DOUBLE PERIODIC ARRAYS WITH APPLICATIONS

By

José R. Ortiz-Ubarri

A thesis submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

in

COMPUTING AND INFORMATION SCIENCE AND ENGINEERING

UNIVERSITY OF PUERTO RICO
MAYAGÜEZ CAMPUS

May, 2010

Approved by:

Dorothy Bollman, Ph.D. Member, Graduate Committee	Date
Carlos Corrada Bravo, Ph.D. Member, Graduate Committee	Date
Pedro I. Rivera Vega, Ph.D. Member, Graduate Committee	Date
Edusmildo Orozco, Ph.D. Member, Graduate Committee	Date
Oscar Moreno de Ayala, Ph.D. President, Graduate Committee	Date
Luis R. Pericchi, Ph.D. Representative of Graduate Studies	Date
Nestor Rodriguez, Ph.D Chairperson of the Department	Date

Abstract of Dissertation Presented to the Graduate School
of the University of Puerto Rico in Partial Fulfillment of the
Requirements for the Degree of Doctor of Philosophy

DOUBLE PERIODIC ARRAYS WITH APPLICATIONS

By

José R. Ortiz-Ubarri

May 2010

Chair: Oscar Moreno
Major Department: Computing and Information Science and Engineering

Algebraic constructions of families of double periodic arrays with good auto- and cross-correlation have been used for applications in frequency hopping radar and sonar, Optical Code Division Multiple Access, design of experiments, and more recently in Digital Watermarking. We need the family size of these constructions to be as large as possible to increase multiple user or multiple target detection capacity.

In this work we introduce the concept of Group Permutable Constant Weight Codes and we extend the Johnson Bound, to bound the cardinality of families of binary and non-binary Group Permutable Constant Weight Codes. These bounds are used to prove the optimality of some of our new constructions of Double Periodic Arrays.

We also present three methods to construct families of Double Periodic Arrays. A method to increase the weight of double periodic arrays (Method A). With this method we deal with the need of double periodic arrays with the weight as large as possible while maintaining a good correlation value.

We present a new method to increase the size of families of double periodic arrays (Method B).There are only a few families of double periodic arrays with

perfect correlation properties. In many cases the new constructions generated with Method B result in new families of double periodic arrays with perfect correlation properties and in all cases at least the original correlation properties are preserved.

Finally we present a combination of Method A and Method B to produce new families of double periodic constructions with increased family size and weight (Method C). When Method C is applied to a double periodic array we obtain new Fuja type families of double periodic arrays with unequal correlation constrains. More specifically, we obtain new families of double periodic arrays with cross-correlation much lower than auto-correlation ($\lambda_c < \lambda_a$).

Resumen de Disertación Presentado a Escuela Graduada
de la Universidad de Puerto Rico como requisito parcial de los
Requerimientos para el grado de Doctorado de Filosofía

ARREGLOS DOBLE PERIODICOS CON APLICACIONES

Por

José R. Ortiz-Ubarri

Mayo 2010

Consejero: Oscar Moreno
Departamento: Computación y Ciencias de Información e Ingeniería

Construcciones algebraícas de arreglos doble periódicos con buena auto y correlación cruzada han sido utilizadas en aplicaciones de radares y sonares de salto de frecuencia, Acceso Multiple por Division de Código Optico, diseo de experimentos, y mas recientemente en Watermarking Digital. Necesitamos que el tamaño de las familias de estas construcciones sean lo mas largo posible para aumentar la capacidad de usuarios o la capacidad para detectar multiples blancos.

En este trabajo introducimos el concepto de Códigos con Peso Constante de Grupos Permutables y extendemos la cota de Johnson, para acotar el tamaño de las familias de Códigos con Peso Constante de Grupos Permutables binarios y no binarios. Estas cotas se usan para probar la optimalidad de algunas de nuestras nuevas construcciones de arreglos doble periódicos.

También presentamos tres métodos para construir familias de arreglos doble periódicos. Un método para aumentar el peso de los arreglos doble periódicos (Método A). Con este método lidiamos con la necesidad de arreglos doble periódicos con peso tan grande como posible mientras se mantiene un buen valor de correlación.

Presentamos un nuevo método para aumentar el tamaño de las familias de construcciones doble periódicas (Método B). Solo hay unas pocas familias de arreglos doble periódicos con propiedades de correlación perfecta. En muchos casos las construcciones nuevas generadas con el Método B resultan en nuevas familias de arreglos doble periódicos con correlación perfecta y en todos los casos como mínimo las propiedades originales de correlación se preservan.

Finalmente presentamos una combinación del Método A y el Método B para producir nuevas familias de construcciones doble periódicas con el tamaño de la familia y el peso aumentado (Método C). Cuando se aplica el Método C se obtienen nuevas familias de arreglos doble periódicos del tipo Fuja con limitaciones de correlación diferente. Específcamente, se obtienen nuevas familias de arreglos doble periódicos con correlación cruzada mucho menor que la auto-correlación ($\lambda_c < \lambda_a$).

To my father José R. Ortiz Miranda who passed away a year before my graduation. He was always the biggest supporter of my studies and the proudest dad. I know he will always be there. To my dear wife Kariluz Dávila Diaz who has been my support and strength during these years. To my loved baby Kariany Luz Ortiz Dávila who is my new inspiration in life. Her smile will always cheer my days. To my loved family; my mother Luz Ubarri, my sister Juliester Ortiz, my brother Julio Ortiz, and my grandmother Esther Ubarri. To my other babies Juan Andres, Jean Michael, and Andrea Joan. To my extended family Andres, Aida, Yaniliz, and Juan. And finally to all the professors and mentors that had put their effort and time in my education, specially to my advisor Dr. Oscar Moreno, Dr. Pedro I. Rivera and Dr. Carlos Corrada.

To God...

ACKNOWLEDGMENTS

I would like to thank Dr. Oscar Moreno for his dedication and guidance through all my academic life including my doctorate dissertation work; his friendship and help in other aspects of my life. I also thank my early mentors Dr. Pedro Rivera, Dr. Heeralal Janwa, and Dr. Carlos Corrada because of their contribution on the development of my love for the Computer Sciences and Engineering. Thanks to the valuable suggestions of the rest of my graduate committee members: Dr. Dorothy Bollman, and Dr. Edusmildo Orozco. Also to Dr. Reza Omrani who helped in this work and the papers the work produced with his valuable suggestions and reviews.

I would also like to thank the High Performance Computing facility (HPCf) and the Resource Center for Sciences and Engineering, for supporting my research work. Thanks to the HPCf directors Dr. Guy Cormier and Dr. Humberto Ortiz and to my colleagues Ramon Sierra, William Caban, Carlos Rodríguez, Elena Leyderman, and Daniel Ayala among others for their support, encouragement and friendship through these years. Humberto thanks for being able to read every paper and every document I needed help reviewing.

Thanks to my wife Kariluz Dávila Diaz for helping with the presentations, and with the organization and reviewing of some of my figures and documents.

Thanks to Pablo Rebollo for setting up the video conference equipment every time I needed to take a remote course from the Mayagüez Campus. Thanks to the Computer Information Sciences and Engineering staff for their help, specially to Sarah I. Ferrer. Sarah was always there to help me in everything I needed. She would solve any administrative or bureaucratic problem I would present to her and more. She is an example of an excellent public server.

Thanks to God...

This work was partially supported by the High Performance Computing facility of the University of Puerto Rico under the PR AABRE grant #P20RR016470 from the National Institute of Health and the Gauss Research Laboratory under the SCORE grant #S06GM08102.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Z_p	Integers module p where p is prime.
Z_n	Integers module n.
GF(q)	Galois Field $q = p^m$.
F_p	Finite Field module p.
CRT	Chinese Remainder Theorem.
DPA	Doble Periodic Array.
CWC	Constant Weight Code.
GPCWC	Group Permutable Constant Weight Code.
GPDPA	Group Permutable Double Periodic Arrays.
JB	Johnson Bound.
QR	Quadratic Residue.
QNR	Quadratic Non Residue.
WIM	Weight Increasing Method.
MZKZ	Moreno Zhang Kumar Zinoviev.
MOM	Moreno Omrani Maric.
OOC	Optical Orthogonal Codes.
2-D OOC	2 dimensional Optical Orthogonal Code.
WDM	Wavelength-Division-Multiplexing.
CPCWC	Cyclically Permutable Constant Weight Code.
OPPW	One Pulse Per Wavelength.
AM-OPPW	At Most One Pulse Per Wavelength.
OPPTS	One Pulse Per Time Slot.
AM-OPPTS	At Most One Pulse Per Time Slot.
DDS	Distinct Different Sets.
BIBD	Balanced Incomplete Block Design.
CDMA	Code Division Multiple Access.
OCDMA	Optical Code Division Multiple Access.
WCDMA	Wireless Code Division Multiple Access.

LIST OF SYMBOLS

p	Prime p.
n	Code size.
ω	Code weight.
λ	Code correlation.
Φ	Code family size.
λ_a	Code auto-correlation.
λ_c	Code cross-correlation.
ω'	Column Sequence weight.
λ'	Column Sequence correlation
α	Primite element α.
β	Primite element β.
s^i	Periodic Sequence s shifted i positions.
mod	Modulo
$\oplus_n$	Sum modulo n.
$\ominus_n$	Substract module n.
f_n	Frequency n.
t_n	Time n.

CHAPTER 1
INTRODUCTION

1.1 Multiple Target radar and sonar

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

Costas and sonar sequences were respectively introduced by Costas [9] and Golomb [16] to deal with the following problem:

"There is 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 can be used to determine the velocity of the target, and the time it took to make the round trip can be used 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. The case when $m = n$ is called a Costa type signal, and the general case is called a sonar type signal.

The Costas signal is 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 returns to the observer, the signal is shifted in both time and frequency, and then from the shifts, both range and velocity can be determined. The amount of shifts is determined by comparing all shifts of the transmitted signal with the returning signal. This method is known as the auto-correlation. The auto-correlation 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^*.

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

$$C(r, s) = 0 \text{ if } |r| \geq n \text{ or if } |s| > n$$

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

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.

The following is the formal definition of Costas arrays, but first we need to define the distinct difference property.

Definition 1.1.1. *A function $f : N \to M$ has the distinct difference property if for all integers h, i and j, with $1 \leq h \leq n - 1$ and $1 \leq i, j \leq n - h$,*

$$f(i + h) - f(i) = f(j + h) - f(j) \text{ implies } i = j.$$

Definition 1.1.2. *A Costas array is an $n \times n$ permutation matrix $(a_{i,j})$ such that n^2 vectors connecting two 1's of the matrix are all distinct as vectors. Equivalently a Costas sequence of length n is a permutation $f : N \to N$ with the distinct different property.*

Example.

a) A Costas Sequence:

2 4 3 1

2 -1 -2

1 -3

b) Not a Costas Sequence:

2 1 4 3

-1 3 -1

2 2

Next is the mathematical definition of the aperiodic autocorrelation for an $n \times n$ matrix.

Definition 1.1.3. *The aperiodic auto-correlation of A is $\leq \lambda$ if*

$$\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} A(i+\alpha, j+\tau)A(i,j) \leq \lambda \tag{1.1}$$

for any $\alpha \leq n, \tau \leq n$, the maximum such λ is the auto-correlation.

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 using the Doppler effect, and the correlation properties. 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 [23]) is for any n obtain the largest possible m.

Definition 1.1.4. *An $m \times n$ sonar sequence is a function $f : N \to M$ with the distinct different property.*

In [13] Freedman et al. proved that for $n > 3$ there are no two different Costas sequences with cross-correlation 1 as they have in their auto-correlation. Since for the case of multiple targets and other applications discussed later in this introduction, we need sets of sequences with good auto- and cross-correlation properties

(correlation values as low as possible) our group and researchers in the area had settled for constructing sets of sequences with nearly ideal properties, or in other words cross-correlation 2. Later in this work we call these sets: families of sequences or families of arrays.

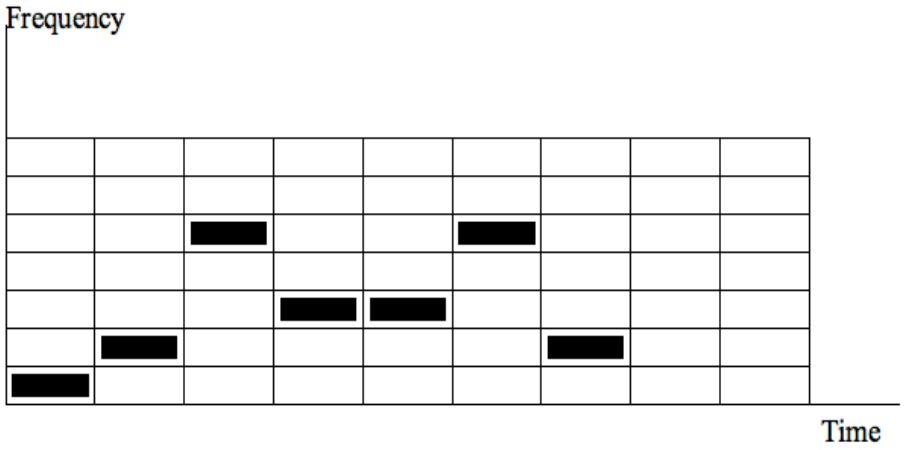


Figure 1–1: Frequency Hopping

In spread spectrum communications sequences with good correlation properties are used to spread the data sent through a communication channel to avoid its interception and to avoid channel jamming from a third party. Similar to Costas and sonar the signal consists of one or more frequencies being chosen from a set of available frequencies, for transmission at each of a set of time intervals. The interception of the signal is avoided by dividing the signal in codewords which are unknown by the interceptor but known by the receiver such that only the receiver can decode the signal. To be able to jam the communication channel, the entire set of frequencies available to spread the signal needs to be filled with noise, such thing is very costly.

1.2 Optical CDMA

In modern communications that make use of Code Division Multiple Access (CDMA) sequences with good correlation properties are used for multiple access in wireless and optical communication. A message sent in a communication channel using code with good auto and cross-correlation properties can be easily recovered

(decoded) in the other side of communication. Furthermore the use of code with good cross-correlation properties allow multiple users communication limiting signal interference. Similar to the application of radar and sonars: for Wireless CDMA (WCDMA) the signal consists on a set of frequencies chosen from a set of available frequencies, for transmission at each of a set of time intervals.

For the case of Optical CDMA (OCDMA) there are different approaches for the Code Division:

- In one approach the signal consists on fiber optic cables chosen from a set of available fiber optics cables (instead of frequencies), for transmission at each of a set of time intervals.
- In the second approach the signal consists on a set of wave-lenghts (colors) chosen from a set of available wave-lenghts for transmission over a single fiber optic cable, for transmission at each of a set of time intervals.
- And the third approach we consider the one dimensional case where the signal consists in time frames with the size of the code, and the time slots are 1 depending on the code assigned to the transmitter. (See Figure 1–2)

The sequence properties needed for Optical Communications, and the relationship between Optical Communications with the application of sonar and Costas is presented with more detail in section 2.2.

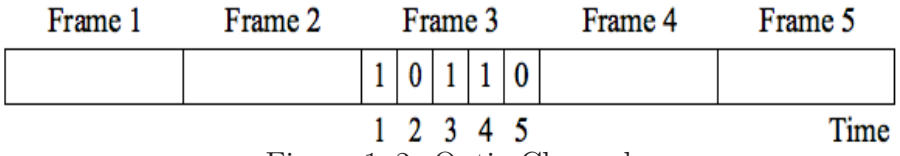


Figure 1–2: Optic Channel

1.3 Digital Watermarking

More recently sequences with good auto- and cross-correlation have been used in the area of digital watermarking because the correlation properties make watermarks more difficult to detect, damage or remove from a digital medium. The idea is similar to the application of spread spectrum communications where a secret message is

spread into a channel in order to make the secret message difficult to be intercepted or removed from the communication channel. In digital watermarking the watermark is the secret message, and the digital medium is the communication channel.

Tirkel *et al.* [36, 39–41] introduced the application of spread spectrum communications into digital watermarking, using m-sequences as the arrays for the watermarks. Also I.J. Cox *et al.* presented a technique of embedding digital watermarking based in inserting the watermark into the spectral components of a digital image using techniques analogous to spread spectrum communication [10, 12].

Digital watermarking applications require constructions of two dimensional sequences with good correlation properties. More specifically Digital watermarking requires as many two dimensional sequences as possible with both good, auto- and cross-correlation. Furthermore, it is necessary to have double-periodic sequences[1] with as many dots as possible. Through this document by dots we mean any non zero value in the matrix representation of the sequences. For example in the case of Costas, sonar and Optical Orthogonal Codes (OOC) the number of dots is the number of 1's in their matrix representation.

Previous work [28, 30, 37] describes how to increase the weight of a double periodic array using periodic shift sequences as columns. In the past Tirkel and Hall applied this method to the Moreno-Maric construction [38] to generate new matrices with good auto and cross correlation for watermarking. For detailed information on digital watermarking, its applications, and the applications of frequency hopping in digital watermarking please review Appendix B.

[1] we will refer to them as Double Periodic Arrays later in this work

1.4 Thesis Outline

In this work we start by introducing the concepts of Constant Weight Codes (CWC), Optical Orthogonal Codes (OOC), Distinct Different Sets (DDS), Double Periodic Arrays (DPA) and the relationship among them.

In chapter 3 we present the new concept of Group Permutable Constant Weight Codes (GPCWC), Group Permutable Double Periodic Arrays (GPDPA), and present improvements to the Johnson Bound to bound the cardinality of the family of GPCWC.

In chapter 4 we present a method to increase the weight of double periodic arrays. Then in chapter 5 we present methods to increase the size of families of double periodic arrays without increasing their correlation properties. One method to increase the size of families of double periodic arrays that uses the Chinese Reminder Theorem (CRT) which is due to (Moreno-Omrani-Maric), and our new method to increase the size of families of double periodic arrays without the need of the CRT Using these methods we obtain new families of double periodic arrays with optimal correlation properties.

Finally in chapter 6 we combine the methods from Chapter 4 and Chapter 5 to produce new families of DPA with increased weight and increased family size, resulting in new families of DPA with cross-correlation values different to the auto-correlation, i.e $\lambda_a \neq \lambda_c$. In fact our new constructions generate families of arrays where $\lambda_c < \lambda_a$.

The correlation property ($\lambda_c < \lambda_a$) is very important as discussed by Yang and Fuja in [4]. The auto-correlation properties of an array is used for synchronization, to check that a sequences is unlike cyclic shifts of itself. While the cross-correlation properties is used to check that a sequence is unlike cyclic shifts of other distinct sequences, thus cross-correlation serves for synchronization and user identification.

Therefore with better cross-correlation properties we are able to achieve a very important part of any frequency hopping communication which is user identification.

CHAPTER 2
CONSTANT WEIGHT CODES

In this chapter we introduce the concept of Constant Weight Codes, Optical Orthogonal Codes, Distinct Different Sets, and Double Periodic Arrays. We present the main bounds on the cardinality of CWC and OOC. And also explain the relationship among the CWC, OOC, DDS, and DPA.

All the codes generated in this work are nonlinear constant weight codes. The main characteristic of nonlinear codes is their Hamming distance.

Definition 2.0.1. *The Hamming distance between two codewords of equal length is the number of positions at which the corresponding symbols are different.*

Example. *The Hamming distance between codeword (011001) and codeword (010101) is 2, because symbols in positions 3 and 4 are different. The Hamming distance between codeword (2,1,7,3,4) and (2,2,7,4,3) is 3, because symbols in positions 2, 4 and 5 are different.*

Definition 2.0.2. *A (n, k) linear code of length n and rank k is a linear subspace with dimension k of the vector space $\mathbb{F}_q^n$ where $\mathbb{F}_q$ is the finite field with q elements. If C has Hamming distance d then we also say that C is a linear (n, k, d) code over $\mathbb{F}_q$.*

Such codes with parameters q are called a q-ary codes. For example codes with $q = 2$ are called binary codes, codes with $q = 3$ are called ternary codes, and so on.

Definition 2.0.3. *Let V be a vector space over the field K, and let W be a subset of V. Then W is a subspace if and only if it satisfies the following 3 conditions:*

- *The zero vector, 0, is in W.*

- *If u and v are elements of W, then the sum u + v is an element of W.*
- *If u is an element of W and c is a scalar from K, then the scalar product cu is an element of W.*

Example. *The code C = { (10111), (11110), (01001), (00000) } is an example of a binary* $(5, 2)$ *linear code.*

Note that if you chose any two codewords $c_1, c_2 \in C$*, then* $(c_1 + c_2) \in C$

Definition 2.0.4. *A* (n, k, d) *nonlinear code is a code with length n, size k (k codewords), and minimum Hamming distance d in the vector space* $\mathbb{F}_q^n$*, where* $\mathbb{F}_q$ *is the finite field with q elements.*

Example. *The code C = { (10110), (01101), (11010), (10101), (01011) } is an example of a binary* $(5, 5, 2)$ *nonlinear code.*

Note that $(10110) + (01101) = (11011) \notin C$*.*

Definition 2.0.5. *Hamming Weight is the number of nonzero digits in a codeword.*

Definition 2.0.6. *A binary* (n, ω, λ) *Constant Weight Code (CWC) is a binary {0,1} code of length n in which every codeword has Hamming weight equal to* ω *and the real inner product between any two codewords does not exceed* λ[1] *.*

Example. *The Hamming weight of codeword 0,1,1,0,0,1 is 3.*

A binary constant weight code is a binary nonlinear code where all the codewords have constant hamming weight ω. The previous example is also a (5, 3, 2) Constant Weight Code with k codewords. The number of codewords in a Constant Weigh Code is denoted by $A(n, \omega, \lambda)$.

Example. *The code C = { (10110), (01101), (11010), (10101), (01011) } is an example of a binary* $(5, 3, 2)$ *Constant Weight Code; which is also a (5, 5, 2) nonlinear code with constant Hamming weigh 3.*

[1] The real inner product (λ) is related to the minimum Hamming distance (d) by the equation $d = 2(\omega - \lambda)$.

2.1 Bounds on Constant Weight Codes

Let $A(n, \omega, \lambda)$ denote the largest possible size (number of codewords) of a constant-weight, binary $\{0, 1\}$ code of length n in which every codeword has Hamming weight equal to ω and the real inner product between any two codewords does not exceed λ. In [18] Johnson presented three principal bounds on the cardinality of constant weight codes that has been referred as the Johnson Bound A, B, and C.

Theorem 1. *(Johnson Bound A)*

$$A(n, \omega, \lambda) \leq \left\lfloor \frac{n}{\omega} \left\lfloor \frac{n-1}{\omega-1} \left\lfloor \frac{n-2}{\omega-2} \cdots \left\lfloor \frac{n-\lambda}{\omega-\lambda} \right\rfloor \right\rfloor \right\rfloor \right\rfloor \tag{2.1}$$

Lemma 1.

$$A(n, \omega, \lambda) \leq \left\lfloor \frac{n}{\omega} A(n-1, \omega-1, \lambda-1) \right\rfloor \tag{2.2}$$

Proof. Assume a constant weight code (n, ω, λ), C of size $A(n, \omega, \lambda)$. If we arrange all the codewords in rows of a matrix, the total weight of the matrix is $\omega A(n, \omega, \lambda)$. There are on average, $\frac{\omega}{n} A(n, \omega, \lambda)$ 1s in each column. It follows that there exists a column c having at least $\frac{\omega}{n} A(n, \omega, \lambda)$, 1s. However, the number of occurrences of 1 in column c cannot exceed $A(n-1, \omega-1, \lambda-1)$. This is because if we select all the rows that contain a 1 in columns c, and then delete this column c from all these rows, we will obtain a constant weight code of length $n-1$, weight $\omega-1$ and correlation value $\lambda-1$. □

Example. *Given a CWC with length $n = 10$, hamming weight $\omega = 5$, and correlation value $\lambda = 2$. The maximum size of this CWC is given by*

$$A(10, 5, 2) \leq \left\lfloor \frac{10}{5} \left\lfloor \frac{9}{4} \left\lfloor \frac{8}{3} \right\rfloor \right\rfloor \right\rfloor \leq 8 \tag{2.3}$$

Theorem 2. *(Johnson Bound B) Provided $\omega^2 > n\lambda$*

$$A(n, \omega, \lambda) \leq \left\lfloor \frac{n(\omega-\lambda)}{\omega^2 - n\lambda} \right\rfloor \tag{2.4}$$

Proof. Assume a constant weight code (n, ω, λ), C of size $A(n, \omega, \lambda)$. Let the codewords form the rows of a matrix M and let us compute the sum of the inner product of every pair of rows:

$$\sum_{i \neq j} c_i.c_j \leq \binom{A(n, \omega, \lambda)}{2} \lambda$$

Next let assume each column j in M has ω_j 1s. Then we have

$$\sum_{i \neq j} c_i.c_j = \sum_{j=1}^{n} \binom{\omega_j}{2} = \sum_{j=1}^{n} \frac{\omega_j(\omega_j - 1)}{2} = \frac{1}{2} \left(\sum_{j=1}^{n} \omega_j^2 - \sum_{j=0}^{n} \omega_j \right) =$$
$$\frac{1}{2} \left(\sum_{j=1}^{n} \omega_j^2 - A(n, \omega, \lambda)\omega \right)$$

It follows that

$$\sum_{j=1}^{n} \omega_j^2 \leq A(n, \omega, \lambda)^2 \lambda - A(n, \omega, \lambda)(\lambda - \omega)$$

Minimum of the left hand side should satisfy the same inequality and the minimum occurs when all ω_js are equal which lead to $\omega_j = \dfrac{A(n, \omega, \lambda)\omega}{n}$

$$n \left(\frac{A(n, \omega, \lambda)\omega}{n} \right)^2 \leq A(n, \omega, \lambda)^2 \lambda - A(n, \omega, \lambda)(\lambda - \omega) \Rightarrow$$
$$(\omega^2 - n\lambda) A(n, \omega, \lambda) \leq n(\omega - \lambda)$$

□

Example. *Given a CWC with length* $n = 5$*, hamming weight* $\omega = 5$*, and correlation value* $\lambda = 4$*. Since* $\omega^2 = 25 > n\lambda = 20$*. The maximum size of this CWC is given by*

$$A(5, 5, 4) \leq \left\lfloor \frac{5(5-4)}{25-20} \right\rfloor \leq 1 \tag{2.5}$$

The third Johnson bound is known as the hybrid of bounds A and B. Let l, be the smallest integer, $1 \leq l \leq \lambda - 1$, such that $(\omega - l)^2 > (n - l)(\lambda - l)$. By combining Johnson bounds A and B the following bound is obtained:

Theorem 3. *(Johnson Bound C)*

$$A(n, \omega, \lambda) \leq \left\lfloor \frac{n}{\omega} \left\lfloor \frac{n-1}{\omega - 1} \ldots \left\lfloor \frac{n-(l-1)}{\omega-(l-1)} h \right\rfloor \right\rfloor \right\rfloor \tag{2.6}$$

with $h = \left\lfloor \dfrac{(n-l)(\omega-\lambda)}{(\omega-l)^2 - (n-l)(\lambda-l)} \right\rfloor$

Using Collorary 5 from Agrell, Vardy, and Zeger [1]

$$A(n, \omega, \lambda) \leq \left\lfloor \frac{n(\omega-\lambda)}{\omega^2 - n\lambda} \right\rfloor \qquad \omega^2 - n\lambda \geq \omega - \lambda \tag{2.7}$$

$$A(n, \omega, \lambda) \leq n \quad 0 < \omega^2 - n\lambda \leq \omega - \lambda \tag{2.8}$$

$$A(n, \omega, \lambda) \leq 2n - 2 \qquad \omega^2 - n\lambda = 0 \tag{2.9}$$

the following improvement to the Johnson Bound B and C was provided [34]:

Theorem 4. *(Moreno et al., Improved Johnson Bound B for CWC)*

Provided $\omega^2 > n\lambda$

$$A(n, \omega, \lambda) \leq min\left(n, \left\lfloor \frac{n(\omega-\lambda)}{\omega^2 - n\lambda} \right\rfloor\right) \tag{2.10}$$

Provided $\omega^2 = n\lambda$

$$A(n, \omega, \lambda) \leq 2n - 2 \tag{2.11}$$

Theorem 5. *(Moreno et al., Improved Johnson Bound C for CWC) Provided* l*, is some integer,* $1 \leq l \leq \lambda - 1$*, such that* $(\omega - l)^2 > (n - l)(\lambda - l)$*.*

$$A(n, \omega, \lambda) \leq \left\lfloor \frac{n}{\omega} \left\lfloor \frac{n-1}{\omega - 1} \ldots \left\lfloor \frac{n-(l-1)}{\omega-(l-1)} h \right\rfloor \right\rfloor \right\rfloor \tag{2.12}$$

$$with\ h = min\left(n-l, \left\lfloor \frac{(n-l)(\omega-\lambda)}{(\omega-l)^2-(n-l)(\lambda-l)} \right\rfloor\right)$$

The improvements to the Johnson Bound B and C are specially useful for bounds in OCCs and Group Permutable Constant Weight Codes. The concept of GPCWC is introduced in chapter 3.

In this section we introduced the concept of CWC and presented bounds on the cardinality of the codes. In sections 2.2.3 and 2.3.2 respectively we present some improvements to the bounds on CWC to bound the cardinality of 1-D OOC, and the cardinality 2-D OOC. And in Chapter 3 we introduce improvements to the bounds on CWC to bound the cardinality of Group Permutable Constant Weight Codes.

2.2 OOC, DDS, Double Periodic Arrays of families and their equivalence

In this section we define the concepts of OOC and DDS; and review the correspondence between the set of (n, ω, λ)-OOC's and the set of (v, k, t)-DDS's.

2.2.1 1-D Optical Orthogonal Codes

Definition 2.2.2. *An (n, ω, λ) Optical Orthogonal Code [5] (OOC) C where $1 \leq \lambda \leq \omega \leq n$, is a family of {0,1}-sequences of length n, Hamming weight ω, and maximum correlation λ satisfying:*

$$\sum_{k=0}^{n-1} x(k)y(k \oplus_n \tau) \leq \lambda \tag{2.13}$$

for every pair of codewords x, y in C whenever either $x \neq y$ or $\tau \neq 0$, and $\oplus_n$ denotes addition modulo n.

Example. *The code $C = \{$ (10110) $\}$ is an example of a binary $(5, 3, 2)$ Optical Orthogonal Code with 1 codeword. More examples of OOCs can be found in section 5.1.*

2.2.3 Bounds on 1-D Optical Orthogonal Codes

For a given set of values of n, ω, λ, let $\Phi(n, \omega, \lambda)$, denote the largest possible cardinality of an (n, ω, λ) OOC, and P the cardinality of a specific construction. Since $\Phi(n, \omega, \lambda)$ denotes the largest possible size of a 1-D OOC , an OOC C of size P is said to be optimal when

$$P = \Phi(n, \omega, \lambda)$$

and asymptotically optimal if:

$$\lim_{n \to \infty} \frac{P}{\Phi(n, \omega, \lambda)} = 1$$

An upper bound [6] by Chung and Kumar derived from the Johnson Bound [18] on the cardinality of constant weight codes $A(n, 2(\omega - \lambda), \omega)$ states that:

$$P \leq \Phi(n, \omega, \lambda) \leq \left\lfloor \frac{A(n, \omega, \lambda)}{n} \right\rfloor \tag{2.14}$$

Theorem 6. *(Chung et al., Improved Johnson Bound A for OOCs)*

$$P \leq \Phi(n, \omega, \lambda) \leq \left\lfloor \frac{1}{\omega} \left\lfloor \frac{n-1}{\omega - 1} \left\lfloor \frac{n-2}{\omega - 2} \cdots \left\lfloor \frac{n-\lambda}{\omega - \lambda} \right\rfloor \right\rfloor \right\rfloor \right\rfloor \tag{2.15}$$

Proof. The proof is straight forward by applying Equation (2.14) to the Johnson Bound A.

□

Theorem 7. *(Moreno et al., Improved Johnson Bound B for OOCs)*

Provided $\omega^2 > n\lambda$

$$\Phi(n, \omega, \lambda) \leq min \left(1, \left\lfloor \frac{(\omega - \lambda)}{\omega^2 - n\lambda} \right\rfloor \right) \tag{2.16}$$

Provided $\omega^2 = n\lambda$

$$\Phi(n, \omega, \lambda) \leq 1 \tag{2.17}$$

Proof. The proof is straight forward by applying Equation (2.14) to the Improved Johnson Bound B of Equations (2.10) and (2.9). □

Example. *Given an OOC with length* $n = 12$*, hamming weight* $\omega = 6$*, and correlation value* $\lambda = 3$*. Since* $n\lambda = 36$ *and* $\omega^2 = 36$ *The maximum size of this OOC is given by*

$$\Phi(12, 6, 3) \leq 1 \tag{2.18}$$

Theorem 8. *(Moreno et al., Improved Johnson Bound C for OOCs)*

Provided l*, is some integer,* $1 \leq l \leq \lambda - 1$*, such that* $(\omega - l)^2 > (n - l)(\lambda - l)$*.*

$$\Phi(n, \omega, \lambda) \leq \left\lfloor \frac{1}{\omega} \left\lfloor \frac{n-1}{\omega - 1} \cdots \left\lfloor \frac{n-(l-1)}{\omega-(l-1)} h \right\rfloor \right\rfloor \right\rfloor \tag{2.19}$$

with $h = min\left(n - l, \left\lfloor \frac{(n-l)(\omega-\lambda)}{(\omega-l)^2 - (n-l)(\lambda-l)} \right\rfloor\right)$

Proof. Proof is similar to the proof in Theorem 7. □

To the best of our knowledge the improvement to the Johnson Bound B and C as applied to 1-D OOCs were introduced by our group in [34].

2.2.4 Distinct Different Sets

Definition 2.2.5. *A* (k, v)*-Distinct Difference Set (DDS) [7] 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 2. *(Moreno et al.) There is a one to one onto correspondence between the set of (n, ω, λ)-OOC's and the set of (v, k, t)-DDS's 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 $\lambda = 1$. □

2.2.6 OOC's is the same concept as that of Double Periodic Arrays

Let $A = [A(i, j)]$ and $B = [B(i, j)]$ be $r \times s$ matrices having 0,1 entries, and r and s are relatively prime.

2.2.7 Double Periodic Arrays

Definition 2.2.8. *The double-periodic cross-correlation between any pair A and B of a set or family of arrays is $\leq \lambda$ if*

$$\sum_{i=0}^{r-1} \sum_{j=0}^{s-1} A(i \oplus_r \alpha, j \oplus_s \tau) B(i, j) \leq \lambda \tag{2.20}$$

for any $\alpha \leq r, \tau \leq s$, where $\oplus_m$ denotes addition modulo m. The maximum such λ is the correlation. The double-periodic auto-correlation is also obtained with equation 2.20 but 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, $0 \leq L \leq rs - 1$. For example if $A[i, j] = 1$, $a(L) = L$ iff $(i \mod r) = L$ and $(j \mod s) = L$.

From the previous definitions the following theorem is obtained:

Theorem 9. *(Moreno et al.) The collection of one-dimensional periodic auto- and cross-correlation values of a family of codes 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. *(Moreno et al.) 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.*

In the case when the auto- and cross-correlation are different an OOC with parameters $(n, \omega, \lambda_a, \lambda_c)$ is a code with length n, Hamming weight ω, auto-correlation λ_a, and cross-correlation λ_c. If the auto-correlation and the cross-correlation are equal we will use only λ, and the parameters (n, ω, λ). We define $\Phi(n, \omega, \lambda_a, \lambda_c,)$ and $\Phi(n, \omega, \lambda)$ the size of the family; i.e. the size of the set of codewords that meet the same auto- and cross-correlation properties.

2.3 2-D Optical Orthogonal Codes

There are two ways of spreading information for multiple access on 2-D Optical Orthogonal Codes.

- Spreading over a set of fiber optics and time.
- Spreading over a set of wave-lengths and time, known as Wavelength-Division-Multiplexing (WDM).

The concept is similar to spread spectrum communication but the transmission medium is a fiber optic cable or a set of fiber optic cables instead of frequencies.

Definition 2.3.1. *An 2-D $(m \times n, \omega, \lambda)$ Optical Orthogonal Code [31] (OOC) C where $1 \leq \lambda \leq \omega \leq mn$, is a family of $\{0,1\}$-sequences of m rows and n columns,*

Hamming weight ω, and maximum correlation λ satisfying:

$$\sum_{k=1}^{m}\sum_{t=0}^{n-1} x(k,t)y(k,(t \oplus_n \tau)) \leq \lambda \tag{2.21}$$

whenever either $x \neq y$ or $\tau \neq 0$.

Note that by definition every DPA is a 2-D OOC but not otherwise because DPA are periodic in both time and wave-length while 2-D OOC requires periodicity only in time.

To simplify the WDM implementation, additional restrictions on the codewords may be placed such as [31]:

- one-pulse per wavelength(OPPW) restriction: each row of every code array in C must have Hamming weight 1.
- the at-most one-pulse per wavelength(AM-OPPW) restriction: each row of each code in C must have Hamming weight ≤ 1.
- one-pulse per time slot (OPPTS) restriction: each column of every code in C is required to have Hamming Weight $= 1$.
- the at most one-pulse per time slot (AM-OPPTS) restriction: each column of each code in C must have Hamming weight ≤ 1.

2.3.2 Bounds on 2-D OOCs

Omrani and Kumar [31] improved the Johnson Bound to obtain the following bounds on the cardinality of the families of 2-D OOCs.

If C is a $(m \times n, \omega, \lambda)$ 2-D OOC, then by including every column-cyclic shift of each codeword in C one can construct a constant weight code using any mapping that reorders the elements of a $m \times n$ array to form a 1-D string of length mn . The resultant constant weight code has parameters (mn, ω, λ) and size $= n|C|$. This observation allows to translate bounds on constant weight codes to bounds on 2-D OOCs:

$$\Phi(m \times n, \omega, \lambda) \leq \left\lfloor \frac{A(m \times n, \omega, \lambda)}{n} \right\rfloor \tag{2.22}$$

Theorem 10. *(Omrani and Kumar, Improved Johnson Bound A for 2-D OOCs)*

$$P \leq \Phi(m \times n, \omega, \lambda) \leq \left\lfloor \frac{m}{\omega} \left\lfloor \frac{mn-1}{\omega-1} \left\lfloor \frac{mn-2}{\omega-2} \ldots \left\lfloor \frac{mn-\lambda}{\omega-\lambda} \right\rfloor \right\rfloor \right\rfloor \right\rfloor \tag{2.23}$$

Proof. The proof is straight forward by applying Equation (2.22) to the Johnson Bound A.

□

Theorem 11. *(Omrani and Kumar, Improved Johnson Bound B for 2-D OOCs)*

Provided $\omega^2 \geq mn\lambda$

$$\Phi(m \times n, \omega, \lambda) \leq min\left(m, \left\lfloor \frac{m(\omega-\lambda)}{\omega^2 - n\lambda} \right\rfloor\right) \tag{2.24}$$

Proof. The proof is straight forward by applying Equation (2.22) to the Johnson Bound B for CWC. □

Theorem 12. *(Omrani and Kumar, Improved Johnson Bound C for 2-D OOCs)*

Provided l*, is some integer,* $1 \leq l \leq \lambda - 1$*, such that* $(\omega - l)^2 > (mn - l)(\lambda - l)$*.*

$$\Phi(n, \omega, \lambda) \leq \left\lfloor \frac{m}{\omega} \left\lfloor \frac{mn-1}{\omega-1} \ldots \left\lfloor \frac{mn-(l-1)}{\omega-(l-1)} h \right\rfloor \right\rfloor \right\rfloor \tag{2.25}$$

with $h = min\left(mn - l, \left\lfloor \frac{(mn-l)(\omega-\lambda)}{(\omega-l)^2 - (mn-l)(\lambda-l)} \right\rfloor\right)$

Proof. Proof is similar to the proof in Theorem 11. □

Remark: Note that Omrani and Kumar improvements to the Johnson Bounds are based in the assumption that the 2-D OOC is mapped into a 1-D string.

2.4 Well Known Families of Double Periodic Arrays

Double periodic arrays are sequences that meet the double periodic auto- and cross-correlation properties (see definition 2.2.8). In simple words DPAs are 2-D

arrays whose correlation value does not change when they are periodically shifted in both coordinates (columns and rows). In this section we present well known sonar and Costas double periodic constructions that are used later in the next chapters to apply the new methods to increase the weight and size of DPA to produce new families of DPAs.

2.4.1 Quadratic family

Construction 1. ***Quadratic Construction*** *[14]: Let p be any odd prime; let k be a integer not congruent to 0 (mod p). Then $f : \{0, 1, \ldots, p-1\} \rightarrow \{0, 1, \ldots, p-1\}$ defined by $f(x) = kx^2 \pmod p$ is a family of OOC's with parameters $(p \times p, \omega = p, \lambda_a = 1, \lambda_c = 2)$, periodicity $p \times p$, and $\Phi = (p-1)$.*

4	0	0	1	1	0
3	0	0	0	0	0
2	0	0	0	0	0
1	0	1	0	0	1
0	1	0	0	0	0
	0	1	2	3	4

Figure 2–1: 5x5 Quadric DPA with $f(x) = x^2$ and $p = 5$

Example. *Let $p = 5$ and $f(x) = kx^2$, the family for the Quadratic Construction is*

$$for \quad k = 1 \quad (0, 1, 4, 4, 1)$$

$$for \quad k = 2 \quad (0, 2, 3, 3, 2)$$

$$for \quad k = 3 \quad (0, 3, 2, 2, 3)$$

$$for \quad k = 4 \quad (0, 4, 1, 1, 4)$$

with parameters $(5 \times 5, 5, 1, 2)$.

When $k = 1$ and $p = 5$, $f(0) = 0$, $f(1) = 1^2 \ mod\ 5 = 1$, $f(2) = 2^2 \ mod\ 5 = 4$, $f(3) = 3^2 \ mod\ 5 = 4$, $f(4) = 4^2 \ mod\ 5 = 1$.

2.4.2 Hyperbolic family

4	0	0	0	1	0
3	0	1	0	0	0
2	0	0	1	0	0
1	1	0	0	0	0
0	0	0	0	0	0
	0	1	2	3	4

Figure 2–2: 5x5 Hyperbolic DPA with $f(x) = 1/x$ and $p = 5$

Construction 2. ***Hyperbolic Construction:*** *[20] Let p be any odd prime; let $k, x \in \mathbb{Z}_p$, $k, x = 1 \ldots p-1$. Then $f : \{1, 2, \ldots, p-1\} \to \{1, 2, \ldots, p-1\}$ defined by $f(x) = \frac{k}{x}$ is a family of OOC's with parameters $(n = p \times p, \omega = p-1, \lambda = 2)$, periodicity $p \times p$ and $\Phi = (p-1)$.*

Example. *Let $p = 5$ the family for the Hyperbolic Construction is*

$$for \quad k = 1 \quad (1, 3, 2, 4, *)$$

$$for \quad k = 2 \quad (2, 1, 4, 3, *)$$

$$for \quad k = 3 \quad (3, 4, 1, 2, *)$$

$$for \quad k = 4 \quad (4, 2, 3, 1, *)$$

with parameters $(5 \times 5, 4, 2)$.

Note the asterisk at the end of the sequences. This asterisk represents an empty (all zero values) column that we have to add to the end of the array in order to make it double periodic. See example 2.4.2

2.4.3 Welch family

Construction 3. ***Welch Construction :*** *[15, 16] Let α be a primitive root of an odd prime p. Then the array with $\alpha_k = \alpha^k (mod\ p), 1 \leq k \leq p-1$ is an OOC with parameters $(n = p \times (p-1), \omega = p-1, \lambda = 1)$, periodicity $p \times (p-1)$ and $\Phi = 1$.*

4	0	1	0	0
3	1	0	0	0
2	0	0	1	0
1	0	0	0	1
0	0	0	0	0
	0	1	2	3

Figure 2–3: 5x4 Welch DPA with $\alpha = 3$ and $p = 5$

Example. *Let $\alpha = 3$ and $p = 5$ the family for the Welch Construction is (3, 4, 2, 1) with parameters $(5 \times 4, 4, 1)$.*

In more details the Welch DPA in this example is obtained by $\alpha_1 = 3^1\ mod\ 5 = 3$, $\alpha_2 = 3^2\ mod\ 5 = 4$, $\alpha_3 = 3^3\ mod\ 5 = 2$, and $\alpha_4 = 3^4\ mod\ 5 = 1$.

2.4.4 Lempel-Golomb family

Construction 4. ***Lempel-Golomb*** *[15, 16]: Let α and β be primitive elements in the finite field $\boldsymbol{F}_q$ where $q = p^m$. Then the sequence $\alpha_i = log_\beta(1-\alpha^i)$ where i goes from 1 to $q-2$ is a Costas sequence of size $p^m - 2$. This is equivalent to saying that in the position i of the sequence there is a j if and only if $\alpha^i + \beta^j = 1$. The double periodicity of this construction is $(q-1) \times (q-1)$ and its autocorrelation is 1.*

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

Figure 2–4: 6x6 Lempel-Golomb DPA with $\alpha = 3$, $\beta = 5$, and $q = 7$

Example. *Let $\alpha = 3$ and $\beta = 5$ primitive elements in the finite field $\boldsymbol{F}_7$ the family for the Lempel Construction is (1, 3, 4, 2, 5, *) with parameters $(6 \times 6, 5, 1)$.*

The Lempel-Golomb DPA in this example is obtained by:

$$\begin{aligned}
\alpha^1 = 3, \quad \beta^1 = 5, \quad (3+5) \ mod\ 7 = 1 \\
\alpha^2 = 9, \quad \beta^3 = 125, \quad (9+125) \ mod\ 7 = 1 \\
\alpha^3 = 27, \quad \beta^4 = 625, \quad (27+625) \ mod\ 7 = 1 \\
\alpha^4 = 81, \quad \beta^2 = 25 \quad (81+25) \ mod\ 7 = 1 \\
\alpha^5 = 243, \quad \beta^5 = 3125 \quad (243+3125) \ mod\ 7 = 1
\end{aligned}$$

2.4.5 Moreno-Maric family

Construction 5. ***Moreno-Maric*** *[24]: Whenever $x^2 + x + \alpha$ is irreducible, and α primitive in $GF(q)$, $q = p^n$, then the polynomial $\frac{-\alpha}{(x+1)}$ gives a cycle (permutation) of length $q + 1$. The set of non-equivalent permutations obtained after applying the linear transformations $f(x_i) = kx_i$ and $f(x_i) = \frac{k}{x_i}$ for $k = 1 \ldots q-1$ to the permutation sequence obtained by the recursion:*

$$T : x_{i+1} = \frac{-\alpha}{(x_i + 1)}, \ \textit{starting with } x_0 = 0$$

produce a family of OOC with parameters $(n = (q+1) \times (q+1), \omega = q+1, \lambda = 2)$, periodicity $(q+1) \times (q+1)$ and $\Phi = q - 1$.

Example. *Let $q = 7$ and $\alpha = 3$ using the recursion: $T : x_{i+1} = \frac{-\alpha}{(x_i+1)}$ we obtain the sequence $(0, 4, 5, 3, 1, 2, 6, \infty)$. See table 2–1.*

7	0	0	0	0	0	1	0	0
6	0	0	0	0	0	0	1	0
5	0	0	0	0	0	0	0	1
4	0	1	0	0	0	0	0	0
3	0	0	1	0	0	0	0	0
2	0	0	0	0	1	0	0	0
1	0	0	0	1	0	0	0	0
0	1	0	0	0	0	0	0	0
	0	1	2	3	4	5	6	7

Figure 2–5: 8x8 Moreno-Maric double-periodic array with $\alpha = 3$, and $q = 7$

Table 2–1: Moreno-Maric recursion with q = 7

$$\begin{array}{lcll} x_0 & = & 0 & \\ x_1 & = & \frac{4}{0+1} & = 4 \\ x_2 & = & \frac{4}{4+1} & = 5 \\ x_3 & = & \frac{4}{5+1} & = 3 \\ x_4 & = & \frac{4}{3+1} & = 1 \\ x_5 & = & \frac{4}{1+1} & = 2 \\ x_6 & = & \frac{4}{2+1} & = 6 \\ x_7 & = & \frac{4}{6+1} & = \infty \end{array}$$

Applying the linear transformation $f(x_i) = kx_i$ we obtain the following permutation sequences:

$$for \quad k = 1 \quad 0, 4, 5, 3, 1, 2, 6, \infty$$

$$for \quad k = 3 \quad 0, 5, 1, 2, 3, 6, 4, \infty$$

$$for \quad k = 6 \quad 0, 3, 2, 4, 6, 5, 1, \infty$$

Applying the linear transformation $f(x_i) = \frac{k}{x_i}$ we obtain the following permutation sequences:

$$for \quad k = 1 \quad \infty, 2, 3, 5, 1, 4, 6, 0$$

$$for \quad k = 2 \quad \infty, 4, 6, 3, 2, 1, 5, 0$$

$$for \quad k = 4 \quad \infty, 1, 5, 6, 4, 2, 3, 0$$

The set of the non-equivalent permutation sequences obtained applying the linear transformations is the family of the Moreno-Maric construction with parameters $(8 \times 8, 8, 2)$ *and* $\Phi = 6$.

Table 2–2: Known Families of Double Periodic arrays

Construction	**Periodicity**	ω	Φ	λ_a	λ_c
Quadratic	$p \times p$	p	$p-1$	1	2
Hyperbolic	$p \times p$	$p-1$	$p-1$	2	2
Welch	$p \times (p-1)$	$p-1$	1	1	n/a
Lempel-Golomb	$(q-1) \times (q-1)$	$q-2$	1	1	n/a
Moreno-Maric	$(q+1) \times (q+1)$	$q+1$	$q-1$	2	2

2.4.6 Section Summary

Table 2–2 summarizes the parameters and properties of the double periodic arrays presented in this section. These constructions are going to be used through the next chapters of this work. In Chapter 4 we increase their weight utilizing a periodic sequence as column sequence. In the next section we describe a few periodic sequences that can be used to increase the weight of DPA, specially those whose column size is prime.

2.5 Periodic Binary Sequences

In Chapters 4 and 6 we present constructions of double periodic families using the well known constructions of sonars: Quadratic and Hyperbolic, and the well known constructions of Costas: Welch, Lempel-Golomb, and Moreno-Maric defined in section 2.4 .

To produce these new constructions we apply a method to increase the weight of DPA based on matrix column multiplication (See chapter 4). The columns used are binary periodic sequences with good correlation properties. In this work we call them column sequences.

The size of the column sequence depends on the size of the columns of the DPA of the sonar or Costas to be used. In the case of the Quadratic matrix of size $(p \times p)$, the Welch matrix of size $(p \times p-1)$, and the Hyperbolic matrix of size $(p \times p)$ the

column sequence needed is of size p. There are two well known periodic binary constructions of size p that we can utilize.

An element $i \in GF(p)$, $i \neq 0$ is said to be a quadratic residue (QR) mod p if i is the square of some element of $GF(p)$, and to be a quadratic non-residue (QNR) mod p otherwise. The element 0 is neither QR mod p nor QNR mod p. [30]

Theorem 13. *A Legendre sequence is a periodic binary sequence* $l = (l_0, l_1, \ldots, l_{p-1})$ *where* p *is a prime and* $\frac{(p-1)}{2}$ *is odd, such that* $l_i = 0$ *if* i *is a QR module* p *and* $l_i = 1$ *if* i *is a QNR mod* p*, and* l_0 *can be either 0 or 1.*

Remark: In our work we set $l_0 = 1$ to obtain the greatest weight of the periodic sequence.

Lemma 3. *The weight of the binary Legendre sequence is* $\omega = \frac{(p+1)}{2}$*, and its correlation is* $\lambda = \frac{(p+1)}{4}$.

Example. *Let* $p = 7$ *such that* $p = \frac{(7-1)}{2} = 3$ *is odd. The QR of the* $GF(p)$ *are* $1 = 1^2$, $2 = 3^2$, *and* $4 = 2^2$. *The QNR of the* $GF(p)$ *are 3, 5, and 6. Chose* $l_0 = 1$. *The Legendre sequence of size 7 is* $(1, 0, 0, 1, 0, 1, 1)$.

Alternatively for the purpose of this work and for the applications of binary sequences as columns in most of our constructions introduced in Chapters 4 and 6, there is another construction of binary sequences which produces sequences of size p called binary m-sequences. There exists binary m-sequences of length $2^n - 1$ for every integer $n > 1$. Hence, there exists a binary m-sequence of size p if and only if $p = 2^n - 1$ [30].

For the cases when we use a Lempel-Golomb DPA of size $(q-1) \times (q-1)$, we need periodic sequences of size $q - 1$ and with the Moreno-Maric DPA of size $(q+1)\times(q+1)$, we need periodic sequences of size $q+1$. There are many constructions of binary periodic sequences that produce special cases where the length is equal to $(q-1)$ or $(q+1)$ but not in general like the constructions for periodic sequences of

size p. For example for size $q-1$ there are m-sequences whenever $q=2^n$ and and $q-1$ is prime.

In Chapters 4 and 6 we use special cases of sequences to give examples of the new constructions obtained. For example we use the Milewski [21] ternary periodic sequence of size 8 with the Moreno-Maric construction of size (8×8). For such reason, for the sake of clarity, in the next chapters we give results based on the Legendre sequences for the Quadratic, Welch, and Hyperbolic constructions, and general results for the Lempel-Golomb and Moreno-Maric constructions independent of the (size, weight, and correlation) parameters of periodic sequences.

2.6 Chapter Summary

In this Chapter we introduce the historical background of arrays with good auto- and cross-correlation properties. Also we describe the different applications of these arrays. We define the concept of Constant Weigh Codes, Double Periodic Arrays, Distinct Different Sets, 1-D Optical Orthogonal Codes, and 2-D Optical Orthogonal codes, and the relationship among them. We provide the Johnson Bound improvements used to bound the cardinality of the families of 1-D and 2-D Optical Orthogonal Codes. Finally we reviewed the well known families of double periodic arrays that are used through the remaining Chapters of this work: Quadratic, Hyperbolic, Welch, Lempel-Golomb, and Moreno-Maric. Finally we described the column sequences used in Chapters 4 and 6.

CHAPTER 3
GROUP PERMUTABLE CONSTANT WEIGHT CODES

In this chapter we introduce the new concept of Group Permutable Constant Weight Codes (GPCWC). GPCWC are a class of Constant Weight Codes with the double periodicity property. Meaning that every two dimensional periodic shift is also a codeword of a Constant Weight Code. For more details in CWC please refer to section 2. In this chapter we formally define the concept GPCWC and introduce improvements to the Johnson Bound, to bound the family size of Group Permutable Constant Weight Codes.

In the past we have used the Johnson bound improvements for OOCs to check the optimality of DPA with row and column length relatively prime. In this work we obtain different DPAs where the row and column length are not relatively prime. In the next sections we prove that DPAs with correlation less than their weight ($\lambda < \omega$) are GPCWC, such that we can use the improvements to the Johnson bound on GPCWC to prove the optimality of some of our DPA families.

Massey [30] defined a cyclically permutable code to be a binary block code of block length N such that each codeword has cyclic order N(has N distinct cyclic shifts) and such that the codewords are cyclically distinct (no codeword can be obtained by the cyclic shifting of another codeword).

Let $\mathbf{R}$ denote the operator that shifts the columns of a Double Periodic Array (DPA) periodically one position to the right, and let $\mathbf{D}$ denote the operator that shifts the rows of a DPA periodically one position down.

For a DPA

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \\ j & k & l \end{pmatrix}$$

we have that

$$\mathbf{R}(A) = \begin{pmatrix} c & a & b \\ f & d & e \\ i & g & h \\ l & j & k \end{pmatrix}$$

$$\mathbf{D}(A) = \begin{pmatrix} j & k & l \\ a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

and

$$\mathbf{DR}(A) = \begin{pmatrix} l & j & k \\ c & a & b \\ f & d & e \\ i & g & h \end{pmatrix}$$

Definition 3.0.1. *A ($\mathbb{Z}_m \times \mathbb{Z}_n$) Group permutable constant weight code ($\mathbb{Z}_m \times \mathbb{Z}_n$ GPCWC) C is a 2-D code with rows length m and column length n*

- *such that each codeword in C can be periodically permuted m times in the rows with the operator $\boldsymbol{R}$ and periodically permuted n times in the columns with the operator $\boldsymbol{D}$(i.e. has mn distinct double periodic shifts),*
- *and such that no codeword in C can be obtained by the double periodic shifting, one or more times, of another codeword in C.*

For GPCWC and their applications we want the correlation values to be as low as possible than its code weight. If the code weight is equal to the auto correlation value it means that in some point two different double periodic shift of a codeword has the same result, therefore that codeword does not have mn distinct double periodic shifts. If the code's weight is equal to the cross correlation value then a codeword can be obtained by the double periodic shifting, one or more times, of another codeword. Therefore if the correlation value of a code is equal to the code's weight, the code is not a GPCWC.

3.1 Bounds on Group Permutable Constant Weight Codes

If C is a $(m \times n, \omega, \lambda)$ $(\mathbb{Z}_m \times \mathbb{Z}_n)$ GPCWC, then by including every double periodically permuted shift of the rows and columns of each codeword in C one can construct a CWC with parameters $(m \times n, \omega, \lambda)$ and size $(mn)|C|$.

From this observation an easy upper bound derived from the Johnson bound A $A(m \times n, \omega, \lambda)$ states that:

$$\Phi(m \times n, \omega, \lambda) \leq \left\lfloor \frac{A(m \times n, \omega, \lambda)}{mn} \right\rfloor \tag{3.1}$$

Theorem 14. *(Moreno and Ortiz, Johnson Bound A)*

$$\Phi(m \times n, \omega, \lambda) \leq \left\lfloor \frac{1}{\omega} \left\lfloor \frac{(mn)-1}{\omega-1} \left\lfloor \frac{(mn)-2}{\omega-2} \cdots \left\lfloor \frac{(mn)-\lambda}{\omega-\lambda} \right\rfloor \right\rfloor \right\rfloor \right\rfloor \tag{3.2}$$

Proof. The proof comes from applying Equation 3.1 to the Johnson Bound A.

$$\Phi(m \times n, \omega, \lambda) \leq \left\lfloor \frac{1}{mn} \left\lfloor \frac{mn}{\omega} \left\lfloor \frac{(mn)-1}{\omega-1} \cdots \left\lfloor \frac{(mn)-\lambda}{\omega-\lambda} \right\rfloor \right\rfloor \right\rfloor \right\rfloor \tag{3.3}$$

$$\leq \left\lfloor \frac{1}{\omega} \left\lfloor \frac{(mn)-1}{\omega-1} \cdots \left\lfloor \frac{(mn)-\lambda}{\omega-\lambda} \right\rfloor \right\rfloor \right\rfloor \tag{3.4}$$

□

Example. *Given a GPCWC with $m = 5$ rows and $n = 4$ columns, hamming weight $\omega = 4$, and correlation value $\lambda = 1$. The maximum size of this CWC is given by*

$$\Phi(5 \times 4, 4, 1) \leq \left\lfloor \frac{1}{4} \left\lfloor \frac{20-1}{3} \right\rfloor \right\rfloor \leq 1 \tag{3.5}$$

Theorem 15. *(Moreno and Ortiz) Let n, m, ω, λ be integers, $mn > 1$, $1 \leq \omega \leq mn$, $0 \leq \lambda \leq \omega$. Then the size $\Phi(m \times n, \omega, \lambda)$ of an GPCWC having parameters $(m \times n, \omega, \lambda)$ satisfies:*

$\Phi(m \times n, \omega, \lambda) \leq 1$ *if* $\omega^2 > mn\lambda$.

The following proof is a modification to the proof from Chung and Kumar on OOCs to GPCWC.

Proof. Assume the contrary. Let $x(i, j)$ and $y(i, j)$, $0 \leq i < m$, $0 \leq j < n$, be two distinct codewords. Since

$$\sum_{\alpha=0}^{m-1} \sum_{\tau=0}^{n-1} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x(i, j) y(i \oplus_m \alpha, j \oplus_n \tau) = \omega^2 \tag{3.6}$$

and

$$\lambda \geq \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x(i, j) y(i \oplus_m \alpha, j \oplus_n \tau) \tag{3.7}$$

for all α and τ we have $mn\lambda \geq \omega^2$ which is a contradiction. □

A more general upper bound derived from the Johnson bound B and the Collorary 5 from Agrell, Vardy, and Seger on CWC [1] states that

Theorem 16. *(Moreno and Ortiz, Johnson Bound B)*

Provided $\omega^2 > (mn)\lambda$,

$$\Phi(m \times n, \omega, \lambda) \quad \leq \quad min\left(1, \left\lfloor \frac{(\omega - \lambda)}{\omega^2 - n\lambda} \right\rfloor\right) \tag{3.8}$$

Provided $\omega^2 = (mn)\lambda$,

$$\Phi(mn, \omega, \lambda) \leq 1 \tag{3.9}$$

Proof. The proof is similar to the proof for Theorem 14, by applying the Equation 3.1 to Johnson Bound B improved with the Collorary 5 by Agrell, Vardy and Seger on CWC.

Provided $\omega^2 - mn\lambda \geq \omega - \lambda$

$$\Phi(m \times n, \omega, \lambda) \leq \frac{1}{mn}\left\lfloor \frac{(mn)(\omega - \lambda)}{\omega^2 - (mn)\lambda} \right\rfloor \tag{3.10}$$

$$\leq \left\lfloor \frac{(\omega - \lambda)}{\omega^2 - n\lambda} \right\rfloor \tag{3.11}$$

Provided $0 < \omega^2 - mn\lambda \leq \omega - \lambda$

$$\Phi(m \times n, \omega, \lambda) \leq \frac{1}{mn} mn \tag{3.12}$$

$$\leq 1 \tag{3.13}$$

Provided $\omega^2 = (mn)\lambda$,

$$\Phi(mn, \omega, \lambda) \leq \left\lfloor \frac{2(mn) - 2}{mn} \right\rfloor \leq \left\lfloor 2 - \frac{2}{mn} \right\rfloor \tag{3.14}$$

$$\leq 1 \tag{3.15}$$

□

Example. *Given a GPCWC with* $m = 5$ *rows and* $n = 5$ *columns, hamming weight* $\omega = 15$*, and correlation value* $\lambda = 9$*. Since* $mn\lambda = 225$ *and* $\omega^2 = 225$ *The maximum size of this GPCWC is given by*

$$\Phi(5 \times 5, 15, 9) \leq 1 \tag{3.16}$$

A third bound for GPCWC is obtained by the following improvement to the Johnson Bound C (an hybrid of JB A and improved JB B)

Theorem 17. *(Moreno and Ortiz, Johnson Bound C) Provided l, is some integer, $1 \leq l \leq \lambda - 1$, such that $(\omega - l)^2 > ((mn) - l)(\lambda - l)$.*

$$\Phi(m \times n, \omega, \lambda) \leq \left\lfloor \frac{1}{\omega} \left\lfloor \frac{(mn)-1}{\omega - 1} \cdots \left\lfloor \frac{(mn)-(l-1)}{\omega-(l-1)} h \right\rfloor \right\rfloor \right\rfloor \tag{3.17}$$

$$\text{with } h = min\left((mn) - l, \left\lfloor \frac{((mn)-l)(\omega-\lambda)}{(\omega-l)^2 - ((mn)-l)(\lambda-l)} \right\rfloor\right)$$

Proof. The proof is similar to the proof in Theorem 16. □

In general terms the way the JB C works is that when $\lambda > 1$ and $\omega^2 < mn\lambda$ the Johnson Bound A is used until a point l from where the Johnson Bound B can be used because $(\omega - l)^2 \geq (mn - l)(\lambda - l)$, and finally both results are multiplied to obtain the bound.

3.2 Group Permutable Double Periodic Array

Definition 3.2.1. *A $(m \times n, \omega, \lambda)$ $\{(\mathbb{Z}_m \times \mathbb{Z}_n), < \boldsymbol{R}, \boldsymbol{D} >\}$ group permutable DPA (GPDPA) C is a 2-D binary {0,1} code with m columns and n rows in which every codeword has Hamming weight equal to ω, $1 \leq \lambda < \omega < mn$, and satisfies the double periodicity property:*

$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x(i,j)x(i \oplus_m \alpha, j \oplus_n \tau) \leq \lambda \tag{3.18}$$

for all codewords $x \in C$ and for any $1 \leq \alpha < m, 1 \leq \tau < n$, where $\oplus_n$ denotes addition modulo n.

$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x(i,j)y(i \oplus_m \alpha, j \oplus_n \tau) \leq \lambda \tag{3.19}$$

for all codewords $x, y \in C$ and for any $0 \leq \alpha < m, 0 \leq \tau < n$, where $\oplus_n$ denotes addition modulo n.

In the past we have used the Johnson bound improvements for OOCs to check the optimality of DPA with row and column length relatively prime. In this work

we obtain different DPAs where the row and column length are not relatively prime. Here we prove that DPAs with correlation lower than their weight ($\lambda < \omega$) or GPDPA are also GPCWC, such that we can use the improvements to the Johnson bound on GPCWC to prove the optimality of some of our DPA families.

Lemma 4. *(Moreno and Ortiz) Whenever* $1 \leq \lambda < \omega$*, each array of a* $(m \times n, \omega, \lambda)$*-GPDPA family has* mn *distinct double periodic shifts.*

Proof. Assume the contrary, and select two different double periodic shifts c and c' from the same array such that they are equal. Since they are equal all the ones of c coincides with the ones of c', and therefore the correlation of c and c' is equal to the weight of the GPDPA family($\lambda = \omega$), implying that the auto-correlation of the family must also be equal to the weight of the family, which is a contradiction. □

Lemma 5. *(Moreno and Ortiz) Whenever* $1 \leq \lambda < \omega$*, no GPDPA array can be obtained by the double periodic shifting, one or more times, of another GPDPA.*

Proof. Assume the contrary and select two arrays c and c' of a $(m \times n, \omega, \lambda)$-GPDPA with $\Phi > 1$ with a double periodic shift of the array c equal to the array c', it follows that the correlation between c and c' is equal to the weight of the GPDPA family($\lambda = \omega$), implying that the cross-correlation of the GPDPA family is also equal to the weight of the GPDPA family, which is a contradiction. □

Theorem 18. *(Moreno and Ortiz) Whenever* $1 \leq \lambda < \omega$*, a* $(m \times n, \omega, \lambda)$ *- GPDPA produces a* $\{\mathbb{Z}_m \times \mathbb{Z}_n, < R, D >\}$ *GPCWC.*

Proof. The proof of this theorem follows from lemmas 4, and 5. □

3.3 Non-binary Group Permutable Constant Weight Codes

Given two codewords over an alphabet of size $(T + 1)$ containing 0, we define their Hamming correlation to be the number of nonzero agreements between the two codewords.

Theorem 19. *(Omrani and Kumar) If $A(\Lambda, \omega, \lambda)$ is the maximum possible size of a constant weight code over an alphabet of size $(T+1)$ containing the element 0, of length Λ, Hamming weight ω and correlation $\leq \lambda$, then $A(\Lambda, \omega, \lambda)$ is bounded by the following upper bound:*

$$A(\Lambda, \omega, \lambda) \leq \left\lfloor \frac{T\Lambda}{\omega} \left\lfloor \frac{T(\Lambda-1)}{\omega-1} \cdots \left\lfloor \frac{T(\Lambda-\lambda)}{\omega-\lambda} \right\rfloor \right\rfloor \right\rfloor \tag{3.20}$$

Remark: This generalization of the Johnson Bound to non-binary constant weight codes was presented by Omrani and Kumar in [31].

Since a Group Permutable Constant Weight Code can be regarded as a constant weight code over an alphabet of size $(n+1)$, the bound 3.20 can be translated to the following bound on the size of Group Permutable Constant Weight Codes .

Theorem 20. *(Ortiz and Moreno),*

Given a $(m \times n, \omega, \lambda)$-GPCWC the bound on the number of codewords in the family is given by:

$$\Phi(m \times n, \omega, \lambda) \leq \left\lfloor \frac{1}{\omega} \left\lfloor \frac{n(m-1)}{\omega-1} \cdots \left\lfloor \frac{n(m-\lambda)}{\omega-\lambda} \right\rfloor \right\rfloor \right\rfloor \tag{3.21}$$

Proof. The proof comes from applying Equation 3.1 to the Omrani-Kumar generalization of the Johnson Bound for non-binary constant weight codes Equation 3.20 with $T = n$ and $\Lambda = m$.

□

Example. *Given a non-binary GPCWC with length $m = 5$ rows and $n = 25$ columns, hamming weight $\omega = 5$, and correlation value $\lambda = 1$. The maximum size of this CWC is given by*

$$\Phi(10, 5, 2) \leq \left\lfloor \frac{1}{5} \left\lfloor \frac{25(4)}{4} \right\rfloor \right\rfloor \leq 5 \tag{3.22}$$

Theorem 21. *(Ortiz and Moreno)*

Given a $(m \times n, \omega, \lambda)$*-GPCWC with* $m = \omega$*, the bound on the number of codewords in the family is given by:*

$$\Phi(m \times n, \omega, \lambda) \leq \left\lfloor \frac{n^{\lambda}}{\omega} \right\rfloor \tag{3.23}$$

Proof. Substitute m by ω in Equation 3.21 □

3.4 Chapter Summary

In this chapter we introduced the new concept of Group Permutable Constant Weight Codes and present improvements to the Johnson Bound (A, B, and C) to provide bounds on the family size of binary and non-binary Group Permutable Constant Weight Codes . Group Permutable Constant Weight Codes have applications in 1-D Optical Orthogonal Codes, 2-D Optical Orthogonal Codes, Multiple Target radar and sonars, and Digital Watermarking. The bounds that we introduce can be used to proof optimality of Double Periodic Arrays when the row and column length are not relatively prime.

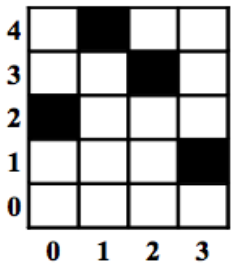
CHAPTER 4
WEIGHT INCREASING METHOD

Previous work [28, 30, 37, 38] describes how to increase the weight of a DPA using periodic shift sequences as columns. This is only for the case where the DPA have at most a single one per column. In the past Tirkel and Hall applied this method with the Moreno-Maric construction [38] to create new matrices with good auto- and cross-correlation properties.

In this Chapter we review the method to increase the weight of double periodic constructions and call it Method A (Weight Increasing Method). It is important to review the Weight Increasing Method because it is used in Chapter 6 combined with new methods to increase the size of families of double periodic arrays (Chapter 5) to produce new families of double periodic arrays with cross-correlation $<$ auto-correlation. Here we also present theorems to calculate the new auto- and cross-correlation of the families obtained after applying the Weight Increasing Method to the original double-periodic families[1] .

Method A (Weight Increasing Method): Let $W_{n,m}$ be a DPA of size $n \times m$, weight ω, auto-correlation λ_a and cross-correlation λ_c. Let s be a cyclically shifted periodic sequence of size n, weight ω' and correlation λ'. The Weight Increasing Method (WIM) consists in replacing the columns of the double periodic matrix

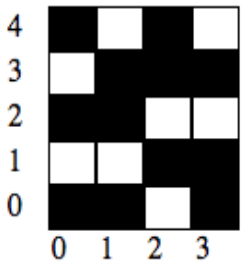
[1] To the best of the author's knowledge, the theorems for the auto- and cross-correlation obtained after applying the Weight Increasing Method as presented by the author, and applied to DPAs are new



(a) 5x4 Welch array

4	1	0	1	0
3	0	1	1	1
2	1	1	0	0
1	0	0	1	1
0	1	1	0	1
	0	1	2	3

(b) 5x4 Welch array with binary column sequence



(c) 5x4 Welch array with Column Sequence

4	-1	1	-1	1
3	1	-1	-1	0
2	0	-1	1	1
1	1	1	0	-1
0	-1	0	1	-1
	0	1	2	3

(d) 5x4 Welch array with ternary Column Sequence

Figure 4–1: 5x4 Welch array with and w/o column sequence

$W_{n,m}$ with the periodic sequence s. The size of s is the same size of the columns of the DPA. We call s the column sequence. (See Figure 4–1(a)-4–1(b)).

Start with a DPA $W_{n,m}$ of size $n \times m$. Then find a periodic sequence s of size n with good correlation properties to use as column sequence. Construct s^l, $l = 1 \ldots n-1$ such that s^l is the result of shifting the sequence s, l times to the same direction (right or left).

For example for the result in Figure 4–1(b) we use the Legendre sequence $s = (1,0,1,1,0)$ and the set s^l is constructed as follows:

$$\begin{aligned} s^0 &= (1,0,1,1,0) \\ s^1 &= (0,1,1,0,1) \\ s^2 &= (1,1,0,1,0) \\ s^3 &= (1,0,1,0,1) \\ s^4 &= (0,1,0,1,1) \end{aligned}$$

Now for each column j in W, find the row i where $W_{i,j} = 1$ and replace the column j with the sequence s^i.

Figure 4–1(b) is an example of a 5×4 Welch DPA $(0,2),(1,4),(2,3),(4,1)$ with the columns replaced by a binary Legendre sequence (1,0,1,1,0) of size 5. And Figure 4–2 is a second example of a 5×5 Quadratic DPA $(0,0),(1,1),(2,4),(3,4),(4,1)$ with the columns replaced by the Legendre sequence (1,0,1,1,0).

Method A applied to a Welch array of size $p(p-1)$ using a binary 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.

In section 4.1 we present the DPAs with increased weight obtained after applying Method A to the Quadratic, Welch, Hyperbolic, Lempel-Golomb and Moreno-Maric DPA constructions.

In general to obtain the correlation of the new double periodic families obtained after applying Method A: Let $W_{n,m}$ be a double periodic matrix of size $n \times m$, weight ω, auto-correlation λ_a and cross-correlation λ_c. Let s be a cyclically shifted periodic sequence of size n, weight ω' and correlation λ'.

Theorem 22. *(Moreno and Ortiz) The auto-correlation properties of the double periodic families obtained after applying Method A is* $\lambda' \times m + \lambda_a(\omega' - \lambda')$.

Proof. Let matrix $A_{n,m}$ be a DPA obtained after applying Method A with a column sequence with correlation λ'. If we correlate a shifted version of matrix A, call it matrix $B_{n,m}$. Each column of matrix A correlates with a column of matrix B. But the column in matrix B is a shifted version of a column in matrix A. Therefore if all columns are different shifted versions, we obtain that the correlation is $m \times \lambda'$.

But we know that the original matrix (before applying Method A) has auto-correlation λ_a, therefore we know that at most λ_a columns in the matrix A can be exactly the same to a column in matrix B where all ω' symbols (dots) correlate. Therefore in the new correlation we need to add the dots or symbols that are not taken in consideration by $m \times \lambda'$, which is $\lambda_a(\omega' - \lambda')$.

Therefore the auto-correlation of a new DPA A obtained from applying Method A to a DPA of size $n \times m$ with auto-correlation λ_a using a periodic sequence of size n, weight ω', and correlation λ' is $\lambda' \times m + \lambda_a(\omega' - \lambda')$.

□

Theorem 23. *(Ortiz and Moreno) The cross-correlation properties of the double periodic family obtained after applying Method A is* $\lambda' \times m + \lambda_c(\omega' - \lambda')$.

Proof. The proof is similar to the proof on auto-correlation, but matrix B is a different matrix in the family; and this time a column in matrix A will be exactly the same to a column in matrix B λ_c times. □

Remark Method A works with any non-binary periodic sequence used as column sequence. Note that the parameters in our theorems 22 and 23 are independent of whether the column sequence is binary or not. We mostly use binary examples for the sake of clarity.

4.1 Families of Double Periodic Arrays with Increased Weight

In the introduction we described digital watermarking as an example of arrays that need to have many dots (weight increased). Here we present more double periodic families constructed using the Method A (WIM) described in section 4. Proof for the following theorems come from applying Method A to the well know families of DPAs and the results of Theorems 22 and 23.

4.1.1 Quadratic families

4	0	0	1	1	0
3	0	0	0	0	0
2	0	0	0	0	0
1	0	1	0	0	1
0	1	0	0	0	0
	0	1	2	3	4

(a) 5x5 Quadratic array

4	1	0	0	0	0
3	0	1	1	1	1
2	1	0	1	1	0
1	1	1	0	0	1
0	0	1	1	1	1
	0	1	2	3	4

(b) 5x5 Quadratic array with binary Column Sequence

Figure 4–2: 5x5 Quadratic array with and w/o Column Sequence

Theorem 24. *(Moreno and Ortiz) Applying Method A to the Quadratic Construction using a Legendre sequence as a column produces OOCs with parameters* $(p \times p, \omega = \frac{(p^2+p)}{2}, \lambda_a \leq \frac{(p+1)^2}{4}, \lambda_c \leq \frac{(p^2+3p+2)}{4}$*, periodicity* $p \times p$*, and* $\Phi = (p-1)$*.*

Proof. Following Method A, the new weight is given by $p \times \left(\frac{p+1}{2}\right)$. The auto- and cross-correlation properties are given by Theorem 22 and Theorem 23 respectively.

□

4	1	0	0	0	0
3	0	1	1	1	1
2	1	0	1	1	0
1	1	1	0	0	1
0	0	1	1	1	1
	0	1	2	3	4

Figure 4–3: 5x5 Quadric DPA with $f(x) = x^2$ after WIM

Example. *Let $p = 5$ and (1,0,1,1,0) the column sequence, the Quadratic family obtained after applying Method A to the Quadratic family { (0, 1, 4, 4, 1) for $k = 1$, (0, 2, 3, 3, 2) for $k = 2$, (0, 3, 2, 2, 3) for $k = 3$, (0, 4, 1, 1, 4) for $k = 4$} is:*

$$
\begin{aligned}
for \quad k = 1 \quad & (0,1),(0,2),(0,4),(1,0),(1,1),(1,3),(2,0),(2,2),(2,3),\\
& (3,0),(3,2),(3,3),(4,0),(4,1),(4,3)\\
for \quad k = 2 \quad & (0,1),(0,2),(0,4),(1,0),(1,2),(1,4),(2,1),(2,3),(2,4),\\
& (3,1),(3,3),(3,4),(4,0),(4,2),(4,4)\\
for \quad k = 3 \quad & (0,1),(0,2),(0,4),(1,1),(1,3),(1,4),(2,0),(2,2),(2,4),\\
& (3,0),(3,2),(3,4),(4,1),(4,3),(4,4)\\
for \quad k = 4 \quad & (0,1),(0,2),(0,4),(1,0),(1,2),(1,3),(2,0),(2,1),(2,3),\\
& (3,0),(3,1),(3,3),(4,0),(4,2),(4,3)
\end{aligned}
$$

and (1,0,1,1,0) the column sequence,

with parameters $(5 \times 5, 15, 9, 11)$.

Figure 4–2 is an example of the double-periodic Quadratic 5×5 matrix sequence with $p = 5$, $k = 1$ (Figure 4–2(a)), and the same double-periodic Quadratic matrix with the columns replaced by the Legendre sequence (1,0,1,1,0) (Figure 4–2(b)).

4.1.2 Hyperbolic families

4	0	1	1	0	0
3	1	1	0	1	0
2	0	0	1	1	0
1	1	1	0	0	0
0	1	0	1	1	0
	0	1	2	3	4

Figure 4–4: 5x5 Hyperbolic DPA with $f(x) = 1/x$ after WIM

Theorem 25. *(Moreno and Ortiz) Applying Method A to the Hyperbolic Construction using a Legendre sequence as a column produces OOCs with parameters* $(p \times p, \omega = \frac{(p^2-1)}{2}, \lambda \leq \frac{(p+1)^2}{4})$*, periodicity* $p \times p$*, and* $\Phi = (p-1)$*.*

Proof. Following Method A, the new weight is given by $(p-1)\times\left(\frac{p+1}{2}\right)$. The auto- and cross-correlation properties are given by Theorem 22 and Theorem 23 respectively. □

Example. *Let* $p = 5$ *and (1,0,1,1,0) the column sequence, the Hyperbolic family obtained after applying Method A to the Hyperbolic family {(1, 3, 2, 4, *) for* $k = 1$*, (2, 1, 4, 3, *) for* $k = 2$*, (3, 4, 1, 2, *) for* $k = 3$*, (4, 2, 3, 1, *) for* $k = 4$*} is:*

$$
\begin{aligned}
for \quad k=1 \quad & (0,0),(0,1),(0,3),(1,1),(1,3),(1,4),(2,0),(2,2),(2,4),\\
& (3,0),(3,2),(3,3)\\
for \quad k=2 \quad & (0,0),(0,2),(0,4),(1,0),(1,1),(1,3),(2,0),(2,2),(2,3),\\
& (3,1),(3,3),(3,4)\\
for \quad k=3 \quad & (0,1),(0,3),(0,4),(1,0),(1,2),(1,3),(2,0),(2,1),(2,3),\\
& (3,0),(3,2),(3,4)\\
for \quad k=4 \quad & (0,0),(0,2),(0,3),(1,0),(1,2),(1,4),(2,1),(2,3),(2,4),\\
& (3,0),(3,1),(3,3)
\end{aligned}
$$

with parameters $(5 \times 5, 12, 9)$*.*

4.1.3 Welch families

Theorem 26. *(Moreno and Ortiz) Method A applied to a Welch array of size* $p(p-1)$ *using a binary Legendre sequence as a column produces OOCs with parameters* $(n, \omega, \lambda) = (p(p-1), \frac{p^2-1}{2}, [\frac{p(p+1)}{4}])$*.*

Proof. Following Method A, the new weight is given by $(p-1) \times \left(\frac{p+1}{2}\right)$. The autocorrelation value is given by Theorem 22. □

4	1	0	1	0
3	1	1	0	1
2	0	1	1	0
1	1	0	0	1
0	0	1	1	1
	0	1	2	3

Figure 4–5: 5x4 Welch DPA with $\alpha = 3$ and $p = 5$ after WIM

Example. *Let $p = 5, \alpha = 3$ and (1,0,1,1,0) the column sequence, the Welch family obtained after applying Method A to the Welch sequence (3, 4, 2, 1) is:*

$$(0,0),(0,2),(0,4),$$
$$(1,0),(1,2),(1,3),$$
$$(2,1),(2,3),(2,4),$$
$$(3,0),(3,1),(3,3)$$

with parameters $(5 \times 4, 12, 8)$.

See Figure 4–1(b) presented previously.

4.1.4 Lempel-Golomb families

Theorem 27. *(Moreno and Ortiz) Method A applied to a Lempel-Golomb array of size $(q-1) \times (q-1)$ using a binary sequence of weight ω' and correlation λ' produces OOCs with parameters $(n, \omega, \lambda) = ((q-1) \times (q-1), (q-2)\omega', \lambda'(q-3) + \omega')$.*

Proof. Following Method A, the new weight is given by $(q-2) \times \omega'$. The autocorrelation value is given by Theorem 22. □

Example. *For Lempel-Golomb we use a case where $q-1$ is prime. Let $q = 2^3, \alpha = 3, \beta = \alpha$ and the Legendre sequence (1, 0, 0, 1, 0, 1, 1) the column sequence,*

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

Figure 4–6: 7x7 Lempel-Golomb DPA with $\alpha = 3$ and $q = 2^3$ after WIM

*the Lempel-Golomb family obtained after applying Method A to the Lempel-Golomb sequence (3, 6, 1, 5, 4, 2, *) is:*

$$(0,2),(0,3),(0,4),(0,6),$$
$$(1,0),(1,2),(1,5),(1,6),$$
$$(2,0),(2,1),(2,2),(2,4),$$
$$(3,1),(3,4),(3,5),(3,6),$$
$$(4,0),(4,3),(4,4),(4,5),$$
$$(5,1),(5,2),(5,3),(5,5)$$

with parameters $(7 \times 7, 24, 14)$.

4.1.5 Moreno-Maric families

Theorem 28. *(Moreno and Ortiz) Method A applied to the Moreno-Maric array of size* $(q+1)\times(q+1)$ *using a binary sequence of weight* ω' *and correlation* λ' *produces OOCs with parameters* $(n, \omega, \lambda) = ((q+1)\times(q+1), (q+1)\omega', \lambda'(q-1)+2\omega')$.

Proof. Following Method A, the new weight is given by $(q+1)\times\omega'$. The auto- and cross-correlation properties are given by Theorem 22 and Theorem 23 respectively.

□

7	1	1	-1	i	-1	1	i	1
6	1	-1	i	-1	1	1	1	i
5	i	i	1	1	-1	1	1	-1
4	-1	1	1	-1	i	i	1	1
3	1	1	1	i	1	-1	i	-1
2	-1	1	i	1	1	1	-1	i
1	i	i	-1	1	1	-1	1	1
0	1	-1	1	1	i	i	-1	1
	0	1	2	3	4	5	6	7

Figure 4–7: 8x8 Moreno-Maric double-periodic array with $\alpha = 3$ and $q = 7$ after WIM

Example. *To show an example of the WIM applied to the Moreno-Maric construction we use the ternary periodic sequence (1, 1, i , -1, 1, -1, i, 1) of size 8 from the Milewski [21] construction as column sequence applied to the sequence (0, 4, 3, 6, 5, 1, 2, 7) of the family of the 8x8 Moreno-Maric construction with $q = 7$ and $\alpha = 3$. See figure 4–7.*

In Chapter 6 we use the DPA with weight increased presented in this section combined with the methods to increase the size of DPA families presented in Chapter 5 to produce new families of DPAs with $\lambda_c < \lambda_a$.

4.2 Optimal GPCWC constructions

Theorem 29. *(Moreno and Ortiz) The $(p \times p, \omega = \frac{(p^2+p)}{2}, \lambda \leq \frac{(p+1)^2}{4})$ DPA with family size 1 obtained after applying Method A to a Quadratic array is optimal with respect to the Johnson Bound B modification for GPCWC .*

Proof. The resulting double periodic array obtained after applying Method A to a Quadratic array has $\lambda \leq \frac{(p+1)^2}{4} < \omega = \frac{(p^2+p)}{2}$, and has double periodicity $p \times p$.

By Lemma 4 the double periodic Quadratic construction has p^2 distinct double periodic shifts, and no array can be obtained by the double periodic shifting, one or more times, of another array.

By Theorem 18 our $(p \times p, \omega, \lambda)$-GPDPA Quadratic construction is also a $\{\mathbb{Z}_p \times \mathbb{Z}_p, < \mathbf{R}, \mathbf{D} >\}$ GPCWC.

It follows that from each codeword of the Quadratic GPCWC we obtain p^2 CWC. Using our improvement of the Johnson Bound B for GPCWC we determine that $\omega^2 = n\lambda$.

$$\begin{aligned} \omega^2 &= \frac{p^4 + 2p^3 + p^2}{4} && (4.1) \\ n\lambda &= p^2\left(\frac{(p+1)^2}{4}\right) && (4.2) \\ n\lambda &= \frac{p^4 + 2p^3 + p^2}{4} && (4.3) \\ \omega^2 - n\lambda &= 0 && (4.4) \end{aligned}$$

and $\Phi(p \times p, \omega = \frac{(p^2+p)}{2}, \lambda \leq \frac{(p+1)^2}{4}) \leq 1$. □

4.3 Chapter Summary

Here in this chapter we presented a method to increase the weight of DPAs (Method A). Applying Method A to DPAs increase the correlation value of the new families. This increase in correlation is obtained by the equations in Theorems 22 and 22. Using this method we obtain an optimal construction in the size of the families with respect to the improvement to the Johnson Bound B for Group Permutable Constant Weight Codes.

Some applications like Digital Watermarking require the families of double-periodic constructions to have a balanced weight. In other words for our examples we want the number of ones to be approximately half the size of the arrays. All the codes in this chapter can be used for application of 2-D Optical Orthogonal Codes. The Welch code can be used in 1-D Optical Orthogonal Codes if we use the Chinese Remainder Theorem to arrange the code in one dimension. Digital Watermarking applications require the family size to be as big as possible to be able to handle multiple users. Families with family size one like the Welch family are not really useful for Digital Watermarking.

Table 4.3 is a summary of the new DPAs that we obtain after applying Method A.

Table 4–1: New DPA using the Weight Increasing Method

Construction	**Periodicity**	ω	Φ	λ_a	λ_c
Quadratic	$p \times p$	$\frac{(p^2+p)}{2}$	p	$\frac{(p+1)^2}{4}$	$\frac{(p^2+3p+2)}{4}$
Hyperbolic	$p \times p$	$\frac{(p^2-1)}{2}$	p	$\frac{(p+1)^2}{4}$	$\frac{(p+1)^2}{4}$
Welch	$p \times (p-1)$	$\frac{(p^2-1)}{2}$	p	$\frac{(p^2+p)}{4}$	N/A
Lempel-Golomb	$(q-1) \times (q-1)$	$(q-2)\omega'$	p	$\lambda'(q-3)+\omega'$	N/A
Moreno-Maric	$(q+1) \times (q+1)$	$(q+1)\omega'$	p	$\lambda'(q-1)+2\omega'$	$\lambda'(q-1)+2\omega'$

CHAPTER 5
METHOD TO CONSTRUCT DOUBLE PERIODIC ARRAYS WITH OPTIMAL CORRELATION

In previous work [25, 26, 29] our group presented a method to construct families of DPA with perfect correlation from the Welch Costas construction using the Chinese Remainder.[1]

There are not many constructions of multiple target arrays with ideal correlation properties [35]. In this work we extend the number of new constructions with ideal correlation properties, by using a similar method that does not use the CRT. These methods increase the family size of DPAs without changing their original correlation value. Without using the CRT we can apply the new method to any DPA such as the Quadratic, Hyperbolic, Welch, Lempel-Golomb, and Moreno-Maric constructions presented in Chapter 1 section 2.4. In the following sections we describe both methods to increase the size of the families. First in section 5.1 we review the Moreno-Omrani-Maric method and then section 5.2 we describe the method to increase the size of families without using the CRT.

5.1 Moreno-Omrani-Maric method to increase family size of DPA using the Chinese Remainder Theorem

The Moreno-Omarani-Maric (MOM) method to increase the size of the families of double periodic arrays consists in applying a modified method of the Colbourn and

[1] The work presented in [25, 26] are result of this thesis work.

Colbourn construction for cyclic Balanced Incomplete Block Design (BIBD's) to the MZKZ construction (See definition 30). Here we review the MZKZ construction and then review the MOM method to increase the family size of DPA. In section 5.1.1 we present two extended Costas and two sonar constructions obtained from using the MOM method, and give an example using a Welch array of size $n = p(p-1)$ and $p = 5$.

Theorem 30. *(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. [28]) 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 [18] 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:

$$M(i,j) = \begin{cases} 1, & \text{if } f(\alpha^j) = p-1-i \\ 0, & \text{otherwise} \end{cases} \tag{5.1}$$

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 $p(p-1)$:

$$\mu(l) = M(l \mod (p), l \mod (p-1)) \tag{5.2}$$

M.J. Colbourn and C.J. Colbourn [8] proposed two recursive constructions for cyclic BIBD's. Their Construction A was generalized [44] to form DDS recursively. The following is an easy generalization of Colbourn Construction B:

Theorem 31. *(Moreno-Omrani-Maric, Construction B) Given a* (vk, k, t)*-DDS,* $((vk \mod k) = 0)$ *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* $D' = \{D'_i | 1 \leq i \leq t'\}$*.*

Proof is similar to the one in [8]. Lemma 6 will be proved which is the special case that interests in this work.

Theorem 32. ***(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 [18].*

Lemma 6. *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.

The same proof can be used 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 $p-1$. □

5.1.1 Two Multiple Target Families for Extended Costas and for Sonar Arrays

Using the CMZKZ construction, the Chinese Remainder Theorem and Theorem 9 of Section 2.2, since p^i is relatively prime to $p-1$ we obtain:

Construction 1(V): 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): 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. *An example to generate the family of Construction 1(V). Start with a Welch array of Figure 5–1 2,4,3,1. Now notice that (0,2) corresponds to 12 using*

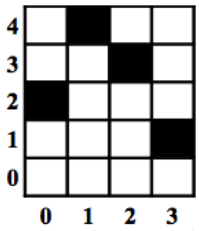


Figure 5–1: 5x4 Welch Costas

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 Remainder Theorem to the Welch array we obtain the OOC* D*:*

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

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 Remainder 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 5–2.

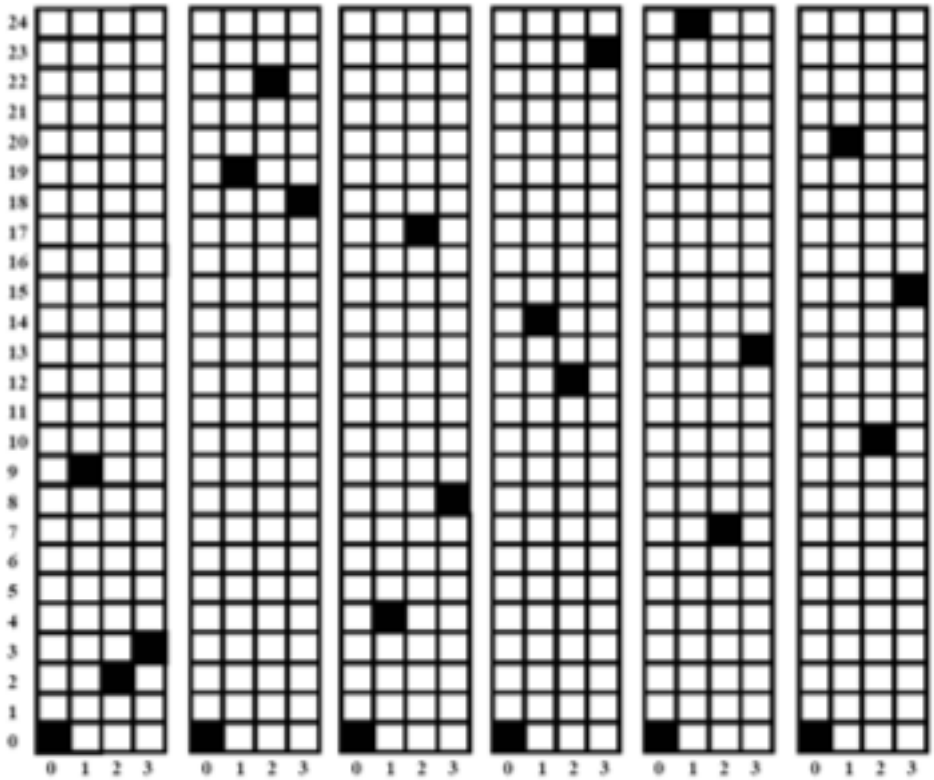


Figure 5–2: 25x4 Moreno-Omrani-Maric sonars family

5.2 New method to increase the family size of DPA without using the Chinese Remainder Theorem

In section 5.1 we reviewed the Moreno-Omrani-Maric method to increase the size of the families of DPAs with length $n = mp$ and $m = (p - 1)$ using the CRT.

In this section we present a new similar method but without the need of using the CRT. [27].[2] Now we can apply the new method to any DPA such as the Quadratic, Hyperbolic, Welch, Lempel-Golomb, and Moreno-Maric constructions presented in Chapter 1 section 2.4. In section 5.3 we present new families of DPAs with optimal correlation properties obtained from applying Method B to those constructions. Some of the DPAs result in new families of extended Costas, sonars, or 2-D Optical Orthogonal Codes.

Method B : (Recursive Construction) Given a $(v \times n, \omega, \lambda)$-OOC, $((vn \bmod n) = 0)$ if $gcd(r, (\omega - 1)!) = 1$, then a $(vr \times n, \omega, \lambda)$-OOC may be constructed as follows. For each $D = (0, d_1, \ldots, d_{\omega-1})$, take the r different sequences $D_j = (0, d_1 + jv, d_2 + 2jv, \ldots, d_{\omega-1} + (\omega - 1)jv)$, $0 \leq j < r$, with addition modulo vr.

Example. *Start with the Quadratic sonar of length* $p = 5$*, and* $k = 1$ $(0, 1, 4, 4, 1)$. *After applying Method B with* $r = 5$ *(gcd(5,4!) = 1) we obtain the family:*

$$for \quad j = 0, \quad D_0 = (0 + 0, 1 + 0, 4 + 0, 4 + 0, 1 + 0) = (0, 1, 4, 4, 1)$$

$$for \quad j = 1, \quad D_1 = (0, 1 + 5, 4 + 10, 4 + 15, 1 + 20) = (0, 6, 14, 19, 21)$$

$$for \quad j = 2, \quad D_2 = (0, 1 + 10, 4 + 20, 4 + 30, 1 + 40) = (0, 11, 24, 9, 16)$$

$$for \quad j = 3, \quad D_3 = (0, 1 + 15, 4 + 30, 4 + 45, 1 + 60) = (0, 16, 9, 24, 11)$$

$$for \quad j = 4, \quad D_4 = (0, 1 + 20, 4 + 40, 4 + 60, 1 + 80) = (0, 21, 19, 14, 6)$$

with parameters $(25 \times 5, 5, 1)$*, and* $\Phi = 5$.

[2] The work presented in [27] is result of this thesis work.

Theorem 33. *(Moreno and Ortiz) Applying method B to a family of* $(v\times n, \omega, \lambda)-$*DPA A, produces a new family of* $(vr \times n, \omega, \lambda)$*-DPAs B with the same auto-correlation value as A.*

Proof. Let $D = (0, d_1, \ldots, d_{\omega-1})$ a (vn, ω, λ)-DPA, applying Method B produces a family of arrays $D_j^{'} = (0, d_1 + vj, d_2 + 2vj, \ldots, d_{\omega-1} + (\omega - 1)vj)$, for $j = 0 \ldots r - 1$.

Let M be the difference matrix for array D such that:

$$M_{i,i+c} = d_i - d_{i+c} \bmod v$$

Lets construct the difference matrix for $D_j^{'}$:

$$M_{i,i+c}^{'} = d_i + ivj - (d_{i+c} + (i + c)vj) \bmod vr$$

$$M_{i,i+c}^{'} = (d_i - d_{i+c}) - vjc \bmod vr$$

vcj is constant and therefore $M_{i,i+c}^{'}$ is the same to another $M_{i',i'+c}^{'}$ if and only if in the difference matrix M of D, $M_{i,i+c} = M_{i',i'+c}$. □

Theorem 34. *(Ortiz and Moreno) Applying Method B to a* $(v \times n, \omega, \lambda_a, \lambda_c)$*-DPA A, produces a new family of* $(vr\times n, \omega, \lambda_a, \lambda_c')$*-DPAs B with cross-correlation* $\lambda_c' \leq 2$.

Proof. Lets construct the difference matrix M' between any two arrays from B constructed with $j = r_1$ and $j = r_2$, $0 \leq r_1, r_2 < r$ such that:

$$M_{i,i+c}^{'} = d_i + ivr_1 - (d_{i+c} + (i + c)vr_2) \bmod vr$$

$$M_{i,i+c}^{'} = (d_i - d_{i+c}) + v(i(r_1 - r_2) - cr_2) \bmod vr$$

The values $(r_1 - r_2)$ and $-cr_2$ are constants in $\mathbb{Z}_p$. Let $i' = i(r_1 - r_2) - cr_2$; as i varies i' cycles in $\mathbb{Z}_p$. Therefore the product $vi' \bmod vr$ for $i' \in \mathbb{Z}_p$ produces multiples of v modulo vr $\{0, v, 2v, \ldots, v(p - 1)\}$.

Since $d_i, d_{i+c} \in \mathbb{Z}_v$ the equation $(d_i - d_{i+c}) + vi' \bmod vr$ produces values of the form $v' + v(i')$ for $v' = \{-v + 1, \ldots, -1, 0, 1, \ldots, v - 1\}$.

Therefore values of the difference $(d_i - d_{i+c}) + vi'$ can only be equal with values of other difference $(d_j - d_{j+c}) + vj'$ iff:

$$(d_i - d_{i+c}) = (d_j - d_{j+c}) \text{ and } vi' = vj' \iff i = j \tag{5.3}$$

or

$$(d_j - d_{j+c}) = -((-(d_i - d_{i+c})) \bmod v) \text{ and } vj' = v(i'+1) \tag{5.4}$$

i. e. $(d_j - d_{j+c}) \bmod v = (d_i - d_{i+c} \bmod v)$.

Equation 5.3 implies that we are comparing the same differences.

Equation 5.4 implies that the difference with i can be equal to another difference with j only once, because of the distance between the multiples vi' and vj'.

Therefore $\lambda'_c < 2$. □

Theorem 35. *(Ortiz and Moreno) Applying Method B to a $(v \times n, \omega, \lambda_a, \lambda_c)$-DPA A with $\lambda = 1$, produces a new family of $(vr \times n, \omega, \lambda_a, \lambda'_c)$-DPAs B with cross-correlation $\lambda'_c = 1$.*

Proof. If $\lambda = 1$ then $(d_i - d_{i+c}) \neq (d_j - d_{j+c})$; and therefore in equation 5.4 $(d_j - d_{j+c}) \neq -((-(d_i - d_{i+c})) \bmod v)$ because $-((-(d_i - d_{i+c})) \bmod v) \bmod \text{v} = (d_i - d_{i+c}) \bmod \text{v}$ and we will have a contradiction in the value of λ.

Therefore $\lambda_c = 1$ □

Theorem 36. *(Ortiz and Moreno) Applying Method B to a family of $(v \times n, \omega, \lambda_a, \lambda_c)$-DPAs A, produces a new family of $(vr \times n, \omega, \lambda_a, \lambda'_c)$-DPAs B with cross-correlation $\lambda'_c \leq max(\lambda_c, min(2, \lambda))$.*

Proof. Proof is similar theorem 34. If the r_1 and r_2 used to construct any two arrays from family B are different $(r_1 \neq r_2)$, then the proof in theorem 34 applies. From theorem 34 and 35 the $\lambda'_c = \min(2, \lambda)$

Now lets construct the difference matrix M' between two arrays from B constructed with $j = r_1$, $0 \leq r_1 < r$ such that:

$$M'_{i,i+c} = d_i + ivr_1 - (d_{i+c} + (i+c)vr_2) \bmod vr$$

$$M'_{i,i+c} = (d_i - d_{i+c}) - vcr_2 \bmod vr$$

$-vcr_2$ is constant and therefore $M'_{i,i+c}$ is the same to another $M'_{j,j+c}$ if and only if in the difference matrix M, $M_{i,i+c} = M_{j,j+c}$. In which case the cross-correlation is $\lambda'_c \leq \lambda_c$.

Therefore $\lambda'_c \leq \max(\lambda_c, \min(2, \lambda))$.

□

Applying this new method to families of double-periodic arrays produces new families of double periodic arrays with increased family size where the auto-correlation does not change and the cross-correlation is less or equal to the original cross-correlation. Next section contains new families of DPAs obtained using Method B and examples.

5.3 New Constructions of Double Periodic Arrays with Optimal Correlation

In this section we present new constructions of families of sonar and extended Costas obtained from applying the general Method B described in section 5.2 to the Quadratic, Hyperbolic, Welch, Moreno-Maric, and Lempel constructions.

5.3.1 Quadratic families

Theorem 37. *(Moreno and Ortiz) Applying Method B to the Quadratic array with* $f(x) = kx^2$ *we obtain a family of DPA with parameters* $(p^2 \times p, \omega = p, \lambda = 1)$, *periodicity* $p^2 \times p$, *and* $\Phi = p$. *And a family of DPAs with parameters* $(p^i \times p, p, 1)$, *periodicity* $p^i \times p$, *and* $\Phi = p^{i-1}$.

Proof. Following Method B with $r = p$, the new column size of the DPA is p^2, because of the modular addition, and the family size is p. When applied recursively the column size of the DPA increase to p^i, and the family size increases to p^{i-1}.

The auto- and cross-correlation properties are given by Theorem 33 and Theorem 35 respectively. □

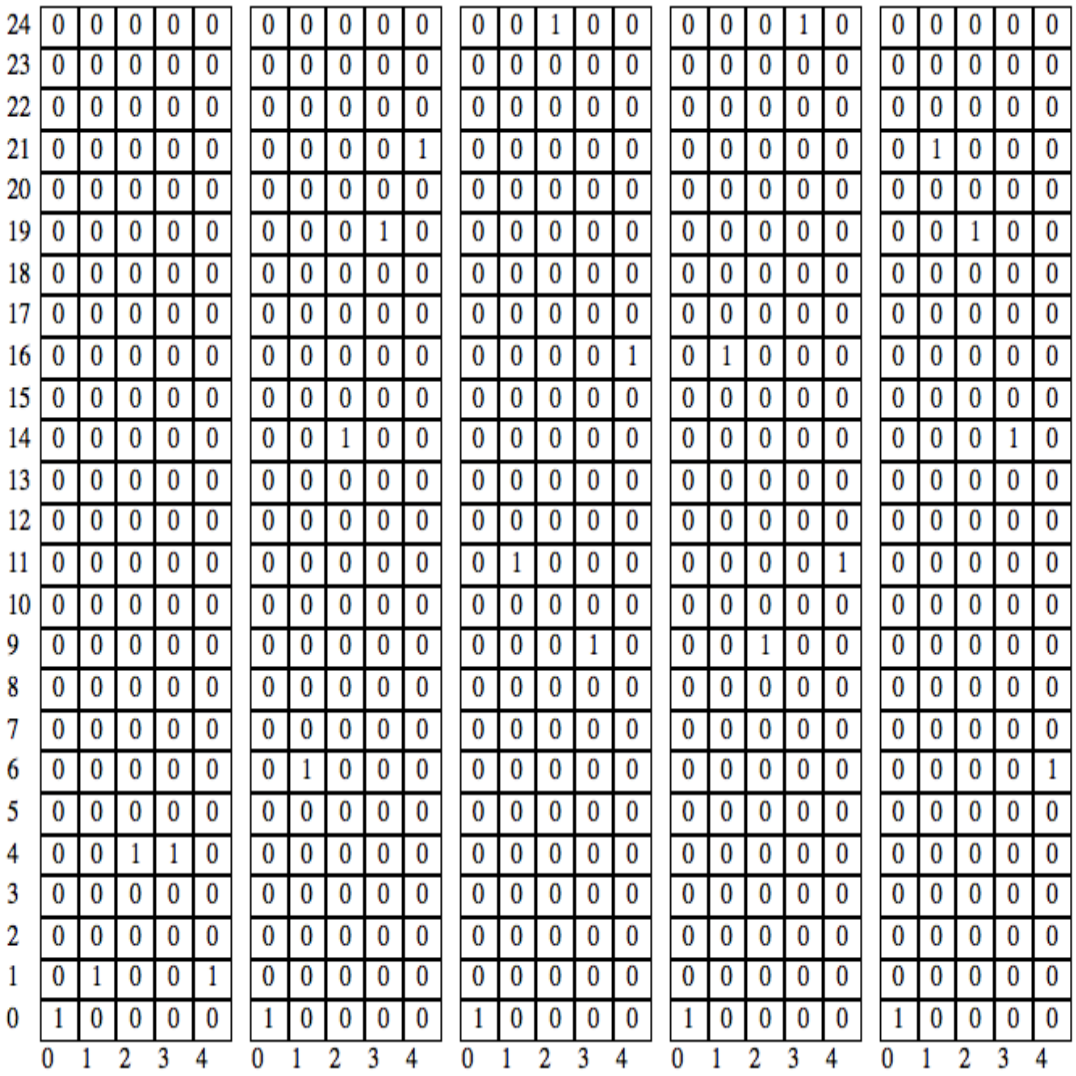


Figure 5–3: 25x5 Quadratic DPA family after applying Method B.

Example. *Let $p = 5$ and $k = 1$, the new DPA family obtained from applying Method B to the Quadratic Construction is*

$$\begin{array}{lll} for & j = 0 & (0, 1, 4, 4, 1) \\ for & j = 1 & (0, 6, 14, 19, 21) \\ for & j = 2 & (0, 11, 24, 9, 16) \\ for & j = 3 & (0, 16, 9, 24, 11) \\ for & j = 4 & (0, 21, 19, 14, 6) \end{array}$$

with parameters $(25 \times 5, 5, 1)$.

Theorem 38. *(Moreno and Ortiz) Applying Method B to the Quadratic family with $f(x) = kx^2$ we obtain a family of DPA with parameters $(p^2 \times p, \omega = p, \lambda_a = 1, \lambda_c = 2)$, periodicity $p^2 \times p$, and $\Phi = (p \times (p-1))$. And a family of DPAs with parameters $(p^i \times p, p, 1, 2)$, periodicity $p^i \times p$, and $\Phi = (p-1) \times p^{i-1}$).*

Proof. Following Method B with $r = p$, the new column size of the DPA is p^2, because of the modular addition, and the family size is $p - 1$ codewords from the original family times p. When applied recursively the column size of the DPA increase to p^i, and the family size increases to $(p-1) \times p^{i-1}$.

The auto- and cross-correlation properties are given by Theorem 33 and Theorem 36 respectively. □

Example. *Let $p = 5$ and $k = 1 \ldots 4$, the new DPA family obtained from applying Method B to the Quadratic family Construction is*

$$
\begin{array}{lll}
k=1 & j=0 & (0,1,4,4,1) \\
 & j=1 & (0,6,14,19,21) \\
 & j=2 & (0,11,24,9,16) \\
 & j=3 & (0,16,9,24,11) \\
 & j=4 & (0,21,19,14,6)
\end{array}
$$

$$
\begin{array}{lll}
k=2 & j=0 & (0,2,3,3,2) \\
 & j=1 & (0,7,13,18,22) \\
 & j=2 & (0,12,23,8,17) \\
 & j=3 & (0,17,8,23,12) \\
 & j=4 & (0,22,18,13,7)
\end{array}
$$

$$
\begin{array}{lll}
k=3 & j=0 & (0,3,2,2,3) \\
 & j=1 & (0,8,12,17,23) \\
 & j=2 & (0,13,22,7,18) \\
 & j=3 & (0,18,7,22,13) \\
 & j=4 & (0,23,17,12,8)
\end{array}
$$

$$\begin{array}{lll} k=4 & j=0 & (0,4,1,1,4) \\ & j=1 & (0,9,11,16,24) \\ & j=2 & (0,14,21,6,19) \\ & j=3 & (0,19,6,21,14) \\ & j=4 & (0,24,16,11,9) \end{array}$$

with parameters $(25 \times 5, 5, 1, 2)$.

5.3.2 Hyperbolic families

Theorem 39. *(Moreno and Ortiz) Applying Method B to the Hyperbolic array with* $f(x) = \frac{k}{x}$ *we obtain a family of OOC with parameters* $(n = p^2 \times p, \omega = p-1, \lambda_a = 2, \lambda_c = 1)$*, periodicity* $p^2 \times p$ *and* $\Phi = p$*. And a family of OOCs with parameters* $(p^i \times p, p-1, 2)$*, periodicity* $p^i \times p$*, and* $\Phi = p^{i-1}$*.*

Proof. Following Method B with $r = p$, the new column size of the DPA is p^2, because of the modular addition, and the family size is p. When applied recursively the column size of the DPA increase to p^i, and the family size is p^{i-1}.

The auto- and cross-correlation properties are given by Theorem 33 and Theorem 34 respectively. □

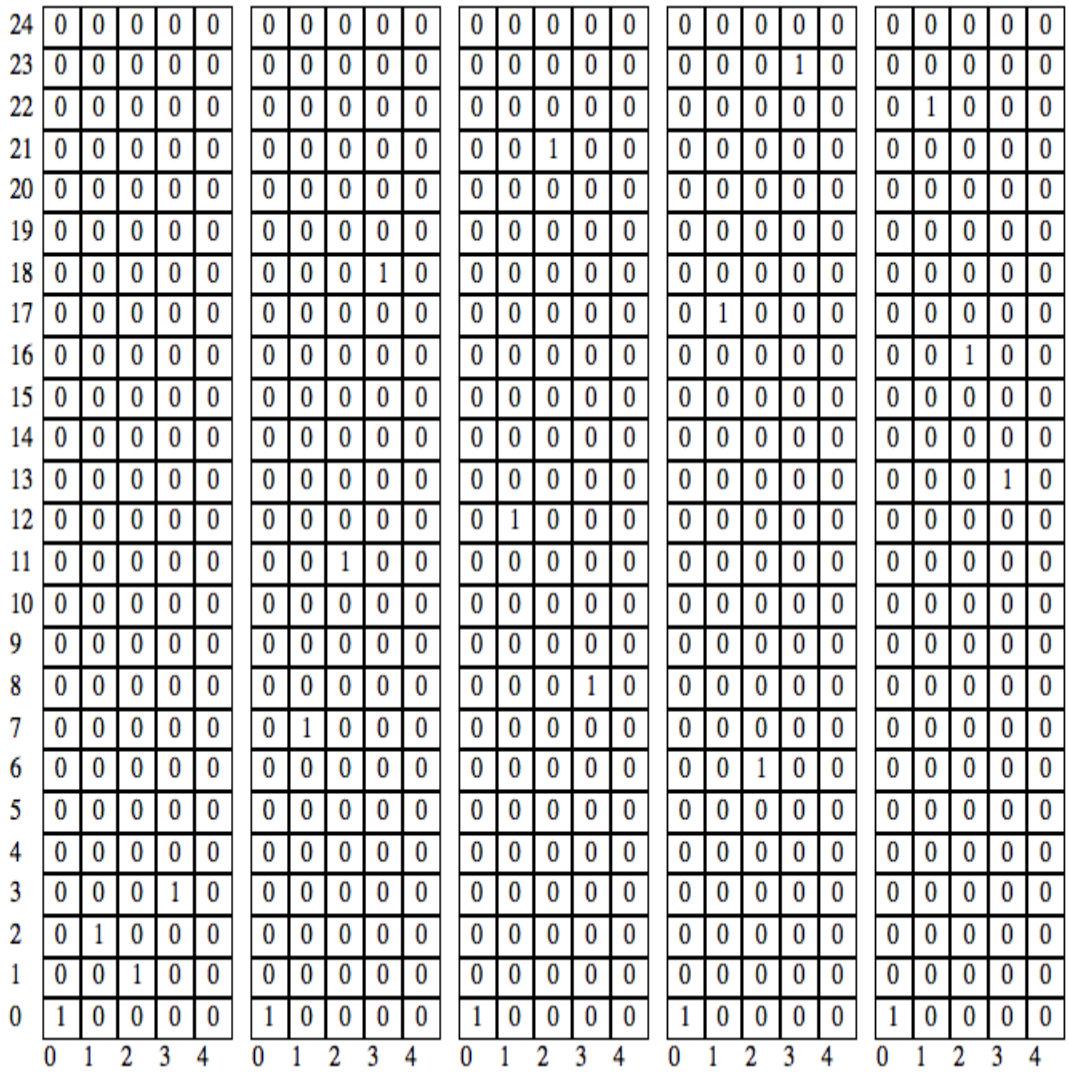


Figure 5–4: 25x5 Hyperbolic DPA family after applying Method B.

Example. *Let $p = 5$ and $k = 1$, the new DPA family obtained from applying Method B to the Hyperbolic array (1, 3, 2,4, *) = (0, 2, 1, 3, *) is:*

$$\begin{aligned} for \quad j = 0 \quad & (0, 2, 1, 3, *) \\ for \quad j = 1 \quad & (0, 7, 11, 18, *) \\ for \quad j = 2 \quad & (0, 12, 21, 8, *) \\ for \quad j = 3 \quad & (0, 17, 6, 23, *) \\ for \quad j = 4 \quad & (0, 22, 16, 13, *) \end{aligned}$$

with parameters $(25 \times 5, 4, 2, 1)$.

Theorem 40. *(Moreno and Ortiz) Applying Method B to the Hyperbolic family with $f(x) = \frac{k}{x}$ we obtain a family of OOC with parameters $(n = p^2 \times p, \omega = p-1, \lambda = 2)$, periodicity $p^2 \times p$ and $\Phi = ((p-1) \times p)$. And a family of OOCs with parameters $(p^i \times p, p-1, 2)$, periodicity $p^i \times p$, and $\Phi = (p-1)p^{i-1}$.*

Proof. Following Method B with $r = p$, the new column size of the DPA is p^2, because of the modular addition, and the family size is $p - 1$ codewords from the original family times p. When applied recursively the column size of the DPA increase to p^i, and the family size increases to p^{i-1}.

The auto- and cross-correlation properties are given by Theorem 33 and Theorem 36 respectively. □

5.3.3 Welch families

Theorem 41. *(Moreno and Ortiz) Applying Method B to the Welch array with $\alpha_k = \alpha^k (mod\ p), 1 \leq k \leq p-1$ we obtain a family of OOCs with parameters $(n = p^2 \times (p-1), \omega = p-1, \lambda = 1)$, periodicity $p^2 \times (p-1)$ and $\Phi = (p)$. And a family of OOCs with parameters $(n = p^i \times (p-1), \omega = p-1, \lambda = 1)$, periodicity $p^i \times (p-1)$ and $\Phi = p^{i-1}$.*

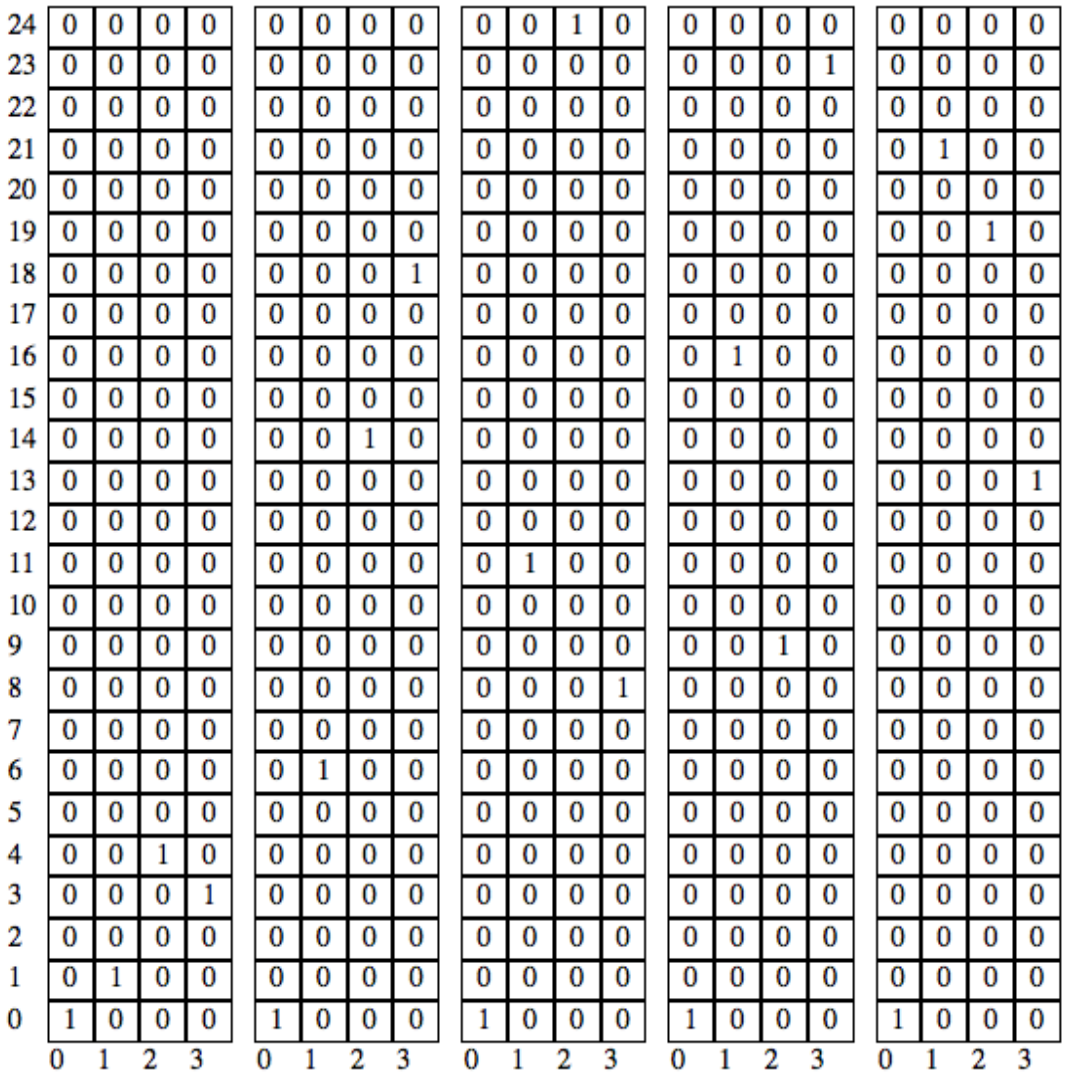


Figure 5–5: 25x4 Welch DPA family after applying Method B.

Proof. Following Method B with $r = p$, the new column size of the DPA is p^2, because of the modular addition, and the family size is p. When applied recursively the column size of the DPA increase to p^i, and the family size increases to p^{i-1}.

The auto- and cross-correlation properties are given by Theorem 33 and Theorem 35 respectively. □

Example. *Let $p = 5$ and $\alpha = 3$, the new DPA family obtained from applying Method B to the Welch array (3, 4, 2, 1) = (0, 1, 4, 3) is:*

$$\begin{aligned} for \quad j = 0 \quad & (0, 1, 4, 3) \\ for \quad j = 1 \quad & (0, 6, 14, 18) \\ for \quad j = 2 \quad & (0, 11, 24, 8) \\ for \quad j = 3 \quad & (0, 16, 9, 23) \\ for \quad j = 4 \quad & (0, 21, 19, 13) \end{aligned}$$

with parameters $(25 \times 4, 4, 1)$.

5.3.4 Lempel-Golomb families

Theorem 42. *(Moreno and Ortiz) Let $q = 2^n$, $n \in \mathbb{N}$ and $q-1$ is a Mersenne prime. Applying Method B to the Lempel-Golomb construction we obtain a family of OOCs with parameters $((q-1)^2 \times (q-1), q-2, 1)$ periodicity $(q-1)^2 \times (q-1)$, and $\Phi = q-1$. And a family of OOCs with parameters $(n = (q-1)^i \times (q-1), \omega = q-2, \lambda = 1)$, periodicity $(q-1)^i \times (q-1)$ and $\Phi = (q-1)^{i-1}$, for $i > 1$ and $i \in \mathbb{N}$.*

Proof. Following Method B with $r = (q-1)$, the new column size of the DPA is $(q-1)^2$, because of the modular addition, and the family size is $q-1$. When applied recursively the column size of the DPA increase to $(q-1)^i$, and the family size increases to $(q-1)^{i-1}$.

The auto- and cross-correlation properties are given by Theorem 33 and Theorem 35 respectively. □

Theorem 43. *(Moreno and Ortiz) Let $(q-2)$, and q be twin primes. Applying Method B to the Lempel-Golomb construction we obtain a family of OOCs with parameters $((q-2)(q-1) \times (q-1), q-2, 1)$ periodicity $(q-2)(q-1) \times (q-1)$, and $\Phi = q-2$. And a family of OOCs with parameters $(n = (q-2)^{i-1}(q-1) \times (q-1), \omega =$*

$q-2, \lambda=1)$, *periodicity* $(q-2)^{i-1}(q-1) \times (q-1)$ *and* $\Phi=(q-2)^{i-1}$, *for* $i>1$ *and* $i \in \mathbb{N}$.

Proof. Following Method B with $r=q-2$, the new column size of the DPA is $(q-2)(q-1)$, because of the modular addition, and the family size is $q-2$. When applied recursively the column size of the DPA increase to $(q-2)^{i-1}(q-1)$, and the family size increases to $(q-2)^{i-1}$.

The auto- and cross-correlation properties are given by Theorem 33 and Theorem 35 respectively. □

Theorem 44. *(Moreno and Ortiz) Let* $q=p$. *Applying Method B to the Lempel-Golomb construction we obtain a family of OOCs with parameters* $(p(p-1) \times (p-1), p-2, 1)$ *periodicity* $p(p-1) \times (p-1)$, *and* $\Phi=p$. *And a family of OOCs with parameters* $(n=p^{i-1}(p-1) \times (p-1), \omega=p-2, \lambda=1)$, *periodicity* $p^i(p-1) \times (p-1)$ *and* $\Phi=p^i$, *for* $i \geq 1$ *and* $i \in \mathbb{N}$.

Proof. Following Method B with $r=p$, the new column size of the DPA is $p(p-1)$, because the modular addition, and the family size is p. When applied recursively the column size of the DPA increase to $p^{i-1}(p-1)$, and the family size increases to p^i.

The auto- and cross-correlation properties are given by Theorem 33 and Theorem 35 respectively. □

Theorem 45. *(Moreno and Ortiz) Let* p *be a prime such that greatest common divisor:* $gcd(p, (\omega-1)!)$. *Applying Method B to the Lempel-Golomb construction we obtain a family of OOCs with parameters* $(p(q-1) \times (q-1), q-2, 1)$ *periodicity* $p(q-1) \times (q-1)$, *and* $\Phi=p$. *And a family of OOCs with parameters* $(n=p^i(q-1) \times (q-1), \omega=q-2, \lambda=1)$, *periodicity* $p^{i-1}(q-1) \times (q-1)$ *and* $\Phi=p^i$, *for* $i \geq 1$ *and* $i \in \mathbb{N}$.

Proof. Following Method B with $r = p$, the new column size of the DPA is $p(q-1)$, because of the modular addition, and the family size is p. When applied recursively the column size of the DPA increase to $p^{i-1}(q-1)$, and the family size increases to p^i.

The auto- and cross-correlation properties are given by Theorem 33 and Theorem 35 respectively. □

Example. *Let $q = 7^1$, $\alpha = 3$, $\beta = 5$, and $r = 7$, the new DPA family obtained from applying Method B to the Lempel-Golomb array (1, 3, 4, 2, 5, *) = (0, 2, 3, 1, 4, *) is:*

$$
\begin{aligned}
for \quad j = 0 \quad & (0, 2, 3, 1, 4, *) \\
for \quad j = 1 \quad & (0, 8, 15, 19, 28, *) \\
for \quad j = 2 \quad & (0, 14, 27, 37, 10, *) \\
for \quad j = 3 \quad & (0, 20, 39, 13, 34, *) \\
for \quad j = 4 \quad & (0, 26, 9, 31, 16, *) \\
for \quad j = 5 \quad & (0, 32, 21, 7, 40, *) \\
for \quad j = 6 \quad & (0, 38, 33, 25, 22, *)
\end{aligned}
$$

with parameters $(42 \times 6, 5, 1)$.

5.3.5 Moreno-Maric families

Theorem 46. *(Moreno and Ortiz) Let p be a prime such that greatest common divisor: $gcd(p, q!)$. Applying Method B to a Moreno-Maric array we obtain a family of OOCs with parameters $(p(q+1) \times (q+1), q+1, 2)$ periodicity $p(q+1) \times (q+1)$, and $\Phi = p$. And a family of OOCs with parameters $(n = p^i(q+1) \times (q+1), \omega = q+1, \lambda = 2)$, periodicity $(p)^i(q+1) \times (q+1)$ and $\Phi = p^i$, for $i \geq 1$ and $i \in \mathbb{N}$.*

Proof. Following Method B with $r = p$, the new column size of the DPA is $p(q+1)$, because of the modular addition, and the family size is p . When applied recursively the column size of the DPA increase to $p^i(q+1)$, and the family size increases to p^i.

The auto- and cross-correlation properties are given by Theorem 33 and Theorem 34 respectively. □

Example. *Let* $q = 7^1$, $\alpha = 3$, *and* $r = 11$, *the new DPA family obtained from applying Method B to the Moreno-Maric array (0, 4, 3, 6, 5, 1, 2, 7) is:*

$$
\begin{aligned}
&for \quad j = 0 \quad (0, 4, 3, 6, 5, 1, 2, 7)\\
&for \quad j = 1 \quad (0, 12, 19, 30, 37, 41, 50, 63)\\
&for \quad j = 2 \quad (0, 20, 35, 54, 69, 81, 10, 31)\\
&for \quad j = 3 \quad (0, 28, 51, 78, 13, 33, 58, 87)\\
&for \quad j = 4 \quad (0, 36, 67, 14, 45, 73, 18, 55)\\
&for \quad j = 5 \quad (0, 44, 83, 38, 77, 25, 66, 23)\\
&for \quad j = 6 \quad (0, 52, 11, 62, 21, 65, 26, 79)\\
&for \quad j = 7 \quad (0, 60, 27, 86, 53, 17, 74, 47)\\
&for \quad j = 8 \quad (0, 68, 43, 22, 85, 57, 34, 15)\\
&for \quad j = 9 \quad (0, 76, 59, 46, 29, 9, 82, 71)\\
&for \quad j = 10 \quad (0, 84, 75, 70, 61, 49, 42, 39)
\end{aligned}
$$

with parameters $(88 \times 8, 8, 2)$.

Theorem 47. *(Moreno and Ortiz) Let* p *be a prime such that greatest common divisor:* $gcd(p, q!)$. *Applying Method B to a Moreno-Maric family we obtain a family of OOCs with parameters* $(p(q+1) \times (q+1), q+1, 2)$ *periodicity* $p(q+1) \times (q+1)$, *and* $\Phi = (q-1)p$. *And a family of OOCs with parameters* $(n = p^i(q+1) \times (q+1), \omega = q+1, \lambda = 2)$, *periodicity* $p^i(q+1) \times (q+1)$ *and* $\Phi = (q-1)p^i$, *for* $i \geq 1$ *and* $i \in \mathbb{N}$.

Proof. Following Method B with $r = p$, the new column size of the DPA is $p(q+1)$, because of the modular addition, and the family size is $(q-1)$ codewords from the original family times p. When applied recursively the column size of the DPA increase to $p^i(q+1)$, and the family size increases to $(q-1)p^i$.

The auto- and cross-correlation properties are given by Theorem 33 and Theorem 36 respectively. □

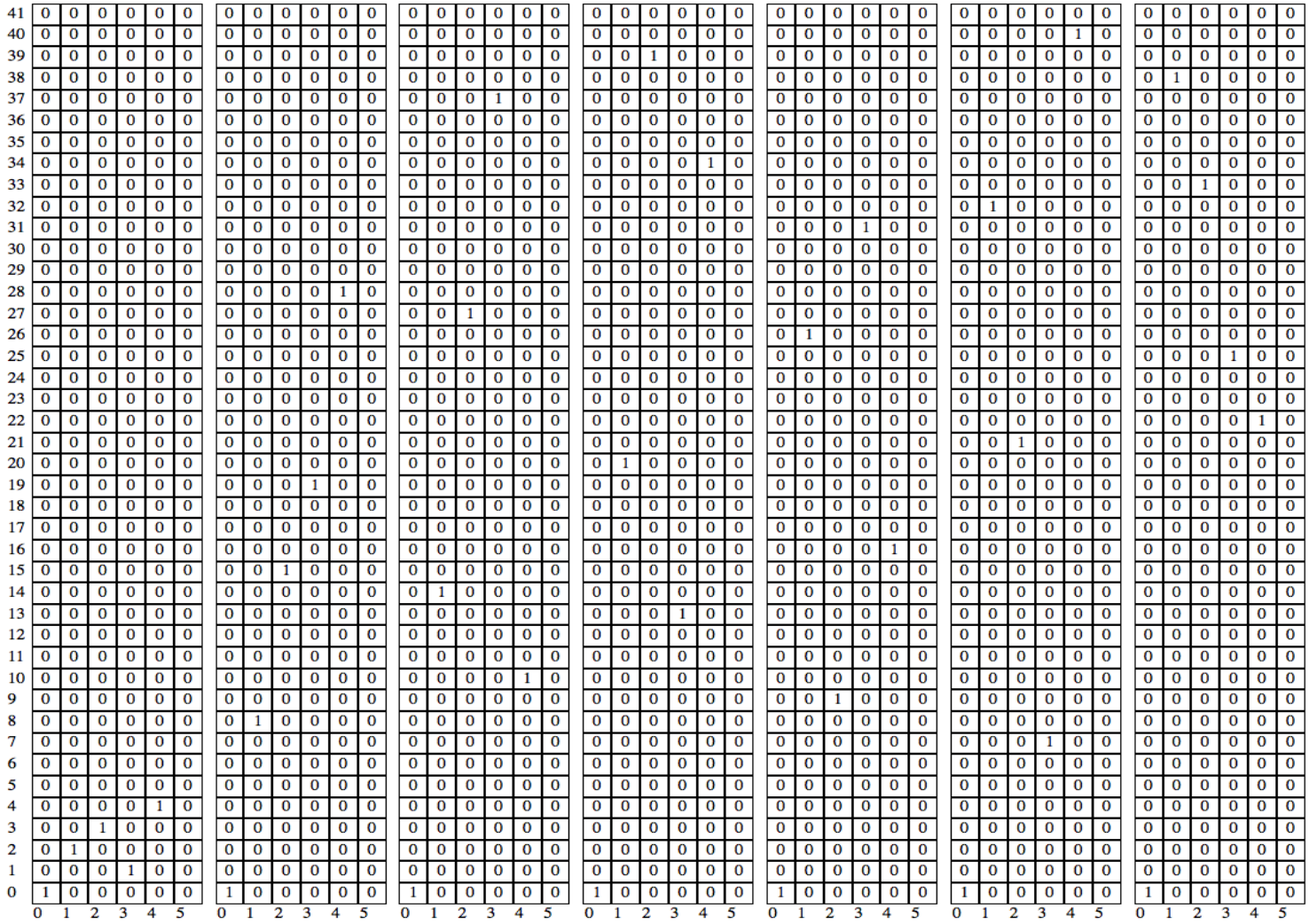


Figure 5–6: 42x6 Lempel-Golomb DPA family after applying Method B.

5.4 Optimal GPCWC constructions

Theorem 48. *(Moreno and Ortiz) The $(p \times p^i, p, 1)$ GPCWC with family size p^{i-1}, obtained after applying Method B to a quadratic array is optimal with respect to the generalization of the Johnson Bound modification for non-binary GPCWC Theorem 20.*

Proof. Using the Johnson Bound modification for non-binary GPCWC Theorem 20.

$$\Phi(p \times p^i, p, 1) \leq \left\lfloor \frac{1}{p} \left\lfloor \frac{p^i(p-1)}{p-1} \right\rfloor \right\rfloor \leq \left\lfloor \frac{p^i}{p} \right\rfloor \leq p^{i-1}$$

Therefore the $(p \times p^i, p, 1)$ GPCWC with family size p^{i-1} is optimal with respect to the generalization of the Johnson Bound modification for non-binary GPCWC Theorem 20. □

Theorem 49. *(Moreno and Ortiz) The $((p-1) \times p^2, p-1, 1)$ GPCWC with family size p, obtained after applying Method B to a quadratic array is asymptotically optimal with respect to the generalization of the Johnson Bound modification for non-binary GPCWC Theorem 20.*

Proof. Using the Johnson Bound modification for non-binary GPCWC Theorem 20.

$$\begin{aligned}\Phi((p-1) \times p^2, p, 1) &\leq \left\lfloor \frac{1}{(p-1)} \left\lfloor \frac{p^2(p-2)}{p-2} \right\rfloor \right\rfloor \leq \left\lfloor \frac{p^2}{(p-1)} \right\rfloor \\ &= \left\lfloor \frac{p^2-1}{p-1} + \frac{1}{p-1} \right\rfloor = \left\lfloor (p+1) + \frac{1}{p-1} \right\rfloor = p+1\end{aligned}$$

To prove that it is asymptotically optimal:

$$\lim_{p \to \infty} \frac{p}{p+1} = 1$$

Therefore the $(p \times p^i, p, 1)$ GPCWC with family size p^{i-1} is optimal with respect to the generalization of the Johnson Bound modification for non-binary GPCWC Theorem 20. □

5.5 Chapter Summary

In this chapter we presented a method to increase the family size of double periodic arrays with optimal correlation (Method B). This construction increase the size of the family of DPAs without changing the original correlation value, and the maximum cross-correlation value is 2 if the original correlation value is more than one. We apply this method to well known families of double-periodic arrays like the Quadratic, Hyperbolic, Welch, Lempel-Golomb, and Moreno-Maric constructions. Using this method we obtain optimal constructions in the size of the families with respect to the improvement to the Johnson Bound A for Group Permutable Constant Weight Codes. Table 5.5 is a summary of the new DPAs that we obtain by using our Method B. Table 5.5 is a summary of the new DPAs that we obtain by applying Method B recursively.

These codes have applications in 1-D Optical Orthogonal Codes, 2-D Optical Orthogonal Codes, and Digital Watermarking. The codes in section 5.1 and the Welch code in section 5.3 are 1-D Optical Orthogonal Codes by using the Chinese Remainder Theorem to arrange them in one dimension. All the codes in this chapter can be used for application of 2-D Optical Orthogonal Codes. Also they can be used in Digital Watermarking but they are not optimal for the application. We can make these constructions optimal for Digital Watermarking if we finding column sequences of size p^i and then apply the Weight Increasing Method (Method A) on them. This remain as part of our future work.

Table 5–1: New Constructions Summary $i = 2$

Construction	**Periodicity**	ω	Φ	λ_a	λ_c
Quadratic	$p^2 \times p$	p	p	1	1
Quadratic $k = 1 \ldots p-1$	$p^2 \times p$	p	$p \times (p-1)$	1	2
Hyperbolic	$p^2 \times p$	$(p-1)$	p	2	1
Hyperbolic $k = 1 \ldots p-1$	$p^2 \times p$	$(p-1)$	$p \times (p-1)$	2	2
Welch	$p^2 \times (p-1)$	$(p-1)$	p	1	1
Lempel-Golomb Mersenne Prime	$(q-1)^2 \times (q-1)$	$(q-2)$	$q-1$	1	1
Lempel-Golomb Twin Primes	$(q-2)(q-1) \times (q-1)$	$(q-2)$	$q-2$	1	1
Lempel-Golomb q prime	$p \times (p-1) \times (p-1)$	$(p-2)$	p	1	1
Lempel-Golomb	$p \times (q-1) \times (q-1)$	$q-2$	p	1	1
Moreno-Maric	$p(q+1) \times (q+1)$	$q+1$	p	2	2
Moreno-Maric family	$p(q+1) \times (q+1)$	$q+1$	$(q-1)p$	2	2

Table 5–2: New Constructions Summary $i > 1$

Construction	**Periodicity**	ω	Φ	λ_a	λ_c
Quadratic	$p^i \times p$	p	p^{i-1}	1	1
Quadratic $k = 1 \ldots p-1$	$p^i \times p$	p	$(p-1)p^{i-1}$	1	2
Hyperbolic	$p^i \times p$	$(p-1)$	p^{i-1}	2	1
Hyperbolic $k = 1 \ldots p-1$	$p^i \times p$	$(p-1)$	$(p-1)p^{i-1}$	2	2
Welch	$p^i \times (p-1)$	$(p-1)$	p^{i-1}	1	1
Lempel-Golomb Mersenne Prime	$(q-1)^i \times (q-1)$	$(q-2)$	$(q-1)^{i-1}$	1	1
Lempel-Golomb Twin Primes	$(q-2)^{i-1}(q-1) \times (q-1)$	$(q-2)$	$(q-2)^{i-1}$	1	1
Lempel-Golomb q prime	$p^i \times (p-1) \times (p-1)$	$(p-2)$	p^i	1	1
Lempel-Golomb	$p^i \times (q-1) \times (q-1)$	$q-2$	p^i	1	1
Moreno-Maric	$p^i(q+1) \times (q+1)$	$q+1$	p^i	2	2
Moreno-Maric family	$p^i(q+1) \times (q+1)$	$q+1$	$(q-1)p^i$	2	2

CHAPTER 6
DOUBLE PERIODIC ARRAYS WITH UNEQUAL CORRELATION CONSTRAINTS ($\lambda_C < \lambda_A$)

Yang and Fuja [4] presented constructions of codes with unequal correlation constraints. Specifically for the case where $\lambda_c = 1 < \lambda_a = 2$. The auto- and cross-correlation properties are used for synchronization and user identification respectively. Fuja and Yang explained that with good cross-correlation we are able to deal with both synchronization and user identification. This is for the case were we can find constructions with a much better cross-correlation than auto-correlation.

The auto-correlation properties of an array are used for synchronization, to check if a sequence is unlike cyclic shifts of itself. While the cross-correlation properties are used to check if a sequence is unlike cyclic shifts of other distinct sequences, thus cross-correlation serves for synchronization and user identification. With better cross-correlation properties we are able to achieve a very important part of any frequency hopping communication which is user identification.

In previous sections we presented methods to increase the weight (Method A, Chapter 4) and to increase the family size (Method B, Section 5) of double-periodic arrays. The weight increasing method is used for security in digital watermarking; and we also use it to obtain families with $\lambda > 1$. The method to increase the family size increase the number of targets or users in any spread spectrum application.

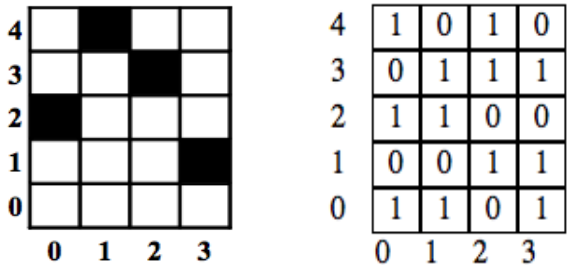
In this Chapter we combine both methods to construct new families of DPA with $\lambda_a > 1$ and $\lambda_c < \lambda_a$. This new method consist in applying the Weight Increasing

Method to a double-periodic construction to obtain new families with $\lambda_a > 1$, and then apply the method to increase the family size that results in new DPA families with $\lambda_c < \lambda_a$.[1] Here we apply our new method to the Quadratic, Hyperbolic, Welch, Lempel-Golomb, and Moreno-Maric DPA constructions. Section 6.1 uses the Moreno-Omrani-Maric method to increase the family size, and section 6.2 uses the general method.

6.1 Method to produce DPA families with Unequal Correlation Constraints using the CRT

We construct families of DPAs from a Welch Costas array using a Legendre sequence as the column sequence and applying the Moreno-Omrani-Maric construction.

Method C: (Ortiz and Moreno)First generate a Welch Costas array, replace the columns with a suitable periodic sequence using Method A, and finally apply the Moreno-Omrani-Maric construction to generate the new family of size $p+1$. See the next example for a detailed explanation.



(a) 5x4 Welch array

(b) 5x4 Welch array with binary column sequence

Figure 6–1: Example: 5x4 Welch array before and after Method A

Example. *Start with the Welch array with points* $(0,2),(1,4),(2,3)$, *and* $(4,1)$. *Using Method A, replace the columns of the matrix in that figure with the periodic sequence* $1,0,1,1,0$ *which is a binary Legendre sequence with auto-correlation 2.*

[1] The work presented in [32] is result of this thesis work, and introduce the new method to construct new families of DPAs with $\lambda_c < \lambda_a$.

Figure 6–1(a) is the Welch array before applying Method A, and figure 6–1(b) is the Welch array after applying Method A.

Now apply the Moreno-Omrani-Maric construction to the new matrix of size $p \times (p-1)$. *The Chinese Remainder for the points in the new matrix are* $(0,0) \to 0$, $(0,2) \to 12$, $(0,4) \to 4$, $(1,0) \to 5$, $(1,2) \to 17$, $(1,3) \to 13$, $(2,1) \to 6$, $(2,3) \to 18$, $(2,4) \to 14$, $(3,0) \to 15$, $(3,1) \to 11$, $(3,3) \to 3$.

From the CRT we obtain $D' = \{0, 3, 4, 5, 6, 11, 12, 13, 14, 15, 17, 18\}$. *Now following the Moreno-Omrani-Maric construction we obtain from* D'*:*

$$
\begin{aligned}
D_1 &= \{0, 3, 4, 5, 6, 11, 12, 13, 14, 15, 17, 18\} \\
D_2 &= \{0, 11, 17, 23, 32, 38, 44, 53, 65, 74, 86, 95\} \\
D_3 &= \{0, 11, 17, 25, 34, 43, 52, 58, 66, 75, 84, 93\} \\
D_4 &= \{0, 11, 17, 24, 33, 46, 55, 63, 72, 78, 85, 94\} \\
D_5 &= \{0, 11, 17, 26, 35, 45, 54, 64, 73, 83, 92, 98\}
\end{aligned}
$$

And multiplying D' *by 5:*

$$
D_6 = \{0, 15, 20, 25, 30, 55, 60, 65, 70, 75, 85, 90\}
$$

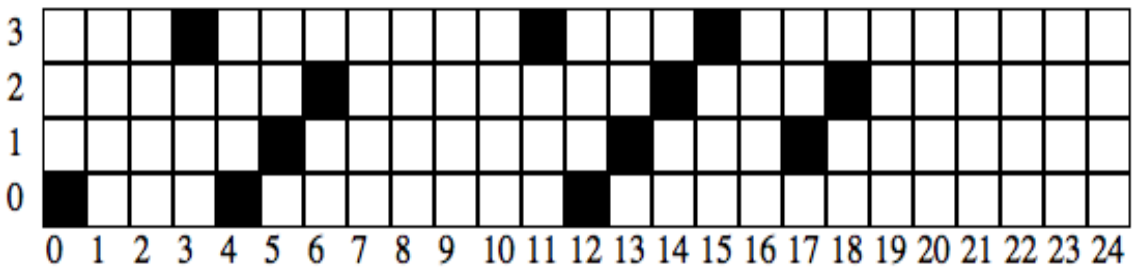


Figure 6–2: 4x25 Matrix Construction using a binary column sequence

Finally apply the CRT again to convert them to 4×25 *matrices. (see Figure 6–2)*

Theorem 50. *(Ortiz and Moreno) Method C applied to a Welch array of size* $p(p-1)$ *using a Legendre sequence as a column produces OOCs with parameters* $(n, \omega, \lambda) = (p^2(p-1), \frac{p^2-1}{2}, \lfloor \frac{p(p+1)}{4} \rfloor)$ *and family size* $p+1$.

Proof. The auto-correlation value of the new families of OOCs is the auto-correlation value obtained after applying Method A to the original Welch Array. Theorem 31 proves that the auto-correlation values does not change after applying the Moreno-Omrani-Maric construction.

□

In our example we construct code sequences with $(n, \omega, \lambda) = (4 \times 25, 12, 8, 4)$. This method produces families of DPAs with $\lambda_c < \lambda_a$. The cross-correlation properties can be proved similar to the proofs of Theorem 52 and Theorem 53.

On the next section we present a general method that works without the need of the CRT.

6.2 Method to produce DPA families with Unequal Correlation Constraints without using the CRT

Here we present a new method similar to Method C but this time we use the method to increase the size of a family of DPAs without using the Chinese Remainder Theorem (CRT).

Method C_2: (Ortiz and Moreno) First generate a double periodic array $(d_0, d_1, \ldots, d_{\omega-1})$ (See section 2.4), then using Method A replace the columns with a suitable periodic sequence s to increase the weight in the matrix and obtain the new matrix $[[s^{d_0}], [s^{d_1}], \ldots, [s^{d_{\omega-1}}]]$. Finally apply the method to increase the number of sequences of double periodic arrays as follows:

For each $D_{v\times n} = [[s^{d_0}], [s^{d_1}], \ldots, [s^{d_{\omega-1}}]]$, where $[s^{d_i}]$ is the new column sequences (shifted d_i times) used in Method A, generate the r different matrices $D^j_{vr\times n}$ such that if $(d_{i,k}) = 1$ then $(d^j_{i,k\oplus_{vr}ijv}) = 1$, for $0 \le j < r$, $0 \le k < v$, and $\oplus_{vr}$ represents addition modulo vr. See next example.

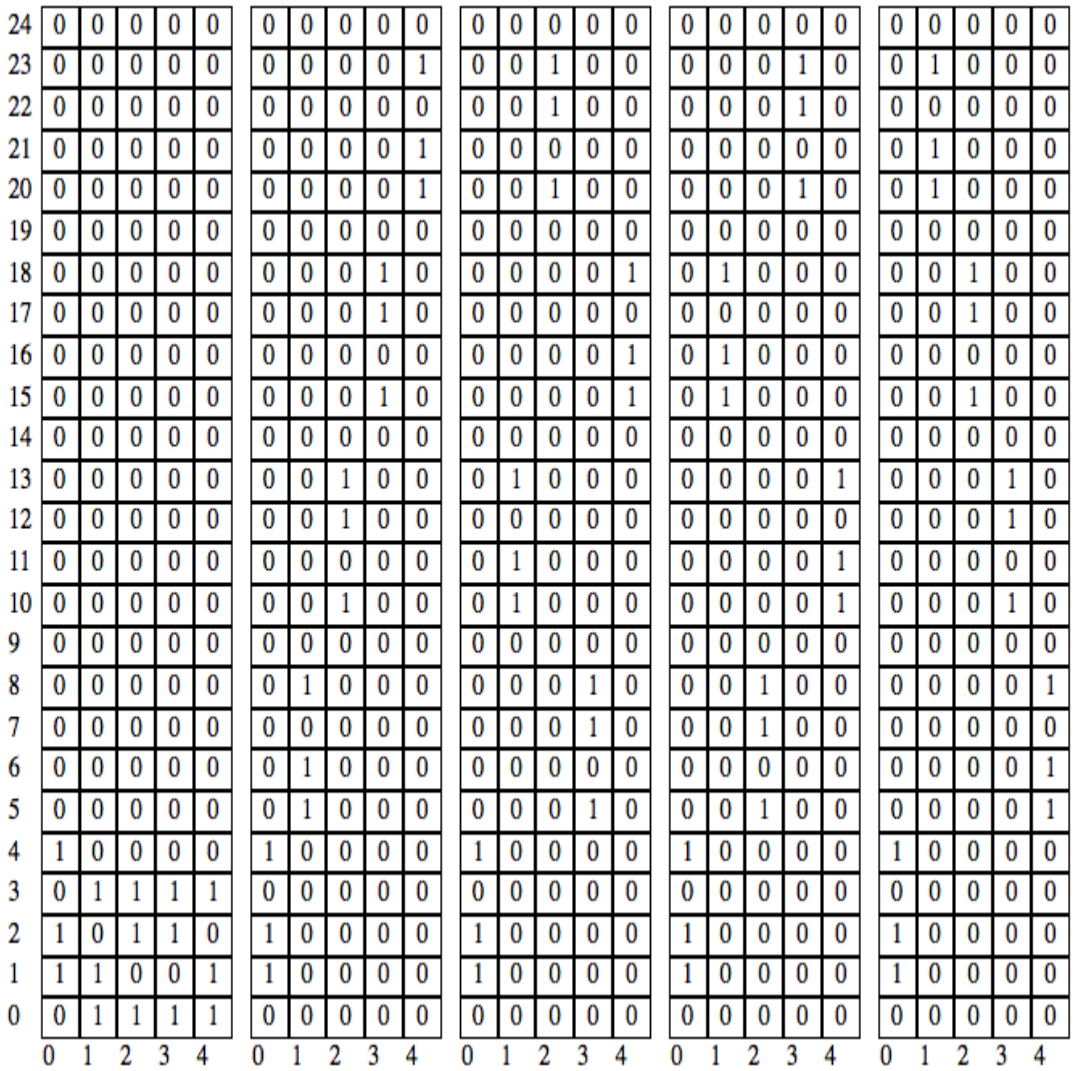


Figure 6–3: 25x5 Quadratic double-periodic family after applying Method C_2.

Example. *Start with the Welch array of Figure 5–1 with points* $(0,2),(1,4),(2,3)$, *and* $(4,1)$. *Using Method A (WIM) replace the columns of the matrix in that figure with the periodic sequence* $1,0,1,1,0$ *which is a binary Legendre sequence with auto-correlation 2. Figure 6–1(a) is the Welch array before applying Method A and figure 6–1(b) is the Welch array after applying Method A.*

Now apply the Method B to the matrix of size $p\times(p-1)$. *Following the Method B we obtain*

$$
\begin{aligned}
D_0 &= \{(0,1),(0,3),(0,4),(1,0),(1,2),(1,3),(2,0),(2,2),\\
&\quad (2,4),(3,0),(3,1),(3,3)\}\\
D_1 &= \{(0,1),(0,3),(0,4),(1,5),(1,7),(1,8),(2,10),(2,12),\\
&\quad (2,14),(3,15),(3,16),(3,18)\}\\
D_2 &= \{(0,1),(0,3),(0,4),(1,10),(1,12),(1,13),(2,20),(2,22),\\
&\quad (2,24),(3,5),(3,6),(3,8)\}\\
D_3 &= \{(0,1),(0,3),(0,4),(1,15),(1,17),(1,18),(2,5),(2,7),\\
&\quad (2,9),(3,20),(3,21),(3,23)\}\\
D_4 &= \{(0,1),(0,3),(0,4),(1,20),(1,22),(1,23),(2,15),(2,17),\\
&\quad (2,19),(3,10),(3,11),(3,13)\}
\end{aligned}
$$

Figure 6–3 is the graphical representation of applying Method C_2 to the Quadratic sonar of size $p = 5$.

Theorem 51. *(Ortiz and Moreno) Applying method C to a family of* $(v\times n, \omega, \lambda)-$*DPA A, produces a new family of* $(vr \times n, \omega, \lambda)$*-DPAs B with the same auto-correlation value as A.*

Note the proof is similar to the proof 33 for Method B auto-correlation. But in this theorem the difference values of the matrix M, is a set of differences because s^{d_i} and $s^{d_{i+c}}$ are column sequences with weight $\omega > 1$.

Proof. Let $D_{v\times n} = [[s^{d_0}], [s^{d_1}, \ldots, s^{d_{\omega-1}}]$ a $(v \times n, \omega, \lambda)$-DPA, applying Method C produces a family of arrays $D^j_{vr\times n}$ such that if $(d_{i,k}) = 1$ then $(d^j_{i,k\oplus_{vr}ivj}) = 1$.

Let M be the difference matrix for array $D_{v\times n}$ such that:

$$M_{i,i+c} = \{x - z \bmod v | (d_{i,x}) = 1 \text{ and } (d_{i+c,z}) = 1\}$$

$$M'_{i,i+c} = \{x + ijv - (z - (i+c)jv) \bmod vr | (d_{i,x}) = 1 \text{ and } (d_{i+c,z}) = 1\}$$

$$M'_{i,i+c} = \{(x - z) - jvc \bmod vr | (d_{i,x} \bmod vr) = 1 \text{ and } (d_{i+c,z}) = 1)\}$$

Therefore the differences in $M'_{i,i+c}$ are going to be the same in $M'_{i,i+c}$ or in another $M'_{j,j+c}$ if and only if they are also the same in $M_{i,i+c}$ or $M_{j,j+c}$.

□

Theorem 52. *(Ortiz and Moreno) Applying Method C to a $(v \times n, \omega, \lambda_a, \lambda_c)$-DPA A using a periodic sequence s with parameters (v, ω', λ'), produces a new family of $(vr \times n, \omega, \lambda_a, \lambda'_c)$-DPAs B with cross-correlation $\lambda'_c \leq 2\omega'$.*

Proof. Lets construct the difference matrix M' between any two arrays from B constructed with $j = r_1$ and $j = r_2$, $0 \leq r_1, r_2 < r$ such that:

$$M'_{i,i+c} = \{x + ivr_1 - (z + (i+c)vr_2) \bmod vr | (d_{x,i}) = 1 \text{ and } (d_{z,i+c}) = 1\}$$

$$M'_{i,i+c} = \{(x - z) + v(i(r_1 - ir_2) - cr_2) \bmod vr | (d_{x,i}) = 1 \text{ and } (d_{z,i+c}) = 1\}$$

The values $(r_1 - r_2)$ and $-cr_2$ are constants in $\mathbb{Z}_p$. Let $i' = i(r_1 - r_2) - cr_2$; as i varies i' cycles in $\mathbb{Z}_p$. Therefore the product $vi' \bmod vr$ for $i' \in \mathbb{Z}_p$ produces multiples of v modulo vr $\{0, v, 2v, \ldots, v(p-1)\}$.

Since $x, z \in \mathbb{Z}_v$ the equation $(x - z) + vi' \bmod vr$ produces values of the form $v' + v(i')$ for $v' = \{-v + 1, \ldots, -1, 0, 1, \ldots, v - 1\}$.

Therefore values of the difference $(x - z) + vi'$ can only be equal with values of other difference $(x' - z') + vj'$ iff:

$$(x - y) = (x' - z') \text{ and } v(i') = v(j') \iff i = j \tag{6.1}$$

or

$$(x' - z') = -((-(x - z)) \bmod v) \text{ and } v(j') = v(i' \pm 1) \tag{6.2}$$

i. e. $(x' - z') \bmod v = (x - z) \bmod v$.

Equation 6.1 implies that we are comparing the same column differences. In which case we can have at most ω' differences with the same value.

Equation 6.2 implies that the difference with column i can be equal to another difference with column j at most ω' times , because of the distance between the multiples vi' and vj'.

Therefore $\lambda'_c < 2\omega'$. □

Theorem 53. *(Ortiz and Moreno) Applying Method C to a family of $(v \times n, \omega, \lambda_a, \lambda_c)$-DPAs A using a periodic sequence s with parameters (v, ω', λ'), produces a new family of $(vr \times n, \omega, \lambda_a, \lambda'_c)$-DPAs B with cross-correlation $\lambda'_c \leq (n \times \lambda' + \lambda_c(\omega' - \lambda'))$.*

Proof. Proof is similar theorem 52. If the r_1 and r_2 used to construct any two arrays from family B are different $(r_1 \neq r_2)$, then the proof in theorem 52 applies.

Now lets construct the difference matrix M' between two arrays from B constructed with $j = r_1$, $0 \leq r_1 < r$ such that:

$$M'_{i,i+c} = \{x + ivr_1 - (z + (i + c)vr_2) \bmod vr | (d_{x,i}) = 1 \text{ and } (d_{z,i+c}) = 1\}$$

$$M'_{i,i+c} = \{(x - z) - vcr_2) \bmod vr | (d_{x,i}) = 1 \text{ and } (d_{z,i+c}) = 1\}$$

$-vcr_2$ is constant and therefore $M'_{i,i+c}$ is the same to another $M'_{j,j+c}$ if and only if in the difference matrix M, $M_{i,i+c} = M_{j,j+c}$. In which case the cross-correlation is $\lambda'_c \leq n \times \lambda' + \lambda_c(\omega' - \lambda')$.

Therefore $\lambda'_c \leq (n \times \lambda' + \lambda_c(\omega' - \lambda'))$ □

6.3 New families of Double Periodic Arrays with Unequal Constraints

Following Method C_2 we construct different families of arrays with increased weight and increased family size. The auto-correlation for the arrays in these new families is the same auto-correlation of the original arrays after applying the Weight

Increasing Method (Method A). Which for the Quadratic, Hyperbolic, and Welch constructions increase quadraticly with respect to the prime p. However with Theorem 52 we obtain that the cross-correlation of these new constructions increases linearly with respect of its weight, thereby producing constructions with cross-correlation lower than auto-correlation.

In general the following equation calculates the auto-correlation values of the construction after applying Method A, which is also kept after applying methods C and C_2:

$$\lambda' \times m + \lambda_a(\omega' - \lambda') \tag{6.3}$$

where λ' is the auto-correlation of the periodic column sequence, λ_a the original correlation of the double periodic array before applying Method A, ω' the weight of the column sequence, and m the number of columns with weight.

An interesting property of the following families is that $\lambda_c < \lambda_a$. Yang and Fuja [4] write about the importance of this sequences with $\lambda_c \neq \lambda_a$ and define family size bounds derived from the Johnson Bound, and the lower bound for odd prime n by Wei.

6.3.1 Quadratic families

Theorem 54. *(Ortiz and Moreno) Let $k, x \in \mathbb{Z}_p$. Then applying Method C_2 to a Quadratic array with $f(x) = kx^2$ we obtain a family of OOC with parameters $(p^2 \times p, \omega = \frac{(p^2+p)}{2}, \lambda_a \leq \frac{(p^2+p)}{4}, \lambda_c \leq p+1)$, periodicity $p^2 \times p$, and $\Phi = p$.*

Proof. The new weight of the DPA comes from applying Method A, and the new column size comes from the application of Method B.

The auto- and cross-correlation properties are given by Theorem 51 and Theorem 52 respectively. □

Example. *Let $p = 5$, $k = 1$, and the Legendre (1, 0, 1, 1, 0) the column sequence, the family for the Quadratic Construction is*

$$
\begin{aligned}
for \quad i = 0 \quad & \{(0,1),(0,2),(0,4),(1,0),(1,1),(1,3),(2,0),(2,2),(2,3),\\
& (3,0),(3,2),(3,3),(4,0),(4,1),(4,3)\}\\
for \quad i = 1 \quad & \{(0,1),(0,2),(0,4),(1,5),(1,6),(1,8),(2,10),(2,12),(2,13),\\
& (3,15),(3,17),(3,18),(4,20),(4,21),(4,23)\}\\
for \quad i = 2 \quad & \{(0,1),(0,2),(0,4),(1,10),(1,11),(1,13),(2,20),(2,22),(2,23),\\
& (3,5),(3,7),(3,8),(4,15),(4,16),(4,18)\}\\
for \quad i = 3 \quad & \{(0,1),(0,2),(0,4),(1,15),(1,16),(1,18),(2,5),(2,7),(2,8),\\
& (3,20),(3,22),(3,23),(4,10),(4,11),(4,13)\}\\
for \quad i = 4 \quad & \{(0,1),(0,2),(0,4),(1,20),(1,21),(1,23),(2,15),(2,17),(2,18),\\
& (3,10),(3,12),(3,13),(4,5),(4,6),(4,8)\}
\end{aligned}
$$

with parameters $(25 \times 5, 15, 9, 4)$. Figure 6–3 shows the graphical representation for the family in this example.

Theorem 55. *(Ortiz and Moreno) Let $k, x \in \mathbb{Z}_p$, $k \ldots p-1$. Then applying Method C_2 to the Quadratic family with $f(x) = kx^2$ we obtain a family of OOC with parameters $(p^2 \times p, \omega = \frac{(p^2+p)}{2}, \lambda_a \leq \frac{(p^2+p)}{4}, \lambda_c \leq \frac{(p^2+3p+2)}{4})$, periodicity $p^2 \times p$, and $\Phi = p \times (p-1)$.*

Proof. The new weight of the DPA comes from applying Method A, and the new column size comes from the application of Method B.

The auto- and cross-correlation properties are given by Theorem 51 and Theorem 53 respectively. □

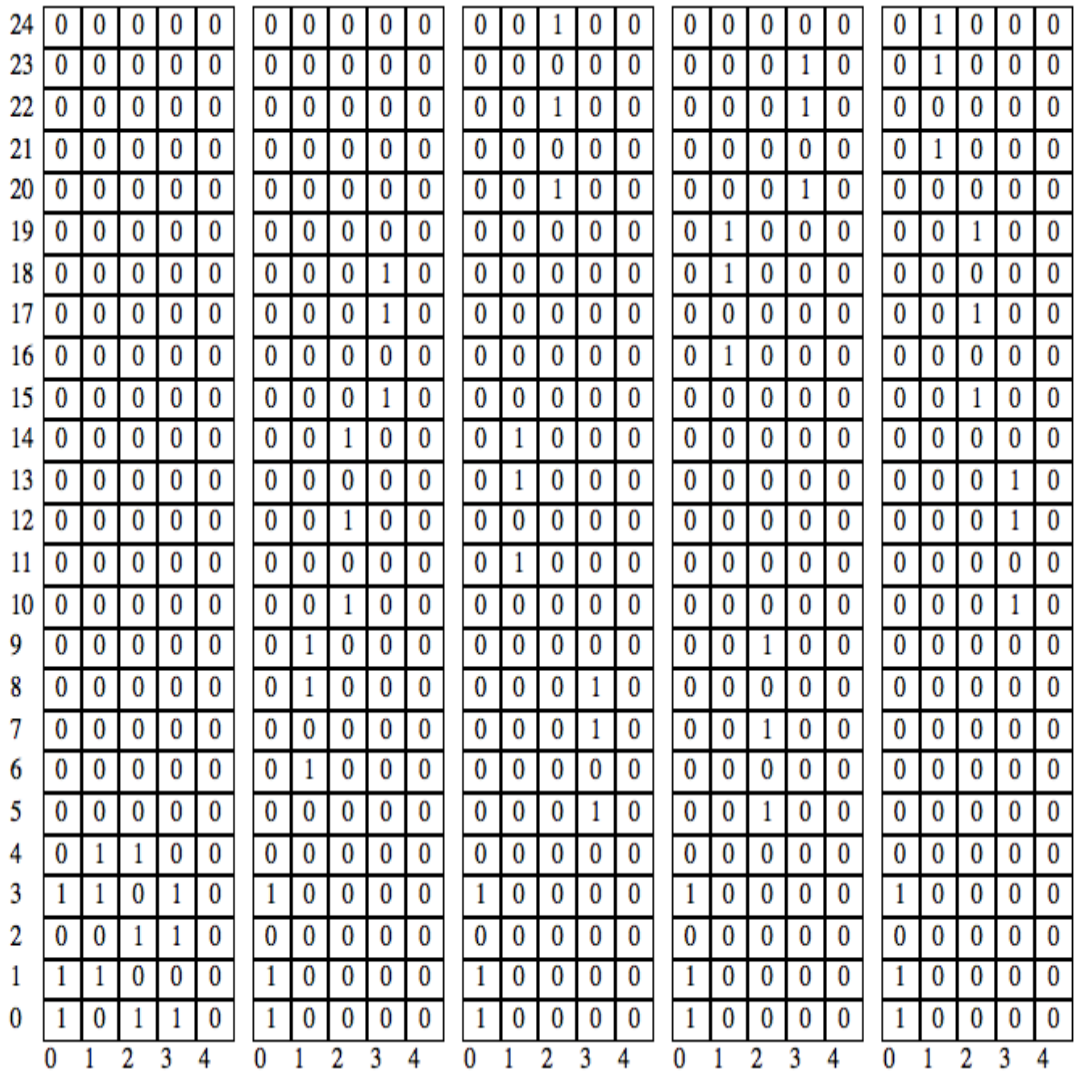


Figure 6–4: 25x5 Hyperbolic double-periodic family after applying Method C_2.

6.3.2 Hyperbolic families

Theorem 56. *(Ortiz and Moreno) Let $k, x \in \mathbb{Z}_p$, $x = 1 \ldots p-1$, $k \neq 0$. Then applying Method C_2 to an Hyperbolic array with $f(x) = \frac{k}{x}$ we obtain a family of OOC with parameters $(n = p^2 \times p, \omega = \frac{(p^2-1)}{2}, \lambda_a \leq \frac{(p^2+p)}{4}, \lambda_c \leq p+1)$, periodicity $p^2 \times p$ and $\Phi = p$.*

Proof. The new weight of the DPA comes from applying Method A, and the new column size comes from the application of Method B.

The auto- and cross-correlation properties are given by Theorem 51 and Theorem 52 respectively. □

Theorem 57. *(Ortiz and Moreno) Let $k, x \in \mathbb{Z}_p$, $k, x = 1 \ldots p-1$. Then applying Method C_2 to the Hyperbolic family with $f(x) = \frac{k}{x}$ we obtain a family of OOC with parameters $(n = p^2 \times p, \omega = \frac{(p^2-1)}{2}, \lambda \leq \frac{(p^2+p)}{4})$, periodicity $p^2 \times p$ and $\Phi = p \times (p-1)$.*

Proof. The new weight of the DPA comes from applying Method A, and the new column size comes from the application of Method B.

The auto- and cross-correlation properties are given by Theorem 51 and Theorem 53 respectively. □

6.3.3 Welch families

Theorem 58. *Let α be a primitive root of an odd prime p. Then applying Method C_2 to the Welch array with $\alpha_k = \alpha^k (mod\, p), 1 \leq k \leq p-1$ we obtain a family of OOCs with parameters $(n = p^2 \times p - 1, \omega = \frac{(p^2-1)}{2}, \lambda_a = \frac{(p^2+p)}{4}, \lambda_c \leq p+1)$, periodicity $p^2 \times (p-1)$ and $\Phi = p$.*

Proof. The new weight of the DPA comes from applying Method A, and the new column size comes from the application of Method B.

The auto- and cross-correlation properties are given by Theorem 51 and Theorem 52 respectively. □

24	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0
22	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
18	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0
16	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0
14	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1
12	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
10	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	1
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
8	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0
7	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
5	0	0	0	0	0	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0
4	1	0	1	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0
3	1	1	0	1	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0
2	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	1	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0
0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3

Figure 6–5: 25x4 Welch double-periodic family after applying Method C_2.

6.3.4 Lempel-Golomb families

For the next Lempel-Golomb constructions review definition 4. For the Lempel-Golomb constructions we give auto-correlation values independent of the column sequence used. Column sequences of size $(q-1)$ should be used in all cases. To understand the expected auto-correlation value given in the following definitions, recall that ω' is the weight of the column sequence, and λ' is the auto-correlation value of the column sequence.

Theorem 59. *(Ortiz and Moreno) Let $q = 2^n$, $n \in \mathbb{N}$ and $q-1$ is a Mersenne prime. Applying Method C_2 to the Lempel-Golomb construction we obtain a family*

of OOCs with parameters $((q-1)^2 \times (q-1), (q-2)\omega', \lambda_a = \lambda'(q-3)+\omega', \lambda_c \leq 2\omega')$ *periodicity* $(q-1)^2 \times (q-1)$, *and* $\Phi = q-1$.

Proof. The new weight of the DPA comes from applying Method A, and the new column size comes from the application of Method B.

The auto- and cross-correlation properties are given by Theorem 51 and Theorem 52 respectively. □

Theorem 60. *(Ortiz and Moreno) Let* $(q-2)$, *and* q *be twin primes. Applying Method* C_2 *to the Lempel-Golomb construction we obtain a family of OOCs with parameters* $((q-2)(q-1)\times(q-1), (q-2)\omega', \lambda_a = \lambda'(q-3)+\omega', \lambda_c \leq 2\omega')$ *periodicity* $(q-2)(q-1) \times (q-1)$, *and* $\Phi = q-2$.

Proof. The new weight of the DPA comes from applying Method A, and the new column size comes from the application of Method B.

The auto- and cross-correlation properties are given by Theorem 51 and Theorem 52 respectively. □

Theorem 61. *(Ortiz and Moreno) Let* $q = p$. *Applying Method* C_2 *to the Lempel-Golomb construction we obtain a family of OOCs with parameters* $(p(p-1) \times (p-1), (p-2)\omega', \lambda_a = \lambda'(p-3)+\omega', \lambda_c \leq 2\omega')$ *periodicity* $p(p-1) \times (p-1)$, *and* $\Phi = p$.

Proof. The new weight of the DPA comes from applying Method A, and the new column size comes from the application of Method B.

The auto- and cross-correlation properties are given by Theorem 51 and Theorem 52 respectively. □

Theorem 62. *(Ortiz and Moreno) Let* p *be a prime such that* $gcd(p, (\omega-1)!)$. *Applying Method* C_2 *to the Lempel-Golomb construction we obtain a family of OOCs with parameters* $(p(q-1)\times(q-1), (q-2)\omega', \lambda_a = \lambda'(q-3)+\omega', \lambda_c \leq 2\omega')$ *periodicity* $p(q-1) \times (q-1)$, *and* $\Phi = p$.

Proof. The new weight of the DPA comes from applying Method A, and the new column size comes from the application of Method B.

The auto- and cross-correlation properties are given by Theorem 51 and Theorem 52 respectively. □

6.3.5 Moreno-Maric families

Theorem 63. *(Ortiz and Moreno) Let p be a prime such that greatest common divisor: $gcd(p, q!)$. Applying Method C_2 to a Moreno-Maric array we obtain a family of OOCs with parameters $(p(q+1)\times(q+1), (q+1)\omega', \lambda'(q-1)+2\omega', 2\omega')$ periodicity $p(q+1)\times(q+1)$, and $\Phi = p$.*

Proof. The new weight of the DPA comes from applying Method A, and the new column size comes from the application of Method B.

The auto- and cross-correlation properties are given by Theorem 51 and Theorem 52 respectively. □

Theorem 64. *(Ortiz and Moreno) Let p be a prime such that greatest common divisor: $gcd(p, q!)$. Applying Method C_2 to a Moreno-Maric array we obtain a family of OOCs with parameters $(p(q+1)\times(q+1), (q+1)\omega', \lambda'(q-1)+2\omega', \lambda'(q-1)+2\omega')$ periodicity $p(q+1)\times(q+1)$, and $\Phi = p(q-1)$.*

Proof. The new weight of the DPA comes from applying Method A, and the new column size comes from the application of Method B.

The auto- and cross-correlation properties are given by Theorem 51 and Theorem 53 respectively. □

6.4 Chapter Summary

Chapter 6 presents a combination of the Weight Increasing Method of DPAs (Method A) from Chapter 4 and the method to increase the size of families (Method B) from Chapter 5 to produce new families of double periodic constructions with

increased family size and weight (Method C). When Method C is applied to a double periodic array we obtain new families of double periodic arrays with unequal correlation constrains. More specifically, we obtain new families of double periodic arrays with cross-correlation much lower than auto-correlation ($\lambda_c < \lambda_a$). As explained by Fuja and Yang with good cross-correlation we are able to deal with both synchronization and user identification. Table 6.4 is a summary of the new DPAs with correlation value more than one ($\lambda > 1$) that we obtain by applying Method C to well known DPA families. Table 6.4 is a summary of the new DPAs that we obtain after applying Method C with unequal correlation constrains ($\lambda_c < \lambda_a$).

These codes have applications in 1-D Optical Orthogonal Codes, 2-D Optical Orthogonal Codes , and Digital Watermarking. For Digital Watermarking these families are not optimal because the weight of the families is not balanced with respect to the length of the array. The codes in section 6.1 and the Welch code in section 6.2 are 1-D Optical Orthogonal Codes by using the Chinese Remainder Theorem to arrange them in one dimension. All the codes in this chapter can be used for application of 2-D Optical Orthogonal Codes.

Table 6–1: New DPA families Summary with Method C applied to a family of DPA with $\Phi > 1$

Construction	**Periodicity**	ω	Φ	λ_a	λ_c
Quadratic	$p^2 \times p$	$\frac{(p^2+p)}{2}$	p	$\frac{(p+1)^2}{4}$	$p+1$
Quadratic $k = 1 \ldots p-1$	$p^2 \times p$	$\frac{(p^2+p)}{2}$	$p \times (p-1)$	$\frac{(p+1)^2}{4}$	$\frac{(p^2+3p+2)}{4}$
Hyperbolic	$p^2 \times p$	$\frac{(p^2-1)}{2}$	p	$\frac{(p+1)^2}{4}$	$p+1$
Hyperbolic $k = 1 \ldots p-1$	$p^2 \times p$	$\frac{(p^2-1)}{2}$	$p \times (p-1)$	$\frac{(p+1)^2}{4}$	$\frac{(p^2+p)}{4}$
Welch	$p^2 \times (p-1)$	$\frac{(p^2-1)}{2}$	p	$\frac{(p^2+p)}{4}$	$p+1$
Lempel-Golomb Mersenne Prime	$(q-1)^2 \times (q-1)$	$(q-2)\omega'$	p	$\lambda'(q-3)+\omega'$	$2\omega'$
Lempel-Golomb Twin Primes	$(q-2)(q-1) \times (q-1)$	$(q-2)\omega'$	p	$\lambda'(q-3)+\omega'$	$2\omega'$
Lempel-Golomb q prime	$p(p-1) \times (p-1)$	$(p-2)\omega'$	p	$\lambda'(p-3)+\omega'$	$2\omega'$
Lempel-Golomb	$p(q-1) \times (q-1)$	$(q-2)\omega'$	p	$\lambda'(q-3)+\omega'$	$2\omega'$
Moreno-Maric	$p(q+1) \times (q+1)$	$(q+1)\omega'$	p	$\lambda'(q-1)+2\omega'$	$2\omega'$
Moreno-Maric $k = 1 \ldots p-1$	$p(q+1) \times (q+1)$	$(q+1)\omega'$	$p \times (p-1)$	$\lambda'(q-1)+2\omega'$	$\lambda'(q-1)+2\omega'$

Table 6–2: New DPA families Summary $\lambda_c < \lambda_a$

Construction	**Periodicity**	ω	Φ	λ_a	λ_c
Quadratic	$p^2 \times p$	$\frac{(p^2+p)}{2}$	p	$\frac{(p+1)^2}{4}$	$p+1$
Hyperbolic	$p^2 \times p$	$\frac{(p^2-1)}{2}$	p	$\frac{(p+1)^2}{4}$	$p+1$
Welch	$p^2 \times (p-1)$	$\frac{(p^2-1)}{2}$	p	$\frac{(p^2+p)}{4}$	$p+1$
Lempel-Golomb Mersenne Prime	$(q-1)^2 \times (q-1)$	$(q-2)\omega'$	p	$\lambda'(q-3)+\omega'$	$2\omega'$
Lempel-Golomb Twin Primes	$(q-2)(q-1) \times (q-1)$	$(q-2)\omega'$	p	$\lambda'(q-3)+\omega'$	$2\omega'$
Lempel-Golomb q prime	$p(p-1) \times (p-1)$	$(p-2)\omega'$	p	$\lambda'(p-3)+\omega'$	$2\omega'$
Lempel-Golomb	$p(q-1) \times (q-1)$	$(q-2)\omega'$	p	$\lambda'(q-3)+\omega'$	$2\omega'$
Moreno-Maric	$p(q+1) \times (q+1)$	$(q+1)\omega'$	p	$\lambda'(q-1)+2\omega'$	$2\omega'$

CHAPTER 7
ETHICS

7.1 Computer Ethics

Computer Ethics started as a field of applied ethics when Walter Maner, a professor of Medical Ethics course from the Old Dominion University noticed that the ethical questions and problems considered in his course were more complicated or altered when computers got involved. [3] He realized that many new ethics problems arise just because of the use of computers. For such reason he concluded that there should be a new branch of applied ethics similar to already existing fields like medical and business ethics, and he named it "computer ethics". Important to note is that three decades before Maner, Norbert Wiener combined the concepts of cybernetics with ideas from digital computing, and foresaw some of today's computer ethics issues.

7.2 Computer Sciences Ethics

Wright in [43] said that science and engineering are commonly distinguished as two different sorts of activities. Science, generally speaking, is the pursuit of theoretical results, while engineering seeks to apply those results through the creation and refinement of technology. If engineering requires an ethical position beyond professional codes of conduct, as Bugliarello notes [2], then a discipline such as Computer Sciences, which spans both theory and application, and that touches so many facets of life, should be grounded in an equally (or stronger) ethical foundation.

The cite from Wright besides making sense, also invites the computer science researchers like myself to be aware of ethics in our study field. Many computer

science researchers believe that ethics in computer science is not a matter of concern since mathematics, computer codes, and a bunch of bits can not kill or harm a human being. But ethics involves more than that.

Wright also said in [42]: Computer science and software engineering, and the technologies the discipline is responsible for, touch nearly every aspect of our world, and researchers in these disciplines bear a great responsibility to the world to conduct and report their research in an ethical manner. This is what we, computer science researchers, should have in mind and is what we did with our research work.

7.3 Ethical Issues raised by our research work

7.3.1 Optical Communications

Our codes can be used to facilitate multiple user capacity in optical communications. Such property is important to improve the channel capacity of a optical communication media. If such codes are known, and other security measures are not taken. The message transmitted using these codes can be obtained by a third party for illegal use, or simply violating the privacy rights of the users that send the data. Knowledge of how this codes are generated or how this codes work can also lead to the damage of the data sent in an optical communication system that uses them. Finally these codes are used to improve the communication systems that are essential today in our life.

7.3.2 Multiple Target Recognition

Multiple Target Recognition allows the detection of projectiles, aircrafts and submarines in noisy environments, such information can be used to improve the national security and the defense. Sonar and radars are also used for simple things as for recognizing the presence of fishes, or reefs under the water, and also can be used to detect enemy submarines under the water or projectiles under the water.

Another good application of codes for multiple target recognition is to map the ionosphere. Knowing how the ionosphere behaves helps to predict the behavior of

atmospherics disasters such as: storms and hurricanes. Also the ability to be able to predict the atmospheric behavior serves as information to know when a nation is fragile and susceptible to attacks. This information can be used to know how and when to improve national security under certain atmospheric events, or to know how or when to attack another enemy nation in war times.

7.3.3 Digital Watermarking

The major ethical issue raised by digital watermarking is that many people believe that information should be free. However our research helps in the development of digital watermarking which is used to combat the illegal sharing of copyrighted digital information. Right now digital content is very easy to share, and copyrighted content owners see this as a business problem. The idea behind watermarking is to provide a method to authenticate digital information which is copyrighted, and the idea behind copyright laws is to grant a reward for the efforts of an information producer, or owner.

A successfully detected digital watermark can be removed from a copyrighted digital media and then help to create ways to remove watermarks used similarly in other digital content, thereby leaving the original digital content available for illegal reproduction. Inserting watermarks over already watermarked digital medium is a common attack to digitally watermarked information, therefore the results of this research work could lead to attacks to other methods of watermarking. A better explanation of digital watermarking attacks can be found in appendix B.2.

Another important ethical issue raised is that databases storing the information of the families of arrays used for watermarks in digital information have to be fully secured. The access to that information could lead to the probability of removing the watermarks added to a digital media using that stored information.

Digital watermarking also allow users to track their works through the Internet. This ability could be abused by authoritarian forces. Also the legitimate pursuit

of rights could infringe the rights of privacy of those whom copyright owners are pursuing. At the end, owners and systems, would be looking where their work is not supposed to be, rather than where the work is rightly and lawfully stored.

Addition of watermarks will affect the authenticity and integrity of the digital information to be protected. Copyright owners could want their product to be copyrighted as securely as a consumer would like to obtain the original, integral and authentic product they are consuming.

7.4 Responsible Research Conduct

In computer science, metrics and analysis methods are primary instruments for measuring, corroborate or disprove research hypothesis. In our research work we developed computer code to generate preliminary results and to analyze the double periodicity properties, and correlation properties of the codes that we generated. Those results served to make the conjectures in the cross-correlation properties of our new families of DPAs, that later we analyzed and prove using mathematical reasoning.

7.5 Documenting and reporting research

As researchers we share our results in the form of articles or papers at conferences related to the field of Information Theory. Also the fact that we need to release this dissertation document proves our will to report and share our results with the rest of the research community. Every theorem that we present we also provide a formal mathematical proof or at least provide a reference of where it can be found; if the theorem comes from previous work.

The ability to duplicate the work of other researchers is perhaps the most fundamental principle and responsibility of science. In our methods we modify previous work by Colbourn and Colbourn in Distinct Different Sets. We replicated their method and then applied our modifications in order to obtain the results that we expected, and to be able to apply those results in different areas and fields such

as optical communications and digital watermarking. We carefully cite the earlier work done in Distinct Different Sets, Optical Orthogonal Codes, and in algebraic constructions with good correlation constrains that we use through our work. In this way we acknowledge the previous work done in the area, we validate their results, and obtain new results to share to a broad research community.

CHAPTER 8
CONCLUSION

8.1 Summary

In this work we begin by introducing the concept of Group Permutable Constant Weight Codes, and with the proof that Double Periodic Arrays with full double periodicity, and correlation value lower than the code weight produce GPCWC. These constructions have applications in frequency hopping radar and sonar, optical Code Division Multiple Access, design of experiments, and more recently, in digital watermarking. We also extend the Johnson Bound, to bound the cardinality of families of GPCWC, which are used to prove optimality of some of the new Double Periodic Arrays that we present in this work.

There are only a few constructions of families of double periodic arrays with perfect correlation properties. In Chapter 5 we presented a new recursive method to construct families of DPA with perfect correlation properties. The method increase the size of families of DPAs without changing the original correlation value. We present new constructions of DPAs with perfect correlation properties and new optimal constructions with respect to our Johnson Bound A modification for Group Permutable Constant Weight Codes. These codes are useful for applications on 1-D Optical Orthogonal Codes, 2-D Optical Orthogonal Codes, Multiple Target radar and sonars, experiment design and Digital Watermarking.

In Chapter 4 we present a method to increase the weight of double periodic arrays (Weight Increasing Method). This is useful for security reasons in Digital Watermarking applications. Using this method we obtain an optimal construction

of Double Periodic Arrays with respect to our Johnson Bound B modification for GPCWC. These codes are useful for applications on 1-D Optical Orthogonal Codes, 2-D Optical Orthogonal Codes, and Digital Watermarking.

Then we combine the method to increase the size of the families of DPAs and the Weight Increasing Method in Chapter 6 to obtain new families of DPAs with unequal correlation constrains. Specifically constructions of DPAs with cross-correlation lower than the auto-correlation. The auto- and cross-correlation properties are used for synchronization and user identification respectively. Fuja and Yang explained that with good cross-correlation we are able to deal with both synchronization and user identification. This is for the case were we can find constructions with a much better cross-correlation than auto-correlation. In Chapter 6 we present new constructions of DPAs where the cross-correlation is much better than the auto-correlation. These codes are useful for applications on 1-D Optical Orthogonal Codes, 2-D Optical Orthogonal Codes, and Digital Watermarking.

8.2 Future Work

Recently Double Periodic Arrays with good auto- and cross-correlation properties have been used for applications in Digital Watermarking. Digital Watermarking requires families of Double Periodic arrays as large as possible to be able to handle multiple users, and also requires the weight of the families to be balanced with respect to the length of the arrays for security robustness.

Most of our work in this research was originally inspired in finding ways to increase family size, and increasing the weight of Double Periodic Arrays. More work has to be done since the families obtained in Chapter 4 are heavy and balanced but for most of them the size of the family is small. And the size of the families produced in Chapter 5 are large, but are not balanced with respect to the length. We aim in finding column sequences suitable to apply Method A to the families

produced in Chapter 5 and be able obtain large families of Double Periodic Arrays with balanced weight.

We also plan in further developing the new area of Group Permutable Constant Weight Codes and the area of families of Double Periodic Arrays with unequal correlation constrains. We will accomplish this by working on finding new algebraic constructions of Double Periodic Arrays, and possibly the parallel computing generation of Double Periodic Arrays.

APPENDICES

APPENDIX A
SPREAD SPECTRUM COMMUNICATIONS APPLICATIONS

Spread spectrum is a method where modulation is performed according to a secret code, which spreads the signal across a wider bandwidth. This work concentrates in secret codes, that are called sequences, that have good auto and cross correlation properties. These sequences have been studied by our group for their applications in frequency hopping radars and sonar, and communications.

A.1 Frequency Hopping Radar and Sonars

In a frequency hopping radar or sonar system, the signal consists of one or more frequencies chosen from a set $\{f_1, f_2, \ldots, f_m\}$ of available frequencies, for transmission at each of a set $\{t_1, t_2, \ldots, t_n\}$ 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 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 $1 \leq f \leq n$ and $1 \leq t \leq n$)

If we have another Costas type 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 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 [23]) is for any n obtain the largest possible m.

A.2 Channel Data Protection

In spread spectrum communications the data sent in a communication channel is spread through different frequencies and time to avoid data interception and channel jamming. As the data to be sent is spread through different frequencies, the interceptor will need to either break the secret code used to spread the data, or

to collect all the data sent through all the frequency channels and try to reconstruct it. The frequency jamming is avoided because the "enemy" would have to jam all frequency channels in order to add noise to the data which is very costly. This method of communication is specially useful in the military during war.

A.3 CDMA

Code Division Multiple Access (CDMA) is used in wireless to allow the access to multiple users dividing user data through frequencies and time as in spread spectrum communication. You need to have good cross-correlation to avoid data interference among the users in the network. The data is also spread through frequencies and time. In Optical CDMA (OCDMA) the idea is the same but the data is spread through a set of fiber optics cable and time.

A.4 Watermarking Applications

More recently sequences with good auto and cross-correlation are being used in Digital Watermarking because they make watermarks more robust. The idea is still similar to spread spectrum communications where a secret is spread into a digital medium in order to make it more difficult to be intercepted or removed. Tirkel *et al.* [36, 39–41] proposed the application of spread spectrum communications into digital watermarking, using m-sequences as the arrays for the watermarks. Also I.J. Cox *et al* presented a technique of embedding digital watermarking based in inserting the watermark into the spectral components of the image using techniques analogous to spread spectrum communication [10, 12]. Later Tirkel *et al.* [37, 38] presented a method to generate arrays suitable for digital watermarking from double-periodic constructions such as constructions for Sonar and Costas using cyclic sequences as columns.

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 perfect auto and cross-correlation allow the addition of multiple arrays to increase information capacity and watermark security.

APPENDIX B
DIGITAL WATERMARKING

Watermarking has been used for several years to hide information or to authenticate originality of the content of different objects. A daily example includes the watermarks inserted in US dollars which asserts the authenticity of the bills.

Watermarking is related to the fields of information hiding and steganography. Information hiding deals with making information imperceptible or keeping secret the existence of information. Steganography, which means covered writing, is the art of communicating in a way which hides a secret message in the main information [17]. Information hiding techniques are used in both steganography and watermarking, but in watermarking, as opposed to steganography, robustness against attacks plays a major role. An example often used [33] to describe the origins of watermarking is a story from Herodotus, where a slave is tattooed with a message in his scalp and held until new hair grew to hide the message. Later the slave was sent with the secret message to the Ionian city of Miletus. Another example is paper watermarks, the first paper watermark appeared nearly 700 years ago in handmade paper-making. The oldest recognized watermarked paper has origins in Fabriano, Italy in 1292. Nowadays, techniques for information hiding are used everywhere where sensible or secret data needs to be communicated through a medium, and the data needs to be imperceptible for possible attackers or malicious users.

The growth of networks speeds, the Internet, and the digital media sharing have facilitated the problem of illegal duplication or distribution of copyrighted digital data. Such problems have created the need for more effective tools for copyright

protection, and consequently the need for effective research on the field of Digital Watermarking. Digital Watermarking is the process that embeds imperceptible data called watermark into a multimedia object such that the watermark, can be detected or extracted later to make an assertion about the object.

Some authors [17, 22] also describe the embedding of perceptible data into a multimedia object as digital watermarking. Examples of embedding perceptible data is the addition of visible marks to the copyrighted image/video media found in web pages, where the owner of the media embeds a label describing the web address where the media was originally published, or the addition of audio describing the author of a sound or video media. These techniques of adding perceptible marks to digital media is very easy to manipulate or alter to remove the mark. In order to make a perceptible mark difficult to remove you need to place the mark in a large or important area of the medium thereby affecting the fidelity.

A good digital watermarking practice involves imperceptibility, robustness (attack resistance), media fidelity, and provides enough information to unambiguously identify the owner.

B.1 Applications and Properties

Owner Identification is possibly the main application of Digital Watermarking needed today. The owner of a copyrighted digital object would like to be able to identify his work against others misusing it. For example, in the case that a copyrighted work is misused, the copyright holders need an effective way to prove the presence of a copyright notice in the distributed material. The owner would need an effective and robust method to embed a copyright notice in a digital medium. The simple addition of a copyright notice at the foot of an image would be easy to remove.

In the book Digital Watermarking from J. Cox *et al.* [11] they describe **Broadcast Monitoring** where advertisers pay for commercial to appear in a broadcasting

media (radio, tv, etc). The problem is that advertisers want to be sure that the broadcasting media is broadcasting all the commercials space that they paid for. One solution is to have persons monitoring the broadcast channels and to record what they hear or see. A better solution would be to use computation to detect watermarks in the signal of the broadcast channel that identifies the owner of the commercials.

Transaction Tracking, another application of watermarking is related to the protection of copyrights. In this case the owner embeds an unique watermark into each copy of his digital work to keep track of the owner of the copy. Therefore if any copy is misused, (e.g. found in a P2P program) the copyright owner can identify who is responsible of that copy being illegally distributed.

There are more applications of watermarking, like **content authentication** where the owner embed a digital signature and wants this signature to be difficult to remove from the digital work. The **copy control** is when the watermark should be detected by a copy device and the copy device reacts by not allowing the illegal copy or making a bad copy of the original work. More detailed information about watermarking applications can be found in [11, 17, 19, 22, 33].

Watermarking systems are composed of defining properties that differentiate watermarking from other information hiding fields like steganography and cryptography. Some of these properties interpretations and importance depend on the requirements of the application of the watermark. Here we describe some of the most important properties like embedding effectiveness, fidelity, robustness, security and detection effectiveness.

Embedding effectiveness is obtained if an embedded watermark can later be detected with a high probability. It is desirable to obtain 100% of effectiveness but this will mean higher cost of other properties like fidelity. The **fidelity** in watermarking means how perceptually similar is the original work compared to

different watermarked versions of itself. In some cases, like in art works, fidelity is very important and providing the best fidelity may result in non perfect embedding effectiveness. When detecting a watermark, besides wanting to have a high probability of detection, you also need to have a low rate of false positive detection. This is the **Detection Effectiveness**. A false positive detection of a watermark is when the detector detects the watermark, but the work was not watermarked or it was not watermarked specifically with the watermark it was searching.

Watermarking systems also provide the capacity of encode data payload into the original works. A watermark that encodes N bits is called an N-bits watermark, and that system can be used to encode 2^N messages, like for example 2^N different owner IDs.

Two important properties of watermarking, that also help to differentiate watermarking from other information hiding fields are **robustness** and **security**. Watermarking robustness is the ability to detect the watermark after the watermarked work has been exposed to common different signal processing operations, and security is similar to robustness but with the difference that the signal processing operations are used to attack the watermarked work. Example of attacks are unauthorized removal of the watermark, unauthorized embedding of watermarks, and unauthorized watermark detection. An example of watermark removal is called collusion attack. The attacker uses different copies of a given watermarked work, each with a different watermark, and then combines them to obtain an original unwatermarked copy. In the next section we are going to describe different watermark attacks.

B.2 Attacks

In the previous section we described watermarking robustness and security. We call **attack** a signal processing operation that can affect the robustness and the security of a watermarking system. The following attacks can be intentional or

unintentional and some of them refer only to image or video attacks. Some of them are used to eliminate the possibility of detecting a watermark, others to generate an unwatermarked copy of the original. [11, 17, 19, 22, 33].

1. Lossy compression: commonly used compression schemes like JPEG, MPEG and MP3 can degrade the data quality and also result in irretrievable loss of data, therefore losing data required to detect a watermark.
2. Geometric distortions: cropping and translation for audio, video or images. Rotation and scaling.
3. Gaussian noise addition
4. Spatial filtering: used to obtain enhanced images, video, or audio by applying filter function or filter operator of the media space.
5. Common signal processing operations: (D/A, A/D conversion, resampling, requantization, dithering distortion, re-compression, color reduction (video, image)
6. Printing and rescanning
7. Adding a watermark to a watermarked work.
8. Collusion: Combining different copies of a given watermarked work with different watermarks to obtain the original unwatermarked copy
9. Forgery: authorized recipients of watermarked copies of a work, collude to form another copy with a valid watermark with the intention o framing a 3rd party.
10. Use of tools like Unzing and Stirmark to remove data embedded by commercially available programs.

B.3 Watermarking Embedding and Detection

In this research the methods of embedding messages of interest are based on messages represented as sequences or sum of sequences [11]. The fist method called Direct Message Coding assigns an unique sequence for each message. The second

called Multi-symbol Message Coding uses the properties of code division multiplexing to make possible the embedding of messages with fewer codes than in Direct Message Coding.

In Direct Message Coding, one unique sequence codeword is assigned to represent each message. Therefore for a set of messages $\mathbf{M}$ we need a set of $\mid \mathbf{M} \mid$ sequence code. The detector needs to compute correlation for each of the $\mid \mathbf{M} \mid$ sequence codewords, and the message that corresponds to the sequence codeword is the sequence with the best correlation with the watermarked medium. In this method of embedding if you wanted to encode 16 bits of information you need a family of codes with $2^{16} = 65,536$ codes. This method works if the amount of information is relatively small, but in the case of needing to represent 100 bits of information we will have a computational problem in the detection side. The next subsection shows how to fix this problem.

REFERENCE LIST

[1] Erik Agrell, Alexander Vardy, and Kenneth Zeger. Upper bounds for constant-weight codes. *IEEE Trans. Inform. Theory*, 46:2373–2395, 2000.

[2] G. Bugliarello. Machine, modications of nature, and engineering ethics. *The Bridge*, 32(3):14–18, Fall 2002.

[3] Terrell Ward Bynum. Computer ethics: Its birth and its future. *Ethics and Information Technology*, 3, 2001.

[4] Guu chang Yang and Thomas E. Fuja. Optical orthogonal codes with unequal auto- and cross-correlation constraints. *IEEE Transactions on Information Theory*, 41(1):96–106, 1995.

[5] Fan R. K. Chung, Jawad A. Salehi, and Victor K.-W. Wei. Correction to optical orthogonal codes: Design, analysis, and applications (may 89 595-604). *IEEE Transactions on Information Theory*, 38(4):1429–, 1992.

[6] Habong Chung and P. Vijay Kumar. Optical orthogonal codes-new bounds and an optimal construction. *IEEE Transactions on Information Theory*, 36(4):866–, 1990.

[7] C.J. Colbourn and J.H. Dinitz. *The CRC Handbook of Combinatorial Designs*. CRC Press, 1996.

[8] M.J. Colbourn and C.J. Colbourn. Recursive constructions for cyclic block designs. *Journal of Statistical Planning and Inference*, 10:97–103, 1984.

[9] J.P. Costas. Medium constraints on sonar design and performance. *FASCON Convention Record*, pages 68A–68L, 1975.

[10] Ingemar Cox, Joe Kilian, Tom Leighton, and Talal Shamoon. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12):1673–1687, 1997.

[11] Ingemar Cox, Matthew L. Miller, and Jeffery A. Bloom. *Digital watermarking*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2002.

[12] Ingemar J. Cox, Joe Killian, Tom Leighton, and Talal Shamoon. Secure spread spectrum watermarking for images, audio, and video. In *IEEE International Conference on Image Processing (ICIP'96)*, volume III, pages 243–246, 1996.

[13] A. Freedman and N. Levanon. 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*, volume 73, pages 1530–1531, October 1985.

[14] R. Gagliardi, J. Robbins, and Herbert Taylor. acquisition sequences in ppm communications". *IEEE Transactions on Communications*, 33(5):738–744, September 1987.

[15] Solomon Golomb. Algebraic constructions for Costas arrays. *Journal Of Combinatorial Theory Series A*, 37(1):13–21, 1984.

[16] S.W. Golomb and H. Taylor. Two-dimensional syncronization patterns for minimum ambiguity. *IEEE Trans. Information Theory*, IT-28:600–604, July 1982.

[17] Frank Hartung and Martin Kutter. Multimedia watermarking techniques. *Proceedings of the IEEE (USA)*, 87(7):1079–1107, 1999.

[18] S.M. Johnson. A new upper bound for error-correcting codes. *IEEE Trans. on Information Theory*, IT(8):203–207, April 1962.

[19] Stefan Katzenbeisser and Fabien A. Petitcolas. *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House, Inc., Norwood, MA, USA, 2000.

[20] Svetislav Maric and Edward Titlebaum. A class of frequency hopped codes with nearly ideal characteristics for use in multiple-access spread-spectrum communications and radar and sonar syatems. *IEEE Transactions on Communication Theory*, 40(9):1442–1446, September 1992.

[21] A. Milewski. Periodic sequences with optimal properties for channel estimation and fast start-up equalization. *IBM J. Res. Develop*, 27(5):426–431, 1982.

[22] S. Mohanty. Digital watermarking: A tutorial review.

[23] O. Moreno, R. A. Games, and H. Taylor. Sonar sequences from costas arrays and the best known sonar sequences with up to 100 symbols. *IEEE Trans. Information Theory*, 39:1985–1987, November 1993.

[24] O. Moreno and S.V. Maric. A new family of frequency-hop codes. *IEEE Trans. in Communications*, 48(8):1241–1244, August 2000.

[25] O. Moreno and J. Ortiz-Ubarri. Double periodic arrays with good correlation for applications in watermarking. In *Proceedings of the Third International Workshop on Signal Design and Its Applications in Communications*, pages 214–218, Chengdu, China, September 2007.

[26] O. Moreno and J. Ortiz-Ubarri. Double periodic arrays with optimal correlation for applications in watermarking. In *Sequences, Subsequences, and Consequences*, volume LNCS 4893, pages 82–94, Los Angeles, CA, USA, 2007.

[27] O. Moreno and J. Ortiz-Ubarri. A new method to construct double periodic arrays with optimal correlation. In *IEEE Information Theory Workshop*, Taormina, Sicily, Italy, October 2009.

[28] O. Moreno, Z. Zhang, P.V. Kumar, and V. Zinoviev. New constructions of optimal cyclically permutable constant weight codes. *IEEE Trans. Information Theory*, 41:548–555, March 1995.

[29] Oscar Moreno, Reza Omrani, and S.V. Maric. Doubly periodic arrays and a new construction of multiple target sonar and extended costas arrays with perfect

correlation. In *Proc. Int. Symposium on Information Theory*, pages 1643–1647, Seatle, WA, USA, July 2006.

[30] Q. A. Nguyen, L. Gyorfi, and J. L. Massey. Construction of binary constant-weight cyclic codes and cyclically permutable codes. *IEEE Trans. Information Theory*, 38(3):940–949, May 1992.

[31] R. Omrani and P. Vijay Kumar. Improved constructions and bounds for 2-d optical orthogonal codes. In *Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on*, pages 127–131, Sept. 2005.

[32] J. Ortiz-Ubarri and O. Moreno. Constructions of families with unequal autoand cross-correlation constraints. In *IEEE Proc. Int. Symposium on Information Theory*, pages 134–138, Seoul, Korea, June 2009.

[33] F. Perez-Gonzalez and J.R. Hernandez. A tutorial on digital watermarking. In *Proceedings. IEEE 33rd Annual 1999 International Carnahan Conference on Security Technology*, pages 286–292, Madrid, Spain, 1999.

[34] P. Kumar R. Omrani, O. Moreno. Improved johnson bounds for optical orthogonal codes with $\lambda > 1$ and some optimal constructions. In *Proc. Int. Symposium on Information Theory*, pages 259–263, 2005.

[35] H. Y. Song and S. W. Golomb. Two-dimensional patterns with optimal auto- and cross-correlation functions. In *Proceedings International Symposium on Information Theory*, page 362, June 1994.

[36] A. Tirkel, R. van Schyndel, and C. Osborne. A two-dimensional digital watermark, 1995.

[37] A. Z. Tirkel and T. E. Hall. Matrix construction using cyclic shifts of a column. In *Proceedings International Symposium on Information Theory*, pages 2050–2054, September 2005.

[38] Andrew Tirkel and Tom Hall. New matrices with good auto and cross-correlation. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, E89-A(9):2315–2321, 2006.

[39] T. Tirkel, C. Osborne, and R. van Schyndel. Image watermarking - a spread spectrum application, 1996.

[40] R. van Schyndel, A. Tirkel, and C. Osborne. Towards a robust digital watermark, 1995.

[41] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne. A digital watermark. In *International Conference on Image Processing*, volume 2, pages 86–90, Austin, Texas, U.S.A., 1994.

[42] David R. Wright. Research ethics and computer science: an unconsummated marriage. In *SIGDOC '06: Proceedings of the 24th annual ACM international conference on Design of communication*, pages 196–201, New York, NY, USA, 2006. ACM.

[43] David R. Wright. Motivation, design, and ubiquity: A discussion of research ethics and computer science. *CoRR*, abs/0706.0484, 2007.

[44] C. Zhi, F. Pingzhi, and J. Fan. Disjoint difference sets, difference triangle sets and related codes. *IEEE Trans. Information Theory*, 38:518–522, March 1992.

BIOGRAPHICAL SKETCH

José R. Ortiz-Ubarri was born in September 27, 1981 in Hato Rey, San Juan, Puerto Rico. José is son of José R. Ortiz Miranda and Luz M. Ubarri-Aponte. José is married to Kariluz Dávila Diaz, Ph.D. and is father of Kariany Luz Ortiz Dávila. In December of 2002 he received his B.S. degree in Computer Sciences from the University of Puerto Rico Río Piedras Campus (UPR-RP). After spending a year as a full time employee for the High Performance Computing facility of the University of Puerto Rico, in January of 2003 he was admitted to the Computing and Information Sciences and Engineering Ph. D. program of the University of Puerto Rico. He worked his dissertation under the supervision of Oscar Moreno de Ayala, Ph.D. in the area of Code Design and Information Theory, while still working as a full time employee for the High Performance Computing facility of the University of Puerto Rico as a Scientific Programmer and System and Network Administrator.

In January of 2000 José R. Ortiz-Ubarri served as a teaching assistant in the laboratory sessions of the Introduction to Programming course of the Department of Computer Sciences of the University of Puerto Rico. He also served as professor for the Computer Science Department at the UPR-RP in Spring of 2007, for the Pre Engineering Department at the UPR-RP in Fall of 2008, and for the Computer Science Department at the UPR-RP in Spring of 2010.

As an employee of the High Performance Computing facility he conducted some research in Network Monitoring and Intrusion Detection for the Internet 2 of the University of Puerto Rico.

From 2001 to 2002 he was a research assistant in the High Performance Computing facility in the area of Network Monitoring and Intrusion Detection for the

Internet 2 under the supervision of Dr. Guy Cormier. He was a research assistant for the summer of 2001 in the Laboratory for Advanced Computing of the University of Kentucky, working in the area of Networks and Distributed Computing under the advise of Dr. Jim Griffioen. Early in 2002 he was a research assistant for the Gauss Research Laboratory of the University of Puerto Rico, working in Optical Communications and Parallel Computing under supervision of Dr. Oscar Moreno de Ayala. Later in 2002 he was a research assistant working in Smart Sensing Net Card for Load Balancing and Redundancy in Multiple Services Environment under the supervision of Dr. Carlos Corrada also in the University of Puerto Rico.

The research conducted by José R. Ortiz-Ubarri during his Ph.D. studies produced the following peer-reviewed papers:

- O. Moreno and J. Ortiz-Ubarri. A New Method to Construct Double Periodic Arrays with Optimal Correlation. IEEE *Proc Information Theory Workshop*, Taormina, Sicily, 2009.
- J. Ortiz-Ubarri and O. Moreno. Families of Constructions with Unequal Auto- and Cross-Correlation Constraints. IEEE *Proc International Symposium on Information Theory*, Seoul, Korea, 2009.
- O. Moreno and J. Ortiz-Ubarri. Double Periodic with Good Correlation for Applications in Watermarking. IEEE *Proc 3rd International Workshop in Signal Design and Its Applications in Communications*, pages 214-218, Chengdu, China, 2007.
- O. Moreno and J. Ortiz-Ubarri. Double Periodic Arrays with Optimal Correlation for Applications in Watermarking. In *Sequences, Subsequences, and Consequences*, volume LNCS 4893, pages 82-94, Los Angeles, CA, USA, 2007.