Double Periodic Arrays with Optimal Correlation for Applications in Watermarking

Oscar Moreno[1] and José Ortiz-Ubarri[2]

[1] Computer Science Department
University Of Puerto Rico
Río Piedras Campus
moreno@uprr.pr
[2] High Performance Computing facility
University of Puerto Rico
jose.ortiz@hpcf.upr.edu

Abstract. Digital watermarking applications require constructions of double-periodic matrices with good correlations. More specifically we need as many matrix sequences as possible with both good auto- and cross-correlation. Furthermore it is necessary to have double-periodic sequences with as many dots as possible.

We have written this paper with the specific intention of providing a theoretical framework for constructions for digital watermarking applications.

In this paper we present a method that increases the number of sequences, and another that increases the number of ones keeping the correlation good and double-periodic. Finally we combine both methods producing families of double-periodic arrays with good correlation and many dots. The method of increasing the number of sequences is due to Moreno, Omrani and Maric. The method to increase the number of dots was started by Nguyen, Lázló and Massey, developed by Moreno, Zhang, Kumar and Zinoviev, and further developed by Tirkel and Hall. The very nice application to digital watermarking is due to Tirkel and Hall.

Finally we obtain two new constructions of Optical Orthogonal Codes: Construction A which produces codes with parameters $(n, \omega, \lambda) = (p(p-1), \frac{p^2-1}{2}, [\frac{p(p+1)}{4}])$ and Construction B which produces families of code with parameters $(n, \omega, \lambda) = (p^2(p-1), \frac{p^2-1}{2}, [\frac{p(p+1)}{4}])$ and family size $p+1$.

Keywords: double-periodic, correlation, watermark, sequences, matrix, array.

1 Background

Sequences with good auto- and cross-correlation have been studied by our group for their applications in frequency hopping radar and sonar, and communications, and more recently in digital watermarking.

S.W. Golomb et al. (Eds.): SSC 2007, LNCS 4893, pp. 82–94, 2007.

Costas and sonar sequences were respectively introduced in [3] and [5] to deal with the following fundamental problem:

"We have an object which is moving towards (or away from) us and we want to determine the distance and velocity of that object."

The solution to the problem makes use of the Doppler effect. Doppler observed that when a signal hits a moving object its frequency changes in direct proportion to the velocity of the moving object relative to the observer. In other words, if the observer sends out a signal towards a moving target, the change between the frequency of the outgoing and that of the returning signal will allow him to determine the velocity of the target, and the time it took to make the round trip will allow him to determine the distance.

In a frequency hopping radar or sonar system, the signal consists of one or more frequencies being chosen from a set $\{f_1, f_2, \ldots, f_m\}$ of available frequencies, for transmission at each of a set of $\{t_1, t_2, \ldots, t_n\}$ of consecutive time intervals. For modeling purposes, it is reasonable to consider the situation in which $m = n$, and where

$$\{f_1, f_2, \ldots, f_n\} = \{t_1, t_2, \ldots, t_n\} = \{1, 2, \ldots, n\}$$

(we will call this last $m = n$ case, a Costas type, and the general case sonar type).

Such a Costas signal is conveniently represented by a $n \times n$ permutation matrix A, where the n rows correspond to the n frequencies, the n columns correspond to the n time intervals, and the entry a_{ij} equals 1 if and only if frequency i is transmitted in time interval j. (Otherwise, $a_{ij} = 0$)

When this signal is reflected from the target and comes back to the observer, it is shifted in both time and frequency, and from the amounts of these shifts, both range and velocity are determined. The observer finds the amounts of these shifts by comparing all shifts (in both time and frequency) of a replica of the transmitted signal with the actual received signal, and finding for which combination of time shift and frequency shift the coincidence is greater. This may be thought of as counting the number of coincidences between 1's in the matrix $A = (a_{ij})$ with 1's in a shifted version A^* of A, in which all entries have been shifted r units to the right (r is negative if there is a shift to the left), and s units upward (s is negative if the shift is downward). The number of such coincidences, $C(r, s)$, is the two-dimensional auto-correlation function between A and A^*, and satisfies the following conditions:

$$C(0, 0) = n$$

$$0 \leq C(r, s) \leq n \text{ except for } r = s = 0$$

(This conforms to the assumption that the signal is 0 outside the intervals $1 \leq f \leq nand1 \leq t \leq n$)

If we have another Costas type of signal represented by a matrix $B = (b_{ij})$, we can similarly define the two-dimensional cross-correlation function by substituting A^* by B^* in the above definition.

In the real world, the returning signal is always noisy. The two-dimensional auto-correlation function, $C(r, s)$, is also called the ambiguity function in radar and sonar literature, and should be thought of as the total "coincidence" between the actual returning noisy signal and the shift of the ideal transmitted signal by r units in time and s units in frequency. Among the 2^{n^2} matrices of 0's and 1's of order n, there are $n!$ permutation matrices, and some of these are not very good as signal patterns for radar and sonar. For example, the $n \times n$ identity matrix I_n can be shifted one unit up and one unit left, and will then produce $n - 1$ coincidences with the original matrix. For large values of n and a noisy environment, the signal pattern I_n would most certainly produce spurious targets, shifted an equal number of units in both time and frequency from the real target.

At a minimum, there is a shift of $A = (a_{ij})$ which will make any of the n 1's land on any of the $n - 1$ remaining 1's, so we know that

$$\min C(r, s) = 1$$

$$\max C(r, s) \geq 1$$

$$\text{for all "codes"} (r, s) \neq (0, 0)$$

where $C(r, s)$ is the ideal ambiguity function of the permutation matrix itself. Consequently J.P. Costas [3] defined the ideal $n \times n$ permutation matrices (which we will call here Costas sequences) as those for which

$$\max C(r, s) = 1 \text{ when } (r, s) \neq (0, 0)$$

By hand computation, he found examples of such matrices for all $n \leq 12$, but was unable to find an example for $n = 13$, and was tempted to conclude that these patterns "die out" beyond $n = 12$.

In the general sonar case, n signals are sent out with frequencies ranging from 1 to m, at times ranging from 1 to n. Once the whole pattern of signals has returned, the velocity and the distance of the object can be determined as mentioned before. For sonars you must have exactly a 1 in every column but the rows can have multiple 1's or they can be empty of 1's. The problem in sonars (see [7]) is for any n obtain the largest possible m.

It has been proven in [4] that for $n > 3$ there are no two different Costas sequences with the same ideal property in their cross-correlation as that they have in their auto-correlation. Since for the case of multiple targets we need sets of sequences with good auto- and cross-correlation properties we had therefore settled for constructing sets of sequences with nearly ideal properties, or in other words cross-correlation 2.

In spread spectrum communications the data sent in a communication channel is spread to avoid its interception and channel jamming; and in modern communications like CDMA for multiple access in wireless and optical communication. Using codes with good auto- and cross-correlation a message sent in a communication channel can then be easily recovered in the other side of communication and furthermore using codes with good cross-correlation allows communication of multiple users limiting signal interference.

Recently sequences with good auto- and cross-correlation have been used in the area of digital watermarking because they make watermarks more difficult to detect, damage or remove from a digital medium. The idea is similar to the spread spectrum communications where a secret message is spread into a channel in order to make it more difficult to be intercepted or removed.

A watermark is an array or a sum of arrays that can carry information. This array is added to a medium in order to make it difficult to perceive. The watermark is recovered by calculating the watermark correlation with the watermarked medium. Families of arrays with perfect or near to perfect auto- and cross-correlation allow the addition of multiple arrays to increase information capacity (or multiple users) and watermark security.

In previous work, families of Costas and sonar arrays have been studied in the area of digital watermarking. The Moreno-Maric construction [12], which generates families of double periodic arrays, was used by Tirkel and Hall in particular because of their near to perfect correlation (2) and the size of its families. In order for watermarks to be more effective it must have many dots. Also it is necessary to have as many sequences with low cross-correlation as possible to combine them and increase the watermark information capacity. The method of using periodic-sequences to replace columns of matrices in order to increase the number of dots in double-periodic sequences was introduced in [10], was previously used by our group [8] and also used by Tirkel and Hall [11] in the area of watermarking. Recently Moreno, Omrani and Maric [9] presented a new construction of double periodic sequences with perfect auto- and cross-correlation. In this work we will use this new construction to generate families of matrices that can be used for digital watermarking.

2 Method to Increase the Number of Sequences without Increasing the Original Correlation Value

Moreno, Omrani and Maric showed how to construct new families of sonars and extended Costas arrays, from a Welch Costas array ($p \times (p-1)$), with auto- and cross-correlation 1. The Welch Costas arrays are constructed as follows:

Welch Construction. Let α be a primitive root of an odd prime p.

Then the array with

$$\alpha_{k,j} = 1, 1 \leq k, j \leq p-1$$

if and only if

$$j \equiv \alpha^k (\bmod\ p), 1 \leq k \leq p-1,$$

otherwise $\alpha_{k,j} = 0$, is a Costas array.

This construction is the first construction of multiple target sonars with perfect auto- and cross-correlation properties. Multiple target arrays are families of arrays used in radar and sonar that are sent to different targets. When the echoes are received the low cross-correlation of the arrays is used to distinguish the distance and velocity of each target. In the case of watermarking we call these arrays multiple user arrays, because instead of using the arrays to distinguish targets we use them to distinguish users.

2.1 OOC, DDS, and Double Periodic Arrays of Families

An (n, ω, λ) Optical Orthogonal Code (OOC) C where $1 \leq \lambda \leq \omega \leq n$, is a family of {0,1}-sequences of length n and Hamming weight ω satisfying:

$$\sum_{k=0}^{n-1} x(k)y(k \oplus_n \tau) \leq \lambda \tag{1}$$

whenever either $x \neq y$ or $\tau \neq 0$. We will refer to λ as the maximum correlation parameter, and Φ as the family size.

A (k, v)-Distinct Difference Set (DDS) [1] is a set $\{c_i | 0 \leq i \leq k-1\}$ of distinct integers such that the $k(k-1)$ differences $c_i - c_j$ where $i \neq j$ are distinct modulo v.

By a (v, k, t)-DDS, we mean a family $(B_i | i \in I, t = |I|)$ of subsets of $\mathbb{Z}_v$ each of cardinality k, such that among the $tk(k-1)$ differences $(a-b | a, b \in B_i; a \neq b; i \in I)$ each nonzero element $g \in \mathbb{Z}_v$ occurs at most once. This notion of a (v, k, t)-DDS is a more recent generalization of the earlier concept of a (k, v)-DDS. A (k, v)-DDS is a (v, k, t)-DDS with parameter $t = 1$.

Lemma 1. *There is a one to one onto correspondence between the set of (n, ω, λ)-OOCs and the set of (v, k, t)-DDSs when $\lambda = 1$ with $n = v$, $k = \omega$ and $\Phi(n, \omega, 1) = t$, and $\Phi(n, \omega, 1)$ is the family size of the OOCs.*

Proof. The incidence vectors associated to the subsets comprising a (v, k, t)-DDS can be seen to form an (n, ω, λ)-OOC of size t with parameters $n = v, w = k$, and $\lambda = 1$. Conversely, given an OOC and a maximal set of cyclically distinct representatives drawn from the code, one obtains a DDS by considering the support of these vectors. Thus, the concept of (v, k, t)-DDS is precisely the same as that of an OOC with $\lambda = 1$.

Let $A = [A(i, j)]$ and $B = [B(i, j)]$ be $r \times s$ matrices having 0,1 entries where r and s are relatively prime. We now have the following definition:

Definition 1. *The double-periodic cross-correlation between A and B is an integer valued function for a change of value (a, b) a in the row and b in the column. In other words the function varies for all (a, b) a less than the first value and b less than the second value of the double periodicity. The function $C(a, b)$ is a integer function defined as follows:*

$$\sum_{i=0}^{r-1} \sum_{j=0}^{s-1} A(i \oplus_r \alpha, j \oplus_s \tau) B(i, j) \leq C(a, b) \tag{2}$$

for any $\alpha \leq r, \tau \leq s$, where $\oplus_m$ denotes addition modulo m the smallest such $C(a,b)$ is the correlation. Auto-correlation is the same with $A = B$. Let $a(.)$ and $b(.)$ be the sequences of length rs associated with the matrices A and B respectively via the Chinese Remainder Theorem, $a(L) = A(L(\mod r), L(\mod s))$ and similarly $b(L) = B(L(\mod r), L(\mod s))$ for all L, $0 \leq L \leq rs-1$.

Definition 2. *Bound on the correlation.*

$$max\ C(a,b) \leq \lambda \ when\ (a,b) \neq (0,0) \tag{3}$$

From the previous definitions we obtain the following theorem:

Theorem 1. *The collection of one-dimensional periodic auto- and cross-correlation values of a family of sequences of length rs is precisely the same as the set of two dimensional double-periodic auto- and cross-correlation values of $r \times s$ matrices associated with these sequences via the residue map, whenever r and s are relatively prime.*

Corollary 1. *The concept of an OOC with auto- and cross-correlation λ is the same as that of a double-periodic multi-target arrays with auto- and cross-correlation λ.*

1) MZKZ Construction A: When m is a divisor of $p-1$, $m|(p-1)$, and p is a prime, the construction of an $(n = mp, w = m, \lambda = 1)$, $\Phi = \frac{p-1}{m}$ OOC (Construction A in Moreno et al [8]) yields a $(v = mp, k = m, \frac{p-1}{m})$-DDS for any $m|(p-1)$. This construction is optimal with respect to the Johnson Bound [6] on the cardinality of a constant weight binary code when $p > 3$ and $m = p-1$. The construction is given for $m = p-1$ in the following:

If we choose any degree one polynomial $f(x)$ over $\mathbb{F}_p$, and fill out the elements of a $p \times (p-1)$ matrix M with the following rule:

$$M(i,j) = \begin{cases} 1, \text{ if } f(\alpha^j) = p-1-i \\ 0, \qquad \text{otherwise} \end{cases} \tag{4}$$

where α is a primitive element of F_p, then the resulting M matrix has one 1 per column and has the double-periodic auto-correlation property. If we apply the Chinese Remainder Theorem to the matrix M we will end up with an OOC sequence μ of length $p(p-1)$:

$$\mu(l) = M(l \mod (p), l \mod (p-1)) \tag{5}$$

2) A New Family of OOC's: M.J. Colbourn and C.J. Colbourn [2] proposed two recursive constructions for cyclic BIBD's. Their Construction A was generalized [13] to form DDS recursively. The following is an easy generalization of Colbourn construction B:

Construction B: Given a (vk, k, t)-DDS, $(vk = 0(\mod k))$ if $gcd(r, (k-1)!) = 1$, then a (vkr, k, rt)-DDS may be constructed as follows. For each $D = \{0, d_1, \ldots, d_{k-1}\}$, take the r difference sets $\{0, d_1 + ikv, d_2 + 2ikv, \ldots, d_{k-1} + (k-1)ikv\}$,

$0 \leq i < r$, with addition performed modulo vkr. If furthermore, there exists an (rk, k, t')-DDS D', then a $(vkr, k, rt + t')$-DDS can be constructed by adding the t' difference sets $\{0, vs_1, \ldots, vs_{k-1}\}$ for each $D'_i = \{0, s_1, \ldots, s_{k-1}\}$ of $D' = \{D'_i | 1 \leq i \leq t'\}$.

A proof of the above is not included (the proof is similar to the one in [2]). In Lemma 2 we will prove the special case that interests us in this paper.

Construction CMZKZ: Applying construction B recursively to MZKZ family A construction, we obtain a $(p^i(p-1), p-1, 1)$-OOC of size $p^{i-1}+p^{i-2}+\cdots+p+1$. This OOC is not optimal with respect to the Johnson Bound [6].

Lemma 2. *In the $(p^i(p-1), p-1, 1)$-OOC of the above construction, all residues occur exactly once except multiples of $p-1$ and p^i.*

Proof. In the base OOC all the residues occur except multiples of p and $p-1$. Now applying the recursive construction to the $(p(p-1), p-1, 1)$ base OOC, in the resulting $(p^2(p-1), p-1, 1)$-OOC all the multiples of residues present in the base OOC will be present in addition to the multiples of p times the residues of the base OOC. So in the new OOC the multiples of $p-1$ do not occur. In addition since the multiples of p were not present in the base residues so in the new OOC the multiples of p^2 also do not occur.

We can use the same proof inductively to prove that in $(p^i(p-1), p-1, 1)$ all the residues occur exactly once except the multiples of p^i and $p-1$.

2.2 Two New Multiple Target Families for Extended Costas and for Sonar Arrays

Using the Chinese Reminder Theorem and Theorem 1 of Section 2.1, since p^i is relatively prime to $p-1$ we obtain:

Construction 1(V): From Section 2.1 we obtain a family of $p^2 \times (p-1)$ sonar arrays with family size of $p+1$ with auto- and cross-correlation 1.

Construction 2(V): A family of $p^i \times (p-1)$ sonar arrays with family size of $p^{i-1} + p^{i-2} + \cdots + 1$ with auto- and cross-correlation 1.

Construction 1(H): From section 2.1 we obtain a family of $(p-1) \times p^2$ extended Costas arrays with family size of $p+1$ with auto- and cross-correlation 1.

Construction 2(H): A family of $(p-1) \times (p^i)$ extended Costas arrays with family size of $p^{i-1} + p^{i-2} + \cdots + 1$ with auto- and cross-correlation 1.

Example 1. An example to generate the family of Construction 1(V). Start with a Welch array of Figure 1 2,4,3,1. Now notice that (0,2) corresponds to 12 using the Chinese Remainder Theorem since $12 \equiv 0 \mod (4)$ and $12 = 2 \mod (5)$. Also $(1, 4) \rightarrow 9$, $(2, 3) \rightarrow 18$, and $(3, 1) \rightarrow 11$. Where in $(x, y) \rightarrow z$, x is the value of the column, y is the value of the row, and z is the Chinese Remainder for (x, y). Applying the Chinese Reminder Theorem to the Welch array we obtain the OOC D:

$$D = \{9, 11, 12, 18\}$$

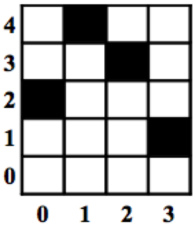


Fig. 1. 5x4 Welch Costas

which is equivalent to D':

$$D' = \{9, 11, 12, 18\}$$

From D' using our construction B we obtain the 6 arrays D_1, D_2, D_3, D_4, D_5 and D_6 as follows: (See section 2.1):

$$D_1 = \{0, 2, 3, 9\} \text{ for } i = 0$$

$$D_2 = \{0, 22, 43, 69\} \text{ for } i = 1$$

$$D_3 = \{0, 29, 42, 83\} \text{ for } i = 2$$

$$D_4 = \{0, 23, 62, 89\} \text{ for } i = 3$$

$$D_5 = \{0, 49, 63, 82\} \text{ for } i = 4$$

Now we multiply D' by 5:

$$D_6 = \{0, 10, 15, 45\}$$

Finally apply the Chinese Reminder Theorem again to each D_i to construct the family of 25×4 sonars arrays of size 6. I.E. To construct sonar S_i for each element $d \in D_i$, calculate $s = (d \mod 4, d \mod 25)) \in S_i$. See Figure 2.

3 Method to Increase the Number of Dots

Previous work [10] [8] [11] describes how to increase the number of dots in a double-periodic matrix sequence using periodic shift sequences. Tirkel and Hall applied this method with the Moreno-Maric construction [12] to create new matrices with good auto- and cross-correlation.

Method A: consists in replacing the columns of a double-periodic matrix W with a cyclically shifted periodic sequence s with the size of the columns of the matrix (See Figure 3(b)). For each column j in W, find the row i where $W_{i,j} = 1$, construct s' such that s' is equal to s cyclically shifted i units, and replace the column j with s'. Figure 3 is an example of a double-periodic Welch 7×6

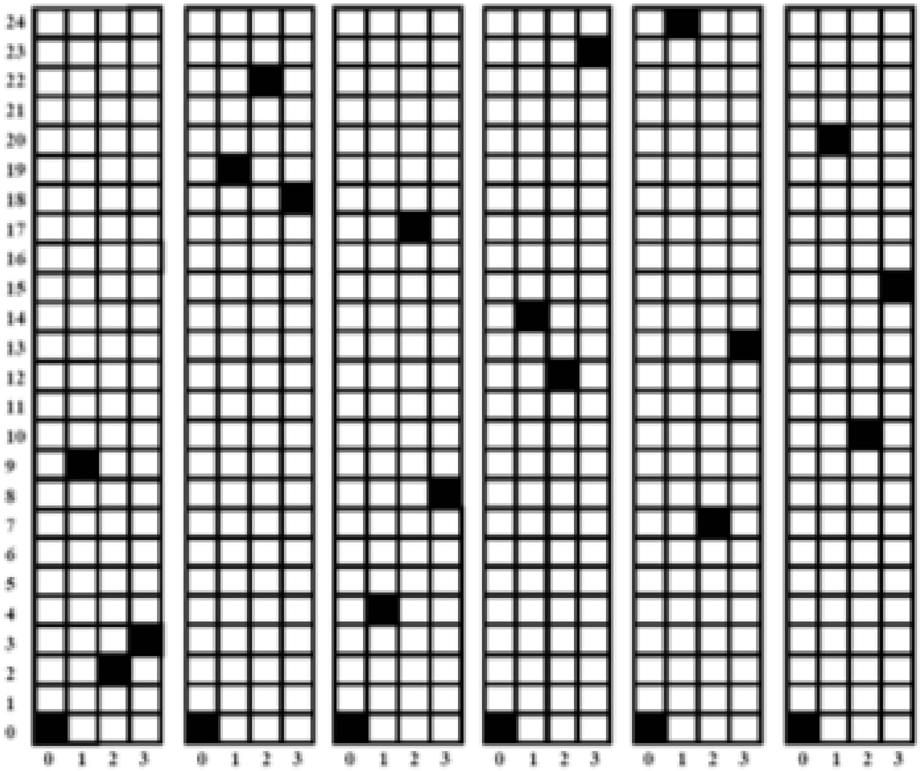


Fig. 2. 25x4 Moreno-Omrani-Maric sonars family

matrix sequence $(0,3),(1,2),(2,6),(3,4),(4,5),(6,1)$ with the columns replaced by a binary m-sequence (0,0,1,1,1,0,1) of size 7.

Proof of the following theorem can be done following the techniques used by Nguyen, Lázló and Massey in [10].

Theorem 2. *Method A applied to a Welch array of size* $p(p-1)$ *using a Legendre sequence as a column produces OOCs with parameters* $(n,\omega,\lambda) = (p(p-1), \frac{p^2-1}{2}, [\frac{p(p+1)}{4}])$*. These codes are asymptotically optimum.*

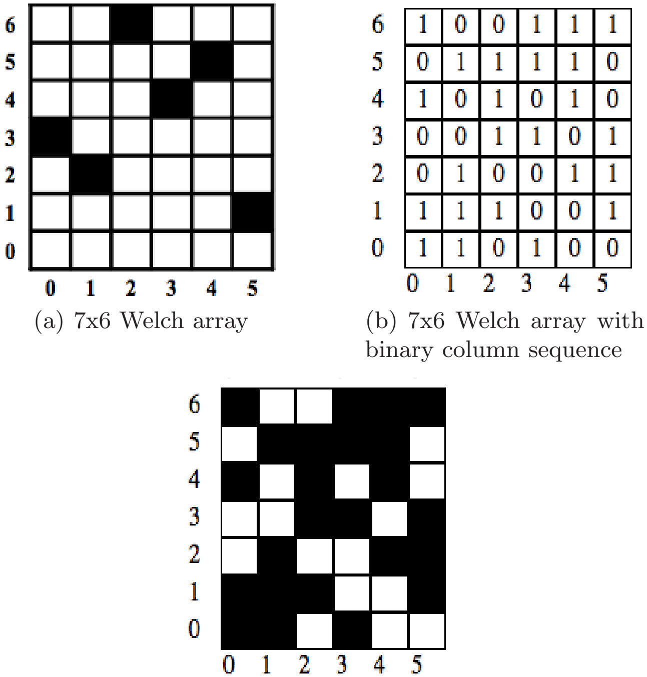
4 New Matrix Construction for Watermarking

In section 2 we showed how to construct families of double-periodic sequences with perfect correlation. This property is very useful in digital watermarking because it reduces the number of false positives in watermark detection. In section 3 we explained how to increase the number of dots in a double-periodic sequence. In the next subsection we will use the Moreno-Omrani-Maric family construction to construct new families of matrices which are more efficient for watermarking by increasing the number of dots in the Moreno-Omrani-Maric construction.

4.1 Method to Increase the Number of Dots and the Number of Sequences with Optimal Correlation

We construct a family of matrices from a Welch Costas array using column sequences and applying the Moreno-Omrani-Maric construction.

Method B: First we generate a Welch Costas array, then we replace the columns with a suitable cyclically shifted periodic sequence to increase the number of dots (filled pixels in images) in the matrix, and finally we apply the Moreno-Omrani-Maric construction to generate the new family of size $p + 1$. (See example 2).



(a) 7x6 Welch array

6	1	0	0	1	1	1
5	0	1	1	1	1	0
4	1	0	1	0	1	0
3	0	0	1	1	0	1
2	0	1	0	0	1	1
1	1	1	1	0	0	1
0	1	1	0	1	0	0
	0	1	2	3	4	5

(b) 7x6 Welch array with binary column sequence

(c) 7x6 Welch array with column sequence

Fig. 3. 7x6 Welch array with and w/o column sequence

Example 2. Start with the Welch array of Figure 3(a) with points $(0, 3), (1, 2)$, $(2, 6), (3, 4), (4, 5)$ and $(5, 1)$. Replace the columns of the matrix in that figure with the periodic sequence $0, 0, 1, 1, 1, 0, 1$ which is a binary m-sequence with auto-correlation 2 (See Figure 3(b)) to form the matrix in figure 3(c).

Now apply the Moreno-Omrani-Maric construction to the new matrix of size $p \times (p-1)$. The Chinese Reminder for the points in the new matrix are $(0,0) \rightarrow 0, (0,1) \rightarrow 36, (0,4) \rightarrow 18, (0,6) \rightarrow 6, (1,0) \rightarrow 7, (1,1) \rightarrow 1, (1,2) \rightarrow 37, (1,5) \rightarrow 19, (2,1) \rightarrow 8, (2,3) \rightarrow 38, (2,4) \rightarrow 32, (2,5) \rightarrow 26, (3,0) \rightarrow 21, (3,3) \rightarrow 3, (3,5) \rightarrow 33, (3,6) \rightarrow 27, (4,2) \rightarrow 16, (4,4) \rightarrow 4, (4,5) \rightarrow 40, (4,6) \rightarrow 34, (5,1) \rightarrow 29, (5,2) \rightarrow 23, (5,3) \rightarrow 17, (5,6) \rightarrow 41$.

From the Chinese Reminder Theorem we obtain D':

$$D_{\prime} = \{0,1,3,4,6,7,8,16,17,18,19,21,23,26,27,29,32,33,34,\\ 36,37,38,40,41\}$$

Now following the Moreno-Omrani-Maric construction we obtain from D':

$$\begin{aligned}
D_1 &= \{0,1,3,4,6,7,8,16,17,18,19,21,23,26,27,29,32,33,34,\\
&\quad 36,37,38,40,41\}\\
D_2 &= \{0,16,27,38,43,59,71,82,87,102,116,125,130,145,159,174,189,202,217,\\
&\quad 233,246,260,278,289\}\\
D_3 &= \{0,16,27,38,48,63,76,85,101,113,124,133,149,162,171,186,200,209,218,\\
&\quad 236,247,256,271,285\}\\
D_4 &= \{0,16,27,38,49,65,78,88,103,117,127,143,155,166,176,194,205,216,231,\\
&\quad 244,255,270,284,293\}\\
D_5 &= \{0,16,27,38,45,60,74,83,90,105,118,134,152,163,169,185,197,208,214,\\
&\quad 229,243,259,275,288\}\\
D_6 &= \{0,16,27,38,46,61,75,92,110,121,129,144,158,167,175,191,204,211,227,\\
&\quad 239,250,258,273,286\}\\
D_7 &= \{0,16,27,38,50,68,79,91,107,120,132,147,160,172,187,201,213,228,242,\\
&\quad 251,253,269,281,292\}
\end{aligned}$$

And multiplying D' by 7:

$$D_8 = \{0,7,21,28,42,49,56,112,119,126,133,147,161,182,189,203,224,231,238,\\ 252,259,266,280,287\}$$

Finaly apply the Chinese Reminder Theorem again to convert them to 6×49 matrices. (see Figure 4)

Theorem 3. *Method B applied to a Welch array of size $p(p-1)$ using a Legendre sequence as a column produces OOCs with parameters $(n, \omega, \lambda) = (p^2(p-1), \frac{p^2-1}{2}, [\frac{p(p+1)}{4}])$ and family size $p+1$.*

In our example 2 we construct code sequences with $(n, \omega, \lambda) = (6 \times 49, 24, 14)$. These families of matrices can be used in digital watermarking because of their good cross-correlation. In our example the cross-correlation is 14 because of

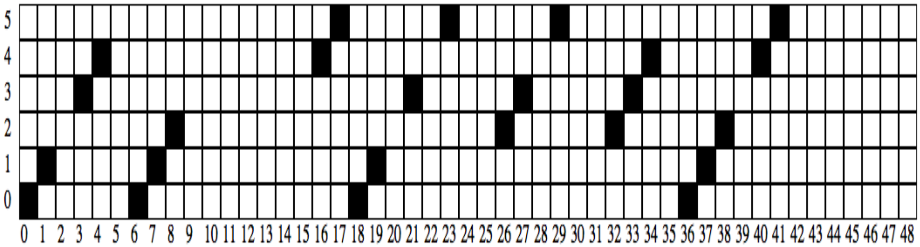


Fig. 4. 6x49 New matrix construction from Welch array 7x6 (rotated 90 degrees to the right)

the choice of the column sequence which auto-correlation is 2. The addition of arrays in the same family allows the watermark to carry more information. In the case of images the use of other methods like interlacing [12] can be also applied to extend families of matrices but increasing the correlation values. Also the selection of the column sequence and its correlation affects the new matrices' cross-correlation.

5 Conclusion

The Moreno-Omrani-Maric construction generates families with perfect auto- and cross-correlation. The matrices generated by this construction have few dots, and we showed a method to increase the number of dots in the matrices making them more effective for watermarking. We take advantage of the perfect correlation properties of the Moreno-Omrani-Maric construction to keep a low cross-correlation between matrices in the same family. In summary we showed a method to increase the number of matrix sequences and the number of dots in those matrices resulting in matrix sequences with good auto- and cross-correlation that can be used in digital watermarking.

We obtain two new constructions of Optical Orthogonal Codes: Construction A which produces codes with parameters $(n, \omega, \lambda) = (p(p-1), \frac{p^2-1}{2}, [\frac{p(p+1)}{4}])$ and construction B which produces families of code with parameters $(n, \omega, \lambda) = (p^2(p-1), \frac{p^2-1}{2}, [\frac{p(p+1)}{4}])$ and family size $p+1$.

Acknowledgments

We would like to thank Dr. Tirkel for introducing our group to the watermarking area. This work is partially supported by the High Performance Computing facility of the University of Puerto Rico under PR AABRE grant #P20RR16470 from the National Institute of Health and the Gauss Research Laboratory under SCORE grant #S06GM08102.

References

1. Coldbourn, C.J, Dinitz, J.H.: The CRC Handbook of Combinatorial Designs. CRC Press, Boca Raton, USA (1996)
2. Coldbourn, M.J., Coldbourn, C.J.: Recursive constructions for cyclic block designs. Journal of Statistical Planning and Inference 10, 97–103 (1984)
3. Costas, J.P.: Medium constraints on sonar design and performance. FASCON Convention Record, 68A–68L (1975)
4. Freedman, A., Levanon, N.: Any two n x n costas signal must have at least one common ambiguity sidelobe if n ¿ 3- a proof. In: Proceedings of the IEEE, vol. 73, pp. 1530–1531. IEEE Computer Society Press, Los Alamitos (October 1985)
5. Golomb, S.W., Taylor, H.: Two-dimensional syncronization patterns for minimum ambiguity. IEEE Trans. Information Theory IT-28, 600–604 (1982)
6. Johnson, S.M.: A new upper bound for error-correcting codes. IEEE Trans. on Information Theory IT(8), 203–207 (1962)
7. Moreno, O., Games, R.A., Taylor, H.: Sonar sequences from costas arrays and the best known sonar sequences with up to 100 symbols. IEEE Trans. Information Theory 39, 1985–1987 (1993)
8. Moreno, O., Zhang, Z., Kumar, P.V., Zinoviev, V.: New constructions of optimal cyclically permutable constant weight codes. IEEE Trans. Information Theory 41, 548–555 (1995)
9. Moreno, O., Omrani, R., Maric, S.V.: A new construction of multiple target sonar and extended costas arrays with perfect correlation. In: Proceedings of the 40th Annual Conference on Information Sciences and Systems, Princeton, NJ, USA (March 2006)
10. Nguyen, Q.A., Gyorfi, L., Massey, J.L.: Construction of binary constant-weight cyclic codes and cyclically permutable codes. IEEE Trans. Information Theory 38(3), 940–949 (1992)
11. Tirkel, A.Z., Hall, T.E.: Matrix construction using cyclic shifts of a column. In: Proceedings International Symposium on Information Theory, pp. 2050–2054 (September 2005)
12. Tirkel, A., Hall, T.: New matrices with good auto and cross-correlation. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. E89-A(9), 2315–2321 (2006)
13. Zhi, C., Pingzhi, F., Fan, J.: Disjoint difference sets, difference triangle sets and related codes. IEEE Trans. Information Theory 38, 518–522 (1992)