \). The autocorrelation func-
tions of these arrays are given by
\[ R_A(i, j) = R_C(i)R_D(j) \]
\[ R_B(i, j) = R_B(i)R_F(j). \]
Hence, to minimize the out-of-phase autocorrelation values, the sequences \( D(y) \) and \( F(y) \) can be chosen as either the perfect sequence or as one of the pseudo-noise sequences. As an illustration, consider \( D(y) \) to be a pseudo-noise sequence of period \( q \). In this case, the autocorrelation function of \( A(x, y) \) is given by
\[ R_A(i, j) = pq \quad (i, j) \equiv (0, 0) \mod (p, q) \]
\[ = qR_C(i) \quad i \not\equiv 0 \mod (p); j \equiv 0 \mod (q) \]
\[ = -p \quad i \equiv 0 \mod (p); j \not\equiv 0 \mod (q) \]
\[ = -R_C(i) \quad i \not\equiv 0 \mod (p); j \not\equiv 0 \mod (q). \]
The normalized largest (in absolute value) sidelobe of the two-dimensional autocorrelation of \( A(x, y) \) is equal to the normalized largest (in absolute value) sidelobe of the one-dimensional autocorrelation of \( C(x) \). The improvement lies, however, in the proportionate number of times the maximum out-of-phase correlation occurs.

To illustrate this point, if the \( C(x) \) and \( E(x) \) sequences are chosen as the cyclically-orthogonal binary sequences of period 18 given previously, and the \( D(y) \) and \( F(y) \) sequences are chosen as the pseudo-noise sequences of period 3, \( ++- \), the resulting arrays
\[
A(x, y) = \begin{bmatrix}
\end{bmatrix}
\]
\[
B(x, y) = \begin{bmatrix}
\end{bmatrix}
\]
can be shown to be cyclically orthogonal. The autocorrelation function of the sequence \( C(x) \) is given by
\[ R_C(i) = [+18 - 10 + 2 + 6 - 6 + 6 - 2 + 9 - 18 + 9 - 2 - 6 + 6 - 6 + 6 + 2 - 10]. \]
Hence, the array \( A(x, y) \) has the following autocorrelation function.
The normalized maximum sidelobe of $C(x)$ is $-1$ and occurs once out of a possible 17 times. The normalized maximum side-lobe of $A(x, y)$ is also $-1$, but it only occurs once out of a possible 53 times.

**APPENDIX A-1. AUTOCORRELATION OF QUADRATIC RESIDUE ARRAYS**

Before presenting the proof of Theorem 2, some helpful properties of the Legendre symbol $(x/p)$ will be introduced. These properties will be presented without proof since they appear in several texts on number theory.

Properties:
1. $(x/p) = (y/p)$ if $x \equiv y \mod (p)$.
2. $(xy/p) = (x/p)(y/p)$.
3. $(x/p) = x^{(p-1)/2} \mod (p)$.

Hence
4. $(1/p) = 1$
5. $(-1/p) = -1$ if $p \equiv 3 \mod (4)$, $(-1/p) = 1$ if $p \equiv 1 \mod (4)$.
6. There are exactly $(p - 1)/2$ quadratic residues and nonresidues in the set $(1, 2, 3, \cdots, p - 1)$ hence,

\[ \sum_{x=1}^{p-1} (x/p) = 0. \]

7. From the above property, the following can be shown to be true:

\[ \sum_{x=1}^{p-1} (x + i)/p = -(i/p) \]

\[ \sum_{x=1}^{p-1} (x/p) = -(-i/p) \]

\[ \sum_{x=1}^{p-1} (x/p)((x + i)/p) = -1. \]

*Proof of Theorem 2.* In order to prove that the arrays have the indicated imbalance properties, consider

\[ D_A = \sum_{x=0}^{p-1} \sum_{y=0}^{q-1} A(x, y) = -1 + \sum_{x=1}^{p-1} (-1) + \sum_{y=1}^{q-1} (1) + \sum_{x=1}^{p-1} (x/p) \sum_{y=1}^{q-1} (y/q). \]
Employing Property 6 one obtains

\[ D_A = q - p - 1 \]

hence,

(a) \( q - p = 0 ; D_A = -1 \)
(b) \( q - p = 2 ; D_A = +1 \)
(c) \( q - p = 4 ; D_A = +3 \)
(d) \( q - p = 6 ; D_A = +5 \).

In order to facilitate the proof of the auto-correlation properties of the arrays, the on-axis and off-axis values will be computed separately.

Consider

\[ j = 0 \mod (q) \]
\[ i \neq 0 \mod (p) \]

and

\[ R_A(i, 0) = \sum_{x=0}^{q-1} \sum_{y=0}^{p-1} A(x, y)A(x + i, y) \]
\[ = A(0, 0)[A(i, 0) + A(-i, 0)] \]
\[ + \sum_{x=1}^{q-1} \sum_{x \neq p-i} A(x, 0)A(x + i, 0) \]
\[ + \sum_{y=1}^{p-1} A(0, y)A(i, y) \]
\[ + \sum_{y=1}^{p-1} A(-i, y)A(0, y) + \sum_{y=1}^{q-1} \sum_{x \neq p-i} A(x, y)A(x + i, y). \]

Now substituting for \( A(x, y) \), \( R_A(i, 0) \) becomes

\[ R_A(i, 0) = (-1)(-2) + \sum_{x=1}^{q-1} \sum_{x \neq p-i} (i/p) \sum_{y=1}^{q-1} (y/q) \]
\[ + (-i/p) \sum_{y=1}^{q-1} (y/q) + \sum_{y=1}^{q-1} (y/q)(y/q) \sum_{x=1}^{q-1} (x/p)((x + i)/p) \]

Employing Properties 6 and 7, one obtains

\[ R_A(i, 0) = 2 + (p - 2) - (q - 1) = p - q + 1 \text{ for all } i. \]
Similarly, consider \( i \equiv 0 \mod (p); j \not\equiv 0 \mod (q) \). Then
\[
R_A(0, j) = \sum_{x=0}^{p-1} \sum_{y=0}^{q-1} A(x, y)A(x, y + j) = A(0, 0)(A(0, j + A)(0, -j)
\]

\[
+ \sum_{y=1}^{q-1} A(0, y)A(0, y + j) + \sum_{x=1}^{p-1} A(x, 0)A(x, j)
\]

\[
+ \sum_{x=1}^{p-1} A(x, -j)A(x, 0) + \sum_{y=1}^{q-1} \sum_{z=1}^{p-1} A(x, y)A(x, y + j).
\]

Substituting for \( A(x, y) \), as before,
\[
R_A(0, j) = -1(1 + 1) + \sum_{y=1}^{q-1} (+1) - (j/q) \sum_{x=1}^{p-1} (x/p)
\]

\[
+ (-j/q) \sum_{x=1}^{p-1} (x/p) + \sum_{x=1}^{p-1} (x/p)(x/p) \sum_{y=1}^{q-1} (y/q)((y + j)/q)
\]

and employing the same properties of \( (x/p) \) yields the following result:
\[
R_A(0, j) = q - p - 3 \quad \text{for all } j; \quad i \equiv 0 \mod (p).
\]

To evaluate the off-axis correlations, consider \( i \not\equiv 0 \mod (p), j \not\equiv 0 \mod (q) \), in which case
\[
R_A(i, j) = A(0, 0)(A(i, j) + A(-i, -j)) + A(0, -j)A(i, 0)
\]

\[
+ A(-i, 0)A(0, j) + \sum_{y=1}^{q-1} A(0, y)A(i, y + j)
\]

\[
+ \sum_{x=1}^{p-1} A(x, 0)A(x + i, j) + \sum_{y=1}^{q-1} A(-i, y)A(0, y + j)
\]

\[
+ \sum_{x=1}^{p-1} A(x, -j)A(x + i, 0) + \sum_{y=1}^{q-1} \sum_{z=1}^{p-1} A(x + i, y + j)A(x, y).
\]

Substituting for \( A(x, y) \), \( R_A(i, j) \) becomes
\[
R_A(i, j) = -1((i/p)(j/q) + (-i/p)(-j/q)) - 2
\]

\[
+ (i/p) \sum_{y=1}^{q-1} ((y + j)/q) - (j/q) \sum_{x=1}^{p-1} ((x + i)/p)
\]
\[ + \left( -\frac{i}{p} \right) \sum_{y=1, y \neq q-i}^{q-1} \left( \frac{y}{p} \right) - \left( -\frac{j}{p} \right) \sum_{z=1, z \neq p-i}^{p-1} \left( \frac{z}{p} \right) \]
\[ + \sum_{y=1}^{q-1} \left( \frac{y}{p} \right) \left( \frac{y + j}{q} \right) \sum_{z=1}^{p-1} \left( \frac{z}{p} \right) \left( \frac{x + i}{p} \right). \]

Again from Property 7, \( R_A(i, j) \) becomes
\[ R_A(i, j) = -\left( \frac{i}{p} \right) \left( \frac{j}{q} \right) + \left( -\frac{i}{p} \right) \left( -\frac{j}{q} \right) = 1 \]
\[ = -\left( \frac{i}{p} \right) \left( \frac{j}{q} \right) \left( 1 + \left( -\frac{1}{p} \right) \left( -\frac{1}{q} \right) \right) - 1, \]

which from Property 5 becomes
(a) \( q - p = 0; R_A(i, j) = -2 \left( \frac{i}{p} \right) \left( \frac{j}{q} \right) - 1 \)
(b) \( q - p = 2; R_A(i, j) = -1 \)
(c) \( q - p = 4; R_A(i, j) = -2 \left( \frac{i}{p} \right) \left( \frac{j}{q} \right) - 1 \)
(d) \( q - p = 6; R_A(i, j) = -1 \)

for all \( i \neq 0 \mod (p), j \neq 0 \mod (q). \)

Hence, as stated previously, the off-axis values will always alternate between +1 and -3 if \( pq \equiv 1 \mod (4) \) and will be -1 if \( pq \equiv 3 \mod (4). \) This completes the proof of the theorem.

APPENDIX A-2. GORDON ARRAYS

We first show that the matrix \( \tilde{A}(x, y) \) defined in Section 5.5 has the shift and add property. That is, we prove that
\[ \tilde{A}(x, y) \oplus \tilde{A}(x + i, y + k) = \tilde{A}(x + i', y + k') \]
if \( (i, k) \neq (0, 0) \mod (p, q). \)

**Proof:**
\[ \tilde{A}(x, y) \oplus \tilde{A}(x + i, y + k) = L(\gamma^{xq+y+vp}) + L(\gamma^{(x+iv)q+(y+k)p}) \]
\[ = L(\gamma^{xq+y+vp}(1 + \gamma^{iq+kp})) \]

since \( L(\quad) \) is a linear operator. But since \( \gamma \) is a primitive element of \( GF(2^N) \), \( 1 + \gamma^{iq+kp} \) is given as
\[ 1 + \gamma^{iq+kp} = 0 \quad iq + kp \equiv 0 \mod (pq) \]
\[ = \gamma^{i} \quad iq + kp \neq 0 \mod (pq), \]
where ℓ is some nonzero integer that depends upon the shifts i and k. But for \( 0 \leq i < p, 0 \leq k < q, (i, k) \neq (0, 0), iq + kp \) cannot be congruent to zero mod \( pq \) since \( p \) and \( q \) are relatively prime. Also, since \( p \) and \( q \) are relatively prime, \( ℓ \) can be written as

\[
\ell = i'q + k'p,
\]
where \( i' \) and \( k' \) are integers.

Thus

\[
\hat{A}(x, y) + \hat{A}(x + i, y + k) = L(\gamma^{iq+kp} \gamma^{i'q+k'p}) = L(\gamma^{(x+i')q+(y+k')p}) = \hat{A}(x + i', y + k'). \quad \text{Q.E.D.}
\]

We next show that \( \hat{A}(x, y) \) has one more one than zero in the area \( pq \).

**Proof:** The elements \( \gamma^{xq+yp} \) are all the distinct nonzero elements of \( \text{GF}(2^N) \). This follows from the fact that if \( \gamma^{xq+yp} = \gamma^{x'q+y'p} \), then \( (xq + yp) \equiv (x'q + y'p) \mod (pq) \) or \( [(x - x')q + (y - y')p] \equiv 0 \mod (pq) \). But since \( p \) and \( q \) are relatively prime, \( x \equiv x' \mod p \) and \( y \equiv y' \mod q \).

Let us now rename the elements of \( \text{GF}(2^N) \), \( \gamma_k \) where \( k = 0, 1, 2, \ldots, 2^N - 1 \) and where \( \gamma_0 = 0 \). Now, since the \( \gamma_k \) are elements of a field, they certainly form an additive group so that

\[
\gamma_i + \gamma_j = \gamma_k.
\]

If we hold \( \gamma_i \) fixed and let \( \gamma_j \) range over all its \( 2^N \) values, then \( \gamma_k \) takes on all the \( 2^N \) distinct values of the field. Now consider

\[
L(\gamma_i + \gamma_j) = L(\gamma_i) + L(\gamma_j) = L(\gamma_k)
\]

and we choose \( \gamma_i \) such that \( L(\gamma_i) = 1 \). (There must be a \( \gamma_i \) such that this is true since \( L(\gamma_i) \) cannot be zero for all \( \gamma_i \).) Thus

\[
1 + L(\gamma_j) = L(\gamma_k).
\]

Now, for every \( \gamma_j \) for which \( L(\gamma_j) = 0 \) (or 1), there must exist a \( \gamma_k \) such that \( L(\gamma_k) = 1 \) (or 0). That is, there are an equal number of \( L(\gamma) \) that yield zero as yield one. But \( L(\gamma_0) = L(0) = 0 \) for any linear operator so that the matrix \( \hat{A}(x, y) \) contains \( (pq + 1)/2 \) ones and \( (pq - 1)/2 \) zeros.

Finally, to compute the autocorrelation function of \( A(x, y) \), we note that
\[ R_A(i, j) = \sum_{x=1}^{p} \sum_{y=1}^{q} A(x, y)A(x + i, y + j) \]
\[ = pq - 2 \sum_{x=1}^{p} \sum_{y=1}^{q} (\tilde{A}(x, y) \oplus \tilde{A}(x + i, y + j)) \]
\[ = pq - 2(pq + 1)/2 = -1 \quad \text{if} \quad (i, j) \neq (0, 0) \mod (p, q) \]
\[ = pq \quad \text{if} \quad (i, j) \equiv (0, 0) \mod (p, q). \]

**APPENDIX A-3. PROOF OF THE AUTOCORRELATION PROPERTY OF THE NONBINARY ARRAY OF SECTION 6**

**Theorem.** The multiple level array of area \( N^2 \) given by

\[ A(x, y) = e^{i(xy)(2\pi/N)} \]

has imbalance

\[ D_A = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} A(x, y) = N \]

and periodic autocorrelation function given by

\[ R_A(s, t) = N^2 \quad \text{if} \quad (s, t) \equiv (0, 0) \mod (N, N) \]
\[ = 0 \quad \text{if} \quad (s, t) \neq (0, 0) \mod (N, N). \]

**Proof:** We first note that the following summation holds:

\[ \sum_{x=0}^{N-1} e^{i\cdot jxk(2\pi/N)} = \begin{cases} N & \text{if} \quad k \equiv 0 \mod (N) \\ 0 & \text{if} \quad k \not\equiv 0 \mod (N). \end{cases} \]

Thus,

\[ R_A(s, t) = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} e^{i(xy)(2\pi/N)} (e^{i(x+1)(y+1)(2\pi/N)})^* \]
\[ = e^{-st(2\pi/N)} \sum_{x=0}^{N-1} e^{-jxt(2\pi/N)} \sum_{y=0}^{N-1} e^{-jys(2\pi/N)}, \]

or from the previous summation

\[ R_A(s, t) = N^2 \quad \text{if} \quad (s, t) \equiv (0, 0) \mod (N, N) \]
\[ = 0 \quad \text{if} \quad (s, t) \neq (0, 0) \mod (N, N). \]

The imbalance of the array also follows readily as
\[ D_A = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} e^{2\pi i (2x+y)} \]
\[ = \sum_{x=0}^{N-1} 1 \]
\[ = N. \]

Received: April 26, 1967 revised: November 14, 1967

References


