CONTRIBUTIONS TO THE THEORY OF COSTAS ARRAYS

Dissertation

zur Erlangung des akademischen Grades

doctor rerum naturalium
(Dr. rer. nat.)

von M.Sc. Ali Ardalani

geb. am 02.07.1990 in Teheran, Iran

genehmigt durch die Fakultät fur Mathematik
der Otto-von-Guericke-Universität Magdeburg

Gutachter: Prof. Dr. Alexander Pott
Otto-von-Guericke-Universität Magdeburg

Prof. Dr. Domingo Gómez Pérez
Universidad de Cantabria, Santander

Prof. Dr. Volker Kaibel
Otto-von-Guericke-Universität Magdeburg

eingereicht am: 24.01.2023
Verteidigung am: 31.05.2023

Abstract

This thesis aims to study Costas arrays from different points of view. A Costas array of size n is an $n \times n$ binary matrix such that no two of the $\binom{n}{2}$ line segments connecting 1s have the same length and slope. Costas arrays are attractive, highly combinatorial objects with applications in radar engineering and signal processing that motivates us to study them carefully. Firstly, we investigated equivalent definitions and the methods, based on finite fields, that allow us to construct Costas arrays for infinitely many sizes, but not all sizes.

There are three main approaches currently being considered to study Costas arrays; algebraic constructions based on finite fields by which we can construct Costas arrays of sizes equal to or a bit less than prime powers (systematically constructed). The other method is computer search, and the third is heuristic techniques. The enumeration of all Costas arrays up to size 29 has been completed via exhaustive search methods, revealing that more than 90% of these arrays are of completely unknown origin, called sporadic Costas arrays. So far, there is a general lack of research on the properties of sporadic Costas arrays, indicating an unclear relationship between sporadic Costas arrays and systematically constructed ones. One possible approach to make a link between systematically constructed Costas arrays and sporadic ones could be defining transformations that transform systematically generated Costas arrays to sporadic ones and vice versa.

Our primary concern is to examine how it is possible to transform a given Costas array to obtain another Costas array or create another array close to being a Costas array and then examine the violation causes to the Costas property. Then, we can investigate the possible ways to eliminate or reduce these violation causes. We introduce a new transformation with the property that we can obtain another Costas array by transforming a given one for some Costas arrays. Surprisingly, some of the systematically constructed Costas arrays produce sporadic Costas arrays after applying the transformation.

Costas arrays have perfect aperiodic properties, a solid property to ask, namely permutation matrices with aperiodic autocorrelation of at most one. By applying our new transformation on a given Costas array, we obtain a new array with the property that the values of its aperiodic autocorrelation function for all possible non-zero shifts are at most two. These arrays are called almost Costas arrays.

We will also examine Costas arrays from permutation points of view and prove that we could not construct a Costas array for a specific class of permutation, namely odd permutation. The distinctness of all line segments formed by joining pairs of ones in a given Costas array implies that a permutation matrix fails to be a Costas array if and only if it includes ones that form a (possibly degenerate) parallelogram. We refer to these parallelograms as forbidden configurations. Therefore, a Costas array has no forbidden configurations. Consequently, a permutation matrix is close to being a Costas array if and only if it contains as few as possible forbidden configurations. With this in mind, we investigate the number of forbidden

configurations in some classes of permutation matrices and introduce a transformation by which we can reduce the total number of forbidden configurations for these classes.

We discover a close relationship between the class of odd permutations and exponential Welch Costas arrays. Exponential Welch Costas arrays have G-symmetric properties. We will show how G-symmetric arrays can be constructed using transforming odd permutations. Moreover, we realized that this transformation significantly reduces the number of forbidden configurations in a given odd permutation array. This perspective also helped us to construct a class of permutation polynomials over finite fields that is differentially at most 6-uniform, meaning the permutation matrices associated with this permutation polynomials have the property that for all possible non-zero shifts, the periodic autocorrelation function values are at most 6. These differentially 6-uniform mappings can be constructed by transforming an inverse function over a finite field. We also observe that constructing G-symmetric permutation matrices from odd permutations leads to much fewer forbidden configurations, meaning the permutation matrices associated with these transformed odd permutations are closer to Costas arrays. Moreover, we will see that all G-symmetric Costas arrays of even sizes can be found by applying this transformation on odd permutations. This attitude allows us to search for G-symmetric Costas arrays by checking the Costas property of $\left(2^{n/2} \cdot \left(\frac{n}{2}\right)!\right)$ permutation matrices instead of $n!$, which results in a notable reduction in the search space.

In the last chapter, we discuss a surprising link between exponential Welch Costas arrays and power mappings constructed over a finite field with p elements, where p is a prime. We determine the maximal aperiodic crosscorrelation of pairs of power mappings using an exhaustive search. In some exceptional cases, we will provide theoretical proof for the maximal crosscorrelation of the family of power mappings. We will discuss how the maximal crosscorrelation of the family of power mappings is almost the same as the maximal crosscorrelation of the family of exponential Welch. This observation motivates us to extend the family of Welch Costas arrays with the family of power mappings and then investigate the maximal crosscorrelation of this extended family. We determine the maximal crosscorrelation of this extended family by exhaustive search. Surprisingly, the maximal crosscorrelation of this extended family is equal to the maximal crosscorrelation of the family of exponential Welch, constructed over a finite field with p elements, where p is not a safe prime. In the case where p is a safe prime also, there is a close relationship that we will discuss. Moreover, we will discuss why providing theoretical proof for our observed results regarding the maximal crosscorrelation of this extended family can be tremendously complex.

Families of arrays with low crosscorrelation properties are desirable for application in multiuser and multiplexing systems. Therefore, families of Costas arrays with low crosscorrelation are beneficial for such applications. With this in mind, we will introduce a subfamily of Lempel-Golomb Costas arrays that indicate lower crosscorrelation than the family of all Lempel-Golomb Costas arrays.

Zusammenfassung

In dieser Dissertation sollen Costas-Matrizen aus verschiedenen Blickwinkeln untersucht werden. Eine Costas-Matrix der Größe n ist eine $n \times n$ 0-1-Matrix, bei der keine zwei der $\binom{n}{2}$ Liniensegmente, die Einsen verbinden, die gleiche Länge und Steigung haben. Costas-Matrizen sind Interessant, kombinatorische Objekte mit Anwendungen in der Radartechnik und der Signalverarbeitung, die uns dazu motivieren, sie sorgfältig zu untersuchen. Zunächst untersuchten wir die äquivalenten Definitionen und die auf endlichen Körpern basierenden Methoden, die es uns erlauben, Costas-Matrizen für unendlich viele Größen, aber nicht für alle Größen, zu konstruieren.

Derzeit werden drei Hauptansätze zur Untersuchung von Costas-Matrizen erwogen: algebraische Konstruktionen auf der Grundlage der Theorie endlicher Körper, mit denen wir Costas-Matrizen mit Größen gleich oder etwas kleiner als Primzahlen konstruieren können (systematisch konstruiert). Die zweite Methode ist die Computersuche, und die dritte sind heuristische Techniken. Die Aufzählung aller Costas-Matrizen bis zur Größe 29 wurde mit Hilfe erschöpfender Suchmethoden abgeschlossen, wobei sich herausstellte, dass mehr als 90% dieser Matrizen völlig unbekannten Ursprungs sind, nämlich die so genannten sporadischen Costas-Matrizen. Bislang ist die Beziehung zwischen sporadischen Costas-Matrizen und systematisch konstruierten Matrizen unklar. Ein möglicher Ansatz, eine Verbindung zwischen systematisch konstruierten Costas-Matrizen und sporadischen Matrizen herzustellen, könnte darin bestehen, Transformationen zu definieren, die systematisch generierte Costas-Matrizen in sporadische umwandeln und umgekehrt.

unser Hauptziel ist es, zu untersuchen, wie es möglich ist, eine gegebene Costas-Matrix umzuwandeln, um eine andere Costas-Matrix zu erhalten oder eine andere Matrix zu erstellen, die einer Costas-Matrix nahe kommt, und dann die Ursachen der Verletzung der Costas-Eigenschaft zu untersuchen. Anschließend können wir untersuchen, wie sich die Ursachen für diese Verstöße beseitigen oder verringern lassen. Wir führen eine neue Transformation ein, die einige Costas-Matrizen in andere Costas-Matrix transformiert. Überraschenderweise ergeben einige der systematisch konstruierten Costas-Matrizen nach Anwendung der Transformation sporadische Costas-Matrizen.

Costas-Matrizen haben perfekte aperiodische Eigenschaften, was bedeutet, dass diese Permutationsmatrizen eine aperiodische Autokorrelation von höchstens eins haben. Durch Anwendung unserer neuen Transformation auf eine gegebene Costas-Matrix erhalten wir eine neue Matrix mit der Eigenschaft, dass die Werte ihrer aperiodischen Autokorrelationsfunktion für alle möglichen Verschiebungen ungleich Null höchstens zwei sind. Diese Matrizen werden als Fast-Costas-Matrizen bezeichnet.

Wir werden Costas-Matrizen auch unter Permutationsgesichtspunkten untersuchen und beweisen, dass wir für eine bestimmte Klasse von

Permutationen, nämlich ungerade Permutationen, keine Costas-Matrizen konstruieren können. Die Unterscheidbarkeit aller Liniensegmente, die durch das Verbinden von Paaren von Einsen in einer gegebenen Costas-Matrize gebildet werden, impliziert, dass eine Permutationsmatrix dann und nur dann keine Costas-Matrix ist, wenn sie Einsen enthält, die ein (möglicherweise entartetes) Parallelogramm bilden. Wir bezeichnen diese Parallelogramme als verbotene Konfigurationen. Eine Costas-Matrix hat also keine verbotenen Konfigurationen. Folglich kommt eine Permutationsmatrix einer Costas-Matrize nur dann nahe, wenn sie so wenige verbotene Konfigurationen wie möglich enthält. Vor diesem Hintergrund untersuchen wir die Anzahl der verbotenen Konfigurationen in einigen Klassen von Permutationsmatrizen und führen eine Transformation ein, mit der wir die Gesamtzahl der verbotenen Konfigurationen für diese Klassen reduzieren können.

Wir entdecken eine enge Beziehung zwischen der Klasse der ungeraden Permutationen und exponentiellen Costas-Matrizen. Exponentielle Costas-Matrizen haben G-symmetrische Eigenschaften. Wir werden zeigen, wie G-symmetrische Matrizen durch Transformation ungerader Permutationen konstruiert werden können. Außerdem haben wir festgestellt, dass diese Transformation die Anzahl der verbotenen Konfigurationen in einer gegebenen Matrize mit ungeraden Permutationen erheblich reduziert. Diese Perspektive hat uns auch geholfen, eine Klasse von Permutationspolynomen über endlichen Körpern zu konstruieren, die differentiell höchstens 6-uniform ist, was bedeutet, dass die Permutationsmatrizen, die mit diesen Permutationspolynomen verbunden sind, die Eigenschaft haben, dass für alle möglichen Nicht-Null-Verschiebungen die periodischen Autokorrelationsfunktionswerte höchstens 6 sind. Diese differentiell 6-uniformen Abbildungen können durch Transformation einer Umkehrfunktion über einen endlichen Körper konstruiert werden. Wir beobachten auch, dass die Konstruktion von G-symmetrischen Permutationsmatrizen aus ungeraden Permutationen zu viel weniger verbotenen Konfigurationen führt, was bedeutet, dass die mit diesen transformierten ungeraden Permutationen verbundenen Permutationsmatrizen näher an Costas-Matrizen sind. Außerdem werden wir sehen, dass alle G-symmetrischen Costas-Matrizen gerader Größe durch Anwendung dieser Transformation auf ungerade Permutationen gefunden werden können. Diese Sichtweise ermöglicht es uns, nach G-symmetrischen Costas-Matrizen zu suchen, indem wir die Costas-Eigenschaft von $\left(2^{n/2} \cdot \left(\frac{n}{2}\right)!\right)$ statt $n!$ Permutationsmatrizen überprüfen, was zu einer beträchtlichen Reduzierung des Suchraums führt.

Im letzten Kapitel diskutieren wir eine überraschende Verbindung zwischen exponentiellen Costas-Matrizen und Potenzabbildungen, die über einem endlichen Körper mit p Elementen konstruiert sind, wobei p eine Primzahl ist. Wir bestimmen die maximale aperiodische Kreuzkorrelation von Paaren von Potenzabbildungen mit Hilfe einer erschöpfenden Suche. In einigen Ausnahmefällen werden wir einen theoretischen Beweis für die maximale Kreuzkorrelation der Familie der Potenzabbildungen liefern.

Wir werden erörtern, dass die maximale Kreuzkorrelation der Familie der Potenzabbildungen fast die gleiche ist wie die maximale Kreuzkorrelation der Familie der exponentiellen Welch. Diese Beobachtung motiviert uns, die Familie der Costas-Matrizen um die Familie der Potenzabbildungen zu erweitern und dann die maximale Kreuzkorrelation dieser erweiterten Familie zu untersuchen. Wir bestimmen die maximale Kreuzkorrelation dieser erweiterten Familie durch erschöpfende Suche. Überraschenderweise ist die maximale Kreuzkorrelation dieser erweiterten Familie gleich der maximalen Kreuzkorrelation der Familie der exponentiellen Welch, die über einem endlichen Körper mit p Elementen konstruiert wurde, wobei p keine sichere Primzahl ist. Auch für den Fall, dass p eine sichere Primzahl ist, gibt es eine enge Beziehung, die wir diskutieren werden. Außerdem werden wir erörtern, warum ein theoretischer Beweis für die von uns beobachteten Ergebnisse bezüglich der maximalen Kreuzkorrelation dieser erweiterten Familie äußerst komplex sein kann.

Familien von Matrizen mit geringer Kreuzkorrelation sind für Anwendungen in Multiuser- und Multiplexing-systemen wünschenswert. Daher sind Familien von Costas-Matrizen mit geringer Kreuzkorrelation für solche Anwendungen von Vorteil. In diesem Sinne werden wir eine Unterfamilie von Costas-Matrizen einführen, die eine geringere Kreuzkorrelation aufweisen als die Familie aller Costas-Matrizen.

Contents

List of Figures

List of Tables

List of Abbreviations

Radar	**R**adio **D**irection **A**nd **R**anging
CC	**C**ross-**C**orrelation
MF	**M**atched **F**ilter
GT	**G**enerated **T**ransferable
NGT	**N**one **G**enerated **T**ransferable
PN	**P**erfect **N**on-linear
APN	**A**lmost **P**erfect **N**on-linear
MIMO	**M**ultiple-**I**nput-**M**ultiple-**O**utput
CDMA	**C**ode-**D**ivision **M**ultiple-**A**ccess
DT	**D**ifference **T**riangle
FC	**F**orbidden **C**onfigurations
CSP	**C**onstraint-**S**atisfaction **P**roblem
m**DRACO**	m-**D**imensional **R**elative **A**nt **C**olony **O**ptimization
ACO	**A**nt **C**olony **O**ptimization

Chapter 1

Overview

In 1965, in the context of sonar detection, J. P. Costas studied a particular class of permutations of n elements to improve the poor target detection performance of radar (radio direction and range) and frequency hopping sonar systems [25]. These classes are now known as Costas Arrays. Radars signals are essentially used to determine the distance and the velocity of a moving target, making them useful in many civil and military applications, like air traffic control, geological observations, aircraft and ship navigation and safety, measurement of speed in industrial applications, remote sensing, surveillance, artillery location, and law enforcement. Roughly speaking, to detect the distance and velocity of a moving target, a bunch of frequencies will send towards a target, and then the time delay until the frequencies, reflected from a target, is received back indicates the distance of the target. Moreover, the target's velocity can be computed by measuring the doppler frequency shift of the reflected signal [75]. S. W. Golomb in [60] explained that in a frequency hopping radar or sonar system, a signal can be represented as an n-by-n permutation matrix, where the n rows correspond to the n available frequencies from the set $\{f_1, \ldots, f_n\}$, and the n columns correspond to the n equal consecutive time intervals $t_1, \ldots, t_n$. This permutation matrix is constructed by placing a one at position (i, j) if and only if frequency f_i is transmitted in time interval t_j. (Otherwise, 0). He also explained that a good signal has the property that when its corresponding permutation matrix is shifted, r units in time and s units in frequency, where r and s are none-zero, have a low correlation with itself. Chapter 1 will discuss the correlation properties of Costas arrays in more detail. Naturally, the first question that comes into mind is how these permutation matrices could be beneficial to improving these systems' performance. The performance of a radar system depends heavily on the following factors:

- The effect of delay resolution.
- Doppler resolution.
- Noise immunity.
- Intentional and unintentional interference.

The Costas idea [27] was to transmit a single frequency f_i from the available frequencies of the set $\{f_1, \ldots, f_n\}$, used only once, in a given time interval t_j in such a way that coincidences between the signal and its time and frequency-shifted copies is minimized. Therefore, the high delay and doppler-resolution can be achieved, and since they are using a matched filter (in radar systems, a matched filter (MF) is obtained by correlating an omitted known signal with the reflected signal to examine the common elements of the out-going signal), the received signal has noise immunity [11]. It is well-known that crosscorrelation (CC) is a particular case of an MF [113]. Due to the importance of signals and sets of signals with suitable correlation properties in digital communication, S. W Golomb and Guang Gong published a book including a comprehensive explanation of how these signals are designed to satisfy the appropriate periodic and aperiodic correlation constraints [56]. Chapter 1 will introduce the mathematical definitions of what we explained so far, along with necessary definitions and theorems that we will need to study Costas arrays.

BY HAND, John P. Costas found examples of Costas arrays of size up to $n = 12$, but he could not construct one of size 13, which made him think that Costas arrays existence may cease to exist from this size. In their investigation into algebraic construction for Costas arrays, L. R. Welch and A. Lempel found constructions and applications for them, and Solomon W. Golomb provided both the first proofs of the validity of the Welch and Lempel constructions and also new construction [54, 55]. After discovering the two main algebraic construction methods, the Welch construction and the Golomb construction, together with some construction techniques obtained by manipulating these constructions [9], there have been no further discoveries of new algebraic constructions.

Although extensive research has been carried out on Costas arrays, many fundamental questions are not yet answered, especially, do Costas arrays exist for all sizes? This question was raised for the first time in a paper by S. Golomb and H. Taylor in 1984, and it is still open [55]. S. W. Golomb conjectured that the number of Costas arrays of size n monotonically increases as n grows. This conjecture was reasonable because the number of Costas arrays approximately doubled from n to $n+1$ for $n = 1, \ldots, 12$. Jerry Silverman [106] computed the number of Costas arrays for every size up to $n = 18$ and found that there are 21104 Costas arrays of size 16, but only 18276 Costas array of size 17. Then the conjecture is disproved by the fact that the number of Costas arrays decreases from order $n = 16$ to order $n = 17$.

According to the two main constructions for Costas arrays, they can be generated for infinitely many sizes but not for all sizes. To the best of our knowledge, since 1984, the smallest sizes for which no Costas array is currently known are 32 and 33. Referring to such difficulties, some authors have mainly been interested in computer search for Costas arrays [26,40,41,43,85,99].

A computer search for Costas arrays has provided a significant opportunity to enhance our understanding of the possible existence pattern for Costas arrays. However, the generalisability of these methods is subject to certain limitations. In particular, all Costas arrays have been found through exhaustive search up to size 29, while the vast majority of them are sporadic [41]. A Costas array is sporadic if it can not be constructed by one of the known systematic constructions. In other words, the sporadic Costas arrays' origin remains unexplained. So far, however, there has been little discussion about the relationship between sporadic Costas arrays and the systematically constructed Costas arrays; this connection has been remained ambiguous, which intrigued us to study this relation more carefully. Our primary concern was to introduce a transformation that links a given systematically constructed Costas array to a sporadic one and vice versa. Keeping this objective in mind, we introduced a new transformation in this thesis, denoted as $\mathcal{A}_k$. This transformation exhibits the desired property mentioned earlier, which will be extensively discussed in Chapter 3. As we mentioned in the abstract section, Costas arrays are known for their perfect aperiodic autocorrelation properties, and our transformation $\mathcal{A}_k$ also preserves this perfect property for a considerable amount of systematically constructed Costas arrays, more precisely, all Lempel-Golomb, logarithmic Welch Costas arrays, and some systematically constructed Costas arrays and sporadic ones. It is worth noting that, however, in the cases that our transformation does not preserve the Costas property, it results in an array with the property that for all possible non-zero shifts, the aperiodic autocorrelation function value is at most two, let us call them almost Costas arrays.

A considerable amount of literature has been published on constructing sequences and arrays with favourable correlation properties [2, 15, 16], primarily based on finite fields, due to their numerous applications in radar and sonar systems [81,83], communication systems, security systems [89,91], data hiding, and critical cryptographic applications [52, 56, 61, 74, 78, 104]; let us call them perfect arrays and sequences [48, 72]. One essential step towards constructing perfect arrays is to study the structural properties of the known one, and these properties might be seen better if we interpret them geometrically. Correll has considered this point of view in [112], from which he studied the forbidden configurations in permutation matrices that cause violations to the Costas property. The notion of the number of forbidden configurations allows us to determine how close a permutation matrix is to being a Costas array. The fewer forbidden configurations in a given permutation matrix allow us to stay closer to a Costas array because there are fewer violations to the Costas property. One natural question that one can ask is, even if there exist such forbidden configurations in a given permutation matrix, is there a way to eliminate or at least reduce the violation causes. Chapter 4 will specifically address the investigation of forbidden configurations within certain types of permutation matrices. To mitigate the presence of these undesirable configurations, we will introduce a transformation denoted as $\mathcal{G}$. The primary aim of this transformation will be to decrease the occurrence of such configurations within the matrices.The experimental evidence confirms that applying this transformation might considerably reduce the number of forbidden configurations.

The two main algebraic Constructions for Costas arrays, similar to the perfect arrays' construction within the aforementioned references, are based on finite fields. Therefore, it makes much sense to consider the properties of the associated polynomials over their underlying finite field. Since

Costas arrays are permutation matrices with Costas property, we are interested in permutation polynomials over finite fields that generate Costas permutations. We will follow this perspective in chapter 4, and we will show that certain permutations, namely odd permutations, fail to construct Costas arrays. We will investigate the properties of these permutations that never present Costas arrays.

Considerable effort has been devoted in the literature to study polynomials over finite fields with good periodic correlation properties, partly due to their applications in cryptography [95–98, 103, 105]. In this regard, polynomials with low differential uniformity received considerable attention, among which perfect non-linear (PN) and almost perfect non-linear (APN) polynomials are the most interesting ones [31,46,66,67,71,122]. Konstantinos Drakakis et al. in [37] and Daniel Panario et al. in [94] have already connected APN permutations on $\mathbb{Z}_n$ and Costas arrays. Konstantinos Drakakis et al. in [37] also explained the main differences between APN mappings and Costas permutations. Chapter 4 investigated a particular class of APN permutations over integer ring $\mathbb{Z}_n$. Moreover, we will discuss that even if our transformation $\mathcal{G}$ improves the aperiodic property of these matrices, in the sense that we obtain arrays with fewer forbidden configurations, it harms the periodic properties of these arrays. Although the periodic properties of these arrays become worse after being transformed, it is possible to introduce a class of permutation polynomials for which this transformation attains differentially at most 6-uniform permutation polynomials over some finite fields.

Arrays and sequences with good auto and crosscorrelation properties lie at the core of many active sensing and communication systems [3, 110], e.g., multiple-input-multiple-output (MIMO) radar systems [63, 64], multiuser and multiplexing systems and code-division multiple-access (CDMA) cellular systems [13, 70, 73, 107, 109, 117]. A desirable family of two-dimensional arrays has the property that each array within this family has perfect autocorrelation property, and the crosscorrelation between any two arrays of this family is as low as possible [111].

Costas arrays are defined by their perfect autocorrelation properties, whereas they show poor crosscorrelation. In 1985, Freedman and Levanon studied the crosscorrelation of Costas arrays, which showed that any two given Costas arrays of the same size have a maximal crosscorrelation of at least 2 [50]. After this discovery, the study of the crosscorrelation of algebraically constructed Costas arrays became more focused by several authors. The most comprehensive work on the maximal crosscorrelation of algebraically constructed Costas arrays was done by Konstantinos Drakakis et al. (2011) [39], in which they also proposed some conjectures regarding the crosscorrelation of Welch and Lempel-Golomb constructions, and they described that low crosscorrelation could be as essential as low autocorrelation, as were also described in [44, 79]. Recently, Domingo Gomez-Perez and Arne Winterhof settled some of the conjectures of Drakakis et al.'s work [62]. Their spectacular method for proving these conjectures reveals how Costas arrays' crosscorrelation offers a rich mathematical behaviour, driving this subject to be worth studying as a mathematical subject, regardless of its applications. With this in mind, we analysed power mappings' auto and crosscorrelation properties over a finite field. Firstly, we computed exhaustively maximal aperiodic auto and crosscorrelation of power mappings over a finite field with p elements for $5 \leq p \leq 271$. We will discuss several interesting observations regarding these computations in the last chapter of this thesis. We will provide theoretical proof for some parts of our observations of the crosscorrelation properties of these families while providing complete proof, unfortunately, has stayed beyond our reach. The main difficulty in doing so is that the system of equations we are dealing with seems intractable and tremendously hard to solve.

Several attempts have been made to construct families of matrices with low aperiodic autocorrelation function values at non-zero shifts and low crosscorrelation between any two of the family members [111]. These arrays have proven to be valuable in the field of digital watermarking. By conducting computational analyses on the aperiodic auto and crosscorrelation properties of power mappings, in conjunction with the introduction of our new transformation $\mathcal{A}_k$, we have successfully generated a new collection of 2D arrays. These arrays exhibit aperiodic auto and crosscorrelation function values of at most two. Specifically, leveraging the capabilities of our transformation $\mathcal{A}_k$, which enables the transformation of a single permutation into a family of permutations, we applied this transformation to the inverse permutation constructed over a finite field with p elements. The objective was to construct a family of arrays characterized by aperiodic auto and crosscorrelation values of at most two. Chapter 5 examines the auto and crosscorrelation properties of this family.

Chapter 2

Introduction

This chapter provides the mathematical background required to study Costas arrays and their correlation properties. We also discuss the approaches that have been adopted so far to study Costas arrays.

2.1 Costas Arrays

There are several ways that Costas arrays can be defined. Each of them offers some critical insight into a better understanding of the properties of Costas arrays. Simply put, a Costas array of size n is an $n \times n$ binary matrix such that there is exactly a single 1 in each row and each column (i.e., it is a permutation matrix) and such that the line segments formed by joining pairs of 1s are all distinct [55]. In other words, a Costas array is a permutation matrix (permutation property) such that no two of the $\binom{n}{2}$ line segments connecting 1s have the same length and slope (Costas property). J. P. Costas in [26] argued on basic engineering principles that the permutation property of binary matrices is as essential as Costas property.
We think of a permutation as a bijective mapping from the set $\{1, 2, \ldots, n\}$ to itself. There are different conventions that we can employ to assign a permutation matrix to a permutation of $\{1, 2, \ldots, n\}$. Let us define our convention as follows.

Throughout this text, we denote by $[n]$ and $[n] - 1$ the set of n elements of the set $\{1, 2, \ldots, n\}$ and $\{0, 1, \ldots, n-1\}$ respectively, for some $n \in \mathbb{N}$.

Definition 2.1. *Let $f : [n] \to [n]$, $n \in \mathbb{N}$ be a bijection, that is a permutation of n elements. Then the corresponding permutation matrix of f, say $A_f = (a_{i,j})$, $i, j \in [n]$, is an $n \times n$ matrix where the entries are given by*

$$a_{i,j} = \begin{cases} 1 & \text{if } i = f(j) \\ 0 & \text{otherwise.} \end{cases}$$

Sometimes it will be more convenient to consider permutations as permutation matrices. Definition 2.1 also tells us how to recover a permutation from a given permutation matrix.
Let $A = (a_{i,j})$, $i, j \in [n]$, be a permutation matrix of size n. Then each column has a unique element equal to 1 and 0's elsewhere. Now we can construct a permutation $\sigma_A : [n] \to [n]$, $n \in \mathbb{N}$, $\sigma_A(j) = i$, if $a_{i,j} = 1$. This

means that each element of the permutation indicates the position of the 1 in the corresponding column of the matrix. The following remark makes the relation between a permutation matrix and its corresponding permutation more explicit.

Remark 2.2. *There is a bijection $\sigma : P_n \to \{f : f \text{ is a bijection on } n \text{ elements}\}$, where P_n is the set of all permutation matrices of size n. More precisely, $\sigma_A = [f(1), \ldots, f(n)]$, where $f(i)$ is the position of the nonzero entry in the ith column of A, counting from top to bottom. It means $f^{-1}(i) = j \Leftrightarrow a_{i,j} = 1$. Throughout this text, the terms "permutation matrix" and "permutation" will be used interchangeably, and we will not distinguish between A and σ_A.*

It is worthwhile to mention that it is customary to depict the 1′s and 0′s of a permutation matrix as dots and blanks, respectively.

Example 2.3. *Consider the permutation $A = [1, 3, 6, 4, 5, 2, 7]$. Suppose that $f : [7] \longrightarrow [7]$ is the permutation corresponding to the matrix A. Since $f(1) = 1$, we have a dot in the first column and the first row. Similarly, since $f(2) = 3$, we have a dot in the second column and third row. In this way, we obtain the matrix that corresponds to the permutation $f : [7] \longrightarrow [7]$ as follows*

$$\begin{array}{c|c|c|c|c|c|c|c|}
 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline
f(1) & \bullet & & & & & & \\ \hline
f(6) & & & & & & \bullet & \\ \hline
f(2) & & \bullet & & & & & \\ \hline
f(4) & & & & \bullet & & & \\ \hline
f(5) & & & & & \bullet & & \\ \hline
f(3) & & & \bullet & & & & \\ \hline
f(7) & & & & & & & \bullet \\ \hline
\end{array}$$

The matrix representation of a Costas permutation allows us to understand and visualize what it means by having distinct line segments that connect pairs of dots. Let us call these line segments the displacement vectors. Utilizing the following definition, we will be equipped to give the first formal definition of a Costas array.

Definition 2.4 (Displacement vectors)**.** *Consider the permutation matrix $A = (a_{i,j})$, $i, j \in [n]$, and let a_{i_1,j_1} and a_{i_2,j_2}, be two nonzero entries of A. Then if $j_1 < j_2$ we call the vector $(j_2 - j_1, i_2 - i_1)$ the displacement vector between a_{i_1,j_1} and a_{i_2,j_2}.*

Definition 2.5 (First definition of Costas arrays [55])**.** *Let $A = (a_{i,j})$, $i, j \in [n]$, be a permutation matrix of size n. Then $A = (a_{i,j})$ is a Costas array if and only if all displacement vectors of the form $\{(j_2 - j_1,\ i_2 - i_1),\ j_1 < j_2,\ j_1, j_2 \in [n]\}$ are distinct.*

As Definition 2.5 expresses, a permutation $f : [n] \longrightarrow [n]$ has the Costas property if and only if the collection of all displacement vectors $\{(i - j, f(i) - f(j)) : i, j \in [n], i > j\}$ does not contain any duplication. Therefore, a straightforward way to verify the Costas property is to group all displacement vectors according to their first coordinate and then check if, in each such group, all the second coordinate values are distinct. The mentioned verification procedure leads to the definition of the difference triangle table of a permutation. In the following section, we will see how the difference triangle could bring advantageous for checking the Costas property in Definition 2.5.

2.2 Difference Triangle Table

The difference triangle table provides an easy way to check whether a given permutation is a Costas array. The difference triangle applies for recording the difference between pairs of entries of a given permutation.

Definition 2.6 (Difference Triangle Table). *Let $A = [f(1), f(2), \ldots, f(n)]$ be a permutation matrix of size n, $n \in \mathbb{N}$. Then the ith row of the difference triangle table of A, let us denote by $T(A)$, for $1 \leq i \leq n-1$, contains the following $n-i$ elements:*

$$t_{i,j} = f(i+j) - f(j), \text{ for } 1 \leq j \leq n-i.$$

Example 2.7. *Consider the permutation $A = [1, 3, 6, 4, 5, 2, 7]$ in example 2.3. The difference triangle table $T(A)$ can be constructed as follows:*

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

As shown in $T(A)$, the elements above the line are the permutation's elements. The first row contains all the differences between adjacent elements, and the second row contains the differences between elements when they are two positions apart, and similarly, the other rows of $T(A)$ have been constructed.

One can easily verify that a displacement vector in a given permutation matrix is associated with an element in its difference triangle table. Let $A = (a_{i,j})$, $i, j \in [n]$, be a permutation matrix of size n, corresponds to a permutation $f : [n] \longrightarrow [n]$, and suppose that k, $1 \leq k \leq n-1$, is a given row of $T(A)$. Associated with an element $f(j+k) - f(j)$, for some j in $[n-k]$, is the displacement vector $(j+k-j, f(j+k) - f(j)) = (k, f(j+k) - f(j))$, as shown in figure 2.1. Therefore, we can conclude that the distinctness of displacement vectors in a permutation A is equivalent to the distinct elements in each row of $T(A)$. The above discussion enables us to give an equivalent definition for Costas arrays.

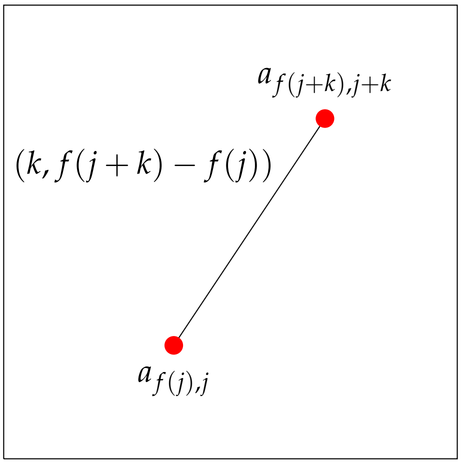


FIGURE 2.1: The displacement vector between two non-zero entries of Permutation matrix A.

Definition 2.8 (Second definition of a Costas array). *Let A be a permutation matrix of size n, $n \in \mathbb{N}$, with the corresponding permutation $[f(1), \ldots, f(n)]$. Then A is a Costas array if each row i, for $1 \leq i \leq n-1$, of the difference triangle table of A contains distinct elements t_{ij}, for $1 \leq j \leq n-i$.*

According to Definition 2.8, the permutation $A = [1, 3, 6, 4, 5, 2, 7]$ in example 2.7 is not a Costas array because, in the third row of $T(A)$, the value 3 is repeated twice. Let us provide an example of a Costas array.

Example 2.9. *Consider the permutation $A = [1, 3, 6, 2, 7, 8, 5, 4]$. Its corresponding permutation matrix and $T(A)$ are as follows*

1	3	6	2	7	8	5	4
2	3	−4	5	1	−3	−1	
5	−1	1	6	−2	−4		
1	4	2	3	−3			
6	5	−1	2				
7	2	−2					
4	1						
3							

●							
			●				
	●						
							●
						●	
		●					
				●			
					●		

We can see that each row of $T(A)$ is free of duplications, meaning A represents a Costas array.

It can be seen how the difference triangle table of a permutation could bring advantages to verifying the Costas property. According to the definition of a difference triangle table, $\sum_{k=1}^{n-1}\binom{n-k}{2} = \binom{n}{3}$ comparisons of pairs of values are needed to verify the Costas property. Analysis of the entries of a difference triangle table have shown a strong connection between the entries of the upper half of a difference triangle table and its lower half, leading to a drastic reduction in the number of pairs which are required to verify to assure whether a given permutation is a Costas array [7]. W. Chang in [18] showed that if the first $\left\lfloor \frac{n-1}{2} \right\rfloor$ rows of a difference triangle table of a permutation of size n do not contain any duplication, the remaining rows are also duplication-free. The following theorem shows how this correlation between the first and second half of a difference triangle table will reduce the number of comparisons.

Theorem 2.10. *Let $A = [f(1), f(2), \ldots, f(n)]$ be a permutation matrix of size n, where $n \in \mathbb{N}$. Then the total number of entries in $T(A)$ that need to be calculated to verify the Costas property of A is*

$$C(n) = \begin{cases} \frac{1}{8}(n-1)(3n-1), & n \text{ odd} \\ \\ \frac{3}{8}n(n-2), & n \text{ even.} \end{cases}$$

Proof. According to the W. Chang's result in [18], we need to consider only the first $\left\lfloor \frac{n-1}{2} \right\rfloor$ of the rows. It can be seen that a row i contains $n-i$ elements. Let us first assume that n is odd, then we have $\left\lfloor \frac{n-1}{2} \right\rfloor = \frac{n-1}{2}$. Then the total number of entries is

$$\begin{aligned} \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} (n-i) &= \sum_{i=1}^{\frac{n-1}{2}} (n-i) \\ &= \sum_{i=1}^{\frac{n-1}{2}} n - \sum_{i=1}^{\frac{n-1}{2}} i \\ &= \frac{n(n-1)}{2} - \left(\frac{(\frac{n-1}{2})(\frac{n-1}{2}+1)}{2} \right) \\ &= \frac{n(n-1)}{2} - \frac{(n-1)(n+1)}{8} \\ &= \frac{1}{8}(n-1)(3n-1). \end{aligned}$$

Now, if n is even, then $\left\lfloor \frac{n-1}{2} \right\rfloor = \frac{n-2}{2}$. Then the total number of entries is

$$\begin{aligned} \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} (n-i) &= \sum_{i=1}^{\frac{n-2}{2}} (n-i) \\ &= \frac{n(n-2)}{2} - \frac{(\frac{n-2}{2})(\frac{n-2}{2}+1)}{2} = \frac{3}{8}n(n-2). \end{aligned}$$

□

Drakakis et al. in [7] showed that the total number of entries in a difference triangle table of a given permutation that must be calculated to verify the Costas property could be further reduced by considering only a subset of entries in the first $\left\lfloor \frac{n-1}{2} \right\rfloor$ rows. We refer the reader to [7] for more details on this result. The rest of this section will discuss more properties of the difference triangle table of a permutation which we will use throughout our study of Costas arrays.

Theorem 2.11 ([33]). *Let A be a permutation matrix of size n, where $n \in \mathbb{N}$. Then the difference triangle of A contains precisely $n-k$ elements equal to k in absolute value, $k = 1, \ldots, n-1$.*

Proof. By induction over n.
(i) Assume $n = 2$. Then $T(A)$ has one of the following forms

$$\sigma_A = [1,2] \qquad\qquad \sigma_A = [2,1]$$

$$\begin{array}{cc} 1 & 2 \\ \hline 1 & \end{array} \qquad\qquad \begin{array}{cc} 2 & 1 \\ \hline \text{-1} & \end{array}$$

Clearly, the statement is true.
(ii) Assume the statement is true for $n \leq s$, and let $n = s+1$. Now we construct a permutation of size s from σ_A by removing the largest element, $s+1$, which lies at the jth position in σ_A. This results in a new array A' with permutation σ'_A. By construction, σ'_A is a permutation of size s, thus the difference triangle $T(A')$ satisfies the proposition to be proved by induction. Then $T(A')$ contains $s-k$ elements equal to k in absolute value, $k = 1, \ldots, s-1$. Now we can insert the element $s+1$ to its previous position and construct again the σ_A from σ'_A. In other words, we can construct $T(A)$ from $T(A')$ by inserting some new elements in each row of $T(A')$. As we can see, these new elements correspond to the differences between $s+1$ and all elements of the set $\{1, ..., s\}$. So, all these differences belong to the set $\{\pm s, \pm(s-1), \pm(s-2), ..., \pm 2, \pm 1\}$. the positive or negative elements will be chosen if the elements of $\{1, ..., s\}$ appear before the jth position or after the jth position, respectively. It is impossible to insert both the positive and the negative of an element of the set $\{\pm s, \pm(s-1), \pm(s-2), ..., \pm 2, \pm 1\}$ to the rows of $T(A)$. By way of contradiction let us assume both positive and negative of an element appear in $T(A)$, so there must exist two elements, say a_k and $a_{k'}$, where $1 \leq k \leq j-1$ and $k' \geq j+1$ such that $|(s+1) - a_k| = |a_{k'} - (s+1)|$. As we can see, $(s+1)$ appears after a_k, so $|(s+1) - a_k| = (s+1) - a_k$. Similarly, $|a_{k'} - (s+1)| = (s+1) - a_{k'}$, because $a_{k'}$ appears after $s+1$. Then $(s+1) - a_k = (s+1) - a_{k'}$ which implies that $a_k = a_{k'}$, which is a contradiction. Then $T(A)$ will contain $s-k+1 = (s+1)-k$ elements equal to k, $k = 1, ..., s-1$ in absolute value, plus one new element equals to $+s$ or $-s$.
This completes the proof. □

Remark 2.12. *The statement of the Theorem 2.11 holds when we have a Costas array because the collection of all Costas arrays is a subset of the collection of all permutation matrices.*

Example 2.13. *Let $A = [3, 1, 6, 2, 5, 4]$ be a permutation matrix of size 6. Then, we have*

3	1	6	2	5	4
-2	5	-4	3	-1	
3	1	-1	2		
-1	4	-2			
2	3				
1					

According to Theorem 2.11, there are precisely $6 - k$ elements equal to k in absolute value, where $k = 1, \ldots, 5$. For instance, if $k = 1$ then we must have 5 elements equal to 1 in absolute value, which is highlighted in the difference triangle of A. Similarly, if $k = 2$ then we must have 4 elements equal to 2 in absolute value, which is checkable from the table.

The following theorem provides an important observation about Costas arrays.

Theorem 2.14 ([33]). *Let $A = [f(1), \ldots, f(n)]$ be a Costas array of size n. Then for any $1 \leq s < t \leq n$, the part $[f(s), \ldots, f(t)]$ of the permutation A, called $A' = [f(s), \ldots, f(t)]$ has the Costas property, meaning all the displacement vectors between dots are distinct; if it so happens that the elements of A' are consecutive integers, that is, there exists an element $a \in \mathbb{N}$ such that $\{f(s), \ldots, f(t)\} = \{a, a + 1, ..., a + t - s - 1\}$ then A' represents a Costas array of size less than n, which is $[f(s) - a + 1, ..., f(t) - a + 1]$.*

Proof. It is clear that A' has the Costas property because each row of $T(A')$ is a subset of the same row of $T(A)$. Moreover, if A' contains consecutive integers, then we can pick the smallest element of A', say a, and scale A' by adding $-a + 1$ to each element in order to make the smallest element of A' equal to 1, meaning we can construct $A'' = [f(s) - a + 1, ..., f(t) - a + 1]$ from A' by adding $-a + 1$ to each element of A'. Then A'' represents a Costas array because the differences between elements of A'' and A' are the same. □

Remark 2.15. *It would be worthwhile to note that when we have a Costas array of size n, removing the element n from its corresponding permutation would not always result in another Costas array of size $n - 1$ with the same ordering. For instance, let $A = [1, 3, 6, 4, 5, 2]$ be a permutation of size 6. Then $T(A)$ is*

1	3	6	4	5	2
2	3	-2	1	-3	
5	1	-1	-2		
3	2	-4			
4	-1				
1					

As we can see, there are no duplicate entries in each row of $T(A)$. So, A is a Costas array. Now if we delete 6 and save the order of elements, we will have the following difference triangle table for $A' = [1, 3, 4, 5, 2]$.

1	3	4	5	2
2	1	1	-3	
3	2	-2		
4	-1			
1				

There are two duplicate entries in the first row. Thus, the permutation matrix A' is not a Costas array.

There are several natural ways to construct a Costas array by performing some manipulations to an existing Costas array. Theorem 2.14 shows one type of these manipulations. Suppose that we have a permutation $f : [n] \to [n]$ such that $f(1) = 1$. Then by removing this element from the beginning of the permutation sequence and then subtracting all the other elements by one, we can construct a Costas array of one less size. We will discuss several of these types of manipulations in section 2.5.

There is another possible way to think of a displacement vector in a permutation matrix. Consider the displacement vector shown in figure 2.1. If we shift the entry $a_{f(j),j}$ by i columns to the right and $f(i+j) - f(j)$ rows upwards, then the entries $a_{f(j),j}$ and $a_{f(i+j),i+j}$ will coincide. As we will see in the next section, this point of view will allow us to utilize the definition of crosscorrelation between two matrices to propose the third equivalent definition of Costas array.

2.3 Cross and autocorrelation

As explained in the previous section, a displacement vector in a permutation matrix $A = (a_{i,j})$, $i, j \in [n]$, between entries $a_{f(j),j}$ and $a_{f(i+j),i+j}$, $i + j \leq n$, represents a shift that displaces $a_{f(j),j}$ to $a_{f(i+j),i+j}$. In 1984, Solomon W. Golomb and Herbert Taylor pointed out the number of such coincidences can be computed using the autocorrelation function [60]. The autocorrelation function provides information about repeating patterns in a given binary matrix. There are two natural ways to regard a binary permutation matrix; one is to think of it as an n-by-n grid and extend it with zeroes to cover the entire euclidian plane, and the other is to consider the array on a torus, meaning that tiling the entire plane using the matrix. These two ways of consideration lead to the notion of the periodic and aperiodic autocorrelation function.

Definition 2.16 (Autocorrelation function)**.** *For a binary matrix $A = (a_{i,j})$, with $1 \leq i, j \leq n$, for $i, j \in \mathbb{Z}$ let*

$$a'_{i,j} = \begin{cases} a_{i,j} & \text{if} \quad 1 \leq i, j \leq n \\ 0 & \text{otherwise.} \end{cases}$$

The aperiodic autocorrelation function value of A at horizontal shift r and vertical shift s, for $r, s \in \mathbb{Z}$, is given by

$$C^a_A(r,s) = \sum_{i,j} a'_{i,j} a'_{i+s,j+r}.$$

and the periodic autocorrelation function of A at horizontal shift r and vertical shift s, for $r, s \in \mathbb{Z}$, is given by

$$C^p_A(r,s) = \sum_{i,j} a_{i,j} a_{1+(i+s-1 \mathit{\ mod\ } n),1+(j+r-1 \mathit{\ mod\ } n)}.$$

We note that, in the above definition, the autocorrelation function value at horizontal shift r and vertical shift s is the number of coincidences between 1's in the matrix A with the 1's in a shifted version of A, in which all the entries have been shifted r units to the right (to the left if r is negative), and s units downwards (upwards if s is negative). It is immediate that the aperiodic autocorrelation function satisfies the following condition:

- $C^a_A(0,0) = n.$
- $C^a_A(r,s) = 0, \quad$ if $|r| \geq n$ or if $|s| \geq n$.
- $0 \leq C^a_A(r,s) < n, \quad$ if $(r,s) \neq (0,0)$.

The difference between the periodic and aperiodic autocorrelation functions is essential to note. Roughly speaking, in the aperiodic case, we shift the matrix and count the number of coincidences in the intersection part of the matrix and its shifted version because everywhere outside the matrix is zero. In contrast, in the periodic case, we consider the intersection part and the parts wrapped around at the boundaries because we compute modulo the size of the matrix. Let us provide an example that computes the value of the autocorrelation function for a specific shift both periodically and aperiodically.

Example 2.17. *Let us compute the periodic and aperiodic autocorrelation function value at shift $(1, -2)$ for the permutation matrix $A = [6, 1, 3, 5, 4, 2]$. The shift $(1, -2)$ means that we shift the matrix by one column to the right and two rows upwards, as shown in figure 2.2. Looking at the intersection, we see that one pair of 1s coincide, showing $C^a_A(1, -2) = 1$. In order to compute the periodic autocorrelation value at this shift, since we do the computations modulo 6, whenever a 1's entry leaves a boundary, it will be back to the matrix from the opposite side. Therefore, the periodic shift of matrix A for the shift $(1, -2)$ gives the following matrix*

$$\begin{array}{|c|c|c|c|c|c|}
\hline
0 & 0 & 0 & 1 & 0 & 0 \\ \hline
0 & 0 & 0 & 0 & 0 & 1 \\ \hline
0 & 0 & 0 & 0 & 1 & 0 \\ \hline
0 & 1 & 0 & 0 & 0 & 0 \\ \hline
0 & 0 & 1 & 0 & 0 & 0 \\ \hline
1 & 0 & 0 & 0 & 0 & 0 \\ \hline
\end{array}$$

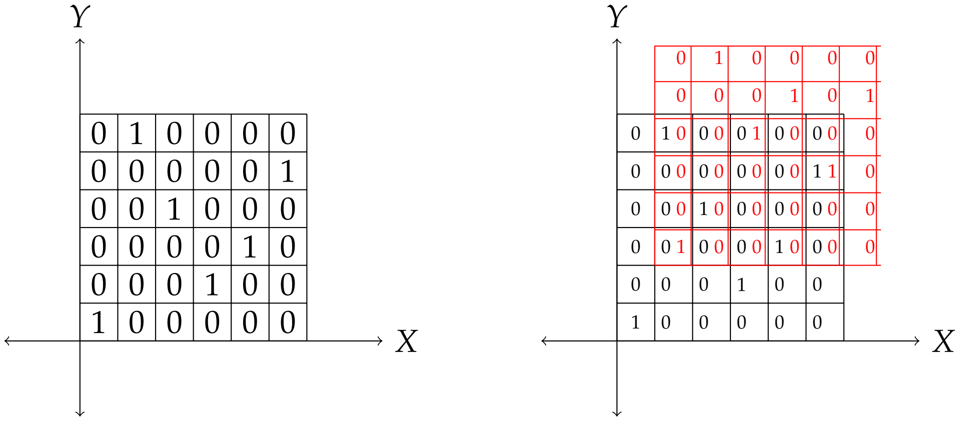


FIGURE 2.2: Aperiodic autocorrelation at shift $(1, -2)$.

Now, if we place matrix A and its shifted version on top of each other, we see that the 1's entries, shown in black, coincide, showing $C^p_A(1, -2) = 2$.

As briefly explained in the above example, we observe that the periodic autocorrelation function of an array can be viewed as a sum of at most four aperiodic autocorrelations.

Observation 2.18. *Let* $A = (a_{i,j})$, $1 \le i, j \le n$ *and* $n \in \mathbb{N}$, *be a binary matrix. The periodic autocorrelation function value of A at shifts* $0 < r \le n-1$ *and* $0 < s \le n-1$ *is equal to the sum of four aperiodic autocorrelations. In other words, we have*

$$C^p_A(r,s) = C^a_A(r,s) + C^a_A(r-n,s) + C^a_A(r,s-n) + C^a_A(r-n,s-n).$$

Proof. According to the definition of the periodic autocorrelation function we have

$$\begin{aligned}
C^p_A(r,s) &= \sum_{i=1}^{n}\sum_{j=1}^{n}\left(a_{i,j}\cdot a_{1+(i+s-1 \bmod n),1+(j+r-1 \bmod n)}\right)\\
&= \sum_{\substack{i=1\\1\le i+s\le n}}^{n}\ \sum_{\substack{j=1\\1\le j+r\le n}}^{n}\left(a_{i,j}\cdot a_{i+s,j+r}\right)\\
&+ \sum_{\substack{i=1\\1\le i+s\le n}}^{n}\ \sum_{\substack{j=1\\n+1\le j+r\le 2n-1}}^{n}\left(a_{i,j}\cdot a_{i+s,j+r}\right)\\
&+ \sum_{\substack{i=1\\n+1\le i+s\le 2n-1}}^{n}\ \sum_{\substack{j=1\\1\le j+r\le n}}^{n}\left(a_{i,j}\cdot a_{i+s,j+r}\right)\\
&+ \sum_{\substack{i=1\\n+1\le i+s\le 2n-1}}^{n}\ \sum_{\substack{j=1\\n+1\le j+r\le 2n-1}}^{n}\left(a_{i,j}\cdot a_{i+s,j+r}\right)\\
&= C^a_A(r,s) + C^a_A(r-n,s) + C^a_A(r,s-n) + C^a_A(r-n,s-n).
\end{aligned}$$

$\square$

Regarding the above observation, we can conclude that the periodic autocorrelation gives an upper bound for the aperiodic one. Making this relation between periodic and aperiodic autocorrelation could bring advantages that we will discuss in the following chapters. In order to see all the values of the aperiodic autocorrelation (periodic) in one glance, it would be more convenient if we record all these values in a $(2n-1)$-by-$(2n-1)$ matrix. We follow [119] in introducing the autocorrelation matrix. Let us denote this matrix by C_A^a (C_A^p), called the autocorrelation matrix of A. Each entry of autocorrelation matrix shows the autocorrelation function value for a particular shift.

Example 2.19. *Let $A = [6,1,3,5,4,2]$ be the permutation matrix in example 2.17 with the following matrix*

	●				
					●
		●			
				●	
			●		
●					

The aperiodic autocorrelation matrix of $A = (a_{i,j})$, $i,j \in [11]$, can be constructed as follows:
For $|r| \leq 5$ and $|s| \leq 5$, we put the autocorrelation function's value at shift (r,s) in entry $a_{6+s,6+r}$. Then we have

$$C_A^a = \begin{bmatrix} 0&0&0&0&0&0&1&0&0&0&0\\ 0&0&0&1&0&0&0&0&0&0&1\\ 0&0&1&0&0&0&0&2&0&0&0\\ 0&0&0&0&2&0&1&0&0&1&0\\ 0&1&0&1&0&0&1&0&2&0&0\\ 0&0&0&0&0&6&0&0&0&0&0\\ 0&0&2&0&1&0&0&1&0&1&0\\ 0&1&0&0&1&0&2&0&0&0&0\\ 0&0&0&2&0&0&0&0&1&0&0\\ 1&0&0&0&0&0&0&1&0&0&0\\ 0&0&0&0&1&0&0&0&0&0&0 \end{bmatrix}$$

As shown in C_A^a, the central position corresponds to the shift $(0,0)$. For $(0,0)$ shift, we place the matrix on top of itself. Therefore, C_A^a counts the number of 1s in matrix A. We saw in example 2.17 that $C_A^a(1,-2) = 1$, so the entry $a_{4,7}$ shows this value, which is 1. Similarly, the C_A^p can be constructed as follows:

$$C_A^p = \begin{bmatrix} 1 & 1 & 2 & 1 & 1 & 0 & 1 & 1 & 2 & 1 & 1 \\ 2 & 1 & 0 & 1 & 2 & 0 & 2 & 1 & 0 & 1 & 2 \\ 0 & 2 & 2 & 2 & 0 & 0 & 0 & 2 & 2 & 2 & 0 \\ 2 & 1 & 0 & 1 & 2 & 0 & 2 & 1 & 0 & 1 & 2 \\ 1 & 1 & 2 & 1 & 1 & 0 & 1 & 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 2 & 1 & 1 & 0 & 1 & 1 & 2 & 1 & 1 \\ 2 & 1 & 0 & 1 & 2 & 0 & 2 & 1 & 0 & 1 & 2 \\ 0 & 2 & 2 & 2 & 0 & 0 & 0 & 2 & 2 & 2 & 0 \\ 2 & 1 & 0 & 1 & 2 & 0 & 2 & 1 & 0 & 1 & 2 \\ 1 & 1 & 2 & 1 & 1 & 0 & 1 & 1 & 2 & 1 & 1 \end{bmatrix}$$

As in example 2.17, we have $C_A^p(1,-2) = 2$, which shows the entry $a_{4,7}$ of C_A^p is equal to 2. It can be seen that entry $a_{8,7}$ in C_A^p equals 2, which shows $C_A^p(1,2) = 2$. Moreover, by utilizing Observation 2.18, one can easily conclude that

$$\begin{aligned} C_A^p(1,2) &= C_A^a(1,2) + C_A^a(-5,2) + C_A^a(1,-4) + C_A^a(-5,-4) \\ &= 2+0+0+0 \\ &= 2. \end{aligned}$$

This example also indicates the connection between periodic and aperiodic autocorrelation functions.

Definition 2.20. *Let $A = (a_{i,j})$, $i,j \in [n]$, be a permutation matrix of size n. We define a $(2n-1)$-by-$(2n-1)$ matrix by placing the value of $C_A^a(r,s)$, for a given shift (r,s), $|r| \leq n-1$, $|s| \leq n-1$, at position $a_{n+s,n+r}$, called the aperiodic autocorrelation matrix of A, C_A^a. Similarly, we define the periodic autocorrelation matrix, C_A^p.*

Matlab provides valuable tools to visualize the autocorrelation matrix. We visualized C_A^p in example 2.19 in Figure 2.3. In the first figure, the x-axis shows the values of the periodic autocorrelation function, and the y-axis depicts the distribution of these elements. In the second figure, we can see also the distribution of the autocorrelation function's values in a three-dimensional plot.

Remark 2.21. *For convenience, we say the periodic autocorrelation of a matrix of size n is equal to x, where $x = max\{C_A^p(r,s) : |r| \leq n, |s| \leq n, (r,s) \neq (0,0)\}$. The value x is also known as off-peak autocorrelation. We adopt the same convention for the aperiodic one.*

One can quickly verify that if aperiodic autocorrelation of a matrix is at least 2, there exist a non-zero shift by which at least two pairs of dots will coincide, meaning there are at least two displacement vectors in the given matrix with the same length and slope, which is a violation of the Costas property. Therefore, we have the following equivalent definition for Costas arrays.

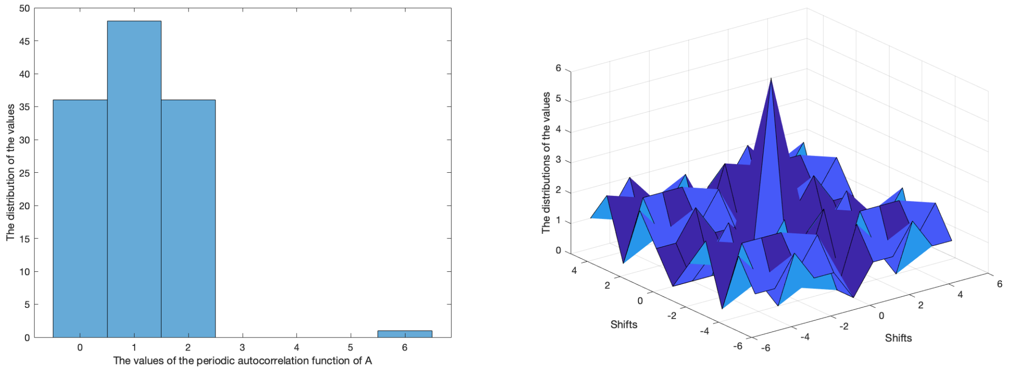


FIGURE 2.3: The visualization of C_A^p in example 2.19.

Definition 2.22 (Third definition of Costas array)**.** *Let A be a permutation matrix of size n, where $n \in \mathbb{N}$. Then A is a Costas array if for any pairs of integers $(r, s) \neq (0, 0)$, the aperiodic autocorrelation function of A satisfies*

$$C_A^a(r, s) \leq 1.$$

From the equivalent definitions of the Costas array, we can conclude the following.

Remark 2.23. *Let $A = (a_{i,j})$, $i, j \in [n]$, be a permutation matrix of size n. It is easy to see that any element $t_{i,j}$ in the row i of the difference triangle table of matrix A represents a displacement vector $(i, f(i + j) - f(j))$ between non-zero entries $a_{f(j),j}$ and $a_{f(i+j),i+j}$. Therefore, we have l repetitions in a row of a difference triangle table if and only if we have l equal displacement vectors if and only if there is a non-zero shift (r, s), $|r| \leq n - 1$, $|s| \leq n - 1$, for which the aperiodic autocorrelation function value is equal to l.*

As in Definition 2.16, if we have another permutation matrix $B = (b_{i,j})$, $i, j \in [n]$, we can similarly define the crosscorrelation function by substituting the shifted version of A by shifted version of B. Let us denote A and B's aperiodic crosscorrelation (periodic) at shift (r, s) by $C_{A,B}^a(r, s)$ $(C_{A,B}^p(r, s))$. We also use the exact definition, as in Definition 2.20, to define the aperiodic (periodic) crosscorrelation matrix, denoted by $C_{A,B}^a$ $(C_{A,B}^p)$. Let us define aperiodic crosscorrelation (periodic) between two matrices.

Definition 2.24 (Crosscorrelation)**.** *For binary matrices $A = (a_{i,j})$ and $B = (b_{i,j})$, with $1 \leq i, j \leq n$, for $i, j \in \mathbb{Z}$ let*

$$a'_{i,j} = \begin{cases} a_{i,j} & \textit{if} \quad 1 \leq i, j \leq n \\ 0 & \textit{otherwise.} \end{cases}$$

and

$$b'_{i,j} = \begin{cases} b_{i,j} & \textit{if} \quad 1 \leq i, j \leq n \\ 0 & \textit{otherwise.} \end{cases}$$

The aperiodic crosscorrelation function value between A and B at at horizontal shift r and vertical shift s is given by

$$C^a_{A,B}(r,s) = \sum_{i,j} a'_{i,j} b'_{i+s,j+r}, \quad for \quad r,s \in \mathbb{Z}.$$

and the periodic crosscorrelation function value between A and B at horizontal shift r and vertical shift s is given by

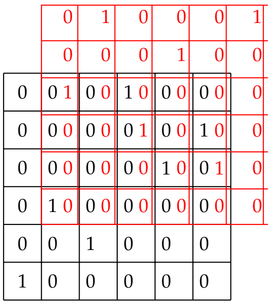
$$C^p_{A,B}(r,s) = \sum_{i,j} a_{i,j} b_{1+(i+s-1 \; mod \; n),1+(j+r-1 \; mod \; n)}, \quad for \quad r,s \in \mathbb{Z}.$$

Definition 2.24 shows that for $n \times n$ binary matrices A and B, and for each possible shift (r,s), their aperiodic crosscorrelation (periodic), $C^a_{A,B}(r,s)$ ($C^p_{A,B}(r,s)$), is defined as the number of overlapping ones between A and a shifted version of B, which has been shifted r columns horizontally to the right (left), if r is positive (negative), and s rows vertically upward (downward), if s is positive (negative). Therefore, the aperiodic crosscorrelation (periodic) matrix is a $(2n-1) \times (2n-1)$ matrix whose entries are $C^a_{A,B}(r,s)$ ($C^p_{A,B}(r,s)$), $0 \leq |r|, |s| \leq n-1$. Let us provide an example of how we can compute the crosscorrelation of two different matrices.

Example 2.25. *Let $A = [6,4,5,1,3,2]$ and $B = [3,1,4,2,5,6]$ be two permutations with the following corresponding matrices*

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

In order to compute the aperiodic crosscorrelation value at shift $(1,-2)$, $C^a_{A,B}(1,-2)$, we shift the matrix B by one column to the right and two rows upwards, and then we place matrix A and the shifted version of the matrix B on top of each other, as shown in the following figure, and we count the number of overlapping ones.



As shown in the above figure, none of the ones is overlapped, meaning $C^a_{A,B}(1,-2) = 0$. We also can construct the aperiodic crosscorrelation matrix as *follow.*

$$C^{a}_{A,B} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The red entry in matrix $C^{a}_{A,B}$ shows the value of $C^{a}_{A,B}(1,-2)$.

2.4 Symmetry

The relevance between a permutation matrix of size $n \times n$ and the permutation of the set $[n]$ allows us to consider Costas arrays as permutations in S_n. Recall that S_n is the symmetric group of degree n and consists of all permutations of the set $[n]$. The purpose of this section is to explain how we can construct a new Costas array from a given one. As we know from group Theory, an action turns a group into a set of symmetries of an object. The concept of symmetry reflects a group action. In order to understand how we can construct new Costas arrays from a given one, we utilize the concept of group actions, and we refer the reader to [100] and [45] for more detail.

Definition 2.26 (Action [100]). *Let $(G, \star)$ be a group, and X a set. A left action of G on X is a map*

$$\begin{aligned} \alpha : G \times X &\longrightarrow X \\ (g, x) &\longmapsto g.x \end{aligned}$$

where we write $\alpha(g, x) = g.x$ such that

1. *$g_1.(g_2.x) = (g_1 \star g_2).x$ for all $x \in X$ and $g_1, g_2 \in G$,*

2. *$e.x = x$ for all $x \in X$, where e is the identity element of G.*

We say that G acts on X.

Since there may be many different actions of a group G on a given set X, the notation of $x.g$ is vague. In context, however, this will not cause any difficulty. One way to think of an action is to visualize that the group G move the points in X around. The first condition says that instead of applying the element g_2 and then g_1, we can apply $g_1 \star g_2$, and the second condition says that the identity element results in no movement.
Recall that if a group G acts on a set X, the (distinct) orbits of G partition G,

where for a fixed element $x \in X$, the orbit of x (under G) is defined as

$$Orb_G(x) = \{y \in X \mid y = g.x \text{ for some } g \in G\} = \{g.x \mid g \in G\} \subseteq X.$$

In order to define an equivalence relation on the set of Costas arrays of a given size, we will use the Orbit-Stabilizer Theorem. The Orbit-Stabilizer Theorem expresses that if a group G acts on a set X, once we know the number of possible ways to send an element $x \in X$ to itself, we also know the number of ways of sending x to any other elements in its orbit. We recall that if G is a group acting on a set X on the left, the stabilizer in G of $x \in X$ is defined as

$$Stab_G(x) = G_x := \{g \in G \mid g.x = x\}.$$

Theorem 2.27 (Orbit Stabilizer Theorem [100]). *Assume that G is a finite group acting on a set X (on the left). Then for any $x \in X$,*

$$|G| = |Orb_G(x)| \cdot |Stab_G(x)|$$

Proof. It is easy to check that $Stab_G(x)$ is a subgroup of G, so by Lagrange's Theorem we can conclude that

$$|G| = [G : Stab_G(x)] \cdot |Stab_G(x)|.$$

Therefore, it is sufficient to prove that

$$[G : Stab_G(x)] = |Orb_G(x)|.$$

For doing so, we will define a bijection between these two sets. Let us define

$$\begin{aligned} \phi : [G : Stab_G(x)] &\longrightarrow Orb_G(x) \\ aStab_G(x) &\longmapsto a.x \end{aligned}$$

for any $a \in G$. We need to show that ϕ is well defined, one-to-one, and onto. Let us assume that for $a, b \in G$, $aStab_G(x) = bStab_G(x)$. To see ϕ is well defined we need to show that $\phi(aStab_G(x)) = \phi(bStab_G(x))$.
Since $aStab_G(x) = bStab_G(x)$, we know that $a \in bStab_G(x)$ so that $a = bh$ for some $h \in Stab_G(x)$. Notice that $h \in Stab_G(x)$ then $h.x = x$. Then

$$\phi(aStab_G(x)) = a \cdot x = (bh) \cdot x = b \cdot (h \cdot x) = b \cdot x = \phi(bStab_G(x))$$

which proves that ϕ is well defined.
Suppose that $y = g \cdot x \in Orb_G(x)$. Then $\phi(gStab_G(x)) = g \cdot x = y$ and we conclude that ϕ is onto.
Finally, suppose that $\phi(aStab_G(x)) = \phi(bStab_G(x))$. Then $a \cdot x = b \cdot x$ and so

$$x = e \cdot x = (a^{-1}a) \cdot x = a^{-1} \cdot (a \cdot x) = a^{-1} \cdot (b \cdot x) = (a^{-1} \cdot b) \cdot x$$

Thus $a^{-1} \cdot b \in Stab_G(x)$. Therefore, $(a^{-1} \cdot b)Stab_G(x) = Stab_G(x)$ and so $aStab_G(x) = bStab_G(x)$ which completes the proof. □

In the rest of this section, we will examine how we can construct a new Costas array from a given one by the action of dihedral group of degree four. We refer the reader to [45] for more details on dihedral groups. Recall that a dihedral group of degree four, denoted by D_8, is the group of symmetries of the square. The group D_8 contains eight elements, four rotational symmetries and four reflection symmetries. The rotations are given by rotating the square by $0^\circ, 90^\circ, 180^\circ$, and 270°, and the four reflections are defined along the four axes: the reflections around diagonals and the reflection around the centre of the square vertically or horizontally.
The elements of D_8 act on any $n \times n$ permutation matrix by rotating and reflecting the position of the entries. The transpose of a matrix $A = (a_{i,j})$, $1 \leq i, j \leq n$, can be obtained by reflecting the entries along its main diagonal, which let us denote by $\mathcal{T}$. In what follows, $\mathcal{T}$ stands for the map

$$\begin{aligned} \mathcal{T} : X_n &\longrightarrow X_n \\ A = (a_{ij}) &\longmapsto T(A) := (a_{j,i}), \end{aligned}$$

where X_n denotes the set of all permutation matrices of size n. Consider the vertical reflection of a permutation matrix, denoted by $\mathcal{S}$, which can be defined using the following map

$$\begin{aligned} \mathcal{S} : X_n &\longrightarrow X_n \\ A = (a_{ij}) &\longmapsto S(A) := (a_{i,n+1-j}). \end{aligned}$$

One can show that $\langle a, b | a^2 = b^2 = (ab)^4 = 1 \rangle$ gives a representation of D_8 in terms of two generators $a = \mathcal{T}$ and $b = \mathcal{S}$ of order 2. Let us provide an example showing how $\mathcal{T}$ and $\mathcal{S}$ generate D_8.

Example 2.28. *Let $A = [3,1,6,2,5,4]$ be a permutation matrix of size 6. Then each of the elements of D_8 that transfers A are illustrated in the Figure 2.4. In other words, letting D_8 act on the checkerboard of A, which is shown as Identity matrix in Figure 2.4, we obtain the action of the elements in the dihedral group D_8 on A. By checking the difference triangle table of each permutations we can see that Costas property holds in all cases.*

Remark 2.29. *According to Example 2.28, one can verify that the elements of the Dihedral group D_8 are generated by $\mathcal{S}$ and $\mathcal{T}$. Then*

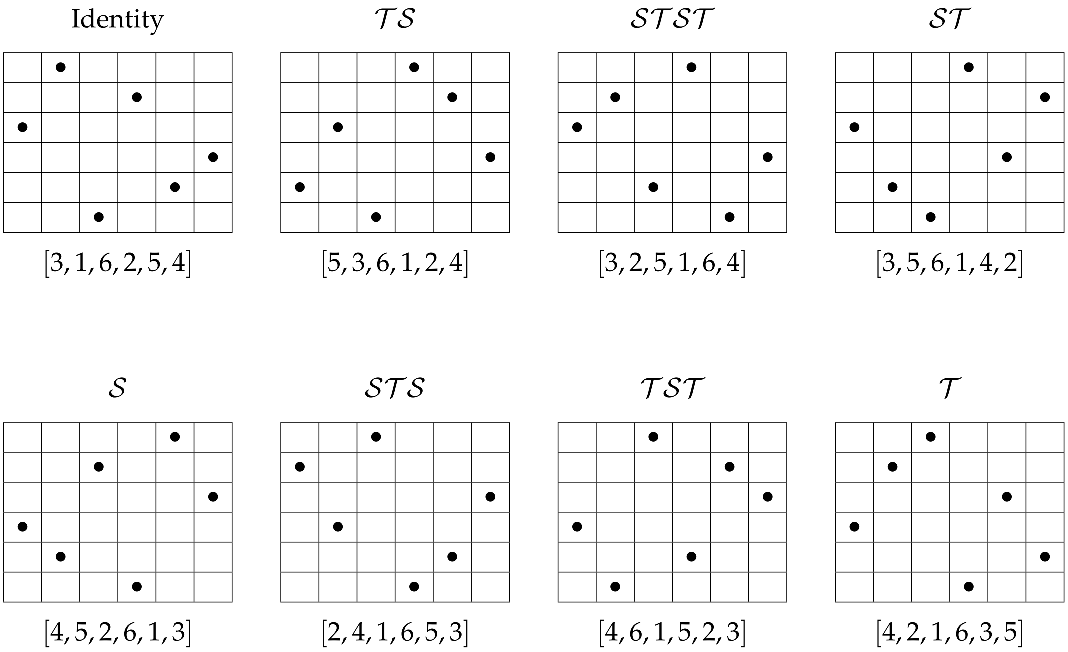
$$D_8 = \{I, \mathcal{S}, \mathcal{T}, \mathcal{ST}, \mathcal{TS}, \mathcal{STS}, \mathcal{TST}, \mathcal{STST}\}.$$

Let us explain how the Dihedral group D_8 in Example 2.28 acts on the set of all Costas arrays by which the Costas property remains invariant.

Theorem 2.30 ([33]). *Suppose that C_n is the set of all Costas arrays of size n, where $n \in \mathbb{N}$. Then, the Dihedral group D_8 acts on C_n.*

Proof. Consider the Dihedral group D_8 generated with two elements $\mathcal{S}$ and $\mathcal{T}$. To see the group D_8 acts on C_n, we will define the following map and one

FIGURE 2.4: The action of D_8 on Costas array A



can easily verify that how the two condition in Definition 2.26 are satisfied.

$$\begin{aligned} \alpha : D_8 \times C_n &\longrightarrow C_n \\ (x, A) &\longmapsto x.A := x(A). \end{aligned}$$

We will show that if A is a Costas array then $\mathcal{T}(A)$ and $\mathcal{S}(A)$ are Costas arrays. Moreover, since all the elements of D_8 are different compositions of $\mathcal{S}$ and $\mathcal{T}$, then for any $x \in D_8$, we can conclude that $x(A)$ is a Costas array. Hence, the image of the map α belongs to C_n.

Let us assume that A is a Costas array with corresponding permutation $\sigma(A) = [f(1), \dots, f(n)]$. By the definition of $\mathcal{S}$, one can verify that $\mathcal{S}(A)$ corresponds to the permutation $\sigma(\mathcal{S}(A)) = [f(n), \dots, f(1)]$. So, the difference triangle table of $\sigma(\mathcal{S}(A))$ is the same as the difference triangle table of $\sigma(A)$, but with opposite entry signs. Then $\mathcal{S}(A)$ is a Costas array.

We claim that $\mathcal{T}(A)$ has the Costas property. Assume it is not a Costas array. Then, according to Definition 2.5, we can find two pairs of 1's such that the displacement vectors between them are equal. By noting that the transpose of A corresponds to the inverse permutation, one can check that

$$\sigma(\mathcal{T}(A)) = [f^{-1}(1), \dots, f^{-1}(n)].$$

To show that $\mathcal{T}(A)$ has the Costas property, let us assume that two pairs of 1's have the following equal displacement vectors

$$(f^{-1}(i+k) - f^{-1}(i), k)$$
$$(f^{-1}(j+k) - f^{-1}(j), k),$$

where $1 \leq i+k, j+k \leq n$. Thus, this requires:

$$f^{-1}(i+k) - f^{-1}(i) = f^{-1}(j+k) - f^{-1}(j). \tag{2.1}$$

According to the last equality, we have the following results:

1) There exists an element $1 \leq x \leq n$ such that $f^{-1}(i+k) = x$. Then $f(x) = i+k$
2) There exists an element $1 \leq y \leq n$ such that $f^{-1}(i) = y$. Then $f(y) = i$
3) There exists an element $1 \leq w \leq n$ such that $f^{-1}(j+k) = w$. Then $f(w) = j+k$
4) There exists an element $1 \leq z \leq n$ such that $f^{-1}(j) = z$. Then $f(z) = j$

Substituting the above values in (2.1) yields $x - y = w - z$. Now from 1 and 2 we can conclude that $f(x) - f(y) = k$. Similarly, from 3 and 4 we have $f(w) - f(z) = k$. Then the displacement vectors $(f(x) - f(y), x - y)$ and $(f(w) - f(z), w - z)$ are equal, which is a contradiction because all the displacement vectors in A should be distinct. Then $\mathcal{T}(A)$ is a Costas array. Therefore, we can conclude that D_8 acts on C_n. □

Remark 2.31. *Since the group D_8 acts on the set C_n, then the (distinct) orbits of D_8 partition C_n. Thus, the equivalence class of A is the $Orb_{D_8}(A)$ of A under the action of D_8.*

Theorem 2.32 ([119]). *Let A be a Costas array of size n, where $n \in \mathbb{N}$. Consider the functions $\mathcal{T}$ and $\mathcal{S}$ in Example 2.28. Then, $|Orb_{D_8}(A)| = 8$ if both $A \neq \mathcal{T}(A)$ and $A \neq \mathcal{STS}(A)$ hold, and $|Orb_{D_8}(A)| = 4$ otherwise; hence, we can construct 3 or 7 more Costas arrays from a given one.*

Proof. One can verify that the orbit of A under the action of D_8 is the set

$$O(A) = \{I(A), \mathcal{TS}(A), \mathcal{STST}(A), \mathcal{ST}(A), \mathcal{T}(A), \mathcal{TST}(A), \mathcal{STS}(A), \mathcal{S}(A)\}.$$

We claim that $O(A)$ has 8 elements if $A \neq \mathcal{T}(A)$ and $A \neq \mathcal{STS}(A)$, and 4 elements otherwise. To do so, we know that the Orbit Stabilizer Theorem 2.27 gives $|Orb_{D_8}(A)| \cdot |Stab_{D_8}(A)| = 8$. Then, to complete the proof, it is enough to prove that

$$|Stab_{D_8}(A)| = \begin{cases} 1 & \text{if } A \neq \mathcal{T}(A) \text{ and } A \neq \mathcal{STS}(A) \\ 2 & \text{otherwise.} \end{cases}$$

Since A is a permutation matrix, $A \neq \mathcal{S}(A)$. So, $\mathcal{S} \notin Stab_{D_8}(A)$. We want to show that $A \neq \mathcal{TST}(A)$. Let $A = (a_{ij})$ for $1 \leq i, j \leq n$. We obtain:

$$\mathcal{TST}(A) = \mathcal{TST}\left((a_{i,j})\right) = \mathcal{TS}\left((a_{j,i})\right) = \mathcal{T}\left((a_{j,n+1-i})\right) = \left(a_{n+1-i,j}\right),$$

and since A is a permutation matrix then $(a_{n+1-i,j}) \neq (a_{i,j})$. Hence, $A \neq \mathcal{TST}(A)$. We will show that $\mathcal{STST}$, $\mathcal{ST}$ and $\mathcal{TS}$ are not in $Stab_{D_8}(A)$. By way of contradiction, suppose that $\mathcal{STST} \in Stab_{D_8}(A)$. Let A be a Costas array of size n. If we apply the transformation $\mathcal{STST}$ on A, we obtain

$$\begin{aligned}\mathcal{STST}\left(\left(a_{i,j}\right)\right) &= \mathcal{STS}\left(\left(a_{j,i}\right)\right)\\ &= \mathcal{ST}\left(\left(a_{j,n+1-i}\right)\right)\\ &= \mathcal{S}\left(\left(a_{n+1-i,j}\right)\right)\\ &= \left(\left(a_{n+1-i,n+1-j}\right)\right).\end{aligned}$$

Therefore, the permutation sequence corresponding to the matrix $\mathcal{STST}(A)$ is $[n+1-f(n), n+1-f(n-1), \ldots, n+1-f(2), n+1-f(1)]$. We claim that $\mathcal{STST}(A)$ is not a Costas array if $\mathcal{STST}(A) = A$, which is a contradiction because the action of D_8 on a set of Costas arrays will preserve the Costas property as shown in Theorem 2.30. If $\mathcal{STST}(A) = A$ then for all $1 \leq j \leq n$ we have $n+1-f(n+1-j) = f(j)$. Substituting $j = 1, 2,$ and then we have

$$n+1-f(n) = f(1) \qquad (2.2)$$

$$n+1-f(n-1) = f(2) \qquad (2.3)$$

Subtracting (2.3) from (2.2) yields $f(n) - f(n-1) = f(2) - f(1)$, violating the Costas property because the values $f(n) - f(n-1)$ and $f(2) - f(1)$ appear in the first row of the difference triangle table of A and can not be equal if A is a Costas array. Therefore, $\mathcal{STST} \notin Stab_{D_8}(A)$. Consequently, $\mathcal{ST} \notin Stab_{D_8}(A)$ because $Stab_{D_8}(A)$ is a subgroup. What is left is to show that $\mathcal{TS} \notin Stab_{D_8}(A)$. Since $Stab_{D_8}(A)$ is a subgroup, it follows that if $\mathcal{TS} \in Stab_{D_8}(A)$, so is $(\mathcal{TS})^{-1}$. But $(\mathcal{TS})^{-1}(A) = \mathcal{S}^{-1}\mathcal{T}^{-1}(A) = \mathcal{ST}(A)$, which is due to the fact that $S^2 = T^2 = 1$, and we already showed that $\mathcal{ST} \notin Stab_{D_8}(A)$. Subsequently, $\mathcal{TS} \notin Stab_{D_8}(A)$.

Therefore, $|Stab_{D_8}(A)| < 3$. Then if $\mathcal{T} \in Stab_{D_8}(A)$ or $\mathcal{STS} \in Stab_{D_8}(A)$ we have $|Stab_{D_8}(A)| = 2$, and otherwise $|Stab_{D_8}(A)| = 1$. □

2.5 Construction Techniques

As we explained in the Overview section, although the foundation of Costas arrays was completely application-oriented, they offer interesting mathematical problems. There are two basic approaches currently being adopted to study Costas arrays. One is the finite field-based construction approach, and the other is computer search.

This section explains these construction methods and the submethods obtained by manipulating the existing constructions. Moreover, we review the main properties of finite fields that we will use and refer to [77] for more details in the theory of finite fields for interested readers, and we provide a summary of the search algorithms' results.

We follow [114] in assuming that all known Costas arrays can be divided up into three distinct categories:

1) **Generated**: A Costas array is called generated if it can be obtained using an algorithm that guarantees the existence of a Costas array and can be constructed using an algebraic technique.

2) **Emergent**: A Costas array is considered emergent if the array emerges from manipulating a generated (or emergent) Costas array.

2) **Sporadic**: A Costas array is sporadic if it has been found through an exhaustive search and is of a completely unknown origin.

After reviewing some basic properties of a finite field, we will discuss these three categories in this chapter.
Let us recall some basic facts about finite fields, and for more details, we refer the reader to [77]. Let p be a prime number. For every power p^r of p, where $r \geq 1$ is a positive integer, there exists a field denoted by $\mathbb{F}_{p^r}$ having exactly p^r elements; and there is essentially only one such field up to isomorphism. If $r = 1$, $\mathbb{F}_p$ is the set of integers $\{0, 1, ..., p-1\}$ modulo p under the operation of addition and multiplication. A fundamental fact about a finite field $\mathbb{F}_q$, where $q = p^r$, is that the multiplicative group of $\mathbb{F}_q$ denoted by $\mathbb{F}_q^\star$ (the set of nonzero elements of $\mathbb{F}_q$) is cyclic. Therefore, $\mathbb{F}_q^\star$ has a generator such that all its successive powers run through all nonzero elements of the field $\mathbb{F}_q$. A generator of $\mathbb{F}_q^\star$ is called a primitive element, and there are $\phi(q-1)$ distinct primitive elements in $\mathbb{F}_q$ where $\phi(x)$ is the Euler's totient function, that gives the number of positive integers less than x relatively prime to x. For further reference, we state the following lemma.

Lemma 2.33 ([86]). *If α is a primitive element of $\mathbb{F}_q$ then α^t is a primitive element of $\mathbb{F}_q$ if and only if $gcd(t, q-1) = 1$.*

2.5.1 The Welch Construction

The Welch Costas arrays were first found by Edgar Gilbert in 1965 [53] and rediscovered in 1982 by Lloyd R. Welch. As we mentioned before, it was S. W. Golomb who proved the validity of this construction [55].

Theorem 2.34 (Exponential Welch Construction [55]). *Let α be a primitive element of $\mathbb{F}_p$, with p a prime and let c be an element of the set $\{0, 1, 2, ..., p-2\}$. Then the $(p-1) \times (p-1)$ permutation matrix, denoted by $W_1^{exp}(p, \alpha, c)$, with $a_{ij} = 1$ if and only if $i \equiv \alpha^{j+c}$ **(mod** p), where $1 \leq i \leq p-1$, $0 \leq j \leq p-2$, is a Costas array.*

Proof. Let us fix an element $c \in \{0, 1, 2, ..., p-2\}$. Since $i \longmapsto \alpha^{i+c}$ (mod p) is a permutation of $\{1, 2, \ldots, p-1\}$ for $0 \leq i \leq p-2$, we have a permutation matrix. On the contrary, suppose that $W_1^{exp}(p, \alpha, c)$ is not a Costas array. Then, there are at least two equal values in a row k, $1 \leq k \leq p-2$, of $T(W_1^{exp}(p, \alpha, c))$, as in Remark 2.23. Assume that for some $1 \leq s < t \leq p-1$, we have

$$\left(\alpha^{s+c+k} \bmod p\right) - \left(\alpha^{s+c} \bmod p\right) = \left(\alpha^{t+c+k} \bmod p\right) - \left(\alpha^{t+c} \bmod p\right).$$

Then, we have

$$\alpha^{s+c}\left(\alpha^{k}-1\right) \bmod p = \alpha^{t+c}\left(\alpha^{k}-1\right) \bmod p.$$

Since $\left(\alpha^{k}-1\right) \not\equiv 0 \bmod p$ and $1 \leq s < t \leq p-1$, this requires $s = t$, which gives a contradiction. Then $W_1^{exp}(p,\alpha,c)$ is a Costas array. □

Example 2.35. *Consider the exponential Welch construction, as in 2.34, for $p = 11$, $\alpha = 2$ and $c = 0$. The permutation $W_1^{exp}(11,2,0) = [1,2,4,8,5,10,9,7,3,6]$ is obtained by raising 2 to successive powers modulo 11 from 0 to 9. The constant c in the definition of exponential Welch suggests it does not matter from which point we can start and any cyclic shift of the permutation is still an exponential Welch, so it is a Costas array. Let us take $c = 3$; then, we construct the permutation $W_1^{exp}(11,2,3) = [8,5,10,9,7,3,6,1,2,4]$, obtained by a cyclic shift of the elements in $W_1^{exp}(11,2,0)$ that sends the first third elements to the end of $W_1^{exp}(11,2,0)$. Let us construct $T(W_1^{exp}(11,2,0))$ and $T(W_1^{exp}(11,2,3))$ as follows:*

1	2	4	8	5	10	9	7	3	6
1	2	4	−3	5	−1	−2	−4	3	
3	6	1	2	4	−3	−6	−1		
7	3	6	1	2	−7	−3			
4	8	5	−1	−2	−4				
9	7	3	−5	1					
8	5	−1	−2						
6	1	2							
2	4								
5									

8	5	10	9	7	3	6	1	2	4
−3	5	−1	−2	−4	3	−5	1	2	
2	4	−3	−6	−1	−2	−4	3		
1	2	−7	−3	−6	−1	−2			
−1	−2	−4	−8	−5	1				
−5	1	−9	−7	−3					
−2	−4	−8	−5						
−7	−3	−6							
−6	−1								
−4									

We can see that each row of these difference triangle tables is free of duplication, meaning $W_1^{exp}(11,2,0)$ and $W_1^{exp}(11,2,3)$ are Costas arrays.

Remark 2.36. *According to the assumption of Theorem 2.34, the corresponding permutation to the exponential Welch Costas array is*

$$W_1^{exp} = [\alpha^{j+c}\ (mod\ p)] \quad for \quad 0 \leq j \leq p-2 \; and \; c \in \{0,1,\ldots,p-2\}.$$

Lemma 2.37. *If there is a dot in any of the four corners of an $n \times n$ Costas array of size n, with $n \in \mathbb{N}$. Then we can remove this dot and its corresponding row and column to obtain an $(n-1) \times (n-1)$ Costas array.*

Proof. Clearly, any violation of the Costas property in reduced version would already be presented in the original pattern. □

The following theorem is an immediate result of Lemma 2.37, from which we obtain an emergent Costas array.

Theorem 2.38 ($W_2^{exp}(p,\alpha)$ exponential Welch)**.** *Let α be a primitive element of $\mathbb{F}_p$, where p is a prime, then permutation $[(\alpha^j \textit{ mod } p) - 1]$ for $1 \leq j \leq p-2$ is a Costas array, denoted by $W_2^{exp}(p,\alpha)$.*

Proof. Let $W_1^{exp}(p,\alpha,0)$ be an exponential Costas array. Since $\alpha^0 = 1 \equiv 1 \pmod{p}$, we always have a dot at top left corner of $W_1^{exp}(p,\alpha,0)$. Regarding lemma 2.37, we can remove this dot and its corresponding row and column to obtain a Costas array of size $p-2$. □

Theorem 2.39 ($W_3^{exp}(p,\alpha)$ exponential Welch)**.** *Suppose that 2 is a primitive element of $\mathbb{F}_p$, where p is a prime. Then, the permutation $[(\alpha^j \textit{ mod } p) - 2]$ for $2 \leq j \leq p-1$ is a Costas array of size $p-3$, denoted by $W_3^{exp}(p,\alpha)$.*

Proof. Since 2 is a primitive element of $\mathbb{F}_p$, $2^0 \equiv 1 \pmod{p}$, and $2^1 \equiv 2 \pmod{p}$. Therefore, we can construct a $W_1^{exp}(p,\alpha,0)$ for which there are two dots at positions $a_{1,1}$ and $a_{2,2}$. Thus we can remove these dots together with their corresponding row and columns to obtain a Costas array of size $p-3$. □

The table below illustrates all variants of exponential Welch Costas arrays' constructions.

TABLE 2.1: The exponential Welch Costas arrays' construction and its submethods. α is a primitive element of the finite field $\mathbb{F}_p$, where p is a prime. (i,j) stands for the dot's position in the permutation matrix, where i shows the row number and j shows the column number of the matrix.

Constructions	Variants	Size	Remarks
Exponential Welch	W_1^{exp}	$p-1$	-
	W_2^{exp}	$p-2$	If $c = 0$, there is a corner dot at position $(1,1)$, which can be removed.
	W_3^{exp}	$p-3$	If $\alpha = 2$, there are dots at positions $(1,1)$ and $(2,2)$. Then dot at position $(2,2)$ after removing dot at position $(1,1)$ is deletable.

According to theorem 2.30, we know that the transpose of an exponential Welch Costas array is again a Costas array, called logarithmic Welch. We follow [37] to propose the following theorem.

Theorem 2.40 (Logarithmic Welch array [37]). *Let α be a primitive element of $\mathbb{F}_p$, with p a prime and c be an element of the set $\{0,1,2,...,p-2\}$. Then the $(p-1)\times(p-1)$ permutation matrix, denoted by $W_1^{log}(p,\alpha,c)$, with $a_{ij}=1$ if and only if $i \equiv c+\log_\alpha j$ mod $(p-1)$, where $1 \le j \le p-1$, $0 \le i \le p-2$, is a Costas array.*

Proof. Suppose that $W_1^{log}(p,\alpha,c) = [(c+\log_\alpha j) \bmod (p-1)]$ for $1 \le j \le p-1$ and a fixed c in $\{0,1,2,...,p-2\}$. By way of contradiction, assume that $W_1^{log}(p,\alpha,c)$ is not a Costas array. Then, at least a row k, $1 \le k \le p-2$, of $T(W_1^{log}(p,\alpha,c))$ with at least one repeated entry exists. Thus, for some $1 \le i < l \le p-1$, we have

$$(\log_\alpha (i+k) - \log_\alpha i) \bmod p-1 = (\log_\alpha (l+k) - \log_\alpha l) \bmod p-1$$

if and only if we have

$$\log_\alpha \tfrac{i+k}{i} \equiv \log_\alpha \tfrac{l+k}{l} \bmod p-1 \Leftrightarrow ik \equiv lk \bmod p-1 \Leftrightarrow i \equiv l \bmod p-1.$$

Since $1 \le i,l \le p-1$, this forces $i=l$, which gives a contradiction. Therefore, $W_1^{log}(p,\alpha,c)$ is a Costas array. □

It is worth noting that the existence of $\log_\alpha j \bmod (p-1)$ in the above theorem can be attributed to the discrete logarithm problem. Since α is a primitive element, every non-zero element j in $\mathbb{F}_p$ can be expressed as a power of α. In other words, there exists an integer x such that $j \equiv \alpha^x \bmod (p)$. By taking the logarithm of both sides with a base of α, we obtain $\log_\alpha j \equiv x \bmod (p-1)$. This demonstrates that for any non-zero element j in $\mathbb{F}p$, it is always possible to find a logarithm base α modulo $(p-1)$, denoted as $\log_\alpha j \bmod (p-1)$, due to the fact that α is a primitive element capable of generating all non-zero elements in $\mathbb{F}_p$.

Remark 2.41. *Theorems 2.38 and 2.39 hold naturally for logarithmic Welch Costas arrays as well.*

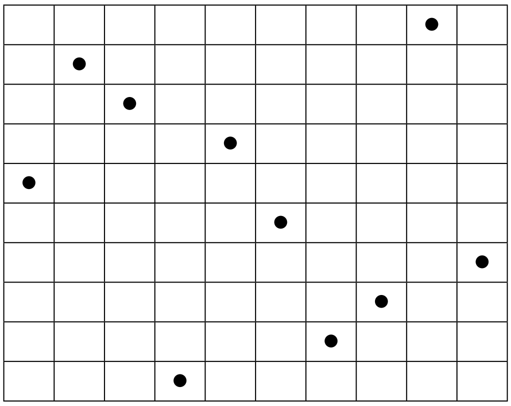
Theorems 2.34 and 2.40 show the two sets of exponential and logarithmic Welch Costas arrays, which form the Welch construction together. As mentioned earlier, we obtain a logarithmic Welch array by transposing an exponential Welch Costas array. It is worth noting that the transpose of an exponential Welch Costas array, $W_1^{exp}(p,\alpha,c)$, with parameters (p,α,c) is not expressible as a logarithmic Welch Costas array with the same parameters regarding our definition of logarithmic Welch. Let us provide an example to make it easier to understand how transposing an exponential Welch can be expressible by a logarithmic Welch Costas array with different parameter c.

Example 2.42. *Since 7 is a primitive element in $\mathbb{F}_{11}$, for $0 \le j \le 9$ and $c=2$, we can construct an exponential Welch Costas array $W_1^{exp}(11,7,2) = [5,2,3,10,4,6,9,8,1,7]$. As in the proof of theorem 2.30, we know that the transpose of a permutation f is defined by f^{-1}. One can easily verify that the transpose of $W_1^{exp}(11,7,2)$ is $[9,2,3,5,1,6,10,8,7,4]$. Let us construct the logarithmic*

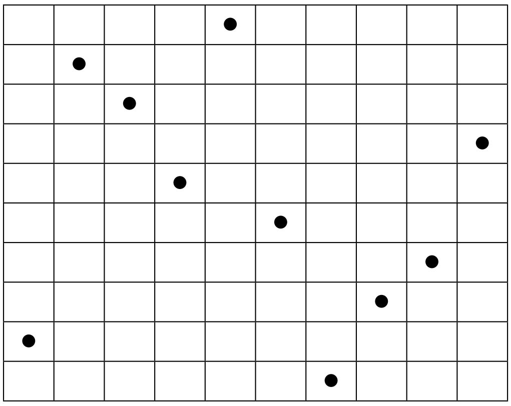
Welch Costas array with the same parameters, $W_1^{log}(11,7,2)$. Using the following calculations

$$\begin{aligned}
&(2+\log_7 1)\ mod\ 10 = 2, && (2+\log_7 2)\ mod\ 10 = 5,\\
&(2+\log_7 3)\ mod\ 10 = 6, && (2+\log_7 4)\ mod\ 10 = 8,\\
&(2+\log_7 5)\ mod\ 10 = 4, && (2+\log_7 6)\ mod\ 10 = 9,\\
&(2+\log_7 7)\ mod\ 10 = 3, && (2+\log_7 8)\ mod\ 10 = 1,\\
&(2+\log_7 9)\ mod\ 10 = 0, && (2+\log_7 10)\ mod\ 10 = 7,
\end{aligned}$$

we can construct $W_1^{log}(11,7,2) = [2,5,6,8,4,9,3,1,0,7]$. In order to have a permutation from 1 to $p-1$, we add all the elements of $W_1^{log}(11,7,2)$ by 1 to acquire $[1,4,5,7,3,8,2,10,9,6]$. As we can see $\left(W_1^{exp}(11,7,2)\right)^T \neq W_1^{log}(11,7,2)$, where T stands for the transpose operation. A trivial verification show that $W_1^{log}(11,7,8) = [8,1,2,4,0,5,9,7,6,3]$, from which, by adding all the elements of $W_1^{log}(11,7,8)$ by one, we obtain $\left(W_1^{exp}(11,7,2)\right)^T = W_1^{log}(11,7,8)$ The permutation matrices of $W_1^{exp}(11,7,2)$ and $W_1^{log}(11,7,8)$ are as follows, respectively:



$W_1^{exp}(11,7,2)$



$W_1^{log}(11,7,8)$

As one can see, matrix $W_1^{log}(11,7,8)$ is obtained by transposing matrix $W_1^{exp}(11,7,2)$.

In general, the following holds:

Observation 2.43. *The transpose of $W_1^{exp}(p,\alpha,c)$ is $W_1^{log}(p,\alpha,-c\ mod\ (p-1))$.*

Proof. One can check that an exponential Welch Costas array $W_1^{exp}(p,\alpha,c)$ can be represented by the bijection $f : \{0,1,\ldots,p-2\} \to \{1,2,\ldots,p-1\}$, which is defined by the formula $f(i) = \alpha^{i+c} \bmod p$. By taking logarithm base α from both sides of this equation, we can see $f^{-1} : \{1,2,\ldots,p-1\} \to \{0,1,\ldots,p-2\}$ can be defined by $f^{-1}(i) = (-c+\log_\alpha i) \bmod (p-1)$. Therefore, $\left(W_1^{exp}(p,\alpha,c)\right)^T = W_1^{log}(p,\alpha,-c \bmod (p-1))$. □

There are two interesting observations about Welch Costas arrays. Firstly, Welch Costas arrays are singly periodic, meaning all circular shifts of the columns of an exponential Welch Costas array are also Costas arrays, and all circular shifts of the rows of a logarithmic Welch Costas array are also Costas arrays [99]. The single periodicity of these arrays results from the effect of parameter c, which is called the offset. In 1984, Golomb and Taylor conjectured that singly periodicity characterizes the Welch construction [60]. This conjecture is still open. Secondly, exponential Costas arrays have the glide-reflection symmetric property, known as G-symmetric [47]. Let us define what we mean by G-symmetric, and then we will discuss this property of exponential Welch. We introduce the notion of glide-reflection symmetry, following Tuvi Etzion [47]. He also provided several valuable constructions of combinatorial designs in which Costas arrays play an essential role, which we will discuss in the next chapter.

Definition 2.44 (G-symmetric property [47]). *Let $A = [f(1), f(2), \ldots, f(n)]$ be a permutation matrix of size n. We say A has G-symmetric property if the following holds:*

- *If n is an even integer and $f\left(i + \frac{n}{2}\right) + f(i) = n + 1$ for $1 \leq i \leq \frac{n}{2}$.*
- *If n is an odd integer, $f(\frac{n+1}{2}) = \frac{n+1}{2}$ and $f\left(i + \frac{n+1}{2}\right) + f(i) = n + 1$ for $1 \leq i < \frac{n+1}{2}$.*

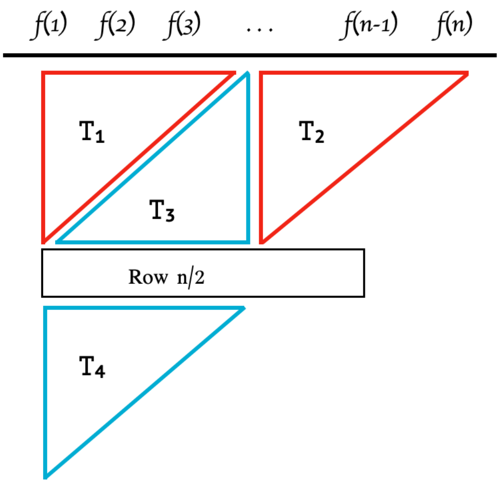
It can be easily seen that exponential Welch Costas arrays have the G-symmetric property. Let p be a prime and α be a primitive element in $\mathbb{F}_p$. As in Definition 2.34, the permutation matrix $A = [\alpha^{c+i} \pmod p]$, for $0 \leq i \leq p-2$, is an exponential Welch Costas array of size $p-1$. Since $p-1$ is even, it is sufficient to show that

$$\alpha^{i+c} \pmod p + \alpha^{i+c+\frac{p-1}{2}} \pmod p = p$$

for $1 \leq i \leq \frac{p-1}{2}$. This is true because $\alpha^{\frac{p-1}{2}} = -1$ over $\mathbb{F}_p$ and

$$\alpha^{i+c} + \alpha^{i+c\frac{p-1}{2}} \equiv \alpha^{i+c}(1 + \alpha^{\frac{p-1}{2}}) \equiv 0 \pmod p.$$

Lemma 2.45 ([119]). *Let $A = [f(1), f(2), ..., f(n)]$ be a G-symmetric Costas array of even size n. Let T_1, T_2, T_3 and T_4 be the triangular regions of the difference triangle table of A showed in the following figure*



The row i of T_1 and T_2 regions contain $\frac{n-2i}{2}$ elements, and T_3 contains i elements. Then

1) $T_2 = -T_1$

2) *The T_3 region's elements in a row k, $1 \le k \le \frac{n}{2} - 1$, are the same as the T_4 region's elements in row $n - k$.*

Proof. For 1, let k be a row of $T(A)$, where $1 \le k \le \frac{n}{2} - 1$. Then the elements in T_2 region for this row are of the form

$$f(j+k) - f(j) \quad \text{for } \tfrac{n}{2} + 1 \le j \le n - k. \tag{2.4}$$

Equivalently, 2.4 is equal to

$$f(\tfrac{n}{2} + j + k) - f(\tfrac{n}{2} + j) \quad \text{for } 1 \le j \le \tfrac{n}{2} - k. \tag{2.5}$$

Since A is G-symmetric, 2.5 is equal to

$$n + 1 - f(j+k) - (n + 1 - f(j)) \quad \text{for } 1 \le j \le \tfrac{n}{2} - k. \tag{2.6}$$

Therefore, $T_2 = -T_1$.
For 2, it can be seen that T_3 region's elements in a row k, $1 \le k \le \frac{n}{2} - 1$, are of the form

$$f(\tfrac{n}{2} + j) - f(\tfrac{n}{2} + j - k) \quad \text{for } 1 \le j \le k. \tag{2.7}$$

Since A is G-symmetric, 2.7 is equal to

$$n + 1 - f(j) - (n + 1 - f(n - k + j)) = f(n - k + j) - f(j) \quad \text{for } 1 \le j \le k,$$

which can be seen these are exactly the elements of row $n - k$ of $T(A)$ for $\frac{n}{2} + 1 \le k \le n - 1$. □

2.5.2 Lempel-Golomb Construction

The previous section discussed one of the main algebraic constructions, Welch construction, and in this section, we will discuss the other one, the

Lempel-Golomb construction. This construction works with two primitive elements of a finite field. These two primitive elements are not necessarily distinct. The case where two primitive elements are equal was pointed out by Lempel and Welch, and S. W. Golomb has generalized this method by taking two distinct primitive elements.

Theorem 2.46 (Lempel-Golomb Construction G_2 [55]). *Let α and β be two primitive elements of $\mathbb{F}_q$ with $q > 2$. Then the $(q-2) \times (q-2)$ permutation matrix with $a_{ij} = 1$ if and only if $\alpha^i + \beta^j = 1$, $1 \leq i, j \leq q-2$, is a Costas array.*

Proof. Our proof starts with the observation that this construction gives a permutation matrix, let us say A. If it is not a permutation matrix, then there is at least one row or one column with at least two non-zero entries. There is no loss of generality in assuming $a_{i_1 j} = 1$ and $a_{i_2 j} = 1$. Therefore, $\alpha^{i_1} + \beta^j = 1$ and $\alpha^{i_2} + \beta^j = 1$, and hence $\alpha^{i_1} = \alpha^{i_2}$. Since $1 \leq i_1, i_2 \leq q-2$, we can conclude that $i_1 = i_2$. So, this is a permutation matrix. From $\alpha^i + \beta^j = 1$, we deduce that

$$\alpha^i + \beta^j = 1 \Leftrightarrow \beta^j = 1 - \alpha^i \Leftrightarrow \log_\beta \beta^j = \log_\beta(1-\alpha^i) \Leftrightarrow j = \log_\beta(1-\alpha^i).$$

Suppose this construction does not give a Costas array. Then, at least one row k, $1 \leq k \leq q-3$, of $T(A)$, containing a repeated value, exists. Assume that for some $1 \leq s < l \leq q-2$, we attain the repeated values in row k as follows:

$$\log_\beta(1-\alpha^{s+k}) - \log_\beta(1-\alpha^s) = \log_\beta(1-\alpha^{l+k}) - \log_\beta(1-\alpha^l),$$

if and only if

$$\log_\beta\left(\tfrac{1-\alpha^{s+k}}{1-\alpha^s}\right) = \log_\beta\left(\tfrac{1-\alpha^{l+k}}{1-\alpha^l}\right) \Leftrightarrow \left(\tfrac{1-\alpha^{s+k}}{1-\alpha^s}\right) = \left(\tfrac{1-\alpha^{l+k}}{1-\alpha^l}\right).$$

By elementary calculation, we obtain

$$\alpha^s(\alpha^k - 1) = \alpha^l(\alpha^k - 1).$$

Since $\alpha^k - 1 \neq 0$, this implies that $\alpha^s = \alpha^l$, and hence $s = l$. Therefore, A is in fact a Costas array. □

Remark 2.47. *In Theorem 2.46, primitive elements α and β are not necessarily distinct. The case where $\alpha = \beta$ is known as Lempel construction. Let us denote this family by L_2.*

Example 2.48. *Consider the quotient ring $\frac{\mathbb{F}_3[x]}{(x^2+1)}$. Since x^2+1 is an irreducible polynomial over $\mathbb{F}_3$, this quotient ring is the finite field with 9 elements. One can check that this field contains the following elements*

$$\{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}.$$

One can verify that the elements $x+1$ and $2x+1$ are generators of the multiplicative group of $\mathbb{F}_9$, because all their successive powers run through all non-zero elements of $\mathbb{F}_9$. Therefore, we can construct a Lempel-Golomb Costas array of size 7 as follows

$$\begin{aligned}
(x+1)^1 + (2x+1)^6 &= 1\\
(x+1)^2 + (2x+1)^3 &= 1\\
(x+1)^3 + (2x+1)^2 &= 1\\
(x+1)^4 + (2x+1)^4 &= 1\\
(x+1)^5 + (2x+1)^5 &= 1\\
(x+1)^6 + (2x+1)^1 &= 1\\
(x+1)^7 + (2x+1)^7 &= 1
\end{aligned}$$

					●	
		●				
	●					
			●			
				●		
●						
						●

Similar to Welch construction, we also can remove corner dots in some cases to obtain Costas arrays of size less than $q-2$. The systematic study of these constructions was reported by W. S. Golomb et al. in 2007 [57]. Table 2.2 collected these constructions together with a construction introduced by W. S. Golomb labelled as T_4 in [59].

2.6 Heuristic Constructions

In Remark 2.15, we saw that removing a dot and its corresponding row and column in the middle of a permutation matrix could be problematic, while Lemma 2.37 showed that removing the corner dots is always possible to obtain a Costas array of smaller sizes. A natural question arises here is it possible to add a corner dot and still have the Costas property? The answer to this question resulted in some heuristic methods by which some Costas arrays have been constructed via adding corner dots and checking whether or not the extended matrix is a Costas array. A more detailed study of these constructions can be found in [35].The most famous heuristic method is the Rickard construction which discovered four previously unknown Costas arrays, two Costas arrays of size 29, one of size 36 and one of size 42 [99].

Definition 2.49 (Rickard Welch construction)**.** *Let α be a primitive element of the finite field $\mathbb{F}_p$, where p is a prime. Consider a $(p-1)$-by-$(p-1)$ Costas array $W_1^{exp}(p,\alpha,c)$, as in Theorem 2.34, and add an empty row at the bottom to attain a p-by-$(p-1)$ matrix. By cyclically shifting the rows of this matrix l times and appending a column to the right of this matrix with a dot in row l, we construct a new permutation matrix of size $p-1$, which may be a Costas array.*

Definition 2.50 (Rickard Golomb construction)**.** *Let α and β be two primitive elements of the finite field $\mathbb{F}_q$, where q is a prime power, and let $A = \left(a_{i,j}\right)$, $1 \leq i,j \leq q-2$, be a Lempel-Golomb Costas array, as in Theorem 2.46. Consider a $q-1$-by-$q-1$ matrix obtained by appending an empty row at the bottom and then*

TABLE 2.2: The Lempel-Golomb construction's submethods. α and β are two primitive elements of the finite field $\mathbb{F}_q$, where q is a prime power. (i, j) stands for the dot's position in the permutation matrix, where i shows the row number and j shows the column number of the matrix.

Constructions	Variants	Size	Remarks
Lempel	L_3	$q-3$	If $\alpha = 2$, then a dot at position $(q-2, q-2)$ can be removed as a corner dot.
Golomb	G_3	$q-3$	If $\alpha^1 + \beta^1 = 1$, then dot at position $(1,1)$ can be removed as a corner dot.
	G_4	$q-4$	If $q = 2^m$, and $\alpha^1 + \beta^1 = 1$, which implies that $\alpha^2 + \beta^2 = 1$. Then dots at position $(1,1)$ and $(2,2)$ can be removed.
	$G_4^\star$	$q-4$	If $\alpha^1 + \beta^1 = 1$ and $\alpha^2 + \beta^{-1} = 1$. Then dot at position $(2, q-2)$ after removing dot at position $(1,1)$ is deletable.
	$G_5^\star$	$q-5$	If $\alpha^1 + \beta^1 = 1$ and $\alpha^2 + \beta^{-1} = 1$, then this implies also $\alpha^{-1} + \beta^2 = 1$, thus dots at positions $(1,1)$, $(2,-1)$ and $(-1,2)$ are deletable.
Taylor	T_4	$q-4$	If $\alpha^2 + \alpha^1 = 1$. Then the dots at positions $(1,2)$ and $(2,1)$ can be removed simultaneously.

an empty column to the right of A. Any cyclic shift of the rows and columns s and t times, respectively, and adding a dot at position (s,t) will result in a new permutation matrix, which may be a Costas array.

J. K. Beard et al. in [9] provided two new heuristic methods to generate Costas arrays, called "Inhom. Add 1" and "Inhom. Sub 1". We refer the reader to [9] for more details on these constructions.

Definition 2.51 (Inhom. Add 1 [9]). *Let α and β be two primitive elements of $\mathbb{F}_q$, where q is a prime power, and let γ be an element in $\mathbb{F}_q$. Let c_1 and c_2 be elements of the set $\{0, 1, \ldots, q-2\}$. Then we can construct a permutation matrix of size $q-1$, with $a_{ij} = 1$ if and only if for $0 \le i, j \le q-2$, $\alpha^{i+c_1} + \beta^{j+c_2} = \gamma$ and $\alpha^{i+c_1} \neq \gamma$, and if $\alpha^{i+c_1} = \gamma$, we add a one at position (i, j), where j is the corresponding integer for which $\beta^{j+c_2} = \gamma$. This permutation matrix may be a Costas array.*

Example 2.52. *Let 2 be the primitive element in $\mathbb{F}_5$. Consider $\gamma = 2$ and $c_1 = c_2 = 0$, then we can construct a 4×4 matrix A by placing a dot at position (i, j), for $0 \le i, j \le 3$, if $2^i + 2^j = 2$ and $2^i \neq 2$. Then, we have $a_{0,0} = a_{2,3} = a_{3,2} = 1$,* *and since* $2^1 = 2$, *we also place a dot at position* $(1,1)$, $a_{1,1} = 1$. *One can easily verify that the corresponding permutation to matrix* A *is* $[1,2,4,3]$, *representing a Costas array.*

Definition 2.53 (Inhom. Sub 1 [9]). *Let* α *and* β *be two primitive elements of* $\mathbb{F}_q$, *where* q *is a prime power, and let* γ *be an element in* $\mathbb{F}_q$. *Let* c_1 *and* c_2 *be elements of the set* $\{0, 1, \ldots, q-2\}$. *Then we can construct a permutation matrix of size* $q-1$, *with* $a_{ij} = 1$ *if and only if for* $0 \le i, j \le q-2$, $\alpha^{i+c_1} - \beta^{j+c_2} = \gamma$ *and* $\alpha^{i+c_1} \neq \gamma$, *and if* $\alpha^{i+c_1} = \gamma$, *we add a one at position* (i,j), *where* j *is the integer for which* $\beta^{j+c_2} = -\gamma \bmod q$. *This permutation matrix may be a Costas array of size* $q-1$.

The other heuristic constructions obtained by adding corner dots can be found in the following table.

Constructions	Variants	Size	Remarks
Welch	W_0	p	Add a corner dot to $W_1^{exp}(p, \alpha, c)$.
Taylor	T_1	$q-1$	Add a corner dot to G_2.
	T_0	q	Add two corner dots to G_2.

TABLE 2.3: Heuristic Constructions obtained by adding corner dots

2.7 Search methods for Costas arrays

As mentioned in the overview section, Costas arrays have been found exhaustively up to size 29. It is worth mentioning that the total run-time of the search for $n = 29$ on a single CPU required the equivalent of 366.55 years, while the real-time required was approximately 230 days due to the high parallelization of the tasks [41]. In 2009, Drakakis et al. published a paper in which they described the size of Costas property checking grows exponentially with n. Thereby, the problem of checking the Costas property is impossible to tackle through the exhaustive search when n becomes large [7]. Databases to various sizes of Costas arrays have been available for many years. James Beard provided a Database of all known Costas arrays up size 1030, which is by far the most extensive database than any other Databases. It is also uploaded to IEEE DataPort [10]. A user-friendly and very powerful GUI extraction utility accompanies the Database. In this thesis, we took advantage of this database on many occasions. Let us denote the number of Costas arrays of size n by $\mathcal{C}_n$. Table 2.4 illustrates all known values of $\mathcal{C}_n$ for sizes 1 through 31 and some extractable information from the Database. Specifically, the number of Costas arrays with diagonal symmetry (there is a dot at position (i,j) if and only if there is a dot at position (j,i)) and G-symmetric property and the number of equivalence classes of each size. In order to understand better the numbers in Table 2.4 , take size 10 as an example. We have 277 equivalence classes in which there are 14 inequivalent Costas arrays with diagonal symmetry, showing $277 - 14 = 263$

equivalence classes contain eight elements and 14 equivalence classes contain four elements. It follows then that we have $263 \times 8 + 4 \times 14 = 2160$ Costas arrays of size 10.

TABLE 2.4: Known Costas arrays enumeration for sizes 1 through 33
$\mathcal{C}_n$ is the number of Costas arrays of size n, the third column shows the number of equivalence classes for each size n, and the fourth and fifth columns illustrate the number of inequivalent Costas arrays of size n with diagonal symmetry and G-symmetric properties, respectively.

Size	$\mathcal{C}_n$	Equivalence Classes	Diagonal Symmetry	G-symmetry
1	1	1	1	1
2	2	1	1	1
3	4	1	1	0
4	12	2	1	2
5	40	6	2	1
6	116	17	5	4
7	200	30	10	0
8	444	60	9	3
9	760	100	10	0
10	2160	227	14	24
11	4368	555	18	0
12	7852	990	17	44
13	12828	1616	25	4
14	17252	2168	23	31
15	19612	2467	31	0
16	21104	2648	20	77
17	18276	2294	19	0
18	15096	1892	10	29
19	10240	1238	6	0
20	6464	810	4	3
21	3536	446	8	0
22	2052	259	5	55
23	872	114	10	0
24	200	25	0	0
25	88	12	2	0
26	56	8	2	0
27	204	29	7	0
28	712	89	0	84
29	164	23	5	0
30	$\geq$664	$\geq$85	$\geq$4	$\geq$60
31	$\geq$8	$\geq$1	$\geq$0	$\geq$0

In table 2.4, we used the sign $\geq$ for Costas arrays of sizes 30 and 31 because the enumeration of these sizes have not been completed. In order to answer the question do Costas arrays exist in all sizes?, we need to introduce a lower bound for $\mathcal{C}_n$ for every $n > 0$, which naturally can be seen as a decision problem. Drakakis showed that this decision problem lies in NP [35].

In 2014, Soltanalian et al. in [108] proposed a sparse formulation of the Costas array search problem, by which they considered the Costas array search problem as an optimization problem. Although their proposed optimization problems are NP-hard, they believe that their formulation may result in more effective control of the Costas array search problem than the brute-force methods.

One can naturally think of the Costas arrays search problem as constraint satisfaction problems (CSPs). CSPs are multi-variable combinatorial problems that can be used when we formulate a problem using a set of decision variables and a set of constraints between variables. The goal is to find an assignment of values to the variables in such a way that these values satisfy a set of constraints. David Vulakh et al. (2022) have recently developed a search algorithm that reduces the time-to-first solution of finding a Costas array of size 16 by a factor of over 300 [116]. They proposed an Ant Colony Optimization (ACO) algorithm for combinatorial CSPs, called m-Dimensional Relative Ant Colony Optimization (mDRACO), concentrating on the Costas array search problem. There have been several developed algorithms to reduce the time complexity of the Costas array search problem, most of which show better performance in finding a solution than the brute-force methods, but none of them could find an example of a Costas array of size 32 so far [1,4,17,20,29,30,121].

It was always a challenging problem to predict the asymptotic behaviour of $\mathcal{C}_n$. The study of the asymptotic behaviour of $\mathcal{C}_n$ has been considered as studying the density of Costas arrays, denoted by $D(n)$, in Costas arrays' literature [22]. The density is defined as

$$D(n) \equiv \frac{\mathcal{C}_n}{n!}.$$

Golomb and Taylor proposed the first conjecture about the asymptotic behaviour of Costas arrays [54]. They conjectured that the density of Costas arrays among permutation matrices tends to zero. In other words,

$$\frac{\mathcal{C}_n}{n!} \to 0 \quad \text{as } n \to \infty.$$

In 1989, Davies published a paper in which he proved

$$\frac{\mathcal{C}_n}{n!} \leq \frac{O(1)}{n}.$$

This result can be found in [28]. Numerical evidence suggested a much faster decay than davies' bound [22], and Drakakis conjectured that the density of Costas arrays decays exponentially [34]. This exciting and core problem of Costas arrays is proved recently by Lutz Warnke, Bill Correll, and Christopher N. Swanson in [118].

2.8 Sporadic Costas arrays

As mentioned in the overview chapter, the vast majority of known Costas arrays up to size 27 are sporadic (are currently unexplained). Little is known about sporadic Costas arrays, and it is not clear whether they occur accidentally in small sizes or if there is an undiscovered construction technique for these arrays. Ken Taylor et al. provided Table 2.5 in [114] for categorizing the Costas arrays database into three distinct categories, introduced in subsection 2.5.

TABLE 2.5: Categorizing the equivalence classes of Costas arrays database according to their origin
(Here the second and third columns show the number of generated and emergent equivalence classes, respectively, and the last column illustrates the number of sporadic Costas arrays of size n.)

Size	Equivalence Classes	Generated	Emergent	Sporadic
1	1	1	0	0
2	1	1	0	0
3	1	1	0	0
4	2	2	0	0
5	6	4	2	0
6	17	7	10	0
7	30	3	27	0
8	60	2	58	0
9	100	5	83	12
10	227	14	151	112
11	555	5	163	387
12	990	14	145	831
13	1616	1	76	1539
14	2168	5	27	2136
15	2467	15	10	2442
16	2648	34	11	2603
17	2294	8	18	2267
18	1892	27	5	1860
19	1238	0	2	1281
20	810	3	1	806
21	446	20	1	425
22	259	56	9	194
23	114	6	10	98
24	25	1	1	23
25	12	7	0	5
26	8	4	2	2
27	29	28	0	1
28	89	88	1	0
29	29	17	6	1

As Table 2.5 indicates, the first sporadic Costas arrays occur at size 9, and size 19 is the first size for which no generated arrays exist. It is apparent from Table 2.5 that very few Costas arrays belong to the generated category, showing the necessity of further work in analyzing the Costas arrays' properties in each category. After size 8, the first sizes for which no sporadic Costas arrays exist are 28 and 29, and for size 27, only one equivalence class of sporadic Costas arrays exists. J. Silverman et al. in [106] developed a probabilistic estimation formula to predict the total number of Costas arrays in each size (C_n), from which they predicted the peak in C_n at size 16. Moreover, they observed that there is the possibility that for $n \geq 30$, the total number of Costas arrays for some of these sizes could be zero. Therefore, there is also the possibility that sporadic Costas arrays cease to exist from specific sizes onwards [34].

The more we understand the properties of sporadic Costas arrays, the more explanation we can provide for the Costas arrays' origin, which may lead to the discovery of a new generation technique. We will follow this point of view in the next chapter, in which we introduce a new transformation by which we can explain the origin of some of these sporadic Costas arrays.

Chapter 3

A new transformation for Costas arrays

Numerous studies have attempted to find structural properties on Costas arrays. Structural properties of Costas arrays will provide a better understanding of Costas arrays and could lead to finding new construction methods [23, 24, 58, 69]. Another possible approach to achieve a deeper understanding of the Costas arrays properties would be finding matrices close to being Costas arrays and then investigating the properties that cause the violation of the Costas property. There are several ways to define when a given permutation matrix is close to being a Costas array. Several authors have introduced definitions derived from relaxing the Costas arrays definition. These types of relaxation can be used to construct two-dimensional synchronization patterns with good autocorrelation properties. Section 2.3 explained that a Costas array of size n has a 3-valued aperiodic autocorrelation function, namely with valued 0, 1, and n (at $(0,0)$ shift). In 1990, Tuvi Etzion in [47] introduced the concept of binary permutation matrices of size n, which has a 4-valued autocorrelation function (with values 0, 1, 2, and n). An $n \times n$ binary permutation matrix has a 4-valued aperiodic autocorrelation function if and only if each pattern of three ones occurs at most once in the given matrix. In his work, he proposed several combinatorial designs derived from Costas arrays with the property that the aperiodic autocorrelation function has four values. In another attempt to relax the definition of Costas arrays, in 2003, Oscar Moreno published a paper introducing the concept of generalized Costas arrays (permutation matrices with maximum aperiodic auto- and crosscorrelation function values of 2), which their constructions and properties are of some interest [80].

This chapter's primary purpose is to introduce a new transformation with the property that, after applying this transformation on the existing Costas arrays, we always obtain permutation matrices with the maximum aperiodic autocorrelation functions value of at most two at none-zero shifts. Surprisingly, this transformation leaves the Costas property invariant for most of the generated Costas arrays, some of the emergent, and some of the sporadic ones. There are examples of generated and emergent Costas arrays with the property that the transformed matrices belong to the sporadic category, meaning that this transformation explains how some of these sporadic Costas arrays are obtained. Consequently, we can reduce the total number of sporadic equivalence classes in Table 2.5 and consider

them emergent Costas arrays. Before going through the details of our new transformation, we will examine the maximum number of common points between two given Costas arrays, from which we can decide if there would be a transformation that links a given Costas array into another one, how many points need to be changed using this transformation.
It is required to explain how we use the Database of all known Costas arrays in this chapter. The database root folder contains the subfolders \Searches and \generated. For convenience, we consider Costas arrays in two classes. The \generated subfolder contains all generated and emergent Costas arrays, and we mean by none-generated the Costas arrays in the \searches subfolder, which are not in the \generated subfolder. We performed all our computations through this chapter on both classes.

3.1 Transforming the existing Costas arrays

As we mentioned in the introductory chapter, we think of a permutation as a rearrangement of the elements of the set $\{1, 2, \ldots, n\}$ into a one-to-one correspondence with $\{1, 2, \ldots, n\}$ itself. To construct a Costas array from a given one, one may ask, what is the smallest set of values of a given Costas permutation that need to be rearranged to obtain another Costas permutation? This question also can be asked differently. What is the size of the set of common points of two given Costas permutations? Answering the second question will reveal the minimum set of dots that need to be rearranged to transform a given Costas permutation into another one. Let us provide the precise definition of the common points between any two permutations of size n.

Definition 3.1 (Common points). *Let $\sigma : [n] \longrightarrow [n]$ and $\gamma : [n] \longrightarrow [n]$ be two permutations of size n. Let us denote the number of common points between σ and γ by $CP(\sigma, \gamma)$, which is given by*

$$CP(\sigma, \gamma) = \#\{i \mid \sigma(i) = \gamma(i)\},$$

where #A denotes the cardinality of a set A.

It is also informative if we know the distributions of the number of common points between any two Costas arrays of size n.

Definition 3.2 (The distribution of the number of common points). *Let us denote a subset of all permutation matrices of size n with t elements by $X_n = \{\sigma_i : \sigma_i : [n] \longrightarrow [n]$ is a bijection and $0 \leq i \leq t\}$. We define for $0 \leq k \leq n-1$,*

$$D_{X_n}(k) = \#\{(\sigma_i, \sigma_j) \mid \sigma_i, \sigma_j \in X_n, 0 \leq i < j \leq t, \text{ and } CP(\sigma_i, \sigma_j) = k\}.$$

That is, $D_{X_n}(k)$ is the number of distinct pairs of elements in X_n that have exactly k common points. Note that since $CP(\sigma_i, \sigma_j) = CP(\sigma_j, \sigma_i)$, we choose $i < j$ in order to avoid over-counting.The set $\{(k, D_{X_n}(k) : 0 \leq k \leq n-1\}$ is the distribution set of the number of common points.

It is worth noting that the number of common points between two given Costas arrays is equal to the value of their crosscorrelation function at $(0,0)$ shift (origin). Drakakis in [36] explained why there is a particular interest in the value of crosscorrelation at the origin. Firstly, this value is the only practical value in a multiuser system where users' clocks are synchronized. Secondly, it is often easier to compute than a given non-zero shift. This section will discuss the crosscorrelation properties of Costas arrays at the origin. Moreover, we provide the most critical observations regarding the crosscorrelation value at the origin (the number of common points between any two Costas arrays).

Let us denote the set of all Costas arrays of size n by C_n. Regarding Definition 3.2, the distribution set of the number of common points of any two elements of C_n is $\{(k, D_{C_n}(k)) : 0 \leq k \leq n-1\}$, and let us denote this set by D_{C_n}. We did a computer search to compute the values mentioned above using the Database of all known Costas arrays from size 2 through 100. We picked any two Costas arrays of a given size n and calculated the number of points they had in common. The more dots any two Costas arrays have in common, the fewer rearrangement we need to apply to transform a Costas array into another one. Therefore, we found the maximum value among the number of common dots of any two given Costas arrays of size n, showing at least how many dots need to rearrange to transform a Costas array into another one. Table 3.1 collected all the values mentioned above.

TABLE 3.1: The distributions of the number of common points: the second column shows the set of ordered pairs $\{(k, D_{C_n}(k))\}$, and the third column illustrates the maximum value of the distribution set, denoted by MD_{C_n}.

size	$\{(k, D_{C_n}(k))\}$	MD_{C_n}
1	—	—
2	$\{(0,1)\}$	0
3	$\{(0,2),(1,4)\}$	1
4	$\{(0,34),(1,16),(2,16)\}$	2
5	$\{(0,274),(1,336),(2,114),(3,56)\}$	3
6	$\{(0,2508),(1,2360),(2,1346),(3,380),(4,76)\}$	4
7	$\{(0,6960),(1,7434),(2,3706),(3,1448),(4,280),(5,72)\}$	5
8	$\{(0,37228),(1,34508),(2,18634),(3,5832),(4,1644),(5,348),(6,152)\}$	6
9	$\{(0,103298),(1,106336),(2,53754),(3,19040),(4,4584),(5,1136),(6,192),(7,80)\}$	7
10	$\{(0,847198),(1,841152),(2,444490),(3,147832),(4,39612),(5,8532),(6,2364),(7,364),(8,176)\}$	8
11	$\{(0,3388642),(1,3509484),(2,1811978),(3,619920),(4,162156),(5,36220),(6,6780),(7,1920),(8,288),(9,140)\}$	9

size	$\{(k, D_{C_n}(k))\}$	MD_{C_n}
12	$\{(0,11142006),(1,11279432),(2,5794372),(3,1959320),(4,512220),(5,107680),(6,22152),(7,3928),(8,1636),(9,144),(10,136)\}$	10
13	$\{(0,29478750),(1,30215332),(2,15544376),(3,5303360),(4,1371972),(5,291260),(6,54624),(7,9816),(8,1752),(9,932),(10,116),(11,88)\}$	11
14	$\{(0,53281396),(1,54584180),(2,28152398),(3,9657464),(4,2491284),(5,522488),(6,96692),(7,16944),(8,3108),(9,660),(10,360),(11,32),(12,120)\}$	12
15	$\{(0,68683920),(1,70601982),(2,36441728),(3,12502000),(4,3241664),(5,685844),(6,122844),(7,20924),(8,3484),(9,780),(10,140),(11,56),(12,24),(13,76)\}$	13
16	$\{(0,79791926),(1,81701472),(2,42079462),(3,14417132),(4,3735092),(5,784540),(6,140688),(7,23248),(8,4204),(9,696),(10,276),(11,60),(12,24),(13,12),(14,24)\}$	14
17	$\{(0,59541992),(1,61312788),(2,31698134),(3,10904332),(4,2820384),(5,592200),(6,106484),(7,17268),(8,2732),(9,500),(10,56),(11,28),(12,4),(13,16),(14,16),(15,16)\}$	15
18	$\{(0,40454286),(1,41861516),(2,21681450),(3,7494292),(4,1947684),(5,409116),(6,74708),(7,11908),(8,1756),(9,272),(10,44),(11,20),(12,8)\}$	12
19	$\{(0,18556592),(1,19244758),(2,10013594),(3,3468588),(4,906476),(5,192392),(6,34472),(7,5732),(8,940),(9,120),(10,16)\}$	10
20	$\{(0,7384300),(1,7661228),(2,3992648),(3,1390936),(4,365328),(5,77480),(6,13616),(7,2492),(8,356),(9,32)\}$	9
21	$\{(0,2196898),(1,2298068),(2,1199254),(3,418228),(4,110012),(5,22764),(6,3968),(7,572),(8,108),(10,4),(11,4)\}$	11
22	$\{(0,766072),(1,751188),(2,411002),(3,134120),(4,33780),(5,6724),(6,1156),(7,252),(8,12),(9,4),(10,16)\}$	10
23	$\{(0,134848),(1,139604),(2,72360),(3,24592),(4,6296),(5,1540),(6,372),(7,100),(8,8),(11,32),(21,4)\}$	21
24	$\{(0,7288),(1,6976),(2,3960),(3,1256),(4,364),(5,48),(6,4),(7,4)\}$	7
25	$\{(0,1032),(1,1876),(2,488),(3,184),(4,248)\}$	4

size	$\{(k, D_{C_n}(k))\}$	MD_{C_n}
26	$\{(0,624),(1,492),(2,304),(3,100),(4,20)\}$	4
27	$\{(0,7784),(1,7084),(2,2954),(3,2208),(4,280),(5,156),(6,72),(13,168)\}$	13
28	$\{(0,128744),(1,50984),(2,49532),(3,8712),(4,13920),(5,452),(6,72),(7,20),(8,8),(14,672)\}$	14
29	$\{(0,3704),(1,4176),(2,2706),(3,1804),(4,476),(5,384),(6,24),(7,8),(9,84)\}$	9
30	$\{(0,110592),(1,52968),(2,37220),(3,8972),(4,2868),(5,3116),(6,3656),(7,4),(10,720)\}$	10
31	$\{(0,12),(1,8),(2,4),(3,4)\}$	3
32	—	—
33	—	—
34	$\{(0,96),(1,32),(2,50),(3,4),(4,8)\}$	4
35	$\{(0,4568),(1,6056),(2,4116),(3,1668),(4,632),(5,432),(7,288),(8,72),(11,336),(17,168)\}$	17
36	$\{(0,216906),(1,75992),(2,61096),(3,12280),(4,14648),(5,656),(6,5236),(7,16),(12,2592),(18,864)\}$	18
37	$\{(0,44),(1,128),(2,68),(3,24),(4,12)\}$	4
38	$\{(0,84),(1,100),(2,44),(3,28),(4,4),(5,16)\}$	5
39	$\{(0,17000),(1,20388),(2,6112),(3,3636),(4,832),(5,384),(6,768),(7,928),(9,704),(19,288)\}$	19
40	$\{(0,454766),(1,154276),(2,155220),(3,26216),(4,25876),(5,1304),(6,260),(7,64),(8,9600),(10,5124),(20,1280)\}$	20
41	$\{(0,4396),(1,4560),(2,4444),(3,2164),(4,1448),(5,1156),(13,168)\}$	13
42	$\{(0,280616),(1,100040),(2,102428),(3,16340),(4,4144),(5,848),(6,17780),(7,40),(8,20),(9,8),(14,1512)\}$	14
43	—	—
44	$\{(0,396),(1,468),(2,152),(3,76),(4,8),(5,24),(6,4)\}$	6
45	$\{(0,61294),(1,62488),(2,28088),(3,9524),(4,356),(5,8),(6,1456),(7,92)\}$	7
46	$\{(0,926632),(1,391408),(2,684030),(3,65456),(4,16380),(5,3328),(6,596),(7,88),(8,16),(9,8),(10,4)\}$	10
47	$\{(0,312),(1,2952),(2,1022),(3,904),(4,768),(5,1280),(6,256),(7,512),(8,64),(11,320),(15,128),(23,128)\}$	23
48	—	—

size	$\{(k, D_{C_n}(k))\}$	MD_{C_n}
49	—	—
50	$\{(0,616),(1,372),(2,182),(3,96),(4,24),(5,36)\}$	5
51	$\{(0,78024),(1,89380),(2,38360),(3,14804),(4,2040),(5,684),(6,1252),(12,288),(25,624)\}$	25
52	$\{(0,1599134),(1,572884),(2,642816),(3,96684),(4,203408),(5,5272),(6,836),(7,156),(8,48),(9,12),(10,4),(26,2496)\}$	26
53	$\{(1,16),(2,4),(3,8)\}$	3
54	—	—
55	$\{(0,2),(1,4)\}$	1
56	$\{(0,846),(1,820),(2,432),(3,100),(4,52),(5,4),(11,24)\}$	11
57	$\{(0,162300),(1,158196),(2,65456),(3,27932),(4,5532),(5,2520),(6,20),(12,784)\}$	12
58	$\{(0,2366500),(1,1007164),(2,1772310),(3,166352),(4,41752),(5,8544),(6,1388),(7,376),(8,48),(9,8),(10,8)\}$	10
59	$\{(0,10000),(1,13524),(2,10988),(3,9820),(4,2316),(5,1252),(7,1024),(8,260),(9,288),(11,864),(14,128),(19,288),(29,288)\}$	29
60	$\{(0,1084490),(1,348472),(2,260276),(3,56416),(4,58300),(5,3040),(6,29300),(7,60),(8,16),(9,8),(10,5760),(12,14400),(13,8),(20,2880),(30,1920)\}$	30
61	$\{(1,34),(2,12),(3,8),(7,4),(14,8)\}$	14
62	$\{(0,7452),(2,7452),(3,1728),(5,1944),(6,2268),(8,1728),(15,216),(20,432)\}$	20
63	—	—
64	$\{(0,334),(1,348),(2,168),(3,64),(4,16),(5,8),(6,4),(7,4)\}$	7
65	$\{(0,27980),(1,28236),(2,26896),(3,19380),(4,4204),(5,6212),(6,408),(7,404),(8,800),(21,440)\}$	21
66	$\{(0,1853676),(1,643092),(2,713632),(3,105648),(4,26160),(5,5424),(6,131752),(7,104),(8,28),(9,4),(22,3960)\}$	22
67	$\{(1,4),(2,2)\}$	2
68	$\{(0,204),(1,172),(2,88),(3,28),(5,4)\}$	5
69	$\{(0,90456),(1,81520),(2,33456),(3,11988),(4,1308),(5,296),(6,1440),(9,3120),(13,1872)\}$	13

size	$\{(k, D_{C_n}(k))\}$	MD_{C_n}
70	$\{(0,2931864),(1,1079716),(2,1421108),(3,178104),(4,45628),(5,8896),(6,1480),(7,276),(8,48),(9,12),(10,58804),(14,25200)\}$	14
71	$\{(0,46956),(1,45644),(2,58008),(3,26928),(4,16504),(5,13360),(6,2888),(7,2448),(8,2016),(9,3456),(10,1152),(11,1536),(14,1152),(17,1536),(23,1248),(35,624)\}$	35
72	$\{(0,3443916),(1,1092004),(2,920760),(3,184208),(4,139660),(5,9672),(6,84720),(7,192),(8,46696),(9,20),(10,8),(12,20736),(18,13824),(24,10368),(36,3456)\}$	36
73	—	—
74	—	—
75	$\{(0,2),(1,4)\}$	1
76	$\{(0,88),(1,100),(2,68),(3,12),(5,4),(8,4)\}$	8
77	$\{(0,44712),(1,69032),(2,47976),(3,44024),(4,8280),(5,9268),(6,96),(7,4),(8,864),(9,576),(25,624)\}$	25
78	$\{(0,3731488),(1,1306564),(2,1455990),(3,217136),(4,53912),(5,11276),(6,269604),(7,232),(8,72),(26,5616)\}$	26
79	$\{(1,16512),(3,6656),(5,2560),(7,3200),(9,1408),(11,512),(15,896),(19,640),(39,256)\}$	39
80	$\{(0,1402),(1,1268),(2,608),(3,124),(4,60),(5,20),(6,4)\}$	6
81	$\{(0,553160),(1,634712),(2,232440),(3,102488),(4,16112),(5,2604),(6,6404)\}$	6
82	$\{(0,9469656),(1,3956284),(2,7222472),(3,661016),(4,164608),(5,32944),(6,5520),(7,892),(8,108),(9,16),(10,4)\}$	10
83	—	—
84	—	—
85	—	—
86	$\{(0,1004),(1,756),(2,464),(3,208),(4,76),(5,32),(6,12),(8,4)\}$	8
87	$\{(0,415780),(1,593628),(2,327372),(3,141208),(4,24756),(5,11896),(6,6720),(7,16720),(9,4000),(21,4160),(43,1680)\}$	43
88	$\{(0,13078044),(1,4562004),(2,5058788),(3,759756),(4,889228),(5,37940),(6,6644),(7,1024),(8,348616),(9,24),(10,8),(11,4),(22,28160),(44,7040)\}$	44
89	—	—
90	—	—

size	$\{(k, D_{C_n}(k))\}$	MD_{C_n}
91	—	—
92	—	—
93	—	—
94	$\{(0,404),(1,300),(2,280),(3,100),(4,36),(13,8)\}$	13
95	$\{(0,134588),(1,154096),(2,148252),(3,124060),(4,41192),(5,23600),(6,8324),(7,12416),(9,4096),(11,4352),(13,1024),(14,1024),(15,1088),(23,2688),(31,1088),(47,1088)\}$	47
96	$\{(0,10803132),(1,3478556),(2,2914324),(3,578864),(4,438592),(5,28256),(6,398352),(7,700),(8,73840),(9,8),(12,98304),(16,18432),(24,24576),(32,9216),(48,6144)\}$	48
97	—	—
98	$\{(0,900),(1,732),(2,410),(3,172),(4,36),(5,16),(6,4),(11,8)\}$	11
99	$\{(0,543828),(1,582684),(2,244352),(3,112500),(4,32884),(5,5972),(6,1608),(7,172),(9,9920),(10,3200),(12,1600),(19,6720),(24,800),(49,1680)\}$	49
100	$\{(0,17216724),(1,5943400),(2,5976400),(3,992684),(4,1749668),(5,50832),(6,9004),(7,1268),(8,236),(9,44),(10,160008),(19,8),(20,80000),(50,8000)\}$	50

Table 3.1 can provide a comprehensive review of the crosscorrelation properties of Costas arrays at origin. Several authors have studied the crosscorrelation properties of Costas arrays and their importance in applications where low aperiodic crosscorrelation is essential. Although most parts of Table 3.1 can be explained using results in the references mentioned earlier, several questions remain unanswered at present. Chapter 1 reviewed most of these studies, and we will provide more details in this section. In 1990, Titlebaum et al. in [115] studied the crosscorrelation of Welch Costas arrays, showing that the maximum value of the crosscorrelation function of any two Welch Costas arrays of size $p-1$ is at most $\frac{p-1}{2}$, and they also showed that if the prime p is of the form $4k+1$ for some integer k, the maximum value can be obtained by a specific choice of primitive elements. Drakakis et al. in [39] also discussed the maximum value of the crosscorrelation of Welch Costas arrays at origin more thoroughly, providing proof and explanation also for the prime number p of the form $4k-1$ for some integer k. We refer the reader to [39] for the proof of the following theorem.

Theorem 3.3 ([39]). *Let α_1 and α_2 be two distinct primitive elements of the finite field $\mathbb{F}_p$, where p is a prime and let $W_1^{exp}(p,\alpha_1,c)$ and $W_1^{exp}(p,\alpha_2,c)$, where $c \in \{0,1,\dots,p-2\}$, be two exponential Welch Costas arrays with corresponding* *matrices A and B, respectively. Let w be the smallest prime divisor of $\frac{p-1}{2}$. Then, for any vertical shift $2-p \leq r \leq p-2$ we obtain*

$$\max C^{a}_{A,B}(r,0) = \frac{p-1}{w}.$$

Let us note that the above theorem discusses more than crosscorrelation at the origin while also considering possible shifts in one direction. The following theorem indicates which choice of primitive elements leads to the maximum value of the common points between any two Welch Costas arrays. We will provide more straightforward proof for the following theorem than the proof in [115].

Theorem 3.4 ([115])**.** *Given any prime p, suppose that p is of the form $4k+1$ for some integer k. Then there are $\frac{\phi(p-1)}{2}$ pairs of distinct exponential Welch Costas arrays with exactly $\frac{p-1}{2}$ common points, where ϕ denotes the Euler's Phi function.*

Proof. Since $p \equiv 1 \bmod 4$, then α is a primitive element of $\mathbb{F}_p$ if and only if $-\alpha$ is [21]. Suppose that $W_1^{exp}(p,\alpha,0)$ is an exponential Costas array as in Theorem 2.34. Since $-\alpha$ is also a primitive element, then we can construct $W_1^{exp}(p,-\alpha,0)$ exponential Costas array. We claim that $W_1^{exp}(p,\alpha,0)$ and $W_1^{exp}(p,-\alpha,0)$ exponential Costas arrays have exactly $\frac{p-1}{2}$ common points. The number of common points can be obtained by finding the number of solutions of the equation

$$\alpha^i \bmod p = (-\alpha)^i \bmod p.$$

Since $-1 = \alpha^{\frac{p-1}{2}}$, then we obtain

$$\alpha^{i\left(\frac{p-1}{2}\right)} \equiv 1 \bmod p. \tag{3.1}$$

It is immediate that Equation 3.1 for any even integer i has a solution. Since $0 \leq i \leq p-2$, then there are $\frac{p-1}{2}$ even integers that provide a solution for Equation 3.1. It is easy to check that there are $\frac{\phi(p-1)}{2}$ such pairs of exponential Welch Costas arrays. □

It is a simple matter to show that any other choice of primitive elements in Theorem 3.4 will lead to the smaller number of common points than $\frac{p-1}{2}$. We follow [39] in proving the following theorem.

Theorem 3.5. *Let α_1 and α_2 be two distinct primitive elements of the finite field $\mathbb{F}_p$, where p is a prime and let $W_1^{exp}(p,\alpha_1,c_1)$ and $W_1^{exp}(p,\alpha_2,c_2)$, where $c_1,c_2 \in \{0,1,\ldots,p-2\}$, be two exponential Welch Costas arrays as in Theorem 2.34. Then the maximum number of common points can be attained if and only if $p \equiv 1$ mod 4 and $\alpha_2 = -\alpha_1 = \alpha_1^{\frac{p-1}{2}+1}$.*

Proof. Clearly, to compute the number of common points, we need to solve the following equation

$$\alpha_1{}^{i+c_1} \bmod p = \alpha_2{}^{i+c_2} \bmod p.$$

Since α_1 and α_2 are primitive elements, then there exists an integer $k \in \{2, \ldots, p-2\}$ such that $gcd(k, p-1) = 1$ and $\alpha_2 = \alpha_1^k$, then by taking logarithm base α_1 from both sides of the above equation, we have

$$(i + c_1) \equiv k(i + c_2) \bmod p - 1 \Leftrightarrow (k-1)i \equiv (c_1 - kc_2) \bmod p - 1.$$

It can be seen that the above congruence has a solution if and only if $d := gcd(k-1, p-1)$ divides $(c_1 - kc_2)$ [101]. If $d|(c_1 - kc_2)$, it has exactly d incongruent solutions modulo $p-1$, and no solution otherwise. Since d is a divisor of $p-1$, then the maximum possible value for d is $\frac{p-1}{2}$, which attains if and only if $gcd\left(\frac{2(k-1)}{p-1}, 2\right) = 1$ if and only if $\frac{2(k-1)}{p-1} = 1$ if and only if $k = \frac{p-1}{2} + 1$, and $gcd(k, p-1) = 1$ simultaneously. Since $1 = gcd\left(\frac{p-1}{2} + 1, p-1\right) = gcd\left(\frac{p-1}{2} + 1, 2\right)$, then we obtain $\frac{p-1}{2} + 1 \equiv 1 \bmod 2$, showing $p \equiv 1 \bmod 4$, which completes the proof. □

Since all known Costas arrays of size $n \geq 28$ are either generated or emergent, it is interesting to investigate whether one can explain the maximum value of the Costas arrays' common points for these sizes. Theorem 3.3 justifies some of the maximum values of the number of common points in Table 3.1, where the size of the Costas arrays is $p-1$ for a prime p. For instance, Table 3.1 illustrates that for $n = 36$, the maximum number of common points is 18. Since 37 is a prime of form $4k+1$ for $k = 9$, the maximum number of common points for Welch Costas arrays is equal to 18, which is the maximum number of common points between any two known Costas arrays of size 36. Using the database of all known Costas arrays, one can check that all Costas arrays of size 36 have been constructed using Welch, $G_5^\star$ (Table 2.2), T_1 (Table 2.3), and Inhom. Add 1 (Definition 2.51).

Having discussed the number of common points of Welch Costas arrays, we will now discuss the number of common points of Lempel-Golomb Costas arrays. The crosscorrelation of Lempel-Golomb Costas arrays at origin (the number of common points) is substantially more complicated than that of Welch Costas arrays. Nevertheless, several attempts have been made to explain Lempel-Golomb arrays' crosscorrelation properties, but a theoretical justification is still an open problem. So far, what we know theoretically about the crosscorrelation of Lempel-Golomb Costas arrays is primarily based on the choice of primitive elements. Drakakis et al. in [39] stated the following theorem that shows a surprising link between the Welch and Lempel-Golomb arrays.

Theorem 3.6 ([39]). *Let A and B be two Lempel-Golomb arrays generated in the field $\mathbb{F}_q$, where q is a prime power, as in Theorem 2.46. Let A and B be G_2 arrays generated by some primitive elements α and β, and α^r and β, respectively, where*

$gcd(r, q-1) = 1, r > 1$. Then

$$\max C^{a}_{A,B}(0,0) = \frac{q-1}{w} - 1,$$

where w is the smallest prime such that $q \equiv 1 \bmod (2w)$ if q is odd, or that $q \equiv 1 \bmod (w)$ if q is even.

The above theorem also helps to explain the maximum number of common points between any two known Costas arrays of sizes $q-2$ for a prime powers q in Table 3.1. For example, for $q = 97$, we can construct Lempel-Golomb Costas arrays of size $n = 95$. Theorem 3.6 shows that the maximum number of common points between two Lempel-Golomb Costas arrays generated by a specific choice of primitive elements is 47 for $q = 97$, which is also the maximum value of the number of common points between any two known Costas arrays of size 95.

Our study of the number of common points in Table 3.6 revealed a curious phenomenon related to G_3 Lempel-Golomb arrays, as in Table 2.2. More precisely, for sizes $n = q-3$, where q is a prime power, in Table 3.6, one can verify that the maximum number of common points is much smaller than those of size $n = q-2$. We went through the database of all known Costas arrays to check how these Costas arrays of size $n = q-3$ have been constructed. We observed that all these arrays are either G_3 or $W_3^{exp}(p,\alpha)$ Costas arrays, as in Theorem 2.39. Therefore, we realized that perhaps a specific subfamily of Lempel-Golomb arrays corresponds to a relatively small number of common points, namely the subfamily of Lempel-Golomb Costas arrays generated in $\mathbb{F}_q$ using primitive elements α and β such that $\alpha + \beta = 1$ in $\mathbb{F}_q$. Let us denote by G_2' the set of Lempel-Golomb Costas arrays constructed by primitive elements α and β with the property that $\alpha + \beta = 1$. We computed the number of common points of this subfamily of Lempel-Golomb Costas arrays for prime powers $8 \le q \le 97$, for which this subfamily contains at least two elements, and the result is shown in the following table.

TABLE 3.2: The distributions of the number of common points of G_2 and G_2': the second and forth columns show the distribution sets of common points of G_2' and G_2, respectively, and the third and fifth columns illustrate the maximum value of these, distribution sets, denoted by $MD_{G_2'}$ and MD_{G_2}, respectively.

prime	$\{(k, D_{G_2'}(k))\}$	$MD_{G_2'}$	$\{(k, D_{G_2}(k))\}$	MD_{G_2}
8	$\{(4,1)\}$	4	$\{(0,54),(3,12)\}$	3
17	$\{(1,2),(2,2),(3,2)\}$	3	$\{(0,256),(1,1344),(2,128),(3,224),(7,64)\}$	7
23	$\{(1,7),(2,7),(6,1)\}$	6	$\{(0,1750),(1,2200),(2,900),(6,100)\}$	6
27	$\{(4,1)\}$	4	$\{(1,936),(4,192)\}$	4

prime	$\{(k, D_{G'_2}(k))\}$	$MD_{G'_2}$	$\{(k, D_{G_2}(k))\}$	MD_{G_2}
29	$\{(2,3),(3,7)\}$	3	$\{(0,4608),(1,3024),(2,1296),(3,1152),(6,72),(13,144)\}$	13
31	$\{(3,1)\}$	3	$\{(0,320),(1,448),(2,256),(3,704),(5,224),(9,64)\}$	9
32	$\{(5,15)\}$	5	$\{(0,13410),(5,2700)\}$	5
37	$\{(1,2),(3,1))\}$	3	$\{(0,1872),(1,2592),(2,3024),(3,1152),(4,576),(5,288),(7,288),(8,72),(11,288),(17,144)\}$	17
41	$\{(1,9),(4,2),(6,4)\}$	6	$\{(0,10496),(1,13056),(2,3840),(3,2048),(4,512),(5,256),(6,768),(7,768),(9,640),(19,256)\}$	19
43	$\{(5,1)\}$	5	$\{(0,1584),(1,1584),(2,3024),(3,1728),(4,1296),(5,936),(13,144)\}$	13
47	$\{(1,16),(2,26),(3,18),(6,6)\}$	6	$\{(0,44770),(1,44044),(2,20328),(3,6292),(6,1452)\}$	6
53	$\{(1,20),(2,15),(3,10),(4,6),(6,4)\}$	6	$\{(0,56448),(1,67392),(2,28224),(3,9792),(4,1728),(6,1152),(12,288),(25,576)\}$	25
59	$\{(1,10),(2,34),(3,22),(4,2),(5,4),(12,6)\}$	12	$\{(0,119560),(1,116032),(2,47040),(3,18816),(4,3136),(5,1568),(12,784)\}$	12
61	$\{(1,8),(2,8),(3,13),(4,2),(5,2),(6,1),(7,1),(8,1)\}$	8	$\{(0,4864),(1,6400),(2,7936),(3,7680),(4,2048),(5,768),(7,1024),(8,256),(9,256),(11,768),(14,128),(19,256),(29,256)\}$	29
64	$\{(8,1),(15,2)\}$	15	$\{(0,7452),(2,7452),(3,1728),(5,1944),(6,2268),(8,1728),(15,216),(20,432)\}$	20

prime	$\{(k, D_{G_2'}(k))\}$	$MD_{G_2'}$	$\{(k, D_{G_2}(k))\}$	MD_{G_2}
67	$\{(1,8),(2,8),(3,13),(4,2),(5,2),(6,1),(7,1),(8,1)\}$	8	$\{(0,16400),(1,14800),(2,20600),(3,16800),(4,3600),(5,5600),(6,400),(7,400),(8,800),(21,400)\}$	21
71	$\{(1,19),(2,4),(3,4),(6,1)\}$	6	$\{(0,71424),(1,57024),(2,23040),(3,7488),(4,576),(6,1440),(9,2880),(13,1728)\}$	13
73	$\{(1,6),(2,2),(3,10),(4,6),(8,1),(10,2),(11,1)\}$	11	$\{(0,27648),(1,23040),(2,46368),(3,22464),(35,576),(5,12960),(4,15552),(7,2304),(6,2880),(9,3456),(10,1152),(11,1440),(8,2016),(14,1152),(17,1440),(23,1152)\}$	23
79	$\{(3,11),(4,3),(9,1)\}$	9	$\{(0,23616),(1,44928),(2,39168),(3,39744),(4,7488),(5,8640),(8,864),(9,576),(25,576)\}$	25
81	$\{(9,1),(7,2)\}$	7	$\{(1,16512),(3,6656),(5,2560)(7,3200),(39,256),(9,1408),(11,512),(15,896),(19,640)\}$	19
83	$\{(1,60),(2,75),(3,31),(4,4),(5,1)\}$	5	$\{(0,460000),(1,529600),(2,185600),(3,83200),(4,12800),(5,1600),(6,6400)\}$	6
89	$\{(1,29),(2,54),(3,40),(4,12),(5,8),(6,6),(7,3),(9,1)\}$	9	$\{(0,324800),(1,488000),(2,278400),(3,124000),(4,20800),(5,11200),(6,6400),(7,16000),(9,4000),(43,1600),(21,4000)\}$	21
97	$\{(1,12),(2,12),(3,19),(4,14),(5,7),(14,2)\}$	14	$\{(0,79872),(1,102400),(2,126976),(3,115712),(4,39936),(5,22528),(6,8192),(7,12288),(9,4096),(11,4096),(13,1024),(14,1024),(15,1024),(47,1024),(23,2560),(31,1024)\}$	31

Table 3.2 reveals interesting observations regarding the number of common points of any two elements of G_2'.

- Since $\alpha + \beta = 1$, there is a dot at the top left corner of any array in G_2'. Therefore, any two elements of G_2' have at least one point in common.
- As one can verify in Table 3.2, for primes p with the property that $\frac{p-1}{2}$ is also a prime (these primes are known as safe primes), the number of common points between G_2' arrays and G_2 arrays are the same or differ by 1. These values are 23, 47, 59 and 83 in this Table. For the other values, one can check that $MD_{G_2'} \leq \frac{MD_{G_2}-1}{2}$.
- For prime powers q in this table, where $8 < q \leq 81$, it can be seen that $MD_{G_2'} \leq MD_{G_2}$.

As we mentioned earlier, it is interesting to find subfamilies of Costas arrays with few common points. This attitude may lead to finding subfamilies of Costas arrays with low crosscorrelation. We will follow this point of view in the last chapter of this thesis.
Since there is no theoretical proof for the crosscorrelation of any two Lempel-Golomb Costas arrays in general, having proof even for exceptional cases may also be fruitful, leading to a better understanding of their behaviour. With this in mind, we state the following theorem that discusses exceptional pairs of Lempel-Golomb Costas arrays containing at most one point in common.

Theorem 3.7. *Let A and B be two Lempel-Golomb arrays generated in the field $\mathbb{F}_q$, where q is a prime power, as in Theorem 2.46. Let A and B be G_2 arrays generated by some primitive elements α_1 and β_1, and α_2 and β_2, respectively, where $\alpha_1\alpha_2 = 1$ and $\beta_1 + \beta_2 = 0$ in $\mathbb{F}_q$. Then the number of common points of A and B is at most one.*

Proof. Let $A = [\log_{\alpha_1}(1 - \beta_1^j)]$ be a G_2 array generated by α_1 and β_1, and let $B = [\log_{\alpha_2}(1 - \beta_2^j)]$ be a G_2 array generated by α_2 and β_2, where $1 \leq j \leq q-2$. Thus, the number of common points of A and B can be obtained by solving the following equation for $1 \leq j \leq q-2$

$$\log_{\alpha_1}(1 - \beta_1^j) = \log_{\alpha_2}(1 - \beta_2^j). \tag{3.2}$$

Since $\alpha_1\alpha_2 = 1$ and $\beta_1 + \beta_2 = 0$ in $\mathbb{F}_q$, it follows that

$$\log_{\alpha_1}(1 - \beta_1^j) = \log_{\alpha_1^{-1}}(1 - (-\beta_1)^j). \tag{3.3}$$

Equivalently,

$$(1 - \beta_1^j)^{-1} = (1 - (-\beta_1)^j) \text{ in } \mathbb{F}_q. \tag{3.4}$$

Therefore, the proof falls naturally into two cases.
Case 1. If j is odd: in this case, by multiplying both sides of Equation 3.4 by $(1 - \beta_1^j)$, we obtain $\beta_1^{2j} = 0$ in $\mathbb{F}_q$, which has no solution because $1 \leq j \leq$

Costas arrays of size 23	Allowable swaps
[23, 5, 12, 17, 11, 3, 20, 10, 13, 2, 15, 21, 19, 16, 9, 4, 6, 7, 22, 8, 18, 14, 1]	1 and 23
[23, 10, 6, 16, 2, 17, 18, 20, 15, 8, 5, 3, 9, 22, 11, 14, 4, 21, 13, 7, 12, 19, 1]	1 and 23
[1, 14, 18, 8, 22, 7, 6, 4, 9, 16, 19, 21, 15, 2, 13, 10, 20, 3, 11, 17, 12, 5, 23]	1 and 23
[1, 19, 12, 7, 13, 21, 4, 14, 11, 22, 9, 3, 5, 8, 15, 20, 18, 17, 2, 16, 6, 10, 23]	1 and 23

TABLE 3.3: Costas arrays of size 23, for which swapping two points results in another Costas array.

$q-2$.

Case 2. If j is even: in this case, by multiplying both sides of Equation 3.4 by $(1-\beta_1^j)$, we obtain $\beta_1^j(\beta_1^j-2)=0$ in $\mathbb{F}_q$, which has only one solution if and only if $\beta_1^j=2$ in $\mathbb{F}_q$. Therefore, in total, Equation 3.4 can have at most one solutions, which completes the proof. □

Table 3.1 also reveals another curious phenomenon regarding the number of common points of Costas arrays of sizes n, for which the majority of Costas arrays are sporadic. Table 3.1 illustrates that $MD(n)=n-2$ for $2\leq n\leq 17$ and $n=23$, showing for these sizes there are Costas arrays for which swapping two points will result in another Costas array. For example, let $A=[1,5,3,8,7,4,6,2]$ be a Costas array of size 8. Then, Changing the value of 1 and 2 gives another Costas array $B=[2,5,3,8,7,4,6,1]$. Drawing $T(A)$ and $T(B)$ shows that A and B are Costas arrays.

1	5	3	8	7	4	6	2
4	−2	5	−1	−3	2	−4	
2	3	4	−4	−1	−2		
7	2	1	−2	−5			
6	−1	3	−6				
3	1	−1					
5	−3						
1							

2	5	3	8	7	4	6	1
3	−2	5	−1	−3	2	−5	
1	3	4	−4	−1	−3		
6	2	1	−2	−6			
5	−1	3	−7				
2	1	−2					
4	−4						
−1							

As we can see in Table 3.1, there are only four arrays of size 23, for which we can swap two points to obtain another Costas array. Size 23 is the largest size after 17, for which this is happening. These arrays are shown in the Table 3.3. One can easily verify that these four arrays of size 23 in Table 3.3 belong to one equivalence class and are sporadic arrays. Since the number of sporadic arrays monotonically decrease from size 16 to 27, one may ask whether it is a property that sporadic Costas arrays have that swapping points result in another Costas array or there are also generated or emergent Costas arrays with this property.

Further analysis of algebraically constructed Costas arrays showed that for

$5 \leq n \leq 200$, there is only one equivalence of the Welch Costas array with the property that only one allowable swap exists for each Costas array in this equivalence class. $W_1^{exp}(7,5,0) = [1,5,4,6,2,3]$ is the representative of this equivalence class, in which 3 and 4 are allowable swaps. Finding the allowable swap for the other elements in this equivalence is a simple matter. Note that if swapping two points in a given Costas array produces another Costas array, these two Costas arrays are not equivalent (relative to the action of D_8). For the other main algebraic construction, there are only two equivalence classes of Lempel-Golomb Costas arrays of sizes 11 and 13, for which swapping two points produces another Costas array. These arrays are shown in Table 3.4. It is worth noting that after swapping two points in the Lempel-Golomb Costas arrays in Table 3.4, the obtained arrays are sporadic Costas arrays.

TABLE 3.4: Lempel-Golomb Costas arrays, for which swapping two points results in another Costas array. The last column provides information on how these Lempel-Golomb Costas arrays are constructed.

Prime	Lempel-Golomb Costas arrays	Allowable swaps	Info
11	X=[7, 8, 2, 4, 3, 1, 6, 9, 5]	1 and 9	$\alpha = 6$ and $\beta = 7$
11	[6, 3, 5, 4, 9, 7, 1, 2, 8]	6 and 8	Diagonal reflection of X
11	[4, 7, 5, 6, 1, 3, 9, 8, 2]	2 and 4	90° rotation of X
11	[3, 2, 8, 6, 7, 9, 4, 1, 5]	1 and 9	Horizontal reflection of X
11	[5, 9, 6, 1, 3, 4, 2, 8, 7]	1 and 9	Vertical reflection of X
11	[5, 1, 4, 9, 7, 6, 8, 2, 3]	1 and 9	180° rotation of X
11	[8, 2, 1, 7, 9, 4, 5, 3, 6]	6 and 8	270° rotation of X
11	[2, 8, 9, 3, 1, 6, 5, 7, 4]	2 and 4	Anti-diagonal reflection of X
13	Y=[3, 10, 1, 9, 6, 5, 7, 11, 4, 2, 8]	8 and 11	$\alpha = 6$ and $\beta = 6$
13	[9, 2, 11, 3, 6, 7, 5, 1, 8, 10, 4]	1 and 4	90° rotation of Y
13	[8, 2, 4, 11, 7, 5, 6, 9, 1, 10, 3]	8 and 11	Vertical reflection of Y
13	[4, 10, 8, 1, 5, 7, 6, 3, 11, 2, 9]	1 and 4	180° rotation of Y

Table 3.1 further demonstrates that for values of n ranging from 24 to 100, if there exists a possibility to transform a given Costas array into another,

at least half of the elements in the corresponding permutation must be rearranged. This observation prompts an important question: Is it feasible to offer a theoretical proof that exchanging the positions of two points within a given Costas array of size $n \geq 24$ can never yield another Costas array? Drawing upon the insights provided in Table 3.1, we formulate the following two conjectures based on the available information.

Conjecture 3.8. *Swapping two points in a given Costas array of size $n \geq 24$ does not preserve Costas property.*

Conjecture 3.9. *The number of common points of two given Costas arrays of size $n \geq 24$ is at most $\frac{n}{2}$.*

Although it seems difficult to prove these conjectures for arbitrary Costas arrays, one might be able to provide theoretical proof for algebraically constructed Costas arrays. It turned out that proving Conjecture 3.8 for Costas arrays with G-symmetric property might be applicable due to several symmetries in the difference triangle table of such Costas arrays. We will provide partial proof for these Costas arrays.

Theorem 3.10. *Let $X = [f(1), f(2), \ldots, f(n)]$ be a G-symmetric Costas arrays of even size n. Swapping two points $f(r)$ and $f(s)$, where $1 \leq r < s \leq n$, in the following cases, will never produce a Costas array.*
Case 1. *If $r, s < \frac{n}{2}$ or $r, s > \frac{n}{2}$.*
Case 2. *If $r < \frac{n}{2}$, $s > \frac{n}{2}$, $s - r \neq \frac{n}{2}$ and r and s have the same parity.*

Proof. For case 1, if $r, s < \frac{n}{2}$, after swapping $f(r)$ and $f(s)$, in row $s - r$ of the difference triangle table of X, we change the value of $f(s) - f(r)$ with $f(r) - f(s)$. Moreover, before swapping $f(r)$ and $f(s)$, in row $s - r$, we have the value $f(\frac{n}{2} + s) - f(\frac{n}{2} + r)$, which will be fixed after swapping $f(r)$ and $f(s)$. By using the G-symmetric property of X, we have

$$f(r) - f(s) = \left(n + 1 - f(\tfrac{n}{2} + r)\right) - \left(n + 1 - f(\tfrac{n}{2} + s)\right) = f(\tfrac{n}{2} + s) - f(\tfrac{n}{2} + r),$$

which shows a repetition in the row $s - r$. Then, swapping $f(r)$ and $f(s)$ will not produce a Costas array.
Now, if $r, s > \frac{n}{2}$, we can have the same argument as above by nothing that

$$f(s - \tfrac{n}{2}) - f(r - \tfrac{n}{2}) = (n + 1 - f(s)) - (n + 1 - f(r)) = f(r) - f(s).$$

For case 2, since r and s have the same parity, both $\frac{r+s}{2}$ and $\frac{s-r}{2}$ are integers. We claim that after swapping $f(r)$ and $f(s)$, we obtain repeated elements in row $\frac{s-r}{2}$ of the difference triangle of X. Since $r < \frac{n}{2}$, depending on whether $\frac{s+r}{2} \leq \frac{n}{2}$ or $\frac{s+r}{2} > \frac{n}{2}$, we have the following cases:
Case 2.1: If $r < \frac{n}{2}$ and $\frac{s+r}{2} \leq \frac{n}{2}$, then in row $\frac{s-r}{2}$, before swapping $f(r)$ and $f(s)$, we have the element $f(\frac{s+r}{2} + \frac{n}{2}) - f(r + \frac{n}{2})$, which will be fixed also after swapping $f(r)$ and $f(s)$. Moreover, in row $\frac{s-r}{2}$, after swapping $f(r)$ and $f(s)$, we change the value of $f(s) - f(\frac{s+r}{2})$ with the value $f(r) - f(\frac{s+r}{2})$.

Using the G-symmetric property of X, we have

$$\begin{aligned} f(r) - f(\tfrac{s+r}{2}) &= \left(n+1-f(r+\tfrac{n}{2})\right) - \left(n+1-f(\tfrac{s+r}{2}+\tfrac{n}{2})\right) \\ &= f(\tfrac{s+r}{2}+\tfrac{n}{2}) - f(r+\tfrac{n}{2}). \end{aligned}$$

It follows that after swapping $f(r)$ and $f(s)$, the elements $f(\frac{s+r}{2}+\frac{n}{2}) - f(r+\frac{n}{2})$ and $f(r) - f(\frac{s+r}{2})$ have the same value in row $\frac{s-r}{2}$.
Case 2.2: If $r < \frac{n}{2}$ and $\frac{s+r}{2} > \frac{n}{2}$, in row $\frac{s-r}{2}$, after swapping $f(r)$ and $f(s)$, we change the value of $f(\frac{s+r}{2}) - f(r)$ with the value $f(\frac{s+r}{2}) - f(s)$. Utilizing the G-symmetric property of X, we obtain

$$\begin{aligned} f(\tfrac{s+r}{2}) - f(s) &= \left(n+1-f(\tfrac{s+r}{2}-\tfrac{n}{2})\right) - \left(n+1-f(s-\tfrac{n}{2})\right) \\ &= f(s-\tfrac{n}{2}) - f(\tfrac{s+r}{2}-\tfrac{n}{2}). \end{aligned}$$

But $f(s-\frac{n}{2}) - f(\frac{s+r}{2}-\frac{n}{2})$ is an element in row $\frac{s-r}{2}$, which will be fixed before and after swapping $f(r)$ and $f(s)$. In this case, we also obtain a repeated value in row $\frac{s-r}{2}$ after swapping $f(r)$ and $f(s)$. Therefore, swapping $f(r)$ and $f(s)$ values will not produce a Costas array. □

We do not have proof for the other cases because it seems challenging to find a pattern for repeating elements that occur in rows of the difference triangle table after swapping two elements. We searched for such patterns by analyzing the difference triangle table of Costas arrays of even sizes with G-symmetric properties before and after swapping. However, even for small sizes, we could not find such patterns that hold in general.
As mentioned earlier there is no Welch Costas array for which swapping two points give another Costas array for $11 \leq p < 200$. As a corollary of Theorem 3.10, we do not obtain another Costas array by swapping two (for those specific swaps mentioned in Theorem 3.10) points in an exponential Welch Costas array because they have G-symmetric property. We decided to write this corollary with the proof because it provides essential insights into understanding the difference triangle table of exponential Welch Costas arrays.

Corollary 3.11. *Let $W_1^{exp}(p,\alpha,c)$ be an exponential Welch Costas array as in Theorem 2.34. Swapping two elements α^r and α^s, where r and s are integers in $\{0,1,\dots,p-2\}$ with $r < s$, of $W_1^{exp}(p,\alpha,c)$, in the following cases, will never produce a Costas array.*
Case 1. *If $r,s < \frac{p-1}{2}$ or $r,s > \frac{p-1}{2}$.*
Case 2. *If $r < \frac{p-1}{2}$, $s > \frac{p-1}{2}$, $s-r \neq \frac{p-1}{2}$ and r and s have the same parity.*

Proof. Without loss of generality, we can choose $c = 0$. Let α be a primitive element of the finite field $\mathbb{F}_p$, where p is a prime, and let $W_1^{exp}(p,\alpha,0) = [\alpha^i \bmod p]$ be a Welch Costas array as in Remark 2.36. Let us begin by proving case 1. Suppose that $r,s < \frac{p-1}{2}$ and $r < s$. In this case, we look at the row $s-r$ of $T\left(W_1^{exp}\right)$ before and after swapping α^r and α^s. Before swapping, the row $s-r$ contains the following elements:

$$\alpha^s - \alpha^r \tag{3.5}$$

$$\alpha^{s+\frac{p-1}{2}} - \alpha^{r+\frac{p-1}{2}} \tag{3.6}$$

Moreover, since $\alpha^{\frac{p-1}{2}} = -1$ over $\mathbb{F}_p$, we have

$$\alpha^s - \alpha^r = -(\alpha^r - \alpha^s) = \alpha^{\frac{p-1}{2}}(\alpha^r - \alpha^s) = \alpha^{r+\frac{p-1}{2}} - \alpha^{s+\frac{p-1}{2}}, \tag{3.7}$$

showing $\alpha^s - \alpha^r$ and $\alpha^{s+\frac{p-1}{2}} - \alpha^{r+\frac{p-1}{2}}$ are equal in absolute value. After swapping, we change the element $\alpha^s - \alpha^r$ with $\alpha^r - \alpha^s$, while the element $\alpha^{s+\frac{p-1}{2}} - \alpha^{r+\frac{p-1}{2}}$ does not change, showing a repetition has occurred after swapping because $\alpha^{s+\frac{p-1}{2}} - \alpha^{r+\frac{p-1}{2}} = \alpha^r - \alpha^s$.
If $r, s > \frac{p-1}{2}$, we can have the same argument, but we should notice that

$$\alpha^{s-\frac{p-1}{2}} - \alpha^{r-\frac{p-1}{2}} = \alpha^r - \alpha^s.$$

For case 2, since r and s have the same parity, both $\frac{r+s}{2}$ and $\frac{s-r}{2}$ are integers. We look at the row $\frac{s-r}{2}$ before and after swapping to find a duplicated entry in this row. Before swapping, the row $\frac{s-r}{2}$ contains the following elements:

$$\alpha^{\frac{s+r}{2}} - \alpha^r, \tag{3.8}$$

$$\alpha^s - \alpha^{\frac{s+r}{2}}. \tag{3.9}$$

Since $s \geq \frac{p-1}{2}$ and $\frac{s+r}{2} > \frac{p-1}{2}$, then we have the element $\alpha^{s-\frac{p-1}{2}} - \alpha^{\frac{s+r}{2}-\frac{p-1}{2}}$ in row $\frac{s-r}{2}$, which will be fixed after swapping α^r and α^s. Moreover, we have

$$\alpha^{s-\frac{p-1}{2}} - \alpha^{\frac{s+r}{2}-\frac{p-1}{2}} = \alpha^{\frac{s+r}{2}} - \alpha^s. \tag{3.10}$$

After swapping, we change the elements 3.8 and 3.9 by the following elements:

$$\alpha^{\frac{s+r}{2}} - \alpha^s, \tag{3.11}$$

$$\alpha^r - \alpha^{\frac{s+r}{2}}. \tag{3.12}$$

From 3.10 and 3.11, we can conclude that there is a repetition after swapping α^r and α^s. □

In conclusion, Conjecture 3.9 in this section proposes that if there is a possibility of transforming a Costas array of size $n \geq 24$ into another Costas array, it would require rearranging at least half of the points. Consequently, the subsequent section will delve into the discussion of a novel transformation that satisfies this particular property.

3.2 A new Transformation

One possible approach to achieve a deeper understanding of Costas arrays properties is to construct a matrix close to a Costas array and then examine whether it is possible to do some modification to get a Costas array out of it. With this in mind, we introduce a new transformation, which enables us to apply this transformation to an existing Costas array to obtain another permutation matrix with the property that the aperiodic autocorrelation function values for all non-zero shifts are at most two. In other words, the aperiodic autocorrelation function of these transformed Costas arrays are four-valued. Let us call these types of permutation matrices "Almost Costas arrays". What follows is the definition of our new transformation, and we will explain how this transformation is beneficial to construct a Costas array from a given one in some cases.
Let $X = [f(1), f(2), ..., f(n)]$ be a Costas array of size n. We plan to construct another bijection g from f and then examine the correlation properties of its corresponding permutation matrix. Suppose that k is a positive integer such that $gcd(k, n+1) = 1$. We define $g : [n] \longrightarrow [n]$, by

$$i \longmapsto f\left(ki \; mod \; n+1\right).$$

We claim that g is a bijection. Note that f is a bijection and $ki \; mod \; (n+1)$ is an integer in $[n]$. It is sufficient to show that g is injective. To do so, if there are integers $i_1, i_2 \in [n]$ such that $g(i_1) = g(i_2)$, then we have

$$f\left(ki_1 \; mod \; n+1\right) = f\left(ki_2 \; mod \; n+1\right).$$

Since f is a bijection, then applying f^{-1} on both sides of the above equation gives

$$ki_1 \; mod \; (n+1) = ki_2 \; mod \; (n+1).$$

Since $gcd(k, n+1) = 1$, then $i_1 = i_2$ that shows g is an injective map. Now we can state the formal definition of our transformation.

Definition 3.12 ([5]). *Let $X = [f(1), f(2), ..., f(n)]$ represent a permutation matrix of size n, where $n \in \mathbb{N}$, and let k be a positive integer such that $gcd(k, n+1) = 1$. We define a bijection $g : [n] \longrightarrow [n]$, by*

$$i \longmapsto f\left(ki \; mod \; n+1\right).$$

We denote the corresponding permutation matrix of g by $\mathcal{A}_k(X)$.

As discussed in the previous Section, Conjecture 3.9 suggested that if transformation $\mathcal{A}_k$ may produce another Costas array, for a given Costas array X of size $n \geq 24$, X and $\mathcal{A}_k(X)$ might have at most $\frac{n}{2}$ points in common. Consequently, to obtain another Costas array after applying $\mathcal{A}_k$, at least half of the points in X might be rearranged. The following theorem shows how many points X and $\mathcal{A}_k(X)$ can have in common.

Theorem 3.13 ([5]). *Let $X = [f(1), f(2), \ldots, f(n)]$ be a Costas array of size n, and let k be a positive integer such that $gcd(k, n+1) = 1$. Then the number of common points between X and $\mathcal{A}_k(X)$ is at most $\lfloor \frac{n}{2} \rfloor$.*

Proof. In order to compute the number of common points between X and $\mathcal{A}_k(X)$, we need to solve the following equation

$$f(i) = f(ki \bmod n+1) \quad \text{for } 1 \leq i \leq n. \tag{3.13}$$

Since f is a bijection, then applying f^{-1} on both sides of Equation 3.13 gives $i = ki \bmod n+1$. Equivalently,

$$(k-1)i \equiv 0 \bmod n+1. \tag{3.14}$$

Setting $d := gcd(k-1, n+1)$, we know that Equation 3.14 has exactly d incongruent solutions modulo $n+1$. Clearly, $d \leq \frac{n+1}{2}$. Therefore, since $1 \leq i \leq n$ and zero is always a solution of Equation 3.14, the number of common points between X and $\mathcal{A}_k(X)$ can not exceed $\frac{n-1}{2}$, which is less than $\lfloor \frac{n}{2} \rfloor$. □

Example 3.14. *Consider the Costas array $X = [1, 7, 4, 8, 2, 3, 6, 5]$ of size 8. Since $gcd(2, 9) = gcd(4, 9) = gcd(5, 9) = gcd(7, 9) = gcd(8, 9) = 1$, we can construct $\mathcal{A}_2(X)$, $\mathcal{A}_4(X)$, $\mathcal{A}_5(X)$, $\mathcal{A}_7(X)$ and $\mathcal{A}_8(X)$. Let us first construct $\mathcal{A}_2(X)$.*

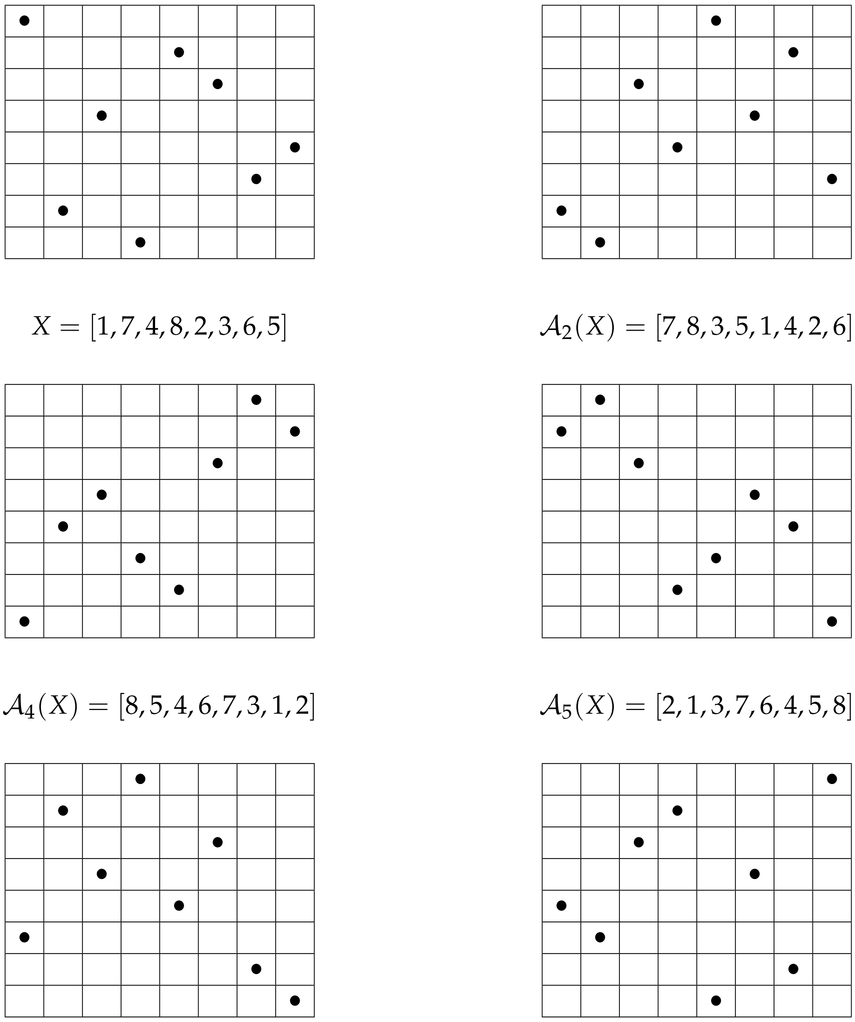
$$\begin{aligned} \mathcal{A}_2(X) &= [f\,(2 \cdot 1 \; mod\; 9)\,, f\,(2 \cdot 2 \; mod\; 9)\,, ..., f\,(2 \cdot 8 \; mod\; 9)] \\ &= [f(2), f(4), f(6), f(8), f(1), f(3), f(5), f(7)] \\ &= [7, 8, 3, 5, 1, 4, 2, 6]. \end{aligned}$$

Similarly, we can construct $\mathcal{A}_4(X)$, $\mathcal{A}_5(X)$, $\mathcal{A}_7(X)$ and $\mathcal{A}_8(X)$. Thus we have $\mathcal{A}_4(X) = [8, 5, 4, 6, 7, 3, 1, 2]$, $\mathcal{A}_5(X) = [2, 1, 3, 7, 6, 4, 5, 8]$, $\mathcal{A}_7(X) = [6, 2, 4, 1, 5, 3, 8, 7]$ and $\mathcal{A}_8(X) = [5, 6, 3, 2, 8, 4, 7, 1]$. The matrices that correspond to these permutations are shown in figure 3.1. One can easily check that $\mathcal{A}_2(X)$, $\mathcal{A}_7(X)$ and $\mathcal{A}_8(X)$ are Costas arrays, but $\mathcal{A}_4(X)$ and $\mathcal{A}_5(X)$ are not Costas arrays.

Example 3.14 indicates that sometimes transformation $\mathcal{A}_k$ produces another Costas array and sometimes does not. For convenience, let us call a Costas array X of size n **transferable** if there is an integer k, where $gcd(k, n+1) = 1$, such that $\mathcal{A}_k(X)$ is again a Costas array. We observed that if an array is transferable, then some of the elements of its equivalence class are also transferable. The observed relation is shown in the following theorem.

Theorem 3.15. *Let X be a transferable Costas array of size n. Then the vertical reflection, horizontal reflection and 180° rotation of X are transferable.*

Proof. Let us denote by X_v, X_h and X_r the Costas arrays obtained by vertical reflection, horizontal reflection and 180° rotation of the Costas array X, respectively. The procedure of proving a Costas array is transferable is to find a positive integer t with the property that $gcd(t, n+1) = 1$ and applying $\mathcal{A}_t$ gives a Costas array. We begin by proving X_v is transferable. One can easily check that $X_v = [f(n+1-i)]$, for $1 \leq i \leq n$. Let us apply the transformation



$X = [1,7,4,8,2,3,6,5]$

$\mathcal{A}_2(X) = [7,8,3,5,1,4,2,6]$

$\mathcal{A}_4(X) = [8,5,4,6,7,3,1,2]$

$\mathcal{A}_5(X) = [2,1,3,7,6,4,5,8]$

$\mathcal{A}_7(X) = [6,2,4,1,5,3,8,7]$

$\mathcal{A}_8(X) = [5,6,3,2,8,4,7,1]$

FIGURE 3.1: The matrix X and all possible transformations, $\mathcal{A}_k(X)$, for k, where $gcd(k,9) = 1$.

for $t = -k$. Then for $1 \leq i \leq n$ we have

$$\begin{aligned}\mathcal{A}_{-k}(X_v) &= [f(-k(n+1-i) \; mod \; n+1)] \\ &= [f(ki \; mod \; n+1))] \\ &= \mathcal{A}_k(X).\end{aligned}$$

Since X is transferable, then $\mathcal{A}_k(X)$ is a Costas array. Thus X_v is transferable. We next prove that X_h is transferable. One can see that the horizontal reflection of X is given by $X_h = [n+1-f(i)]$ for $1 \leq i \leq n$. We apply the transformation for $t = k$. Then we have for $1 \leq i \leq n$

$$\mathcal{A}_k(X_h) = [n+1-f(ki \; mod \; n+1)] = (\mathcal{A}_k(X))_h \, .$$

We already know that $[f(ki \; mod \; n+1)]$ for $1 \leq i \leq n$ is a Costas array. Thus

X_h is transferable. Similarly, we can verify that 180° rotation of X is also transferable. The 180° rotation of X is given by $X_r = [n+1-f(n+1-i)]$ for $1 \leq i \leq n$. Let us take $t=-k$, then we have

$$\begin{aligned} \mathcal{A}_{-k}(X_r) &= [n+1-f(-k(n+1-i) \; mod \; n+1)] \\ &= [n+1-f(ki \; mod \; n+1))] \\ &= (\mathcal{A}_k(X))_h \, . \end{aligned}$$

Similar to the latter case, we can conclude that X_r is transferable, which completes the proof. □

Corollary 3.16 ([5]). *Assume that X and its transpose, X^T, are transferable. Then all the elements of the equivalence class of X are transferable.*

Proof. The proof is straightforward. On account of Theorem 3.15, since X and X^T are transferable, then the vertical reflection, horizontal reflection and 180° rotation of both X and X^T are transferable. Obviously, the vertical reflection, horizontal reflection and 180° rotation of X^T are 270° counterclockwise rotation, 90° counterclockwise rotation and Antidiagonal reflection of X, respectively. It follows that the entire equivalence class of X is transferable. □

Example 3.17. *Consider the Costas array $X = [1,2,9,3,5,10,8,4,7,6]$. One can easily check that $X^T = [1,2,4,8,5,10,9,7,3,6]$. It can be seen that $\mathcal{A}_k(X)$ for $k \in \{2,3,\ldots,9\}$ is Costas array. However, $\mathcal{A}_k(X^T)$ is not transferable.*

The following theorem provides one of the most exciting properties of the transformation $\mathcal{A}_k$.

Theorem 3.18 ([5]). *Let $X = [f(1), f(2), ..., f(n)]$ represent a Costas array of size n, where $n \in \mathbb{N}$, and k is a positive integer such that $gcd(k, n+1) = 1$ and $k \neq 1, n$. Then for all possible shifts $(r,s) \neq (0,0)$, $|r| \leq n$, $|s| \leq n$, we have*

$$C_{\mathcal{A}_k(X)}(r,s) \leq 2.$$

In other words, $\mathcal{A}_k(X)$ is an almost Costas array.

Proof. By way of contradiction, we assume that the aperiodic autocorrelation function of $\mathcal{A}_k(X)$ for a non-zero shift has a value of at least 3. This means there is a row l in the difference triangle table of $\mathcal{A}_k(X)$ in which there are at least three equal entries. Let us say $g(i_1+l)-g(i_1)$, $g(i_2+l)-g(i_2)$, and $g(i_3+l)-g(i_3)$ be equal in row l, where $1 \leq i_1, i_2, i_3, i_1+l, i_2+l, i_3+l \leq n$, and i_1, i_2, and i_3 are all distinct. Regarding Definition 3.12, we have

$$g(i_1+l)-g(i_1) = f(k(i_1+l) \; mod \; n+1) - f(ki_1 \; mod \; n+1). \tag{3.15}$$

$$g(i_2+l)-g(i_2) = f(k(i_2+l) \; mod \; n+1) - f(ki_2 \; mod \; n+1). \tag{3.16}$$

$$g(i_3+l)-g(i_3) = f(k(i_3+l) \; mod \; n+1) - f(ki_3 \; mod \; n+1). \tag{3.17}$$

It follows that

$$g(i_1+l)-g(i_1)=f\left((ki_1+kl)\ mod\ n+1\right)-f\left(ki_1\ mod\ n+1\right). \tag{3.18}$$

$$g(i_2+l)-g(i_2)=f\left((ki_2+kl)\ mod\ n+1\right)-f\left(ki_2\ mod\ n+1\right). \tag{3.19}$$

$$g(i_3+l)-g(i_3)=f\left((ki_3+kl)\ mod\ n+1\right)-f\left(ki_3\ mod\ n+1\right). \tag{3.20}$$

Let us assume that $i'_t = ki_t\ mod\ n+1$, where $t=1,2,3$, and $l' = kl\ mod\ n+1$. Therefore, we have

$$g(i_1+l)-g(i_1)=f((i'_1+l')\ mod\ n+1)-f(i'_1). \tag{3.21}$$

$$g(i_2+l)-g(i_2)=f((i'_2+l')\ mod\ n+1)-f(i'_2). \tag{3.22}$$

$$g(i_3+l)-g(i_3)=f((i'_3+l')\ mod\ n+1)-f(i'_3). \tag{3.23}$$

Clearly, $1 \le i'_t \le n$ and $1 \le l' \le n$, hence it follows that $2 \le i'_t + l' \le 2n$. Moreover, since $1 \le i_t + l \le n$ for $t=1,2,3$ and $gcd(k,n+1)=1$, it follows that $i'_t + l' \neq n+1$. Therefore, we can assume that $i'_t + l' < n+1$ or $i'_t + l' > n+1$. In the latter case, we can conclude that $((i'_t+l')\ mod\ n+1) = i'_t + l' - n - 1$.
We already assumed that the left-hand side of the equations (3.21), (3.22) and (3.23) are equal. hence, we will use the fact that X is a Costas array to obtain a contradiction. To do so, we need to consider four cases:

1. For all $t \in \{1,2,3\}$, we have $i'_t + l' < n+1$.
2. For all $t \in \{1,2,3\}$, we have $i'_t + l' \ge n+1$.
3. For two values of t, where $t \in \{1,2,3\}$, we have $i'_t + l' < n+1$.
4. For two values of t, where $t \in \{1,2,3\}$, we have $i'_t + l' > n+1$.

Case 1. According to the equations (3.21), (3.22) and (3.23), we have

$$f(i'_1+l')-f(i'_1)=f(i'_2+l')-f(i'_2)=f(i'_3+l')-f(i'_3).$$

Since X is a Costas array, $i'_1 = i'_2 = i'_3$ or $l'=0$. Assume that $i'_1 = i'_2$, then

$$ki_1\ mod\ n+1 = ki_2\ mod\ n+1.$$

Since $gcd(k,n+1)=1$, then we can conclude that $i_1\ mod\ n+1 = i_2\ mod\ n+1$. This gives $i_1 = i_2$, because we assumed $1 \le i_1, i_2 \le n$, which gives a contradiction with the fact that i_1 and i_2 are distinct. Moreover, if $l'=0$, then $l=0$. This finishes the proof of case 1.
Case 2. According to the equations (3.21), (3.22) and (3.23), we have

$$f(i'_1+l'-n-1)-f(i'_1)=f(i'_2+l'-n-1)-f(i'_2)=f(i'_3+l'-n-1)-f(i'_3).$$

It follows that

$$f(i'_1) - f(i'_1 + l' - n - 1) = f(i'_2) - f(i'_2 + l' - n - 1).$$

Define that $i''_1 = i'_1 + l' - n - 1$ and $i''_2 = i'_2 + l' - n - 1$. Hence we have

$$f(i''_1 + (n + 1 - l')) - f(i''_1) = f(i''_2 + (n + 1 - l')) - f(i''_2).$$

Clearly, $1 \leq i''_1, i''_2 \leq n$. Assuming $l'' = n + 1 - l'$, we can conclude that $i''_1 = i''_2$ or $l'' = 0$, because X is a Costas array. We know that $l'' \neq 0$, because $1 \leq l' \leq n - 1$. Thus $i''_1 = i''_2$. Therefore, we can conclude that $i'_1 = i'_2$. Now, by a similar argument as in case 1, we can conclude that $i_1 = i_2$ which gives a contradiction.
Case 3. There is no loss of generality in assuming $i'_1 + l' < n + 1$ and $i'_2 + l' < n + 1$. With the same argument as in case 1, we can complete the proof of this case.
Case 4. Without loss of generality we can assume $i'_1 + l' > n + 1$ and $i'_2 + l' > n + 1$. Then we can complete the proof of this case by using the same argument as in case 2.
It follows that assuming repetition of three elements in a row of $\mathcal{A}_k(X)$'s difference triangle table leads to a contradiction. Therefore, in each row of the $\mathcal{A}_k(X)$'s difference triangle table, we do not have a repeated value more than twice. Hence we can conclude that the aperiodic autocorrelation function values of $\mathcal{A}_k(X)$ for all possible non-zero shifts are at most two, which completes the proof. □

As we mentioned in the introductory Section of this chapter, constructing permutation matrices with the property that the aperiodic autocorrelation function is four-valued is is of some interest. Theorem 3.18 indicates that we can construct $\phi(n) - 1$ more permutation matrices from a given Costas array of size n with a four-valued aperiodic autocorrelation function.

Example 3.19. *Consider Costas arrays $X = [9, 3, 5, 6, 2, 12, 7, 4, 8, 11, 10, 1]$ and $Y = [1, 2, 5, 3, 10, 6, 12, 4, 9, 11, 8, 7]$. Since $gcd(12, 7) = 1$, we can construct both $\mathcal{A}_7(X)$ and $\mathcal{A}_7(Y)$. It can be seen that $\mathcal{A}_7(X) = [7, 9, 4, 3, 8, 5, 11, 6, 10, 2, 1, 12]$ and $\mathcal{A}_7(Y) = [12, 1, 4, 2, 9, 5, 11, 3, 8, 10, 7, 6]$. One can easily verify that $\mathcal{A}_7(X)$ is not a Costas array, and $\mathcal{A}_7(Y)$ is a Costas array. The following matrix is the aperiod* *autocorrelation matrix of $\mathcal{A}_7(X)$, $C^a_{\mathcal{A}_7(X)}$.*

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 2 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 2 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 2 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

We can conclude that transformation $\mathcal{A}_k(X)$ sometimes preserves the Costas property. Although $\mathcal{A}_7(X)$ is not a Costas array, as we can see in matrix $C^a_{\mathcal{A}_7(X)}$, the maximum value is two, showing that the permutation matrix $\mathcal{A}_7(X)$ has a four-valued aperiodic autocorrelation function.

Having defined the transformation $\mathcal{A}_k$, we will now discuss how this transformation operates on Welch and Lempel-Golomb Costas arrays.

Theorem 3.20 ([5])**.** *Let X be a logarithmic Welch Costas array. Then $\mathcal{A}_k(X)$, where $\mathcal{A}_k$ is the transformation introduced in Definition 3.12, is also a logarithmic Welch Costas array, obtained by a cyclic shift of the rows of X.*

Proof. Assume that X is a logarithmic Welch Costas array. Then $X = [c + \log_\alpha j \bmod p-1]$ for $1 \le j \le p-1$. We know that the non-zero elements in $\mathbb{F}_p$ form a cyclic group with respect to multiplication. Moreover, according to the discrete logarithm's definition, if we have a cyclic group G of order n, then for any $g_1, g_2 \in G$ and a generator x we have

$$\log_x(g_1 g_2) = (\log_x g_1 + \log_x g_2) \ \mathit{mod}\ n.$$

Therefore, we can conclude that

$$\log_\alpha(kj \ \mathit{mod}\ p) = (\log_\alpha k + \log_\alpha j) \ \mathit{mod}\ (p-1) \tag{3.24}$$

A logarithmic Welch Costas array is a $(p-1) \times (p-1)$ matrix. We explained in section 2.5.1 that Welch Costas arrays are singly periodic, meaning cyclic shifts of the rows of logarithmic Welch is again a logarithmic Welch Costas array. Equivalently, if we add a constant number to all the elements of a logarithmic Welch Costas permutation such that the computations are taking modulo $p-1$, the result is again a logarithmic Welch Costas permutation.

Now, if we take a look at the $\mathcal{A}_k(X)$ permutation, we can see

$$\mathcal{A}_k(X) = [(c + \log_\alpha(kj \; mod \; p) \;\; mod \; p - 1] \, for \; 1 \leq j \leq p - 1.$$

Thus, equality 3.24 shows that

$$\mathcal{A}_k(X) = [(c + \log_\alpha k + \log_\alpha j) \;\; mod \; p - 1],$$

which shows that $\mathcal{A}_k(X)$ is obtained by a cyclic shift of the rows of a logarithmic Welch that completes the proof. □

It is worthwhile to mention that exponential Costas arrays are not always transferable. In fact, what is surprising is that in a few examples of exponential Welch Costas arrays, after applying $\mathcal{A}_k$, we obtain none-generated Costas arrays. We did hope that we might find transferable exponential Welch Costas arrays of size greater than or equal to 30, for which we do not have a complete search to see whether we find a new Costas array. We checked for all exponential Welch Costas arrays up to size 1030 while none of them was transferable, except a few cases of small sizes, collected in table 3.5.

$W_1^{exp}(p, \alpha, c)$ and k	None-generated Costas array
$p = 11, \alpha = 2,$ $c = 3, k = 5$	$[7, 4, 9, 2, 10, 1, 5, 6, 8, 3]$
$p = 11, \alpha = 2,$ $c = 3, k = 6$	$[3, 8, 6, 5, 1, 10, 2, 9, 4, 7]$
$p = 11, \alpha = 6,$ $c = 8, k = 5$	$[4, 7, 2, 9, 1, 10, 6, 5, 3, 8]$
$p = 11, \alpha = 6,$ $c = 8, k = 6$	$[8, 3, 5, 6, 10, 1, 9, 2, 7, 4]$
$p = 23, \alpha = 5,$ $c = 5, k = 2$	$[8, 16, 9, 18, 13, 3, 6, 12, 1, 2, 4, 20, 17, 11, 22, 21, 19, 15, 7, 14, 5, 10]$
$p = 23, \alpha = 5,$ $c = 5, k = 21$	$[10, 5, 14, 7, 15, 19, 21, 22, 11, 17, 20, 4, 2, 1, 12, 6, 3, 13, 18, 9, 16, 8]$
$p = 23, \alpha = 5,$ $c = 16, k = 2$	$[15, 7, 14, 5, 10, 20, 17, 11, 22, 21, 19, 3, 6, 12, 1, 2, 4, 8, 16, 9, 18, 13]$
$p = 23, \alpha = 5,$ $c = 16, k = 21$	$[13, 18, 9, 16, 8, 4, 2, 1, 12, 6, 3, 19, 21, 22, 11, 17, 20, 10, 5, 14, 7, 15]$

TABLE 3.5: All none-generated Costas arrays obtained by transforming exponential Welch Costas arrays.

Additionally, as experimental evidence, it is important to mention that we have extensively examined all known Costas arrays up to size 500. In our investigation, we specifically checked whether applying the transformation $\mathcal{A}_k$ would yield new Costas arrays. However, we have found no instances of transferable Costas arrays up to size 500, except for the logarithmic Welch and Lempel-Golomb Costas arrays.

A natural question arises here; does the transformation in the Definition 3.12

work also for the Lempel-Golomb method? The answer to this question is positively yes. Let us discuss the transformation $\mathcal{A}_k$'s effect on Lempel-Golomb Costas arrays.

Theorem 3.21. *Let X be a Lempel-Golomb Costas array of size $q-2$, where q is a prime power, as in Theorem 2.46. Suppose that $\mathcal{A}_k$ is transformation introduced in Definition 3.12. Then $\mathcal{A}_k(X)$ is again a Lempel-Golomb Costas array. Moreover, let $[X]$ be the equivalence class of the matrix X. Then $\mathcal{A}_k(Y)$, where $Y \in [X]$, is a Costas array.*

Proof. Since X is a Lempel-Golomb Costas array, there are primitive elements α and β of $\mathbb{F}_q$ such that in the array X there is a dot at position (i, j) if and only if $\alpha^i + \beta^j = 1, 1 \leq i, j \leq q-2$. Let us apply the transformation $\mathcal{A}_k$ to X. It follows that in the matrix $\mathcal{A}_k(X)$, there is a dot at position $(ki \; mod \; q-1, j)$ if and only if $\alpha^{ki \; mod \; q-1} + \beta^j = 1, 1 \leq i, j \leq q-2$. According to the Lemma 2.33 and the fact that $gcd(k, q-1) = 1$, we can conclude that $\mathcal{A}_k(X)$ is again a Lempel-Golomb Costas array because α^k is a primitive element as well.
We now proceed by proving that all elements in the equivalence class of X are also Costas arrays. Assume that Y is a matrix in the equivalence class $[X]$. We showed that after applying the transformation $\mathcal{A}_k$ on a Lempel-Golomb Costas array, we obtain another Lempel-Golomb Costas array. Moreover, since the action of the Dihedral group leaves invariant the class of Lempel-Golomb Costas array [88], then $\mathcal{A}_k(Y)$ is again a Lempel-Golomb Costas array. □

3.3 None-generated Costas arrays

Although a considerable amount of literature has been published on Costas arrays, most of these studies have only focused on systematically constructed Costas arrays. Not much has been discovered about none-generated Costas arrays' properties, which indicates the difficulties of finding any common property between generated Costas arrays and none-generated ones [35].
Turning now to the experimental evidence, we went through the database to identify transferable Costas arrays up to size 29. Independent analyses were carried out on generated and none-generated Costas arrays. Table 3.6 contains all information about the number of transferable Costas arrays of each size up to size 29. The previous section showed that logarithmic Welch and Lempel-Golomb Costas arrays are transferable. Therefore, we have infinitely many transferable Costas arrays because we have infinitely many logarithmic Welch and Lempel-Golomb Costas arrays. Another interesting observation is that, in some cases, we can obtain a none-generated Costas array by transforming a generated one. We saw examples of this type in Table 3.5. The last column of Table 3.6 illustrates the total number of transferable generated Costas arrays with the property that the transformed permutations are none-generated Costas arrays.

TABLE 3.6: The total number of transferable Costas arrays per class up to size 29.$\mathcal{C}_n$ stands for the total number of Costas arrays of size n; GT and NGT stand for generated transferable Costas arrays and none-generated transferable Costas arrays, respectively [5].

Size	$\mathcal{C}_n$	GT	NGT	NGT from GT
6	116	60	0	0
7	200	16	0	0
8	444	32	76	24
9	760	24	48	0
10	2160	60	132	20
11	4368	32	48	8
12	7852	52	264	4
13	12828	4	88	4
14	17252	16	144	0
15	19612	80	24	0
16	21104	128	16	0
17	18278	48	0	0
18	15096	108	0	0
19	10240	0	0	0
20	6464	0	0	0
21	3536	120	0	0
22	2052	224	4	4
23	872	32	0	0
24	200	0	0	0
25	88	48	0	0
26	56	0	0	0
27	204	168	0	0
28	712	336	0	0
29	164	80	0	0

3.4 Difference set's point of view

Another practical way to define the transformation $\mathcal{A}_k$ in the Definition 3.12 using dots' positions in a matrix is stated in the following definition.

Definition 3.22. *Suppose that $X = [f(1), f(2), ..., f(n)]$ is a permutation of size n, and k is a positive integer such that $gcd(k, n+1) = 1$. We denote by D the set of all dots' positions in the matrix X. We can consider $D = \{(f(i), i); \quad i \in [n]\}$, as a subset of $\mathbb{Z}^\star_{n+1} \times \mathbb{Z}^\star_{n+1}$, where $\mathbb{Z}^\star_{n+1} = \mathbb{Z}_{n+1} \setminus \{0\}$. Let us define a new set of points $\sigma_k(D)$ as follows:*

$$\sigma_k(D) = \{(f(ki \text{ mod } (n+1)), i); \quad i \in [n]\}.$$

Then we can associate a matrix, let us say $\mathcal{A}_k(X)$, with the set of points $\sigma_k(D)$.

Example 3.23. *Assume that* $X = [1, 3, 6, 4, 5, 2, 7]$. *Let us consider* D *to be the set of points in the matrix* X. *Then, we have*

$$D = \{(1, 1), (3, 2), (6, 3), (4, 4), (5, 5), (2, 6), (7, 7)\}$$

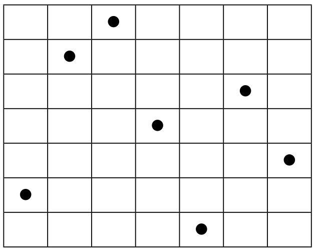
Since $gcd(3, 8) = gcd(5, 8) = gcd(7, 8) = 1$, *then we can construct* $\sigma_3(D)$, $\sigma_5(D)$ *and* $\sigma_7(D)$ *as follows*

$$\sigma_3(D) = \{(6, 1), (2, 2), (1, 3), (4, 4), (7, 5), (3, 6), (5, 7)\},$$

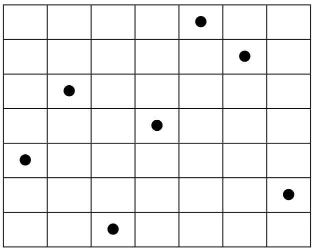
$$\sigma_5(D) = \{((5, 1), (3, 2), (7, 3), (4, 4), (1, 5), (2, 6), (6, 7)\},$$

$$\sigma_7(D) = \{(7, 1), (2, 2), (5, 3), (4, 4), (6, 5), (3, 6), (1, 7)\}.$$

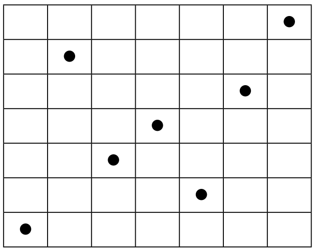
The matrices that correspond to these set of points are as follows.



$\mathcal{A}_3(X) = [6, 2, 1, 4, 7, 3, 5]$



$\mathcal{A}_5(X) = [5, 3, 7, 4, 1, 2, 6]$



$\mathcal{A}_7(X) = [7, 2, 5, 4, 6, 3, 1]$

Let us briefly explain how the set of dot's position in a logarithmic Welch Costas array is equivalent to a direct product difference set. We refer the reader to [87, 102] for more details on direct product difference sets and Costas sequences.

Definition 3.24 (Direct Product Difference Set [51,102]). *Let* H *and* N *be groups (written additively), with* $|H| = n - 1$ *and* $|N| = n$, *where* $n \geq 3$, *and let* $G = H \times N$ *be the direct product of two groups* H *and* N. *Let* D *be a subset of* G *with the property that every element of* $G \setminus \{(H \times \{0\}) \cup (\{0\} \times N)\}$ *can be uniquely represented as pairwise differences of elements of* D, *i.e.,* $d_i - d_j$, *where* $d_i, d_j \in D$. *Moreover, assume that no non-identity element of* $\{(H \times \{0\}) \cup (\{0\} \times N)\}$ *can be represented as the difference of elements in* D. *The set* D *is called a direct product difference set in* G *of order* n.

Example 3.25. *Suppose that* $G = \mathbb{Z}_4 \times \mathbb{Z}_5$. *Consider subset* $D = \{(0, 1), (1, 2), (3, 3), (2, 4)\} \subseteq G$. *Taking all the differences between distinct elements of* D *gives*

$$\begin{array}{ll}
(0,1) - (1,2) = (3,4) & (3,3) - (0,1) = (3,2) \\
(0,1) - (3,3) = (1,3) & (3,3) - (1,2) = (2,1) \\
(0,1) - (2,4) = (2,2) & (3,3) - (2,4) = (1,4) \\
(1,2) - (0,1) = (1,1) & (2,4) - (0,1) = (2,3) \\
(1,2) - (3,3) = (2,4) & (2,4) - (1,2) = (1,2) \\
(1,2) - (2,4) = (3,3) & (2,4) - (3,3) = (3,1).
\end{array}$$

As we can see, these differences between distinct elements of D produce every element of $(\mathbb{Z}_4 \setminus \{0\}) \times (\mathbb{Z}_5 \setminus \{0\})$ precisely once, and no elements of $(\mathbb{Z}_4 \times \{0\}) \cup (\{0\} \times \mathbb{Z}_5)$ appear as a difference between elements in D; therefore, D is a direct product difference set in G of order 5.

The set D given in the above example is derived from the set of the position of dots in the logarithmic Welch Costas array $W^{log}(5,2,0)$, as in Theorem 2.40. Example 3.25 also provides an essential observation about the logarithmic Welch Costas array. In Example 3.25, we take all the differences between distinct elements of D; in the first coordinate, we compute modulo 4, and in the second coordinate, we compute modulo 5. Since $W^{log}(5,2,0)$ is a 4×4 Costas array, if we consider set D as a subset of $\mathbb{Z}_4 \times \mathbb{Z}_4$, and compute the differences between elements in D modulo 4 in the second coordinate, then D is not a direct product difference set in $\mathbb{Z}_4 \times \mathbb{Z}_4$. By considering the elements $(1,2),(4,3),(3,4)$, and $(2,2)$ in D, we obtain $(1,2) - (4,3) = (1,2)$ and $(3,4) - (2,2) = (1,2)$, showing $(1,2)$ is not uniquely obtained by differences between distinct elements of D.
According to the definition of logarithmic Welch Costas array, as in Theorem 2.40, we construct an $(p-1) \times (p-1)$ Costas array $W^{log}(p,\alpha,0)$ by placing a dot at position $(f(i),i)$, where f is a bijective map from $\mathbb{Z}_p \setminus \{0\}$ to $\mathbb{Z}_{p-1}$ defined by $f(i) = \log_\alpha(i)$.
The following theorem clarifies how the set of the positions of dots in an logarithmic Welch Costas array is a direct product difference set. It is worthwhile to mention that there are similarities between the works done in this section and those described by Jane Louise Wodlinger [119] and Drakakis et al., [38,42].

Theorem 3.26. *Let α be a primitive element in $\mathbb{F}_p$, where p is a prime, and let $f : \mathbb{Z}_p \setminus \{0\} \longrightarrow \mathbb{Z}_{p-1}$ be the bijective map defined by $f(i) = \log_\alpha(i)$. Then, the set $D = \{(f(i),i) : 0 < i \leq p-1\}$ is a direct product difference set in $\mathbb{Z}_{p-1} \times \mathbb{Z}_p$ of order p.*

Proof. The proof depends on the injectivity of the following difference map for all $k \in \mathbb{Z}_p \setminus \{0\}$

$$\Delta_{f,k} : \mathbb{Z}_p \setminus \{0,-k\} \longrightarrow \mathbb{Z}_{p-1}, \quad x \longmapsto f(x+k) - f(x).$$

Let us first show that $\Delta_{f,k}$ is injective. Suppose that $\Delta_{f,k}(i) = \Delta_{f,k}(j)$ for some $i,j \in \mathbb{Z}_p \setminus \{0,-k\}$. Then

$$\begin{aligned} & f(i+k) - f(i) = f(j+k) - f(j) \\ \Longleftrightarrow & \log_\alpha(i+k) - \log_\alpha(i) = \log_\alpha(j+k) - \log_\alpha(j) \\ \Longleftrightarrow & \log_\alpha\left(1+\frac{k}{i}\right) = \log_\alpha\left(1+\frac{k}{j}\right) \\ \Longleftrightarrow & 1+\frac{k}{i} = 1+\frac{k}{j}. \end{aligned}$$

Since $i,j \notin \{0,-k\}$, it follows that $i = j$. Thus, $\Delta_{f,k}$ is an injective map for all $k \neq 0$. It can be seen that $Im(\Delta_{f,k}) = \mathbb{Z}_{p-1} \setminus \{0\}$.

Consider $(a,b) \in \mathbb{Z}_{p-1} \times \mathbb{Z}_p$. Assume $(a,b) \notin \left(\mathbb{Z}_{p-1} \times \{0\}\right) \cup \left(\{0\} \times \mathbb{Z}_p\right)$. Due to the fact that $a, b \neq 0$, $\Delta_{f,b}$ is injective, and $Im(\Delta_{f,b}) = \mathbb{Z}_{p-1} \setminus \{0\}$, there exists a unique element $y \in \mathbb{Z}_p \setminus \{0, -b\}$ such that $f(y+b) - f(y) = a$. We define $x := y + b$. Since $y \neq -b$, then $0 < x \leq p-1$. It follows that $(f(x), x)$ and $(f(y), y)$ are elements in D that have been defined uniquely by the element (a,b). Now, taking the difference between these two elements of D yields

$$\begin{aligned}(f(x),x) - (f(y),y) &= (f(y+b), y+b) - (f(y),y)\\ &= (f(y+b) - f(y), y+b-y)\\ &= (a,b).\end{aligned}$$

This shows that (a,b) can be written uniquely as difference from elements in D. If $(f(x) - f(y), x-y) = (i,0)$ for some $i \in \mathbb{Z}_{p-1}$, then $x = y$ and $i = 0$. Moreover, if $(f(x) - f(y), x-y) = (0,j)$ for some $j \in \mathbb{Z}_p$, then $x = y$ because f is injective. Therefore, D is a direct product difference set in $\mathbb{Z}_{p-1} \times \mathbb{Z}_p$ of order p. □

A preliminary observation about difference sets is that if ϕ is a given automorphism of a group G, then a subset $X \subseteq G$ is a difference set if and only if $\phi(X)$ is a difference set [98]. Therefore, it is possible to have more difference sets from a given one utilizing symmetries of G. We will take advantage of this notion to see how our transformation would be beneficial. The dots' positions in a logarithmic Welch Costas of size $p-1$ is a direct product difference set in $\mathbb{Z}_{p-1} \times \mathbb{Z}_p$, so if we add an empty column to right of a logarithmic Welch Costas array, let us call this array an extended logarithmic Welch, this extended array has the property that it contains all non-trivial displacement vectors exactly once, in which the differences are taken periodically. Consequently, the extended array has the property that the periodic autocorrelation function values are at most 1 for all possible non-zero shifts. Let us provide an example that shows the effect of extending an empty column to a logarithmic Welch Costas on its periodic property.

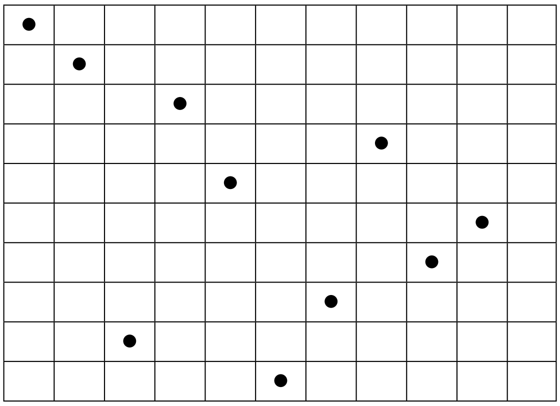
Example 3.27. *Let $\alpha = 2$ be the primitive element of $\mathbb{F}_{11}$. In $\mathbb{F}_{11}$,*

$$1 = 2^0, 2 = 2^1, 3 = 2^8, 4 = 2^2, 5 = 2^4, 6 = 2^9, 7 = 2^7, 8 = 2^3, 9 = 2^6, 10 = 2^5.$$

It follows that $X = [0,1,8,2,4,9,7,3,6,5]$ represents a logarithmic Welch Costas array as in Definition 2.40 with $c = 0$. In order to get a permutation on $[p-1]$, we add all the elements by 1. The following matrix shows the periodic autocorrelation matrix of X:

$$C_X^p = \begin{pmatrix}
1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 2 & 0 & 2 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 2 & 0 & 2 & 1 & 1 & 1 \\
1 & 1 & 2 & 1 & 0 & 1 & 2 & 1 & 1 & 0 & 1 & 1 & 2 & 1 & 0 & 1 & 2 & 1 & 1 \\
1 & 2 & 0 & 1 & 2 & 1 & 0 & 2 & 1 & 0 & 1 & 2 & 0 & 1 & 2 & 1 & 0 & 2 & 1 \\
2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 \\
1 & 2 & 0 & 1 & 2 & 1 & 0 & 2 & 1 & 0 & 1 & 2 & 0 & 1 & 2 & 1 & 0 & 2 & 1 \\
1 & 1 & 2 & 1 & 0 & 1 & 2 & 1 & 1 & 0 & 1 & 1 & 2 & 1 & 0 & 1 & 2 & 1 & 1 \\
1 & 1 & 1 & 2 & 0 & 2 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 2 & 0 & 2 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 10 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 2 & 0 & 2 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 2 & 0 & 2 & 1 & 1 & 1 \\
1 & 1 & 2 & 1 & 0 & 1 & 2 & 1 & 1 & 0 & 1 & 1 & 2 & 1 & 0 & 1 & 2 & 1 & 1 \\
1 & 2 & 0 & 1 & 2 & 1 & 0 & 2 & 1 & 0 & 1 & 2 & 0 & 1 & 2 & 1 & 0 & 2 & 1 \\
2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 \\
1 & 2 & 0 & 1 & 2 & 1 & 0 & 2 & 1 & 0 & 1 & 2 & 0 & 1 & 2 & 1 & 0 & 2 & 1 \\
1 & 1 & 2 & 1 & 0 & 1 & 2 & 1 & 1 & 0 & 1 & 1 & 2 & 1 & 0 & 1 & 2 & 1 & 1 \\
1 & 1 & 1 & 2 & 0 & 2 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 2 & 0 & 2 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 1
\end{pmatrix}$$

Now, we extend X with an empty column to the right, and we denote this extended array by Y as follows



The following matrix shows the periodic autocorrelation matrix of Y

$$C_Y^p = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 10 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}$$

As we can see, the maximum value in C_X^p is 2, and by extending X with an empty column, we obtain the maximum value of 1. Moreover, C_Y^p also shows that all non-trivial displacement vectors appear precisely once, where the array is being considered periodically.

Let us now discuss the effect of applying the transformation $\mathcal{A}_k$, as in Definition 3.22, to the extended logarithmic Welch Costas array. Let $X = [f(1), f(2), ..., f(p-1)]$ represent a logarithmic Welch Costas array as in Theorem 2.40. As we already mentioned, the dots' position in the extended logarithmic Welch Costas array produces a direct product difference set in $\mathbb{Z}_{p-1} \times \mathbb{Z}_p$. Hence, we can apply any automorphism to the set of points of dots' position in an extended logarithmic Welch, and the periodic autocorrelation property will not change at all. Let k be an integer relatively prime to p, and T_k be a mapping on the set of positions of dots in an extended logarithmic Welch Costas array defined as follows

$$\begin{aligned} T_k : \mathbb{Z}_{p-1} \times \mathbb{Z}_p &\to \mathbb{Z}_{p-1} \times \mathbb{Z}_p \\ (i,j) &\mapsto (i,kj) \end{aligned}$$

It is straightforward to check that T_k is an element of the automorphism group of $\mathbb{Z}_{p-1} \times \mathbb{Z}_p$ because k and p are coprime. Therefore, applying T_k to the extended logarithmic Welch Costas array will preserve the periodic property, which is the periodic autocorrelation function value of the extended logarithmic Welch Costas array for all possible non-zero shifts is at most 1. According to observation 2.18, if the periodic autocorrelation function value is at most 1, then the aperiodic autocorrelation function value is also at most 1. In addition, after applying T_k, the empty row in the extended logarithmic Welch Costas array stays fixed, so we can remove it to have an array of size $(p-1) \times (p-1)$, let us denote by Y, with the property that the aperiodic autocorrelation function value for all possible non-zero shifts is at most 1. Therefore, we can conclude that Y is a Costas array. It is a simple matter to check that $Y = \mathcal{A}_k(X)$ because after applying the transformation $\mathcal{A}_k$ to X, we send every element of the set of dots' position (i,j) to $(i, kj \mod p)$. It needs to be noted regarding the definition of $\mathcal{A}_k$, $gcd(k,p) = 1$. What we explained so far gives another proof of Theorem 3.20, showing logarithmic Welch Costas arrays are transferable.

Example 3.28. *Consider the logarithmic Welch Costas array $X = [0,1,8,2,4,9,7,3,6,5]$ in Example 3.27. According to Definition 3.22, the set of dots in X is the set*

$$D = \{(0,1),(1,2),(8,3),(2,4),(4,5),(9,6),(7,7),(3,8),(6,9),(5,10)\}.$$

Since $gcd(2,11) = 1$, then we have

$$\sigma_2(D) = \{(1,1),(2,2),(9,3),(3,4),(5,5),(0,6),(8,7),(4,8),(7,9),(6,10)\}.$$

Thus we can conclude that $\mathcal{A}_2(X) = [1,2,9,3,5,0,8,4,7,6]$. *The following figure shows the visualization of the aperiodic autocorrelation function of* $\mathcal{A}_2(X)$. *One can easily check that* $\mathcal{A}_2(X)$ *is a Costas array.*

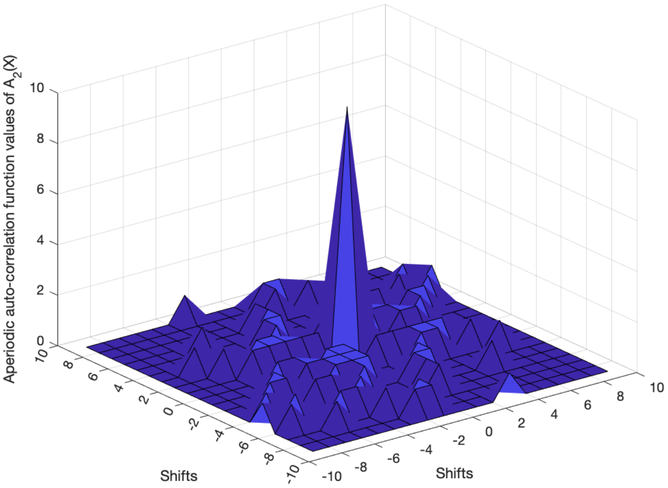


FIGURE 3.3: The visualization of $C^a_{\mathcal{A}_2(X)}$.

Jane Wodlinger [119] showed that if we consider the displacement vectors when we view the array periodically, an extended Lempel-Golomb Costas array (obtained by adding an empty row on the bottom and then an empty column to the right) contains the displacement vector (i, j) exactly once if $\alpha^i \neq \beta^j$ and otherwise never. In other words, the extended Lempel-Golomb Costas array has the property that the periodic autocorrelation function value for all possible non-zero shifts are at most 1. Let k is an integer relatively prime to $q-1$, and let G_2 be a Lempel-Golomb Costas array of size $q-2$, where q is a prime power, as in Theorem 2.46. We denote the extended Lempel-Golomb Costas array by X, and we define a map on the set of positions of dots in X as follows

$$\begin{aligned} T'_k : \mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1} &\to \mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1} \\ (i, j) &\mapsto (i, kj) \end{aligned}$$

It can be seen that T'_k is an element of the automorphism group of $\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$. Therefore, T'_k will preserve the periodic property of the extended Lempel-Golomb Costas arrays, X. Thus, after applying T'_k, we obtain an $(q-1) \times (q-1)$ array, let us denote by Y, with the property that its periodic and aperiodic autocorrelation function's values for all possible non-zero shifts are at most 1. Since the empty row and empty column in X stay fixed after being transformed by T'_k, we can remove them without changing the aperiodic properties of X to obtain an $(q-2) \times (q-2)$ array, denoted by Z. It can be seen that $Z = \mathcal{A}_k(G_2)$ because after applying $\mathcal{A}_k$ on G_2, we send every dot at position (i, j) to $(i, kj \bmod (q-1))$.

Definition 3.29. *A complete Costas array of size n is a matrix X for which one of the following cases gives an array with the property that for all possible non-zero shifts (r, s), $|r| \leq n$, $|s| \leq n$, the periodic autocorrelation values are at most* 1*, $C_X^p(r, s) \leq 1$.*

1. *If we add an empty column on the right of the array.*
2. *If we add an empty row on the bottom of the array and then an empty column on the right.*

We can collect all of the above in the following theorem.

Theorem 3.30. *Assume that X is a complete Costas array of size n, and k is a positive integer such that $gcd(k, n+1) = 1$, then $\mathcal{A}_k(X)$ is a Costas array.*

Proof. Suppose that $f : [n] \longrightarrow [n]$ is the corresponding permutation to the Costas array X. Since f is a permutation of size n, the set of dots' positions in X, say $D = \{(f(i), i) : i \in [n]\}$, can be considered as a subset of $\mathbb{Z}_{n+1}^\star \times \mathbb{Z}_{n+1}^\star$. By adding an empty column to the right of X, we can think of this set of dots' positions as a subset of $\mathbb{Z}_{n+1}^\star \times \mathbb{Z}_{n+1}$. After sending every element at position (i, j) to $(i, kj \bmod (n+1))$. Since $gcd(k, n+1) = 1$, it is straightforward to check that

$$\begin{aligned} T_k : \mathbb{Z}_{n+1}^\star \times \mathbb{Z}_{n+1} &\to \mathbb{Z}_{n+1}^\star \times \mathbb{Z}_{n+1} \\ (i, j) &\mapsto (i, kj), \end{aligned}$$

is an element of the automorphism group of $\mathbb{Z}_{n+1}^\star \times \mathbb{Z}_{n+1}$. Hence, applying T_k to the set of positions of dots in the extended X will preserve its periodic property.

Since X is a complete Costas array, the periodic autocorrelation function of extended X after being transformed by T_k has the property that it can take a value of, at most, 1 for all possible non-zero shifts. It follows that the aperiodic autocorrelation function's values of extended X are at most 1 for all possible non-zero shifts, as shown in Observation 2.18. Furthermore, after applying T_k, the empty column in the extended X stay fixed. Consequently, we can remove this empty column without increasing the maximum value of the aperiodic autocorrelation function of extended X. It follows that the permutation matrix $\mathcal{A}_k(X)$ is a Costas array.

Similar arguments apply to the case where adding an empty row and then an empty column makes a Costas array a complete Costas array. □

It is worth mentioning in passing that among the known Costas arrays up to size 29, apart from the Welch and Lempel-Golomb Costas arrays, none of them qualify as complete Costas arrays.

Chapter 4

A measure for Costas property

This chapter will consider a particular class of permutations, namely odd permutations, from which we can not construct a Costas array. Although most permutations do not produce a Costas array, it is worth discussing why they fail to construct Costas arrays. This chapter attempts to define a measure by which we can examine how far a permutation matrix is from being a Costas array and then examine whether or not it is possible to eliminate or at least reduce the violation causes. It is clear that even reducing the number of violations will lead to staying closer to a Costas array, which is fruitful.

Costas arrays are indeed known for their perfect aperiodic autocorrelation properties. In principle, finding Costas arrays, permutation matrices with aperiodic autocorrelation function values of at most 1 for all possible non-zero shifts, is challenging. Sometimes permutation matrices with low periodic autocorrelation also show perfect aperiodic autocorrelation. Take Welch and Lempel-Golomb constructions as an example where the extended arrays, as explained in Section 3.4, have periodic autocorrelation function values of 0 or 1 for all possible non-zero shifts, which means their aperiodic autocorrelation has the same behaviour because periodic autocorrelation bounds the aperiodic autocorrelation, as shown in Observation 2.18. We will follow this point of view to introduce a transformation that reduces violation causes to the Costas property in some permutations with low periodic autocorrelation properties.

Let us recall that a polynomial $f \in \mathbb{F}_q[x]$ ($\mathbb{F}_q[x]$ denotes the polynomial ring over $\mathbb{F}_q$) is a permutation polynomial of $\mathbb{F}_q$ if the map from $\mathbb{F}_q$ to itself defined by $x \longmapsto f(x)$ is a permutation of $\mathbb{F}_q$. We refer the readers to [77] for more details about this subject. Wensong Chu in [19] discussed the application of permutation polynomials over finite fields in the study of Costas arrays. Since basic algebraic constructions for Costas arrays are based on finite fields, it is reasonable to examine such permutation matrices as permutation polynomials over their underlying finite fields. From this point of view, Wensong Chu also showed that the algebraic construction methods utilize relatively simple permutation polynomials. More precisely, he defined Welch and Lempel-Golomb constructions the following permutation polynomials:

- **Welch Construction**: $W_1^{exp} = [f(x)]$, where $f(x) = x$ and $x = \alpha^{j+c}$, where $f \in \mathbb{F}_p[x]$, α is a primitive element in $\mathbb{F}_p$, $0 \leq j \leq p-2$ and $c \in \{0, \ldots, p-2\}$.

- **Lempel-Golomb Construction**: $G_2 = [\log_\alpha f(x)]$, where $f(x) = 1 - x^m$ and $x = \alpha^j$, where $f \in \mathbb{F}_q[x]$, $gcd(m, q-1) = 1$, α is a primitive element in $\mathbb{F}_q$ and $1 \leq j \leq q-2$.

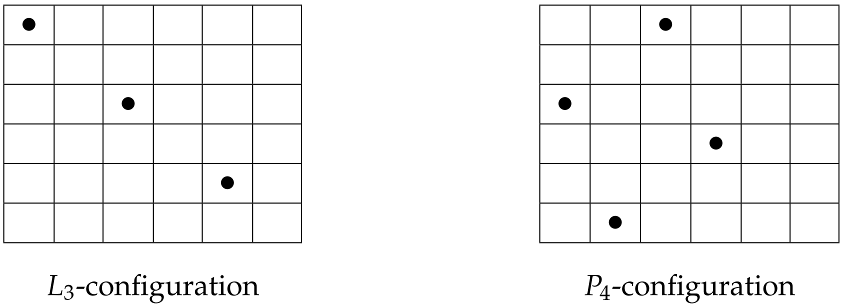
Moreover, he showed that no more Costas arrays from permutation binomials exist by stating the following theorem.

Theorem 4.1 ([19]). *Let α be a primitive element of $\mathbb{F}_q$ and let $f(x) = x^k - ax^j$, $a \in \mathbb{F}_q$ and $k > j \geq 0$ be a permutation polynomial over $\mathbb{F}_q$. If $\left[\log_\alpha f\left(\alpha^j\right)\right]$, $1 \leq j \leq q-2$ is a Costas array, then $gcd(k-j, q-1) = 1$.*

The above theorem shows that for f(x), as in Theorem 4.1, being a permutation polynomial over $\mathbb{F}_q$ with $(k-j, q-1) = 1$, we require that $j = 0$ because if $j \geq 1$, then $f(x) = 0$ has more than one zero.
Following this point of view, we will examine the Costas property of a class of permutations constructed by some permutation polynomials over a finite field, which will not produce Costas permutations; moreover, we will check if it is possible to reduce violation causes in these permutations to stay closer to Costas permutations.
A prerequisite for a permutation matrix to have perfect aperiodic autocorrelation is that its periodic autocorrelation function values must not exceed 4, as one can verify from Observation 2.18. Then this permutation matrix is worth studying because it may be the case therefore that it has perfect aperiodic autocorrelation. One suitable candidate for this approach could be permutation polynomials with low differential uniformity, which has been widely investigated through literature. This chapter also aims to investigate the aperiodic property of these permutation polynomials.

4.1 Forbidden Configurations

Soltanalian et al. in [107] proposed a geometrically equivalent definition of Costas arrays in which a permutation matrix is a Costas array if it does not contain four ones that form a parallelogram; moreover, it is free of lines formed by three equidistant ones. Bill Correl et al. in [112] provided a more refined version of this definition. They considered all possible ways that the arrangements of ones within a permutation matrix violate the Costas property. They referred to such sets of ones as L_3- and P_4-configurations, where an L_3-configuration is defined as a set of three equidistant ones lying on a single line, and a P_4-configuration is defined to be a set of four ones that form a non-degenerate parallelogram. It is worth noting that sets of four ones that form a degenerate parallelogram will violate the Costas property if these four ones are equidistant. However, since one can think of a set of four equidistant ones lying on a single line as two L_3-configurations, we only consider L_3- and P_4-configurations as violation causes to the Costas property; let us call them forbidden configurations. We denote by $FC(X)$ the total number of forbidden configurations in X, where X is a permutation matrix of size n. The matrices in Figure 4.1 shows such forbidden configurations.



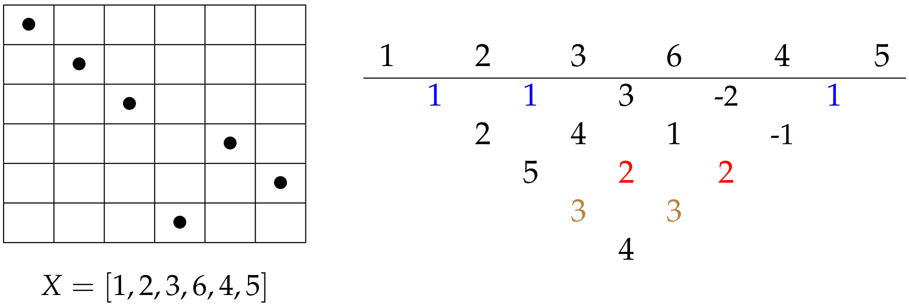
L_3-configuration

P_4-configuration

FIGURE 4.1: Forbidden configurations that violate the Costas property.

Since the total number of forbidden configurations in a given Costas array is zero, a given permutation matrix is close to being a Costas array if the number of forbidden configurations is small. In other words, the fewer forbidden configurations, the more close to being Costas array. The total number of forbidden configurations in a given permutation matrix is closely related to the number of repetitions in each row of its difference triangle table. One can easily verify that an L_3-configuration in a given permutation matrix represents a pair of displacement vectors with the same length and slope, showing a repeated value in a row of its difference triangle table. Moreover, a P_4-configuration depicts two pairs of displacement vectors, each of which has the same length and slope, showing two repeated values in two different rows of its difference triangle table. Let us provide an example that shows this relation.

Example 4.2. *Figure 4.2 illustrates the permutation matrix $X = [1, 2, 3, 6, 4, 5]$ and its corresponding difference triangle table. The first two blue entries in the first row of $T(X)$ correspond to the displacement vectors that form an L_3-configuration. The first and last blue entries in the first row and the repeated brown entries in the fourth row of $T(X)$ correspond to the displacement vectors that form a P_4-configuration. Similarly, the second and last blue entries in the first row and the repeated red entries in the third row of $T(X)$ represents a P_4-configuration.*



1 2 3 6 4 5

1 1 3 -2 1

2 4 1 -1

5 2 2

3 3

4

$X = [1, 2, 3, 6, 4, 5]$

FIGURE 4.2: Permutation matrix X and its corresponding difference triangle table, $T(X)$.

In order to compute the total number of forbidden configurations in a given permutation matrix, we can provide a formula utilizing the difference triangle table with an extra assumption. Our basic assumption is the following. When we count the total number of forbidden configurations, we consider a P_4-configuration as two forbidden configurations. The reason for preferring this is that since a P_4-configuration in a given permutation matrix shows two pairs of equal values in two different rows of a given difference triangle table, by counting a P_4-configuration as two forbidden configurations, we only consider repeated values in each row of the difference triangle table. If one considers a P_4-configuration as only one forbidden configuration, then constructing a formula for this number becomes much more complicated.

Theorem 4.3. *Let X be a permutation matrix of size n. Suppose that ith row of the difference triangle table of X contains values $a_{i1}, a_{i2}, ..., a_{ik}$ with repetitions $n_{i1}, n_{i2}, ..., n_{ik}$ respectively. Then*

$$FC(X) = \sum_{i=1}^{n-1} \sum_{j=1}^{k} \binom{n_{ij}}{2},$$

where $FC(X)$ denotes the total number of forbidden configurations in X.

Proof. It can be seen that any two repeated values in a row of $T(X)$ represent a pair of displacement vectors that form either an L_3-configuration or a pair of displacement vectors of a P_4-configuration. Since we consider a P_4-configuration as two pairs of displacement vectors with the same length and slope, we do not need to find two pairs of repeated values in two different rows of $T(X)$ to avoid over-counting. It is readily seen that in a given row i, we have $\sum_{j=1}^{k} \binom{n_{ij}}{2}$ pairs of displacement vectors with the same length and slope. Summing this expression over all rows of $T(X)$ counts the total number of forbidden configurations in X. Thus,

$$FC(X) = \sum_{i=1}^{n-1} \sum_{j=1}^{k} \binom{n_{ij}}{2},$$

which completes the proof. □

By the definition of a Costas array, we know that a permutation matrix X is a Costas array if each row of its difference triangle table is free of duplication. Thus, the Costas array definition is precisely the property of $FC(X) = 0$. It follows that having a permutation matrix with perfect aperiodic autocorrelation property is equivalent to a zero number of forbidden configurations. It is challenging to design Costas arrays directly. Since most of the permutation matrices of a given size n are not Costas arrays, one approach to constructing a Costas array or a permutation matrix close to a Costas array could be finding transformations that eliminate or reduce the total number of forbidden configurations in a permutation matrix which is not a Costas array. For example, the difference triangle table of the permutation $X = [1, 5, 2, 10, 4, 20, 8, 17, 16, 11, 9, 14, 12, 7, 6, 15, 3, 19, 13, 21, 18, 22]$ is given by

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

One can verify that $FC(X) = 122$. We can construct the permutation sequence $Y = [1,5,2,10,4,20,8,17,16,11,9,22,18,21,13,19,3,15,6,7,12,14]$ from X as follows: we split the permutation sequence X into two equal pieces, let us denote them by $X_1 = [1,5,2,10,4,20,8,17,16,11,9]$ and $X_2 = [14,12,7,6,15,3,19,13,21,18,22]$, and then if we reverse the ordering of the elements in X_2, we obtain $X_3 = [22,18,21,13,19,3,15,6,7,12,14]$. By concatenating X_1 and X_3, we obtain Y with the following difference triangle table.

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

As we can see, there is no repetition in each row of $T(Y)$, showing $FC(Y) = 0$. This simple transformation eliminated all forbidden configurations in X. The array X in this example has a particular property that we will discuss in the next section in more detail.

4.2 Odd Permutation

As discussed in the introductory part of this chapter, we will discuss the Costas property of odd permutations in this section. What follows is the definition of odd permutations.

Definition 4.4. *Let $f : [n] \longrightarrow [n]$ be a permutation of even size n. We say f is an odd permutation if for all $1 \leq i \leq n$, we have*

$$f(i) + f(n+1-i) = n+1.$$

Theorem 4.5. *Let $f : [n] \longrightarrow [n]$ be an odd permutation of even size n. Then f is not a Costas permutation.*

Proof. Let us take two consecutive elements in permutation $[f(i)]$, $i \in [n]$. We claim that there exist a duplicate value in the first row of its difference triangle table. Let us take $f(x)$ and $f(x+1)$ such that $1 \leq x \leq \frac{n}{2} - 1$. Since f is an odd permutation, we have

$$\begin{aligned} f(x+1) - f(x) &= (n+1-f(n-x)) - (n+1-f(n+1-x)) \\ &= f(n-x+1) - f(n-x). \end{aligned}$$

It is easy to check that $f(n-x+1)$ and $f(n-x)$ are also consecutive elements. Thus, the value $f(n-x+1) - f(n-x)$ is also appear in the first row of the difference triangle table of f. Since $n-x+1 \neq x+1$ and $x \neq n-x$, then f can not be a Costas permutation. □

Since we can think of the set of dots' position in a permutation matrix as a subset of $\mathbb{Z}_n \times \mathbb{Z}_n$, it is worthwhile to study permutation polynomials over $\mathbb{Z}_n$ and their property to see if a particular permutation polynomial gives a Costas array or not. A polynomial $f(x) = a_0 + a_1x + a_2x^2 + ... + a_rx^r$ with integral coefficients is called a permutation polynomial over a finite ring if it induces a bijective map from the ring to itself. We are mainly interested in permutation polynomials over $\mathbb{Z}_n$ and $\mathbb{F}_q$. In what follows, we denote by $\mathbb{Z}_n[x]$ the polynomial ring over $\mathbb{Z}_n$.

Definition 4.6 (Odd Permutation Polynomial)**.** *Let $\mathbb{Z}_n$ denote the ring of integers modulo n, where $n \in \mathbb{N}$ is an odd positive integer. A permutation polynomial $f \in \mathbb{Z}_n[x]$ is an odd permutation polynomial if $f(-x) = -f(x)$ for all $x \in \mathbb{Z}_n$.*

The reason for discussing odd permutation polynomials is that zero is a fixed point of any odd permutation polynomial $f \in \mathbb{Z}_n[x]$. Suppose that $f(x) = a_0 + a_1x + a_2x^2 + ... + a_rx^r$ is an odd permutation polynomial over $\mathbb{Z}_n$ of degree r. Since $f(-x) = -f(x)$ for all $x \in \mathbb{Z}_n$, then $f(0) = -f(0)$ implies $a_0 = 0$. Thus $f(0) = 0$. Consequently, after removing zero, we still have a permutation on elements of $\{1, ..., n-1\}$. This property allows us to construct an odd permutation from an odd permutation polynomial. The following observation reveals our intention of constructing odd permutations from odd permutation polynomials.

Observation 4.7. *A permutation polynomial $f \in \mathbb{Z}_n[x]$, where n is an odd integer, will give rise to an odd permutation.*

Proof. Since f is an odd permutation polynomial with $f(0) = 0$, we can construct a permutation matrix of size $n-1$ by placing a dot at position $(i, f(i))$, where $1 \leq i \leq n-1$. Let us represents this matrix by $X = [f(1), \ldots, f(n-1)]$, so X represents a permutation of even size $m := n-1$ with the property that for all $1 \leq i \leq m$ we have:

$$\begin{aligned} f(i) + f(m+1-i) &= f(i) + f(n-i) \\ &= f(i) + f(-i) \\ &= f(i) - f(i) \\ &= m+1. \end{aligned}$$

Thus, X corresponds to an odd permutation. □

As a corollary of Theorem 4.5, we can see that odd permutation polynomials over $\mathbb{Z}_n$ will not produce Costas permutations.

Corollary 4.8. *Let $f \in \mathbb{Z}_n[x]$ be an odd permutation polynomial over $\mathbb{Z}_n$, where n is an odd integer. Then the permutation $[f(i)]$, $i \in \mathbb{Z}_n$ is not a Costas permutation.*

Proof. The proof is the same as the proof of Theorem 4.5. □

Permutation polynomials have been broadly studied since the 19thcentury, and extensive research has been carried out on finding permutation polynomials over finite fields. In order to have some examples of odd permutation polynomials over a finite field, we collect the following theorems from Xiang-dong Hou's survey of recent advances on permutation polynomials over finite fields [32].

Theorem 4.9. ([77]) *The power mapping $f(x) = x^n$ is an odd permutation polynomial of $\mathbb{F}_q$ if and only if $gcd(n, q-1) = 1$.*

Theorem 4.10. ([31]) *The polynomial $f(x) = x^{2^{m+1}+1} + x^3 + x$ is an odd permutation polynomial of $\mathbb{F}_{2^{2m+1}}$.*

Theorem 4.11. *Let $s = 3^{t+1}$ and $a \in \mathbb{F}_{3^{2t+1}}$, where t is a positive integer . Then, $f(x) = x^{2s+3} + (ax)^s - a^2 x$ is an odd permutation polynomial of $\mathbb{F}_{3^{2t+1}}$.*

Theorem 4.12. ([6]) *The polynomial $f(x) = x + x^{2^{(m+2)/2}-1} + x^{2^m - 2^m/2} + 1$, where m is a positive even integer, is an odd permutation polynomial of $\mathbb{F}_{2^m}$*

Theorem 4.13. ([68]) *Let $f(x) = ax + bx^q + x^{2q-1}$ be a polynomial over $\mathbb{F}_{q^2}[x]$, where q is odd. Then, f is an odd permutation polynomial if and only if one of the following is satisfied.*

- $a = b = 0, q \equiv 1, 3 \pmod 6$.
- $(-a)^{\frac{q+1}{2}} = -1$ *or* 3, $b = 0$.

- $ab \neq 0$, $a = b^{1-q}$, $1 - \frac{4a}{b^2}$ *is a square of* $\mathbb{F}_q^*$.
- $ab(a - b^{1-q}) \neq 0$, $1 - \dfrac{4a}{b^2}$ *is a square of* $\mathbb{F}_q^*$, $b^2 - a^2b^{q-1} - 3a = 0$.

The above theorems give examples of odd permutation polynomials, and the introduced reference also contains more such examples. Since a permutation polynomial over $\mathbb{Z}_n$ induces a bijective map from $\mathbb{Z}_n$ to itself, we can represent it with a permutation matrix. From now on, we regard the difference triangle table of a permutation polynomial as the difference triangle table of its corresponding permutation matrix.

4.3 G-symmetric and Odd Permutations

The previous section discussed the Costas property of odd permutations. Although odd permutations do not have the Costas property, we will introduce a transformation from which we considerably reduce the number of forbidden configurations in these permutation matrices. We are mainly interested in odd permutations because there is a close tie between odd permutations and G-symmetric permutations. Essentially, it is possible to construct a G-symmetric permutation from a given odd permutation. Let us explain how we can transform an odd permutation to obtain a G-symmetric permutation, and then we will investigate how this procedure may reduce the total number of forbidden configurations. Let $X = [f(1), \ldots, f(n)]$ be an odd permutation on elements $\{1, 2, ..., n\}$, where n is an even integer. Let us split the permutation X into two equal pieces, $X_1 = [f(1), f(2), ..., f(\frac{n}{2})]$ and $X_2 = [f(\frac{n}{2}+1), f(\frac{n}{2}+2), ..., f(n)]$. We reverse the ordering of the second piece to obtain $X_2' = [f(n), f(n-1), \ldots, f(\frac{n}{2}+1)]$. Then we concatenate X_1 and X_2' to obtain permutation $Y = [f(1), f(2), ..., f(\frac{n}{2}), f(n), f(n-1), ..., f(\frac{n}{2}+1)]$. Let us denote this transformation by $\mathcal{G}$. The following definition gives the formal definition of the transformation $\mathcal{G}$.

Definition 4.14 (Transformation $\mathcal{G}$). *Let $X = [f(1), f(2), \ldots, f(n)]$ be an odd permutation, where n is an even integer. We define a bijective map $g : [n] \longrightarrow [n]$, by*

$$g(i) = \begin{cases} f(i) & 1 \leq i \leq \frac{n}{2} \\ \\ f\left(\frac{3n}{2} + 1 - i\right) & \frac{n}{2} + 1 \leq i \leq n. \end{cases}$$

We denote the corresponding permutation matrix g by $\mathcal{G}(X)$.

Theorem 4.15. *Let $f : [n] \longrightarrow [n]$, where n is an even integer, be an odd permutation with the corresponding permutation matrix X, then $\mathcal{G}(X)$, as in Definition 4.14, has the G-symmetric property.*

Proof. To prove that $\mathcal{G}(X)$ has the G-symmetric property, we need to show that for all $1 \leq i \leq \frac{n}{2}$, we have $g(i) + g\left(\frac{n}{2} + i\right) = n + 1$. From the definition of $\mathcal{G}(X)$ and the fact that $1+\frac{n}{2} \leq i+\frac{n}{2} \leq n$, we can conclude that

$$\begin{aligned} g(i)+g\left(\tfrac{n}{2}+i\right) &= f(i)+f\left(\tfrac{3n}{2}+1-\tfrac{n}{2}-i\right) \\ &= f(i)+f(n-i+1) \\ &= f(i)+n+1-f(i) \\ &= n+1. \end{aligned}$$

The third equality holds because f is an odd permutation. Thus $\mathcal{G}(X)$ has the G-symmetric property. □

Although a Costas array is a permutation matrix with no forbidden configurations, one may ask which permutation matrix contains the maximal number of forbidden configurations. The following theorem provides an answer to this question.

Theorem 4.16. *Let I_n and A_n be the identity matrix of size n, $n \in \mathbb{N}$, and the anti-diagonal matrix of 1's of size n, respectively. Among all permutation matrices of size n, I_n and A_n contain the maximal number of forbidden configurations.*

Proof. Suppose X is a permutation matrix of size n. A maximum number of common points occurs if each row of its difference triangle table has elements with the same values, which can only happen if X is of the form $[a, a+t, a+2t, \ldots, a+nt]$ for some integer $a, t \in [n]$, but X can be a permutation on n elements if $a = i = 1$ or $a = n$ and $i = -1$. It follows that X is either I_n or A_n. □

Another relevant question that one can ask is how many forbidden configurations the identity matrix contains. The result is

Theorem 4.17. *For $n \geq 2$, let I_n be the identity matrix of size n. Then the number of forbidden configurations in I_n is*

$$FC(I_n) = \binom{n}{3}.$$

Proof. It is easy to verify that in row $i, 1 \leq i \leq n-1$, of the difference triangle table of $\mathcal{I}_n$, we have $n-i$ elements with a value equal to i. It follows that the number of forbidden configurations in $\mathcal{I}_n$ can be calculated as follow

$$\begin{aligned} FC(\mathcal{I}_n) &= \sum_{i=1}^{n-1} \binom{n-i}{2} \\ &= \sum_{j=0}^{n-1} \binom{j}{2} \\ &= \sum_{j=0}^{n-1} \frac{j(j-1)}{2} \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{2}\sum_{j=0}^{n-1} j^2 + \frac{1}{2}\sum_{j=0}^{n-1} j \\
&= \frac{1}{2}\left(\frac{n(n-1)(2n-1)}{6} - \frac{n(n-1)}{2}\right) \\
&= \frac{n(n-1)(2n-4)}{12} \\
&= \frac{n(n-1)(n-2)}{6} \\
&= \binom{n}{3}.
\end{aligned}
$$

□

Let us note that the identity matrix is also an odd permutation. Then, in order to have a better understanding of the transformation $\mathcal{G}$'s effect on the number of forbidden configurations in a given odd permutation, we subsequently can apply the transformation $\mathcal{G}$ on an identity matrix to see how much will be the reduction in the number of forbidden configurations. We realized that the transformation $\mathcal{G}$ significantly reduces the number of forbidden configurations in a given identity permutation. We will state a theorem that indicates the desired reduction.

Theorem 4.18. *Let $\mathcal{I}_n$ be an identity permutation of size n, where n is an even integer. Then*

$$
FC(\mathcal{G}(\mathcal{I}_n)) = \begin{cases} \displaystyle\sum_{i=1}^{\frac{n}{2}-1} 2\binom{i}{2} & \frac{n}{2} \text{ is even} \\[2ex] \displaystyle\sum_{i=1}^{\frac{n-2}{4}} 2\binom{\frac{n-2i}{2}}{2} + \sum_{i=\frac{n+2}{4}}^{\frac{n}{2}-1}\left[\binom{\frac{n-2i}{2}}{2} + \binom{\frac{n-2i+2}{2}}{2}\right] & \frac{n}{2} \text{ is odd} \end{cases}
$$

where $FC(\mathcal{G}(\mathcal{I}_n))$ is the total number of forbidden configuration of $\mathcal{G}(\mathcal{I}_n)$ as in Theorem 4.3, and $\mathcal{G}$ is the transformation introduced in Definition 4.14.

Proof. Let us take a row i of the difference triangle table of $\mathcal{G}(\mathcal{I}_n)$. Taking Lemma 2.45 into account, it is easy to verify that in a row i, the first $\frac{n-2i}{2}$ elements in T_1's region have the value equal to i, and the i elements in T_3's region are of the form $(n-k) - (\frac{n}{2} - (i-(k+1)))$ for some integer k in $\{0, 1, ..., i-1\}$, and the $\frac{n-2i}{2}$ elements in T_2's region have the value equal to $-i$. In other words, row i is as follows

$$
[\underbrace{i, i, \ldots, i}_{\frac{n-2i}{2}-\text{times}}, \underbrace{(n-1) - (\tfrac{n}{2} - (i-2)), \ldots, n - (i-1) - \tfrac{n}{2}}_{i-\text{times}}, \underbrace{-i, -i, \ldots, -i}_{\frac{n-2i}{2}-\text{times}}]
$$

To compute the number of forbidden configurations in this row, we first show that none of the elements in the T_3's region can be equal. In fact, if for some distinct integers k_1 and k_2 in $\{0,1,...,i-1\}$ we have

$$(n-k_1)-(\tfrac{n}{2}-(i-(k_1+1)))=(n-k_2)-(\tfrac{n}{2}-(i-(k_2+1))),$$

then we obtain $k_1 = k_2$. On account of Lemma 2.45, since each row of T_3's region is free of duplication, each row of T_4's region is also free of duplication. Thus, for computing the number of forbidden configurations, we can consider the rows of difference triangle table for $1 \leq i \leq \frac{n}{2}-1$. Moreover, we claim that all the elements in T_3's region are positive integers. Suppose, contrary to our claim, that

$$(n-k)-(\tfrac{n}{2}-(i-(k+1)))<0.$$

Thus, we can conclude that $\frac{n}{2}+i < 2k+1$. We also know that $k \leq i-1$ which means that $2k+1 \leq 2i-1$. Thus, $\frac{n}{2}+i < 2i-1$. This contradicts our assumption of $i < \frac{n}{2}$.

So far, we showed that all elements in the T_3's region of the row i are distinct and positive, which means there is no intersection between T_3 and T_2's region in the row i. Since all the elements in T_3's region are distinct, then T_1 and T_3's region can have at most one element in common. In other words, there is only the possibility that there exist an element in T_3's region with a value equal to i.

Suppose that

$$(n-k)-(\tfrac{n}{2}-(i-(k+1)))=i \text{ for some integer } k\in\{0,1,\ldots,i-1\}.$$

Thus, $\frac{n}{2}=2k+1$. Therefore, the proof falls naturally into two cases.

1) if $\frac{n}{2}$ is even, there is no intersection between T_1 and T_3's regions in the row i. Therefore, in this row, there are $\frac{n-2i}{2}$ elements with a value equal to i, and $\frac{n-2i}{2}$ elements with a value equal to $-i$. Thus, the total number of forbidden configurations in $\mathcal{G}(\mathcal{I}_n)$ is

$$\sum_{i=1}^{\frac{n}{2}-1} 2\binom{\frac{n-2i}{2}}{2} = \sum_{i=1}^{\frac{n}{2}-1} 2\binom{i}{2}.$$

2) suppose that $\frac{n}{2}$ is odd. Since $\frac{n}{2} = 2k+1$, $k = \frac{n-2}{4}$. We know that $k \leq i-1$, which means $i \geq \frac{n+2}{4}$. Therefore, in the T_1 and T_3's regions, there are $\frac{n-2i}{2}+1$ elements with a value equal to i, and there are $\frac{n-2i}{2}$ elements with a value equal to $-i$ in the T_2's region. From this we conclude that the number of forbidden configurations can be computed as follows

$$\sum_{i=1}^{\frac{n-2}{4}} 2\binom{\frac{n-2i}{2}}{2} + \sum_{i=\frac{n+2}{4}}^{\frac{n}{2}-1}\left[\binom{\frac{n-2i}{2}}{2}+\binom{\frac{n-2i+2}{2}}{2}\right].$$

□

The above theorem implies that reducing the number of forbidden configurations in an odd permutation might be possible by applying the transformation $\mathcal{G}$. Intuition and computational experiments suggest that the transformation $\mathcal{G}$ reduces the number of the forbidden configurations in all odd permutations of even size n significantly. Our computational experiments revealed that for all odd permutations of even size up to size 14, the transformation $\mathcal{G}$ always reduces the total number of forbidden configurations. Moreover, random sample checks for $n \leq 200$ confirm that transforming an odd permutation to a G-symmetric one will result in fewer forbidden configurations. Figure 4.3 illustrates the transformation $\mathcal{G}$'s effect on all odd permutations of even sizes up to size 14. In these figures, each vertical line contains two points, one red and one blue point. The red points show $FC(X)$, where X is an odd permutation, and the blue points show $FC(\mathcal{G}(X))$. We will formulate the following conjecture based on these

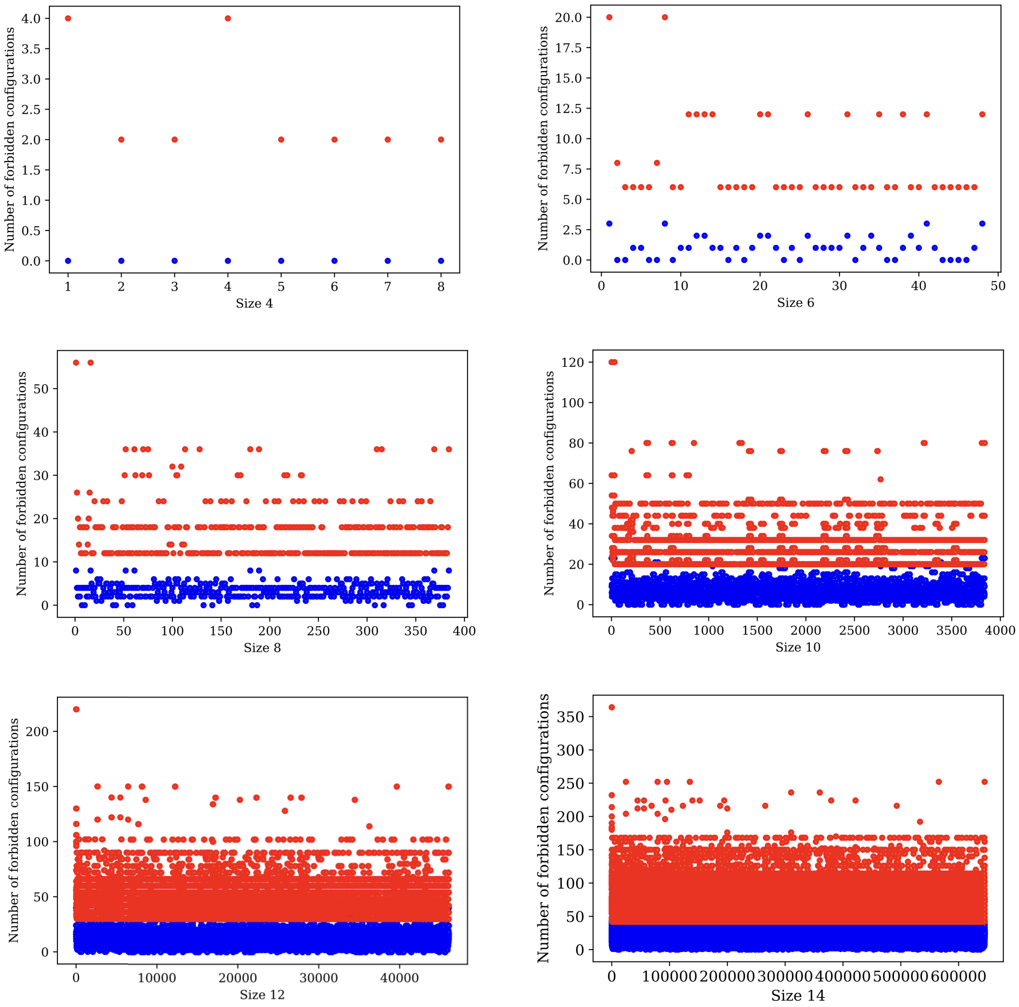


FIGURE 4.3: The number of the forbidden configurations of all odd permutations of sizes 6 − 14 and their corresponding G-symmetric permutations.

experimental computations.

Conjecture 4.19. *Let $X = [f(1), f(2), ..., f(n)]$ be an odd permutation of even size n, where $n \in \mathbb{N}$ is a positive integer. Then, $\mathcal{G}(X)$ has fewer forbidden configurations than X.*

In order to facilitate comparisons of the reduction in the number of forbidden configurations in a given odd permutation and its corresponding G-symmetric array, we computed the ratio of the number of forbidden configurations in a given G-symmetric permutation divided by the number of forbidden configurations in its corresponding odd permutation. In other words, each point shows the value $\frac{FC(\mathcal{G}(X))}{FC(X)}$, where X is an odd permutation. This result is shown in Figure 4.4. One can easily verify that this ratio is always less than 1, meaning the reduction in all cases has been achieved.
It is worth noting that in order to provide a theoretical proof for Conjecture 4.19, one can not show that in each row of the difference triangle table of $\mathcal{G}(X)$, where X is any odd permutation, we obtain fewer forbidden configurations by reducing the number of repeated values, which will lead to fewer forbidden configurations in total. Let us provide an example for this remark.

Example 4.20. *Consider the odd permutation $X = [5, 7, 3, 2, 10, 1, 9, 8, 4, 6]$. We obtain the G-symmetric permutation $\mathcal{G}(X) = [5, 7, 3, 2, 10, 6, 4, 8, 9, 1]$ by applying the transformation $\mathcal{G}$. We construct their difference triangle tables as follows.*

5	7	3	2	10	1	9	8	4	6
2	-4	-1	8	-9	8	-1	-4	2	
-2	-5	7	-1	-1	7	-5	-2		
-3	3	-2	7	-2	3	-3			
5	-6	6	6	-6	5				
-4	2	5	2	-4					
4	1	1	4						
3	-3	3							
-1	-1								
1									

5	7	3	2	10	6	4	8	9	1
2	-4	-1	8	-4	-2	4	1	-8	
-2	-5	7	4	-6	2	5	-7		
-3	3	3	2	-2	3	-3			
5	-1	1	6	-1	-5				
1	-3	5	7	-9					
-1	1	6	-1						
3	2	-2							
4	-6								
-4									

Utilizing Theorem 4.3, one can verify that $FC(X) = 20\binom{2}{2} = 20$ and $FC(\mathcal{G}(X)) = 4\binom{2}{2} + \binom{3}{2} = 7$. As we can see, the number of forbidden configurations has been reduced considerably, but three repeated values of 3 have occurred in the third row of the difference triangle table of $\mathcal{G}(X)$, showing the transformation $\mathcal{G}$ results in an arrangement of some points that constitute more forbidden configurations. In other words, there is a local increase in the number of forbidden configurations, but in total, the number of forbidden configurations has reduced.

We saw in Theorem 4.9 that the mappings of form $f(x) = x^d$ over finite fields with q elements, where q is a prime power, give odd permutation polynomials if $gcd(d, q-1) = 1$. In our case of interest, we consider the permutation polynomial $f(x) = x^{p-2}$ over $\mathbb{F}_p$, where p is an odd prime. This function is known as inverse mapping through literature. Due to several

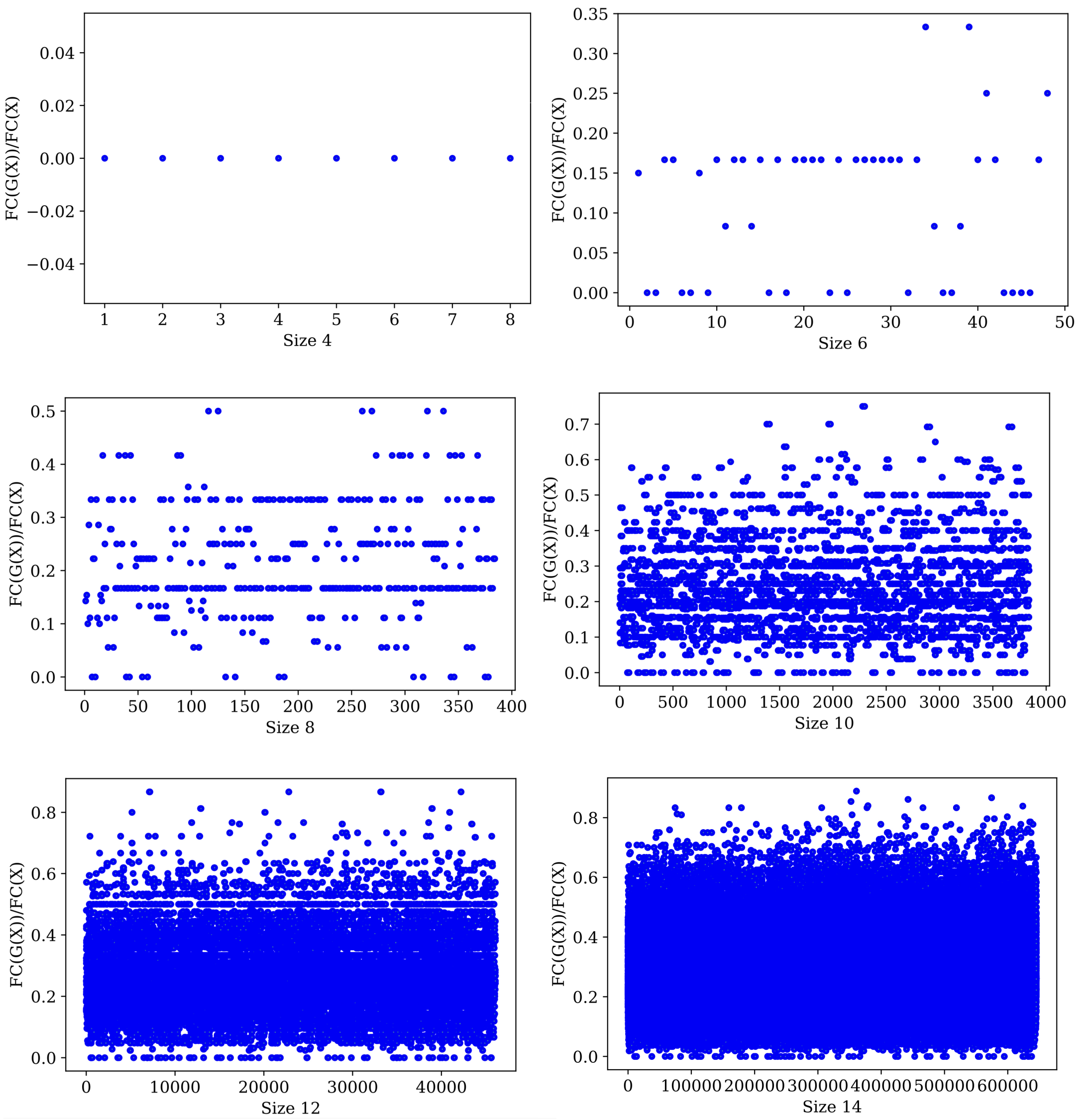


FIGURE 4.4: The values $\frac{FC(\mathcal{G}(X))}{FC(X)}$, where X is an odd permutation of even sizes $4-14$.

applications of inverse functions that we will discuss in the next section, we decided to accomplish an experimental computation to assess the validity of Conjecture 4.19 for this function. Let us provide an example of the transformation $\mathcal{G}$'s effect on inverse function over a finite field.

Example 4.21. *Let $f(x) = x^9$ be the inverse function over $\mathbb{F}_{11}$. The permutation corresponds to f for $1 \leq x \leq 10$ is $X = [1,6,4,3,9,2,8,7,5,10]$, and then $\mathcal{G}(X) = [1,6,4,3,9,10,5,7,8,2]$. Let us draw the difference triangle table of X and $\mathcal{G}(X)$.*

1	6	4	3	9	2	8	7	5	10
5	−2	−1	6	−7	6	−1	−2	5	
3	−3	5	−1	−1	5	−3	3		
2	3	−2	5	−2	3	2			
8	−4	4	4	−4	8				
1	2	3	2	1					
7	1	1	7						
6	−1	6							
4	4								
9									

1	6	4	3	9	10	5	7	8	2
5	−2	−1	6	1	−5	2	1	−6	
3	−3	5	7	−4	−3	3	−5		
2	3	6	2	−2	−2	−3			
8	4	1	4	−1	−8				
9	−1	3	5	−7					
4	1	4	−1						
6	2	−2							
7	−4								
1									

Using Theorem 4.25 we can compute the number of forbidden configurations in X as follows.

$$\sum_{i=1}^{9} \left\lfloor \tfrac{10-i}{2} \right\rfloor \binom{2}{2} = 4+4+3+3+2+2+1+1+0 = 20.$$

Using Theorem 4.3, we have

$$FC(\mathcal{G}(X)) = 2\binom{2}{2} + 2\binom{2}{2} + \binom{2}{2} + \binom{2}{2} = 6.$$

As we expected, the number of forbidden configurations drops significantly. Therefore, $\mathcal{G}(X)$ has fewer violations to the Costas property than X.

Turning to the experimental evidence, we computed the number of forbidden configurations of odd permutations constructed by inverse functions and their transformed version using the transformation $\mathcal{G}$ over a finite field $\mathbb{F}_p$ for prime $5 \leq p \leq 977$, and we visualized the result in Figure 4.5. Figure 4.5 illustrates that the number of forbidden configurations has been reduced by applying the transformation $\mathcal{G}$ on the inverse function over $\mathbb{F}_p$, $5 \leq p \leq 977$. This case study also provides more evidence of the validity of Conjecture 4.19. To have a better estimation of these reductions, we computed the ratio between $FC(X)$ and $FC(\mathcal{G}'(X))$, as shown in Figure 4.6. Figure 4.6 shows that the number of forbidden configurations has been reduced significantly. Our further analysis showed that for $37 \leq p \leq 997$, more than 65% of forbidden configurations have been eliminated after being transformed by $\mathcal{G}$. The following section will discuss odd permutation polynomials more in a periodic setting.

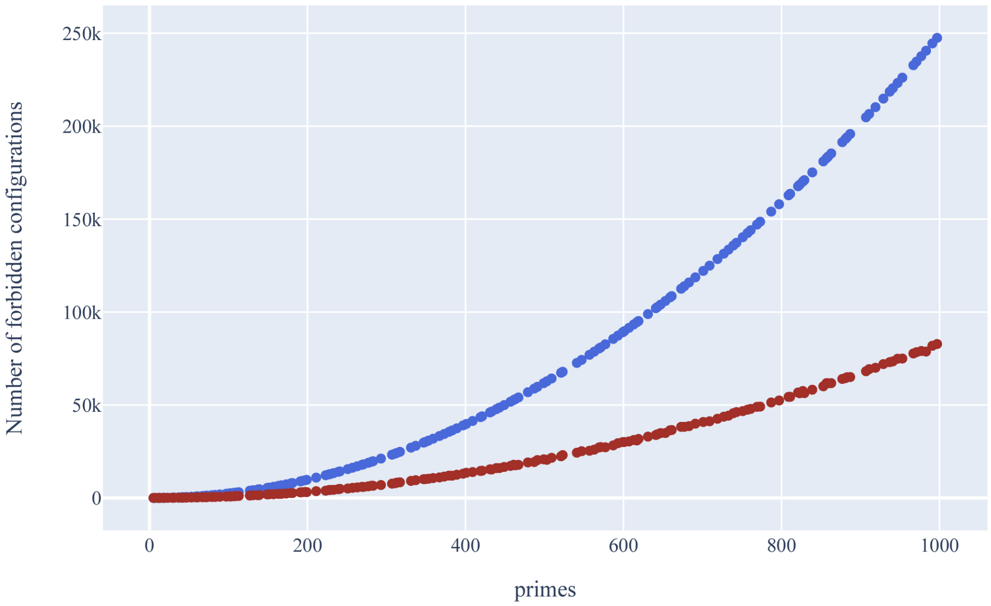


FIGURE 4.5: Values of $FC(X)$ and $FC(\mathcal{G}(X))$, where X is an odd permutation constructed by inverse function over $\mathbb{F}_p$, for $5 \leq p \leq 997$: the blue and red dots correspond to $FC(X)$ and $FC(\mathcal{G}(X))$, respectively.

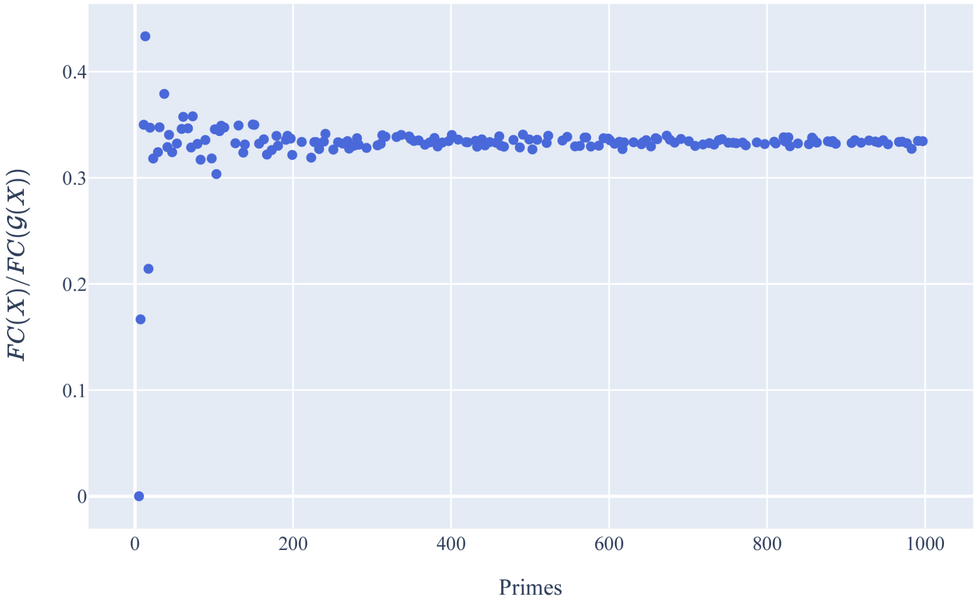


FIGURE 4.6: Values of $\frac{FC(\mathcal{G}(X))}{FC(X)}$, where X is an odd permutation constructed by an inverse function over finite field $\mathbb{F}_p$, for prime $5 \leq p \leq 997$.

4.4 PN/APN mappings

Our investigation of finding an odd permutation X with the property that $\mathcal{G}(X)$ is close to being a Costas array resulted in an interesting observation related to permutation polynomials with low differential uniformity. If we want to stay as close as possible to a Costas array, we require a permutation with a small number of forbidden configurations. Regarding Theorem 4.2, we know that if we have a small number of repetitions in each row of the difference triangle table of a given permutation, we also have a small number of forbidden configurations. Suppose $X = [f(1), f(2), ..., f(n)]$ is a permutation of size n. For any given permutation $f : [n] \longrightarrow [n]$, we can define a function $f' : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ such that $\{(x, f'(x)) : x \in \mathbb{Z}_n\}$ expresses the set of position of dots in the permutation matrix X. It follows that we can think of an element b, where $1 - n \leq b \leq n - 1$, in a row i, $1 \leq i \leq n - 1$, of the difference triangle table of X as a solution to the equation

$$f'(x + i) - f'(x) = b, \text{ for all } 1 \leq x \leq n - i. \tag{4.1}$$

Hence, to avoid repetitions in each row of a difference triangle table, we want Equation (4.1) to have few solutions. It can be seen that any solution to Equation (4.1) is also a solution to the following equation:

$$f'\left((x + i) \bmod (n)\right) - f'(x) \equiv b \bmod (n), \text{ for } x, b \in \mathbb{Z}_n, \tag{4.2}$$

but not the other way around. Thus, the number of solutions of Equation (4.2) provides an upper bound for the number of solutions of Equation (4.1). This attitude helps to investigate the differential properties of functions that express the set of points in permutation matrices [93].

Let G_1 and G_2 be two Abelian groups of the same size n, and let f be a mapping between these two Abelian groups, $f : G_1 \longrightarrow G_2$. For $a \in G_1$, $a \neq 0$ and $b \in G_2$, let us denote the number of solutions $x \in G_2$ of $f(x + a) - f(x) = b$ by $N(a, b)$ and let

$$\triangle_f = max\{N(a, b) | a \in G_1, a \neq 0 \text{ and } b \in G_2\}.$$

According to Nyberg [90], a mapping f is called differentially k-uniform if $\triangle_f = k$. When k is small, f is considered a mapping with low differential uniformity.

Mappings with low differential uniformity have been extensively studied, especially in the last 30 years. This concept is a significant area of interest within the field of cryptography, geometry, combinatorics and coding theory. For applications in cryptography, one would prefer mappings for which $\triangle_f$ is as small as possible. Mappings with low differential uniformity meet our desire to have as few forbidden configurations as possible. The mapping f for which $\triangle_f = 1$ is called perfect nonlinear (PN). Moreover, those mappings for which $\triangle_f = 2$ are called almost perfect nonlinear (APN). Drakakis, Gow and McGuire have already connected the two topics of APN mappings and Costas arrays in [37], where they showed the Welch construction for Costas arrays gives APN permutations, $f : \mathbb{Z}_{p-1} \longrightarrow \mathbb{Z}_{p-1}$, where p is a prime. They also mentioned some critical differences between Costas arrays and PN or APN mappings. Firstly, PN/APN mappings are defined to be mappings between two Abelian groups with the same cardinality, whereas Costas

arrays are defined on integers $\{1, 2, ..., n\}$. Secondly, PN/APN mappings are not necessarily permutations. Lastly, PN/APNness is a periodic property because, for these mappings, $x + a$ could not fall outside the mapping's domain, while this can happen for Costas permutations.
A noticeable fact about APN permutation functions is that the APN property is a periodic property, implying that when its corresponding permutation matrix is wrapped on a torus, it can not have three or more displacement vectors with the same length and slope. Let us explain how we associate a matrix to an odd permutation polynomial.

Definition 4.22. *Let $f \in \mathbb{Z}_n[x]$ be an odd permutation polynomial. The corresponding matrix of f is an $n \times n$ matrix constructed through the two following steps:*

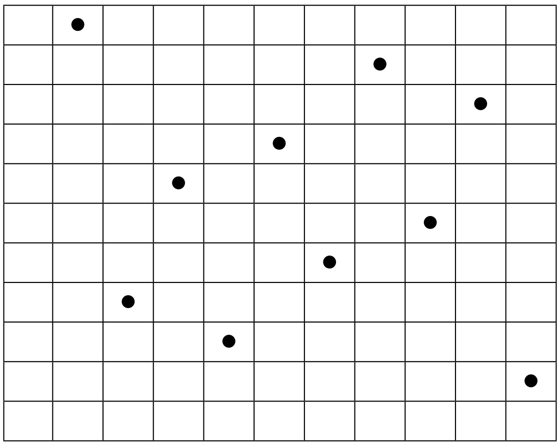
1) *First, we construct a permutation matrix of size $n-1$, say $X = \left(x_{i,j}\right)$, $1 \leq i, j \leq n-1$, where the entries are given by*

$$x_{i,j} = \begin{cases} 1 & \textit{if } i = f(j) \\ 0 & \textit{otherwise.} \end{cases}$$

2) *Next, we extend the constructed permutation matrix X in the previous step by an empty column to the left and then an empty row at the bottom.*

Let us note that the reason for appending an empty column and row is that an odd permutation polynomial maps 0 to 0.

Example 4.23. *Consider the permutation polynomial $f(x) = x^3$ over $\mathbb{Z}_{11}$. It can be seen that $X = [1, 8, 5, 9, 4, 7, 2, 6, 3, 10]$ represents a permutation matrix of size 10 for all $1 \leq x \leq 10$. By extending X with an empty column to the right and then an empty row at the bottom, we obtain the following corresponding matrix to the permutation polynomial f.*



The critical point to note here is that for an odd APN permutation function on $\mathbb{Z}_n$, the property of mapping the element zero to zero plays an important role. We saw in Theorem 4.25 that since we remove the element zero to construct an odd permutation from an odd APN permutation, it is worthwhile to discuss its effect on both periodic and aperiodic properties of its corresponding permutation matrix. According to the definition of the corresponding matrix to an odd permutation, as in Definition 4.22, removing zero leads to removing the empty row and column. Although removing zero in an aperiodic setting will not cause any problems, it will be problematic in a periodic setting, which may change the whole periodic property of the permutation matrix. In other words, removing zero might increase the maximum value of the periodic autocorrelation function values, whereas the maximum value of the aperiodic autocorrelation function will not increase. Let us provide an example for this comment.

Example 4.24. *Consider the corresponding matrix to the permutation polynomial $f(x) = x^3$ over $\mathbb{Z}_{11}$, as in Example 4.23, with the following periodic autocorrelation matrix*

$$C_X^p = \begin{pmatrix}
0&2&0&0&1&2&2&0&2&0&0&0&2&0&0&1&2&2&0&2&0\\
0&1&2&0&2&0&0&2&2&0&0&0&1&2&0&2&0&0&2&2&0\\
1&0&0&2&0&0&2&2&0&2&0&1&0&0&2&0&0&2&2&0&2\\
2&2&1&0&0&0&0&2&0&2&0&2&2&1&0&0&0&0&2&0&2\\
0&0&0&1&2&2&2&0&0&2&0&0&0&0&1&2&2&2&0&0&2\\
2&0&0&2&2&2&1&0&0&0&0&2&0&0&2&2&2&1&0&0&0\\
2&0&2&0&0&0&0&1&2&2&0&2&0&2&0&0&0&0&1&2&2\\
2&0&2&2&0&0&2&0&0&1&0&2&0&2&2&0&0&2&0&0&1\\
0&2&2&0&0&2&0&2&1&0&0&0&2&2&0&0&2&0&2&1&0\\
0&2&0&2&2&1&0&0&2&0&0&0&2&0&2&2&1&0&0&2&0\\
0&0&0&0&0&0&0&0&0&0&10&0&0&0&0&0&0&0&0&0&0\\
0&2&0&0&1&2&2&0&2&0&0&0&2&0&0&1&2&2&0&2&0\\
0&1&2&0&2&0&0&2&2&0&0&0&1&2&0&2&0&0&2&2&0\\
1&0&0&2&0&0&2&2&0&2&0&1&0&0&2&0&0&2&2&0&2\\
2&2&1&0&0&0&0&2&0&2&0&2&2&1&0&0&0&0&2&0&2\\
0&0&0&1&2&2&2&0&0&2&0&0&0&0&1&2&2&2&0&0&2\\
2&0&0&2&2&2&1&0&0&0&0&2&0&0&2&2&2&1&0&0&0\\
2&0&2&0&0&0&0&1&2&2&0&2&0&2&0&0&0&0&1&2&2\\
2&0&2&2&0&0&2&0&0&1&0&2&0&2&2&0&0&2&0&0&1\\
0&2&2&0&0&2&0&2&1&0&0&0&2&2&0&0&2&0&2&1&0\\
0&2&0&2&2&1&0&0&2&0&0&0&2&0&2&2&1&0&0&2&0
\end{pmatrix}$$

Since there in no value greater than or equal to 3 in the matrix C_X^p, except the value 10 which is the value at $(0,0)$ shift, we can conclude that the permutation X has the APN property. If we remove the empty column and empty row X, we obtain a permutation $Y = [1,8,5,9,4,7,2,6,3,10]$ with the following periodic autocorrelation matrix

$$C_Y^p = \begin{pmatrix}
1 & 2 & 0 & 0 & 1 & 4 & 0 & 2 & 0 & 0 & 1 & 2 & 0 & 0 & 1 & 4 & 0 & 2 & 0 \\
0 & 0 & 2 & 2 & 0 & 0 & 2 & 4 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 4 & 0 \\
1 & 0 & 1 & 2 & 0 & 2 & 0 & 0 & 4 & 0 & 1 & 0 & 1 & 2 & 0 & 2 & 0 & 0 & 4 \\
2 & 2 & 0 & 0 & 4 & 0 & 2 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 4 & 0 & 2 & 0 & 0 \\
2 & 0 & 3 & 0 & 0 & 0 & 3 & 0 & 2 & 0 & 2 & 0 & 3 & 0 & 0 & 0 & 3 & 0 & 2 \\
0 & 0 & 2 & 0 & 4 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 2 & 0 & 4 & 0 & 0 & 2 & 2 \\
4 & 0 & 0 & 2 & 0 & 2 & 1 & 0 & 1 & 0 & 4 & 0 & 0 & 2 & 0 & 2 & 1 & 0 & 1 \\
0 & 4 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 4 & 2 & 0 & 0 & 2 & 2 & 0 & 0 \\
0 & 2 & 0 & 4 & 1 & 0 & 0 & 2 & 1 & 0 & 0 & 2 & 0 & 4 & 1 & 0 & 0 & 2 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 10 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 2 & 0 & 0 & 1 & 4 & 0 & 2 & 0 & 0 & 1 & 2 & 0 & 0 & 1 & 4 & 0 & 2 & 0 \\
0 & 0 & 2 & 2 & 0 & 0 & 2 & 4 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 4 & 0 \\
1 & 0 & 1 & 2 & 0 & 2 & 0 & 0 & 4 & 0 & 1 & 0 & 1 & 2 & 0 & 2 & 0 & 0 & 4 \\
2 & 2 & 0 & 0 & 4 & 0 & 2 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 4 & 0 & 2 & 0 & 0 \\
2 & 0 & 3 & 0 & 0 & 0 & 3 & 0 & 2 & 0 & 2 & 0 & 3 & 0 & 0 & 0 & 3 & 0 & 2 \\
0 & 0 & 2 & 0 & 4 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 2 & 0 & 4 & 0 & 0 & 2 & 2 \\
4 & 0 & 0 & 2 & 0 & 2 & 1 & 0 & 1 & 0 & 4 & 0 & 0 & 2 & 0 & 2 & 1 & 0 & 1 \\
0 & 4 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 4 & 2 & 0 & 0 & 2 & 2 & 0 & 0 \\
0 & 2 & 0 & 4 & 1 & 0 & 0 & 2 & 1 & 0 & 0 & 2 & 0 & 4 & 1 & 0 & 0 & 2 & 1
\end{pmatrix}$$

As we can see in the matrix C_Y^p, we have value 4 for all non-zero shifts, showing that after removing 0, the maximum of the periodic autocorrelation function values has increased. It is easy to check that we do not increase the maximum value of the aperiodic autocorrelation functions values by removing 0 because after removing 0, we delete the first values of each row of the difference triangle table of X and removing these values will not increase the number of repetitions in each row. Consequently, the maximum of the aperiodic autocorrelation function values will not increase.

We know that PN permutations do not exist [37]. For this reason, we are mainly interested in odd APN permutation mappings on $\mathbb{Z}_n$ for odd integer n because we know that they will give rise to odd permutations of even sizes, for which applying the transformation $\mathcal{G}$ on such permutations might reduce the number of forbidden configurations. Moreover, the APN property of permutations implies that each row of their difference triangle tables can not contain three or more repeated values. Consequently, since we have more control over the number of repetitions in each row of the difference triangle table of odd APN permutations, we can provide a formula to count the number of forbidden configurations of the odd permutations that we can construct from them.

Theorem 4.25. *Let $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ be an odd APN permutation function, where n is an odd integer. Then f gives rise to an odd permutation $X = [f(1), f(2), ..., f(n-1)]$ on elements $\{1, ..., n-1\}$ with the property that*

$$FC(X) = \sum_{i=1}^{n-1} \left\lfloor \frac{n-i}{2} \right\rfloor .$$

Proof. According to Observation 4.7, we can construct the odd permutation a permutation $X = [f(1), f(2), ..., f(n-1)]$ of even size $n-1$ on elements

$\{1, ..., n-1\}$. In order to compute $FC(X)$, since the function f has APN property, each row of its difference triangle table could not contain values that occur more than twice; moreover, since X is an odd permutation of even size $n-1$, we know that for all $1 \leq i \leq n-1$, we have $f(i) + f(n-i) = n$. Then, in a row k, $1 \leq k \leq n-1$, of the difference triangle table of X for $1 \leq i \leq n-k$ we have

$$f(i+k) - f(i) = n - f(n-k-i) - n - f(n-i) = f(n-i) - f(n-i-k).$$

It can be seen that this row k contains the following values

$$[f(k+1) - f(1), f(k+2) - f(2), \ldots, f(n-1) - f(n-1-k)]\,.$$

It follows that the first $\left\lfloor \frac{n-k}{2} \right\rfloor$ values in the row k are the same as the last $\left\lfloor \frac{n-k}{2} \right\rfloor$ values in this row. Therefore, we can conclude that each row of the difference triangle table of X contains $\left\lfloor \frac{n-k}{2} \right\rfloor$ values that occur precisely twice. Thus, we have

$$FC(X) = \sum_{k=1}^{n-1} \left\lfloor \frac{n-k}{2} \right\rfloor \binom{2}{2} = \sum_{k=1}^{n-1} \left\lfloor \frac{n-k}{2} \right\rfloor.$$

□

The above theorem also provides an upper bound on the number of forbidden configurations of any permutation constructed from an APN function.

Theorem 4.26. *Let $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ be an APN permutation. Take the corresponding $(n-1) \times (n-1)$ matrix X to function f, which is constructed by placing a dot at the position (i, j), where $1 \leq i, j \leq n-1$, if and only if $i = f(j)$; placing 0 otherwise. Then the number of forbidden configurations in X satisfies*

$$FC(X) \leq \sum_{i=1}^{n-1} \left\lfloor \frac{n-i}{2} \right\rfloor.$$

Proof. Since f is an APN permutation, each row of the difference triangle table of X can not contain a value that occurs more than twice. It follows that the maximum number of forbidden configurations can be achieved if all the values in each row of the difference of X appear twice. Since a given row k, $1 \leq k \leq n-1$, of the difference triangle table of X contains at most $\left\lfloor \frac{n-k}{2} \right\rfloor$ values that occur twice, we have

$$FC(X) \leq \sum_{k=1}^{n-1} \left\lfloor \frac{n-k}{2} \right\rfloor \binom{2}{2} = \sum_{k=1}^{n-1} \left\lfloor \frac{n-k}{2} \right\rfloor.$$

□

In view of all that has been mentioned so far, an intriguing question is whether there exist odd APN permutation functions for which applying the transformation $\mathcal{G}$ on odd permutations that we construct from them results in an acceptable periodic property. In the rest of this section, we will follow this point of view for a particular type of permutation polynomials, namely inverse functions over finite fields of odd characteristics.

Power mappings with low differential uniformity have mainly been studied due to their application in cryptography, and these studies showed several values of d for which the power mapping $f(x) = x^d$ over $\mathbb{F}_q$ are PN/APN mappings [8,12,14,31,49,76,120,123–126]. In 1999, Helleseth et al. published a paper in which they showed that if $d = p - 2$, where p is an odd prime and $p \equiv 2 \pmod 3$, the corresponding power mapping over $\mathbb{F}_p$ is APN [65]. As we mentioned earlier, this function is known as the inverse function. Let us provide an example of the effect of transformation $\mathcal{G}$ on an inverse function's aperiodic and periodic properties.

Example 4.27. *Let $f(x) = x^9$ be a power mapping over $\mathbb{F}_{11}$. Since $gcd(9, 10) = 1$ and $11 \equiv 2 \bmod 3$, f is an odd APN permutation. The permutation corresponds to the mapping f for $1 \leq x \leq 10$ is $X = [1, 6, 4, 3, 9, 2, 8, 7, 5, 10]$, and then $\mathcal{G}(X) = [1, 6, 4, 3, 9, 10, 5, 7, 8, 2]$. Using Matlab, figures 4.7, 4.8, 4.9 and 4.10 illustrate the visualization of both the periodic and aperiodic properties of X and $\mathcal{G}(X)$.*

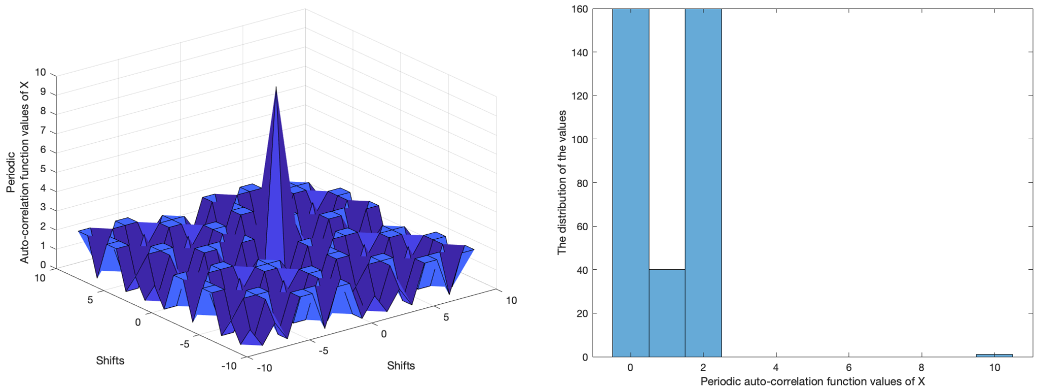


FIGURE 4.7: Visualization of the periodic autocorrelation function values of X.

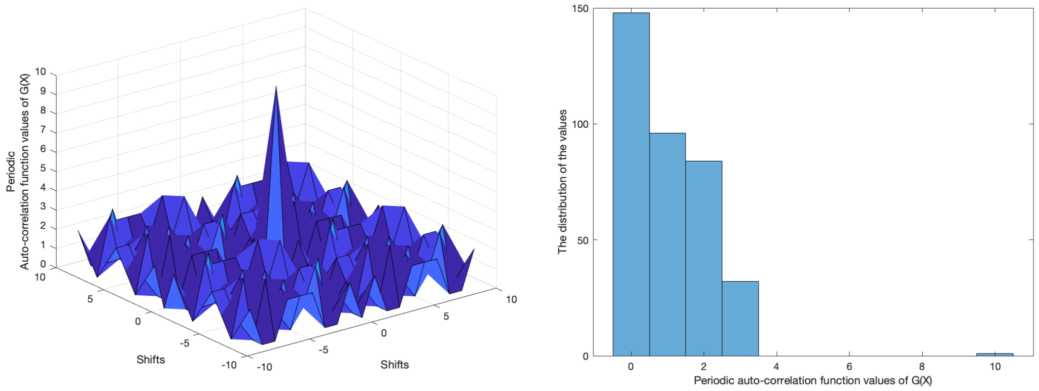


FIGURE 4.8: Visualization of the periodic autocorrelation function values of $\mathcal{G}(X)$.

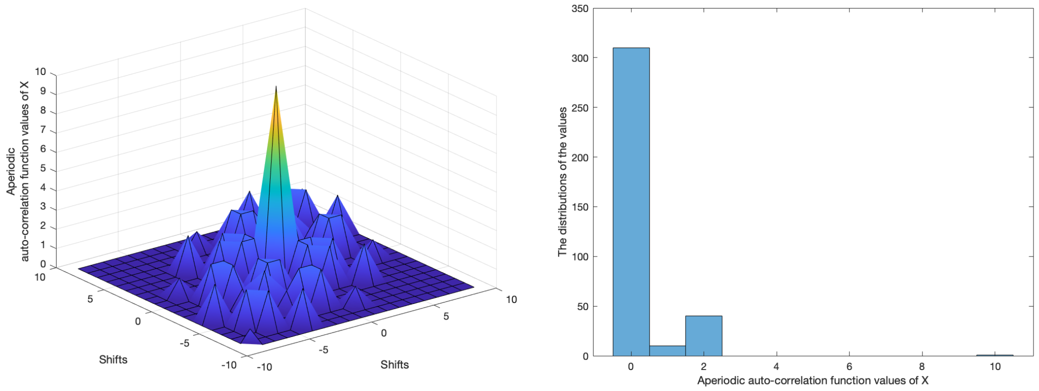


FIGURE 4.9: Visualization of the aperiodic autocorrelation function values of X.

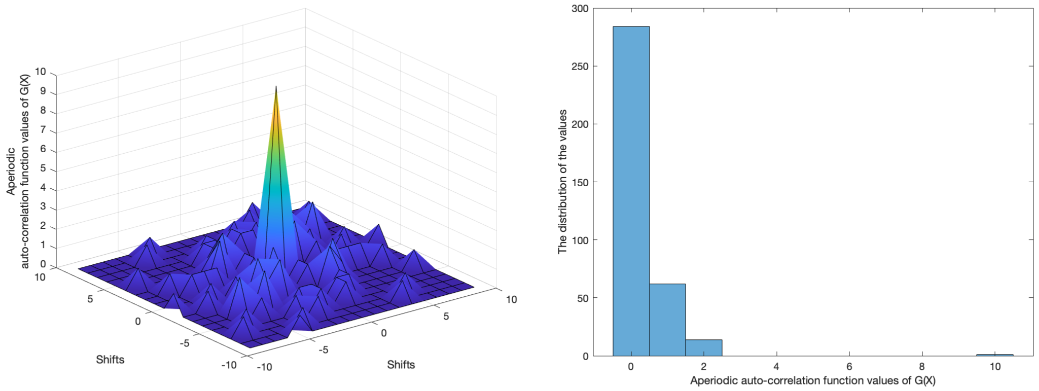


FIGURE 4.10: Visualization of the aperiodic autocorrelation function values of $\mathcal{G}(X)$.

One can verify that applying transformation $\mathcal{G}$ on inverse function $f(x) = x^9$ over $\mathbb{F}_{11}$ has increased the differential uniformity, as shown in Figure

4.8. This phenomenon raises the question of how much we increase the differential uniformity of an inverse function over a finite field by applying the transformation $\mathcal{G}$. As we mentioned earlier, the element zero plays an essential role, and to utilize the APNness property of the inverse function, we can not remove zero. Accordingly, we propose the following generalized definition for the transformation $\mathcal{G}$ that takes the role of zero into account.

Definition 4.28. *Let $f \in \mathbb{Z}_n[x]$ be an odd permutation function with corresponding permutation matrix X of size n, where n is an odd integer. We define a bijective map $g' : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ by*

$$g'(i) = \begin{cases} f(i) & 0 \le i \le \frac{n-1}{2} \\ f\left(\frac{n-1}{2} - i\right) & 1 + \frac{n-1}{2} \le i \le n-1. \end{cases}$$

We denote the corresponding permutation matrix g' by $\mathcal{G}'(X)$.

It would be interesting to assess the differential properties of $\mathcal{G}'(X)$, where X is a permutation matrix that corresponds to a power mapping x^{p-2} over $\mathbb{F}_p$, where p is a prime congruent to 2 modulo 3.

Theorem 4.29. *Let $f(x) = x^{p-2}$ be a mapping over $\mathbb{F}_p$, where $p > 2$ is a prime such that $p \equiv 2 \pmod 3$. Let X be the corresponding permutation matrix to the mapping f, and let $\mathcal{G}'$ be the transformation introduced in Definition 4.28. Then $\mathcal{G}'(X)$ represents a differentially at most 6-uniform mapping over $\mathbb{F}_p$.*

Proof. It can be seen that $\mathcal{G}'(X)$ corresponds to the mapping $g' : \mathbb{F}_p \longrightarrow \mathbb{F}_p$ such that

$$g'(x) = \begin{cases} x^{p-2} & 0 \le x \le \frac{p-1}{2} \\ \left(\frac{p-1}{2} - x\right)^{p-2} & 1 + \frac{p-1}{2} \le x \le p-1. \end{cases}$$

In order to show that g' is differentially at most 6-uniform, we need to discuss the number of solutions $x \in \mathbb{F}_p$ of the equation $g'(x+a) - g'(x) = b$ where $a, b \in \mathbb{F}_p$, which falls naturally into the four following cases:

1) If $0 \le x \le \frac{p-1}{2}$ and $0 \le x + a \le \frac{p-1}{2}$.

2) If $0 \le x \le \frac{p-1}{2}$ and $1 + \frac{p-1}{2} \le x + a \le p - 1$.

3) If $1 + \frac{p-1}{2} \le x \le p-1$ and $1 + \frac{p-1}{2} \le x + a \le p - 1$.

4) If $1 + \frac{p-1}{2} \le x \le p-1$ and $0 \le x + a \le \frac{p-1}{2}$.

For case 1, since $f(x)$ is an odd APN mapping and the fact that for $x \in \mathbb{F}_p$ and fixed $a, b \in \mathbb{F}_p$, we have

$$b = (x+a)^{p-2} - x^{p-2} = (p-x)^{p-2} - (p-x-a)^{p-2}.$$

This equation shows for a fixed $a, b \in \mathbb{F}_p$, if x is a solution of $g'(x+a) - g'(x) = b$ so is $p - x - a$. Since $0 \leq x + a \leq \frac{p-1}{2}$, we can conclude that $\frac{p+1}{2} \leq p - x - a \leq p$. Thus, the equation $g'(x+a) - g'(x) = b$ in the interval that we considered can admit at most one solution when $0 \leq x, x + a \leq \frac{p-1}{2}$. For case 2, it follows immediately that

$$\begin{aligned} g'(x+a) - g'(x) &= \left(\tfrac{p-1}{2} - x - a\right)^{p-2} - x^{p-2} \\ &= \left(\tfrac{p-1}{2} - x - a\right)^{-1} - x^{-1} \\ &= \frac{1}{\frac{p-1}{2} - x - a} - \frac{1}{x} \\ &= \frac{x - \frac{p-1}{2} + x + a}{x\left(\frac{p-1}{2} - x - a\right)} \\ &= \frac{4x + 2a + 1}{-2x^2 - 2ax - x}. \end{aligned}$$

This shows since $g'(x+a) - g'(x) = b$ is equivalent to the equation

$$2bx^2 + (2ab + b + 4)x + 2a + 1 = 0,$$

the equation $g'(x+a) - g'(x) = b$ has at most two solutions for any $b \in \mathbb{F}_p$. For case 3, we have

$$\begin{aligned} g'(x+a) - g'(x) &= (x+a)^{p-2} - \left(\tfrac{p-1}{2} - x\right)^{p-2} \\ &= (x+a)^{-1} - \left(\tfrac{p-1}{2} - x\right)^{-1} \\ &= \frac{1}{x+a} - \frac{2}{p - 1 - 2x} \\ &= \frac{-1 - 2x - 2(x+a)}{(x+a)(-1-2x)} \\ &= \frac{-4x - 2a - 1}{-2x^2 - (2a+1)x - a} \\ &= \frac{4x + 2a + 1}{2x^2 + (2a+1)x + a}. \end{aligned}$$

Therefore, $g'(x+a) - g'(x) = b$ is equivalent to the equation

$$2bx^2 + (2ab + b - 4)x + ab - 2a - 1 = 0,$$

which can have at most two solutions for all $b \in \mathbb{F}_p$.
For case 4, we have

$$\begin{aligned} g'(x+a) - g'(x) &= \left(\tfrac{p-1}{2} - x - a\right)^{p-2} - \left(\tfrac{p-1}{2} - x\right)^{p-2} \\ &= \left(x - \tfrac{p-1}{2}\right)^{-1} - \left(x + a - \tfrac{p-1}{2}\right)^{-1}. \end{aligned}$$

Using the same argument as in case 1 yields $g'(x+a) - g'(x) = b$ has at most one solution for all $b \in \mathbb{F}_p$.
Hence, the number of solutions $x \in \mathbb{F}_p$ of the equation $g'(x+a) - g'(x) = b$ where $a, b \in \mathbb{F}_p$ is at most 6 because we get at most one solution from cases 1 and 4, and at most two solutions from cases 2 and 3. □

Theorem 4.29 states that applying the transformation $\mathcal{G}'$ on inverse functions over a finite field produces permutations with differential uniformity at most 6. However, it is interesting to question how much we reduce the number of forbidden configurations by transforming these functions using $\mathcal{G}'$. We computed the number of forbidden configurations of permutations constructed by inverse functions and their transformed version using the transformation $\mathcal{G}'$ over a finite field $\mathbb{F}_p$ for prime $5 \leq p \leq 977$, and we visualized the result in Figure 4.11. For this computational experiment, we also considered the case where $p \equiv 1 \bmod (3)$ because the number of forbidden configurations can be reduced even if the inverse function is not APN. Moreover, the main difference between this experimental computation and what was discussed in the previous section is that here we consider the effect of element zero for computing the number of forbidden configurations.

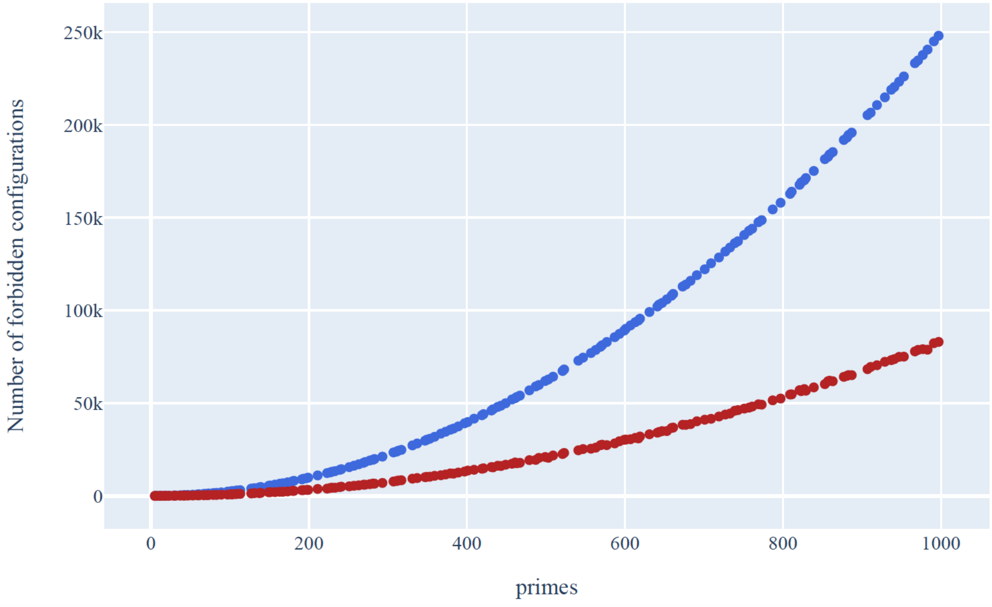


FIGURE 4.11: Values of $FC(X)$ and $FC(\mathcal{G}'(X))$, where X is an inverse function over $\mathbb{F}_p$, for $5 \leq p \leq 997$, is shown in this figure. The blue and red dots correspond to $FC(X)$ and $FC(\mathcal{G}'(X))$, respectively.

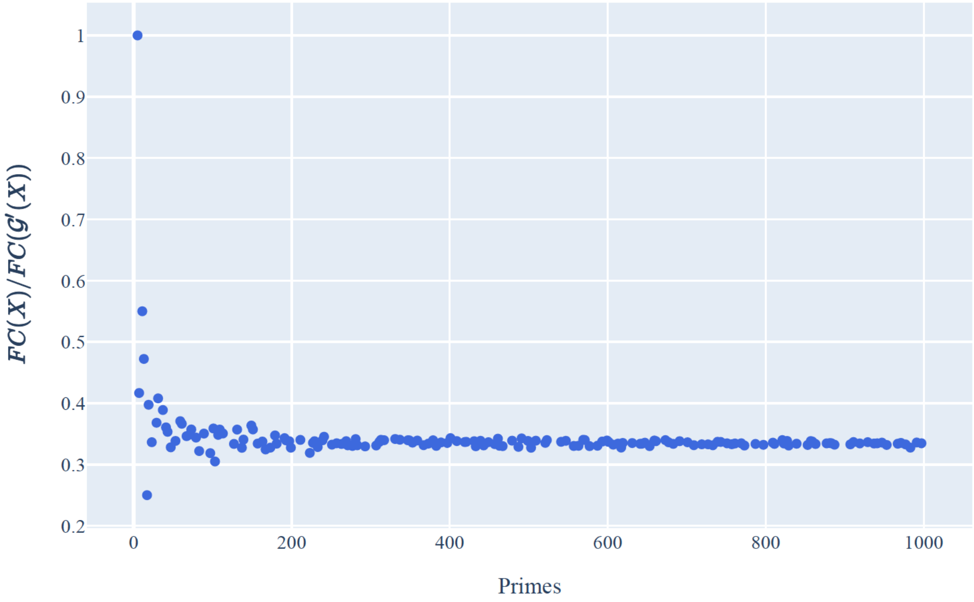


FIGURE 4.12: Values of $\frac{FC(X)}{FC(\mathcal{G}'(X))}$, where X is a permutation constructed by an inverse function over finite field $\mathbb{F}_p$, for prime $5 \leq p \leq 997$.

It is apparent from Figure 4.11 that we obtain a considerable amount of reduction in the number of forbidden configurations in such permutation after being transformed by $\mathcal{G}'$.

In order to have a better estimation of these reductions, we computed the ratio between $FC(X)$ and $FC(\mathcal{G}'(X))$, where X is an inverse function over $\mathbb{F}_p$, as shown in Figure 4.12. Figure 4.12 illustrates that there is only one permutation (constructed over $\mathbb{F}_5$) for which we do not reduce the number of forbidden configurations by applying the transformation $\mathcal{G}'$, and for the others, the required reduction has been achieved. For prime $37 \leq p \leq 977$, Figure 4.12 reveals that there has been a sharp decrease in the number of forbidden configurations, which is indeed remarkable. Interestingly, it can be seen that for prime $37 \leq p \leq 977$, the transformation $\mathcal{G}'$ can eliminate roughly 65% of forbidden configurations in such permutations. Further analysis of these results showed that for primes of the set $\{13, 17, 19, 31, 37, 47, 53, 59, 79\}$, their corresponding permutations are differential 4-uniform, and for other primes in the range mentioned above, they are either differential 5- or 6-uniform.

Overall, the computational results in this Chapter indicate that the transformations $\mathcal{G}$ and $\mathcal{G}'$ significantly reduce the number of forbidden configurations for some odd permutations. However, further work is required to provide theoretical proof for these findings.

4.5 Search algorithm for G-symmetric Costas arrays

In order to search for all G-symmetric Costas arrays of even size n, we do not need to traverse $n!$ permutation matrices because the elements in the first half define the elements in the second half of an G-symmetric permutation. To be more precise, suppose $X = [f(1), \ldots, f(\frac{n}{2})]$ is a permutation matrix of size $\frac{n}{2}$, where n is an even integer and $f(i) \in \{1, 2, \ldots, \frac{n}{2}\}$. By subtracting $n+1$ from all elements of X, we obtain a permutation $Y = [n+1-f(1), \ldots, n+1-f(\frac{n}{2})]$ of size $\frac{n}{2}$ on elements $\{\frac{n}{2}+1, \ldots, n\}$. By concatenating X and Y, we construct the G-symmetric permutation $Z := [f(1), \ldots, f(\frac{n}{2}), n+1-f(1), \ldots, n+1-f(\frac{n}{2})]$ of size n on elements $\{1, 2, \ldots, n\}$. Let us note that swapping any two elements $f(i)$ and $n+1-f(i)$ for $1 \leq i \leq \frac{n}{2}$ will not violate the G-symmetric property. Hence, we have $\left(2^{n/2} \cdot \left(\frac{n}{2}\right)!\right)$ G-symmetric permutations of size n. Consequently, there also exists $\left(2^{n/2} \cdot \left(\frac{n}{2}\right)!\right)$ odd permutations of even size n because applying the transformation $\mathcal{G}$ on a given G-symmetric permutation yields an odd permutation. The above procedure also helps develop a search algorithm for all G-symmetric Costas arrays of even size n. We implemented the above algorithm using python language on a Macbook Air system with 1,6 GHz Dual-Core Intel Core i5 and memory of 8 GB 2133 MHz LPDDR3. The result is shown in the following table. As we mentioned in the introductory part of this chapter, our motivation for reducing the number of forbidden configurations in a given permutation matrix is to stay as close as possible to a Costas array. The algorithm presented above, derived from Theorem 4.15, demonstrates that G-symmetric Costas arrays can be generated by applying the transformation $\mathcal{G}$ to odd permutations.

TABLE 4.1: The result of searching for all G-symmetric Costas arrays of even sizes.

Size	Number of G-symmetric Costas arrays	Searching times (seconds)
4	8	0.017
6	16	0.022
8	16	0.023
10	96	0.099
12	176	1.136
14	124	19.442
16	308	433.375
18	116	10064.090
20	12	153258.804

Another motivation to study odd permutations is that since exponential Welch Costas arrays have the G-symmetric property, it is reasonable to ask what is the property of odd permutations for which applying transformations $\mathcal{G}$ results in G-symmetric Costas arrays. Moreover, using the database of all known Costas arrays, one can easily verify that not all known G-symmetric Costas arrays have been constructed by the exponential Welch construction method. We have analyzed all the odd permutations X of even sizes up to size 28, for which $\mathcal{G}(X)$ is a G-symmetric Costas array, and we observed that it is challenging to find a pattern in these odd permutations. One possible approach to analyzing an odd permutation X with the property that $\mathcal{G}(X)$ is an exponential Welch Costas array is to study the permutation polynomial that generates X. On the one hand, since exponential Welch Costas arrays are constructed using an algebraic method over a finite field, we can easily find the permutation polynomial generating the set of points in X utilizing the Lagrange interpolation method. On the other hand, while an exponential Welch Costas array uses a relatively simple permutation polynomial over a finite field, the odd permutation polynomial obtained by Lagrange interpolation that produces the set of points in X looks more complicated, showing finding a pattern even for such odd permutations is also an arduous task to do. Let us provide an example for this comment.

Example 4.30. *Let $\alpha = 2$ be a primitive element in $\mathbb{F}_{11}$. Take $f(x) = x$, where $x = \alpha^i$ for $0 \leq i \leq 9$. Then, we can construct the exponential Welch Costas array $X = [1, 2, 4, 8, 5, 10, 9, 7, 3, 6]$. It is easy to verify that applying transformation $\mathcal{G}$ on odd permutation $Y = [1, 2, 4, 8, 5, 6, 3, 7, 9, 10]$ gives the permutation X, $\mathcal{G}(Y) = X$. Utilizing the Lagrange interpolation Formula, we can check that*

$$g(x) = 6x^9 + 6x^7 + x^5 + 8x^3 + 2x \text{ over } \mathbb{F}_{11} \setminus \{0\},$$

is the permutation polynomial that generates Y.

Chapter 5

Crosscorrelation Properties of Costas Arrays

Investigating families of arrays with low pairwise crosscorrelation is a continuing concern within digital watermarking, multiplexing, and multiuser systems [36, 82, 111]. Konstantinos Drakakis et al. in [36, 39] discussed why it is essential to study families of Costas arrays with low pairwise crosscorrelation. Moreover, the crosscorrelation of Costas arrays represents a fascinating mathematical problem, showing that this problem is worth studying for its own sake as a mathematical subject. Chapter 3 mainly discussed the crosscorrelation between two algebraically constructed Costas arrays at the origin. We introduced a subfamily of Lempel-Golomb Costas arrays with low crosscorrelation at the origin, and we will discuss this family in more detail in this chapter. For two main reasons, we also investigated the maximal crosscorrelation of the family of power mappings over a finite field. Firstly, while most of the studies of power mappings over a finite field have considered the periodic properties of these functions, we will discuss their aperiodic properties. Secondly, we observed a close relationship between the maximal crosscorrelation of the family of exponential Welch Costas arrays and power mappings, which is remarkable to note because the nature of the two families is entirely different. Finally, we will discuss the effect of our introduced transformation $\mathcal{A}_k$, as in Definition 3.12, on inverse functions over a finite field to introduce a family of arrays of size $p-1$ with auto- and crosscorrelation 2. This chapter only considers aperiodic auto- and crosscorrelation between any two arrays, and all the computations will be performed aperiodically.

5.1 Crosscorrelation of algebraically constructed Costas arrays

Konstantinos Drakakis et al. in [39] provided computational results for the maximal crosscorrelation of the families of exponential Welch and Lempel-Golomb Costas arrays, determined by an exhaustive search, as shown in Table 5.1. Based on their computational results, they presented several exciting explanations for their observations and proposed conjectures on the maximal crosscorrelations of these families. Recently, Domingo Gomez-Perez and Arne Winterhof in [62] settled some of these conjectures. In

particular, they provided proof containing the upper bound for the maximal crosscorrelation of the family of exponential Welch Costas arrays and a subfamily of Lempel-Golomb Costas arrays.
We will consider the family of exponential Welch and Lempel-Golomb Costas arrays as follows.
• **Family of exponential Welch arrays**: for $p \geq 5$, the family $\mathcal{W}_p$ of Welch permutations of $\{1, \dots, p-1\}$, that does not contain cyclic shifts of a given exponential Welch, is

$$\mathcal{W}_p = \{[\alpha^i \bmod p] : 0 \leq i \leq p-2 \text{ and } \alpha \text{ is a primitive element of } \mathbb{F}_p\},$$

of size $\phi(p-1)$, $|\mathcal{W}_p| = \phi(p-1)$, where ϕ is Euler's totient function.
• **Family of Lempel-Golomb arrays**: for a prime power $q = p^m \geq 4$, the family $\mathcal{G}_q$ of Lempel-Golomb permutations of $\{1, \dots, q-2\}$ is

$$\mathcal{G}_q = \left\{\sigma_{\alpha,\beta}(j) : 1 \leq j \leq q-2 \text{ and } \alpha, \beta \text{ are primitive elements of } \mathbb{F}_q\right\},$$

where $\sigma_{\alpha,\beta}(j) = \log_\alpha \left(1 - \beta^j\right) \bmod (q-2)$. Then, the size of this family is $|\mathcal{G}_q| = \frac{\phi^2(q-1)}{m}$.
In section 2.3, we defined auto and crosscorrelation of permutation matrices. Mapping's representation of permutation matrices could bring advantages to define the crosscorrelation between two permutation matrices more practically, as defined in [62].

Definition 5.1 ([62]). *The crosscorrelation $C^a_{f,g}(r,s)$ between two mappings $f, g : [n] \longrightarrow [n]$ at shift (r,s), where $1-n \leq r,s \leq n-1$, is the number of solutions*

$$x \in \{max\{1, 1-r\}, \dots, min\{n, n-r\}\}$$

of the equation

$$f(x) + s = g(x+r). \tag{5.1}$$

For a family $\mathcal{F}$ of matrices, the maximal crosscorrelation, denoted by $C(\mathcal{F})$, is

$$C(\mathcal{F}) = \max_{r,s} \max_{\substack{f,g \in \mathcal{F} \\ f \neq g}} C_{f,g}(r,s).$$

As explained in [39], the red rows of Table 5.1, correspond to the safe primes. A prime p is safe if it can be written as $2r+1$, where r is also prime. The number r associated with a safe prime is called Sophie Germain prime. The following theorem represents the maximal value of the crosscorrelation of the family of Welch Costas permutations.

Theorem 5.2 ([62]). *Let $\mathcal{W}_p$ be the family of exponential Costas arrays, where $p \geq 5$ is a prime, and let t be the smallest prime divisor of $\frac{p-1}{2}$. Then the maximal crosscorrelation of $\mathcal{W}_p$ satisfies*

$$C(\mathcal{W}_p) \begin{cases} \leq 1 + \left\lfloor \left(1 - \frac{2}{p-1}\right) \sqrt{p} \right\rfloor & \text{if } p \text{ is a safe prime,} \\ = \frac{p-1}{t} & \text{otherwise.} \end{cases}$$

TABLE 5.1: Maximal Crosscorrelation's value between pairs of Welch and of Lempel-Golomb Costas arrays: generated in $\mathbb{F}_p$, where p is a prime.

prime	$\mathcal{W}_p$	$\mathcal{G}_p$	prime	$\mathcal{W}_p$	$\mathcal{G}_p$	prime	$\mathcal{W}_p$	$\mathcal{G}_p$
5	2	2	79	26	25	179	6	12
7	2	2	83	5	9	181	90	89
11	3	4	89	44	43	191	38	37
13	6	5	97	48	47	193	96	95
17	8	7	101	50	49	197	98	97
19	6	6	103	34	33	199	66	65
23	4	6	107	5	10	211	70	69
29	14	13	109	54	53	223	74	73
31	10	9	113	56	55	227	6	13
37	18	17	127	42	41	229	114	113
41	20	19	131	26	25	233	116	115
43	14	13	137	68	67	239	34	33
47	5	8	139	46	45	241	120	119
53	26	25	149	74	73	251	50	49
59	5	12	151	50	49	257	128	127
61	30	29	157	78	77	263	7	12
67	22	21	163	54	53	269	134	133
71	14	13	167	6	12	271	90	89
73	36	35	173	86	85			

Domingo Gomez-Perez and Arne Winterhof in [62], provided proof for the maximal crosscorrelation of a subfamily of Lempel-Golomb Costas arrays when one primitive element is considered to be fixed. They considered the following subfamily.

- **The subfamily** $\mathcal{G}'_q$: for $q \geq 4$ and a fixed primitive element β of the field $\mathbb{F}_q$, the subfamily $\mathcal{G}'_q$ of the Lempel-Golomb Costas permutations is defined by

$$\mathcal{G}'_q = \left\{ \sigma'_{\alpha,\beta}(j) : 1 \leq j \leq q-2 \text{ and } \alpha \text{ is a primitive element of } \mathbb{F}_q \right\},$$

where $\sigma'_{\alpha,\beta}(j) = \left[\log_\alpha \left(1-\beta^j\right) \mod (q-2)\right]$. Then, the size of this family is $|\mathcal{G}'_q| = \phi(q-1)$.
The following theorem show the maximal crosscorrelation value of the family $\mathcal{G}'_q$.

Theorem 5.3 ([62],). *Let $\mathcal{G}'_q$ be the subfamily of Lempel-Golomb Costas arrays, where $q \geq 4$ is a prime power. Then the maximal crosscorrelation of this family satisfies*

$$\mathcal{C}(\mathcal{G}'_q) \begin{cases} \leq 1 + \left\lfloor \left(1 - \frac{2}{q-1}\right) \sqrt{q} \right\rfloor & \textit{if } q \textit{ is odd and } t = \frac{q-1}{2}, \\ \leq \left\lfloor \left(1 - \frac{1}{q-1}\right) \left(1 + \sqrt{q}\right) \right\rfloor & \textit{if } q \textit{ is even and } t = q-1, \\ = \frac{p-1}{t} - 1 & \textit{otherwise.} \end{cases}$$

All results presented so far indicate that the crosscorrelation for the family of Lempel-Golomb Costas arrays is still an open problem. Therefore, it is worthwhile to discuss why it is a complex problem. Drakakis et al. in [39], showed how the crosscorrelation for Lempel-Golomb Costas arrays at a given shift is bounded above by the number of solutions of a particular polynomial over a finite field. They provided the following theorem regarding this remark.

Theorem 5.4 ([39]). *For a prime power q, let f and g be two Lempel-Golomb permutations constructed in $\mathbb{F}_q$ by the primitive elements α, β and α^u, β^v, respectively, where $gcd(u, q-1) = gcd(v, q-1) = 1$. Then, the crosscorrelation between f and g at $(r, s) \in \mathbb{Z}^2$ is*

$$C^a_{f,g}(r,s) \leq \left|\left\{x \in \mathbb{F}_q : \alpha^{ur}(1-x)^u + \beta^{vs}x^v - 1 = 0\right\}\right|, \tag{5.2}$$

where the equality will achieve if $r = s = 0$.

The results stated in Theorems 5.3 and 5.4 show that the crosscorrelation correlation of the subfamily $\mathcal{G}'_q$ of the family of Lempel-Golomb Costas arrays at a given shift $(r, s) \in \mathbb{Z}^2$ is the number of solutions of the following equation

$$\alpha^{ur}(1-x)^u + \beta^s x - 1 = 0 \text{ for } x \in \mathbb{F}_q, \tag{5.3}$$

which is obtained by assuming $v = 1$ in Theorem 5.4.

As we discussed in the introductory section of this Chapter, it is interesting to find subfamilies of Costas arrays with low crosscorrelation properties. Theorem 5.3 shows that the proof of this subfamily of Lempel-Golomb is heavily dependent on the choice of primitive elements. With this in mind, we further analyzed the family of Lempel-Golomb Costas arrays to see whether it is possible to find a subfamily with lower crosscorrelation than the family of Lempel-Golomb Costas arrays. This analysis, together with asking the question of the number of solutions of Equation (5.2) if $u = v$, revealed that for a particular subfamily of Lempel-Golomb Costas arrays, a lower maximal crosscorrelation than the family $\mathcal{G}'_q$ could be achieved. We studied the maximal crosscorrelation of the family of Lempel Costas arrays. The family of Lempel Costas arrays is defined below.

• **Family of Lempel Costas arrays**: For a prime power $q \geq 5$ we define the subfamily of $\mathcal{L}_q$ of the family of Lempel-Golomb Costas permutations of $\{1, \ldots, q-2\}$ by

$$\mathcal{L}_q = \{\pi_{\alpha,\alpha}(j) : 1 \leq j \leq q-2 \text{ and } \alpha \text{ primitive element of } \mathbb{F}_q\},$$

where $\pi_{\alpha,\alpha}(j) = \log_\alpha\left(1 - \alpha^j\right) \bmod (q-2)$. Then, the size of this family is $|\mathcal{L}_q| = \phi(q-1)$.

By utilizing Theorem 5.4, It can easily be seen that if we consider two Lempel Costas permutations $\pi_{\alpha,\alpha}$ and π_{α^r,α^r}, where $(r, q-1) = 1$. Then the crosscorrelation between the two permutations at $(u, v) \in \mathbb{Z}^2$ is bounded above by the number of solutions of the polynomial

$$\alpha^{ru}(1-x)^r + \alpha^{rv}x^r - 1 = 0 \text{ with } x \in \mathbb{F}_q \text{ and } x \notin \{0, 1\}. \tag{5.4}$$

TABLE 5.2: Values of the maximal crosscorrelation of two families of Costas arrays, the family of Lempel Costas arrays and a subfamily of Lempel-Golomb Costas arrays.

prime	$C(\mathcal{L}_q)$	$C(\mathcal{G}'_q)$	prime	$C(\mathcal{L}_q)$	$C(\mathcal{G}'_q)$	prime	$C(\mathcal{L}_q)$	$C(\mathcal{G}'_q)$	prime	$C(\mathcal{L}_q)$	$C(\mathcal{G}'_q)$
4	1	1	32	3	5	83	8	5	149	36	73
5	2	1	37	8	17	89	21	43	151	20	49
7	2	2	41	9	19	97	23	47	157	38	77
8	2	3	43	6	13	101	24	49	163	20	53
9	2	3	47	8	5	103	20	33	167	12	12
11	2	3	49	11	23	107	10	5	169	41	83
13	2	5	53	12	25	109	26	53	173	42	85
16	2	5	59	12	5	113	27	55	179	10	10
17	4	7	61	14	29	121	29	59	181	44	89
19	4	6	64	8	20	125	30	61	191	12	37
23	5	4	67	10	21	127	13	41	193	47	95
25	5	11	71	7	13	128	6	7	197	48	97
27	5	4	73	17	35	131	8	25	199	21	65
29	6	13	79	8	25	137	33	67			
31	5	9	81	19	39	139	14	45			

We computed the maximal crosscorrelation of the family of Lempel arrays for prime powers $4 \leq q \leq 199$ using an exhaustive search. Since the size of the two families, $\mathcal{L}_q$ and $\mathcal{G}'_q$, are the same, we decided to compare their maximal crosscorrelation. So, for the prime powers ranging from 4 to 199, we also exhaustively computed the maximal crosscorrelation of the family $\mathcal{G}'_{q'}$. The result is shown in Table 5.2. Based on these computational results, we make the following observations:

- Assuming q is a prime power, $9 \leq q \leq 199$, then the maximal crosscorrelation of the family of Lempel Costas permutations is bounded above by $\left\lfloor \frac{q-1}{4} \right\rfloor$.
- If $q \neq 17$ and $11 \leq q \leq 199$ is a prime power such that $q \equiv 1 \bmod (4)$, the maximal crosscorrelation of the family of Lempel permutations is equal to $\frac{q-1}{4} - 1$.
- In the red rows, prime powers are safe primes, and for these values of primes, $C(\mathcal{G}'_q) \leq C(\mathcal{L}_q)$.
- The unique blue rows correspond to the primes congruent to 1 modulo 4, for which the maximal crosscorrelation equals $\frac{q-1}{4}$.
- The green rows correspond to even prime powers q such that $q-1$ is also prime. In this case, it seems there is no apparent relation between $C(\mathcal{G}'_q)$ and $C(\mathcal{L}_q)$.

The computational evidence on the maximal crosscorrelation between any two Lempel Costas arrays suggests the maximal value can be obtained at the origin if $q \equiv 1 \bmod (4)$. Then, by assuming $u = v = 0$ and exhaustively computing the number of solutions of Equation (5.4) for $4 \leq q \leq 541$, where $q \equiv 1 \bmod (4)$ and $q \neq 9, 17$, we observed that the maximum number of solutions of (5.4) occurs for $r = \frac{q-1}{2} + 1$, which will be $\frac{q-1}{4} - 1$. It is also possible to provide theoretical proof in this case.

Theorem 5.5. *Let $q \geq 4$ be a prime power such that $q \equiv 1 \bmod (4)$. Suppose $r = \frac{q-1}{2} + 1$. Then the number of solutions of the diophantine equation*

$$x^r + (1-x)^r = 1,$$

over $\mathbb{F}_q$ equals $\frac{q-1}{4} - 1$.

Proof. Let α be a primitive element of $\mathbb{F}_q$. Furthermore, assuming $x \notin \{0, 1\}$ (note that $x = 0, 1$ are always solutions). Since each non-zero element of $\mathbb{F}_q$ can be written as α^i for some integer i, then we have $x = \alpha^i$ for some integer $1 \leq i \leq q-2$. Substituting $x = \alpha^i$ into the diophantine equation, yields

$$\left(1 - \alpha^i\right)^r = 1 - \alpha^{ri}.$$

Substituting $r = \frac{q-1}{2} + 1$ into the above equation, we obtain

$$\left(1 - \alpha^i\right)^{\frac{q-1}{2}+1} = 1 - \alpha^{\left(\frac{q-1}{2}+1\right)i}. \tag{5.5}$$

Since $\alpha^{\frac{q-1}{2}} = -1$, it follows that

$$\left(1 - \alpha^i\right)^{\frac{q-1}{2}+1} = 1 - \left(-\alpha^i\right). \tag{5.6}$$

The proof falls naturally into two parts depending on whether $\left(1-\alpha^i\right)^{(q-1)/2} = 1$ or $\left(1-\alpha^i\right)^{(q-1)/2} = -1$ by noticing that

$$\left(\left(1 - \alpha^i\right)^{\frac{q-1}{2}}\right)^2 = \left(1 - \alpha^i\right)^{q-1} = 1 \Longrightarrow \left(1 - \alpha^i\right)^{\frac{q-1}{2}} = \pm 1.$$

Case 1. If $\left(1-\alpha^i\right)^{(q-1)/2} = 1$, the left hand side of (5.6) becomes $\left(1-\alpha^i\right)$. Considering whether i is odd or even, we have the following two cases

$$\left(1 - \alpha^i\right) = \begin{cases} \left(1 - \alpha^i\right) & \text{if } i \text{ is even} \\ \left(1 + \alpha^i\right) & \text{if } i \text{ is odd} \end{cases}.$$

Clearly, if i is odd, we have no solutions because it forces $\alpha^i = 0$. But if i is even, we always have a solution. It is important to note that $\left(1-\alpha^i\right)^{(q-1)/2} = 1$ if $\left(1-\alpha^i\right)$ is a quadratic residue, and we now that modulo an odd prime number q, where $q \equiv 1 \bmod (4)$, half of the residues are quadratic residues. Although there are $\frac{q-3}{2} - 1 = \frac{q-5}{2}$ even numbers between 2 to $q-2$, half of them lead to quadratic residues for $1 - \alpha^i$. It follows that the number of solutions of (5.6) is at most $\frac{q-5}{4}$. Adding 0 and 1 back into the solutions of

(5.6) lead to $\frac{q-5}{4}+2=\frac{q+3}{4}=\frac{q-1}{4}-1$ number of solutions for (5.6), which completes the proof. □

Taking Theorem 5.4 and the data presented in Table 5.2 into account, we can suggest the following conjecture.

Conjecture 5.6. *Let $q \geq 4$ be a prime power and $2 \leq r \leq q-2$ be an integer relatively prime to $q-1$. Let us denote by N_q the number of solutions of the diophantine equation $x^r+(1-x)^r = 1$ over $\mathbb{F}_q$. Then, $N_q \leq \frac{q-1}{4}-1$, where the inequality becomes an equality if $q \equiv 1 \bmod (4)$ and $r = \frac{q-1}{2}+1$.*

More broadly, research is also needed to determine solutions to the diophantine equation $x^r+(1-x)^r = 1$ over $\mathbb{F}_q$, where $2 \leq r \leq q-2$ is an integer relatively prime to $q-1$.

5.2 Crosscorrelation of power mappings

Due to the practical applications of power mappings over a finite field and the fact that almost all studies have considered their periodic properties, we decided to study these objects in an aperiodic setting. This point of view led to an interesting observation regarding the maximal crosscorrelation of the two families of power mappings and exponential Welch Costas arrays generated in $\mathbb{F}_p$, where p is a prime.
We refer the reader to [62] to verify that the proof of Theorems 5.2 and 5.3 is based on character theory; we utilized the same method to provide partial proof for the family of power mappings discussed in this section. We refer to [77] for more details on character theory; however, we will provide the necessary definitions and theorems that we will use.
Exponential sums are essential tools for solving intractable problems involving integers and real numbers. Character theory provides expressions for the number of solutions of equations in a finite abelian group [77]. Let f be an arbitrary map from a finite group G into itself. Then for fixed b in G, the number of solutions of the equation $f(a) = b$ for all b in G, denoted by $N(b)$, is given by

$$N(b) = \frac{1}{|G|}\sum_{a\in G}\sum_{\chi\in G^\wedge}\chi(f(a))\overline{\chi(b)}, \tag{5.7}$$

where $G^\wedge$ is the set of characters of G and the bar denotes complex conjugation. Equation 5.7 is obtained on account of the orthogonality relations for characters, which says:
Let χ and ψ be characters of G. Then

$$\frac{1}{|G|}\sum_{a\in G}\chi(a)\overline{\psi(a)} = \begin{cases} 0 & \text{for } \chi \neq \psi, \\ 1 & \text{for } \chi = \psi. \end{cases} \tag{5.8}$$

Furthermore, if a and b are elements of G, then we have

$$\frac{1}{|G|}\sum_{a\in G^{\wedge}}\chi(a)\overline{\chi(b)}=\begin{cases}0 & \text{for } a\neq b,\\ 1 & \text{for } a=b.\end{cases} \tag{5.9}$$

Rudolf Lidl and Harald Niederreiter in [77] discussed that when we apply the orthogonality relation (5.9) to multiplicative characters of $\mathbb{F}_q$, the following fundamental identity can be achieved. If $a, b \in \mathbb{F}_q^{\star}$, then

$$\sum_{\psi}\psi(a)\overline{\psi(b)}=\begin{cases}0 & \text{for } a\neq b,\\ q-1 & \text{for } a=b,\end{cases} \tag{5.10}$$

where the sum runs through all multiplicative characters ψ of $\mathbb{F}_q$. Then for any $b \in \mathbb{F}_q$ the number of solutions of $f(x) = b$ in $\mathbb{F}_q$, denoted by N, is given by

$$N=\frac{1}{q-1}\sum_{a\in\mathbb{F}_q^{\star}}\sum_{\psi}\psi(f(a))\overline{\psi(b)} \tag{5.11}$$

on account of 5.10.

In the rest of this section, we study the maximal crosscorrelation of the family of power mappings defined below.

• **Family of power mappings**: For a prime $p \geq 5$, let $f : \mathbb{F}_p \longrightarrow \mathbb{F}_p$ be a power mapping, i.e., $f(x) \equiv x^d \bmod p$, where $d \neq 1$ is an integer relatively prime to $p-1$. Since f maps 0 to 0, f generates a permutation of $\{1, 2, \ldots, p-1\}$ by considering $x \in \mathbb{F}_p \setminus \{0\}$. Then, the family $\mathcal{P}_p$ of power mappings is defined by

$$\mathcal{P}_p = \{[x^d \bmod p] : 1 \leq x \leq p-1, \text{ and } gcd(d, p-1) = 1\}.$$

Thus, we have $|\mathcal{P}_p| = \phi(p-1) - 1$ because we already excluded $d = 1$, and the number of relatively prime integers to $p-1$ is given by $\phi(p-1)$.

Considering x in a range from 1 to $p-1$ allows us to construct a permutation of size $p-1$, the same size as the exponential Welch Costas arrays constructed over $\mathbb{F}_p$. Consequently, it is possible to compare the crosscorrelation properties of exponential Welch Costas arrays and power mappings. Using an exhaustive search, we determined the maximal crosscorrelation between any two power mappings over $\mathbb{F}_p$, $5 \leq p \leq 271$. Moreover, since the autocorrelation of a given power mapping is not perfect, we also computed the maximal autocorrelation. Table collects the information on these computational results. We also provided a detailed version of Table 5.3 in the Appendix 6, in which one can check what values of d and which shifts correspond to the maximal value of power mappings' crosscorrelation generated in $\mathbb{F}_p$.

Using information provided in Table 5.3 and the table in Appendix 6, we can make the following observations:

- For non-safe primes, the maximal crosscorrelation of the family of power mapping happens at $(0,0)$ shift, which is equal to the maximal

TABLE 5.3: Maximal Crosscorrelation's value between pairs of power mappings: generated in $\mathbb{F}_p$, where p is a prime.

prime	$\mathcal{W}_p$	$\mathcal{P}_p$	prime	$\mathcal{W}_p$	$\mathcal{P}_p$	prime	$\mathcal{W}_p$	$\mathcal{P}_p$
5	2	2	79	26	26	179	6	10
7	2	2	83	5	9	181	90	90
11	3	3	89	44	44	191	38	38
13	6	6	97	48	48	193	96	96
17	8	8	101	50	50	197	98	98
19	6	6	103	34	34	199	66	66
23	4	6	107	5	10	211	70	70
29	14	14	109	54	54	223	74	74
31	10	10	113	56	56	227	6	10
37	18	18	127	42	42	229	114	114
41	20	20	131	26	26	233	116	116
43	14	14	137	68	68	239	34	34
47	5	8	139	46	46	241	120	120
53	26	26	149	74	74	251	50	50
59	5	12	151	50	50	257	128	128
61	30	30	157	78	78	263	7	12
67	22	22	163	54	54	269	134	134
71	14	14	167	6	12	271	90	90
73	36	36	173	86	86			

crosscorrelation of the family of exponential Welch Costas arrays, as shown in Theorem 5.2, this value is equal to $\frac{p-1}{t}$, where t is the smallest prime divisor of $\frac{p-1}{2}$. We will provide proof for this case.

- For safe primes, the value $\mathcal{C}(\mathcal{P}_p)$ happens at non-zero shifts. It appears then that the value $\mathcal{C}(\mathcal{P}_p)$ is bounded above by $\left\lceil \frac{p-2}{p-1}\left(1+\sqrt{p}\right)\right\rceil$, except for $p = 59$. One can easily verify that this upper bound behaves like the Lempel-Golomb's upper bound, as in Theorem 5.3. We will give partial proof for this case.

- For safe primes, except $p = 11, 23, 83$, the maximal attained for autocorrelation of a power mapping at a non-zero shift.

Let us discuss the crosscorrelation of the family of Power mappings at $(0,0)$ shift (origin). We follow [39] in proving this case.

Theorem 5.7. *Let $f(x) = x^{d_1}$ and $g(x) = x^{d_2}$ be power mappings over $\mathbb{F}_p$, where $p \geq p$ is a prime and $gcd(d_1, p-1) = gcd(d_2, p-1) = 1$, and let t be the smallest prime divisor of $\frac{p-1}{2}$. Then*

$$\max(\mathcal{C}^a_{f,g}(0,0)) = \tfrac{p-1}{t}$$

Proof. In order to compute $\mathcal{C}^a_{f,g}(0,0)$, the goal is to solve

$$x^{d_1} \equiv x^{d_2} \bmod p. \tag{5.12}$$

Let α be a primitive element in $\mathbb{F}_p$, then there exists a positive integer m such that $gcd(m, p-1) = 1$ and $x = \alpha^m$. Then, we have

$$\alpha^{md_1} \equiv \alpha^{md_2} \bmod p \Leftrightarrow m(d_2 - d_1) \equiv 0 \bmod (p-1). \tag{5.13}$$

It is know that 5.13 has exactly $gcd(d_2 - d_1, p-1)$ pair-wise incongruent solutions, and the number of solution of the equation 5.13 can only be a divisor of $p-1$, because the set of solutions of 5.13 form a subgroup of the group of integers modulo $p-1$. When $d_1 \neq d_2$, the maximum number of solutions of equation 5.13 can be $\frac{p-1}{2}$, which happens if and only if $d_2 - d_1 = \frac{p-1}{2}$. Equivalently, $d_2 = d_1 + \frac{p-1}{2}$. Since $gcd(d_2, p-1) = 1$, we have

$$1 = gcd(d_1 + \tfrac{p-1}{2}, p-1) = gcd(d_1 + \tfrac{p-1}{2}, 2).$$

So that, $d_1 + \frac{p-1}{2} \equiv 1 \bmod 2$. It follows that $p \equiv 3 - 2d_1 \bmod 4 \longrightarrow p \equiv 1 \bmod 4$. Therefore, it can be seen that

$$\mathcal{C}(\mathcal{P}_p) = \max_{d_1, d_2 \in X} \left(gcd(d_2 - d_1, p-1) \right),$$

where $X = \{d : 2 \leq d \leq p-2, gcd(d, p-1) = 1\}$, is equal to $\frac{p-1}{2}$ if $p \equiv 1 \bmod 4$. Now, Assume that $p \not\equiv 1 \bmod 4$. Thus $p \equiv 3 \bmod 4$. Let s be a prime with the property that $p \equiv 1 \bmod s$, and let $d_2 - d_1 = k\frac{p-1}{s}$, for some $k \in [p-1]$. Clearly, we have

$$gcd(d_2 - d_1, p-1) = gcd\left(k\tfrac{p-1}{s}, k\tfrac{p-1}{k}\right) = \tfrac{p-1}{s} gcd(k, s) = \tfrac{p-1}{s}. \tag{5.14}$$

Drakakis et al. in [39] have shown that for every prime $p \equiv 3 \bmod 4$ and every prime s with the property that $p \equiv 1 \bmod 2s$, equation 5.13 can have $\frac{p-1}{s}$ roots, which attains its maximum when s is the least possible such prime. □

Next we will prove an upper bound for shift (r, s), where $s = 0$ and arbitrary $r \neq 0$. In other words, we will introduce an upper bound for

$$\max_{r \neq 0} \max_{f,g \in \mathcal{P}_p} \mathcal{C}_{f,g}(r, 0).$$

In this case, the goal is to solve

$$x^{d_1} \equiv (x + r)^{d_2} \bmod p. \tag{5.15}$$

Before going further, since we will utilize the Weil bound for proving this case, it seems reasonable to state the Weil bound theorem here. See [77] for more details.

Theorem 5.8 ([77]). *Let $\mathbb{F}_q$ be a finite field with q elements and let ψ be a multiplicative character of $\mathbb{F}_q$ of order $s > 1$. Suppose $f \in \mathbb{F}_q[x]$ has precisely d distinct roots in its splitting field over $\mathbb{F}_q$, and suppose that f is not an sth power of a polynomial. Then for every $a \in \mathbb{F}_q$ we have*

$$\left| \sum_{x \in \mathbb{F}_q} \psi(af(x)) \right| \leq (d-1)\sqrt{q}.$$

Theorem 5.9. *Let $f(x) = x^{d_1}$ and $g(x) = x^{d_2}$ be power mappings over $\mathbb{F}_p$, where p is a prime and $gcd(d_1, p-1) = gcd(d_2, p-1) = 1$, then for $r \neq 0$, we have*

$$\max(C^a_{f,g}(r,0)) \leq \left\lceil \tfrac{p-2}{p-1}\left(1+\sqrt{p}\right) \right\rceil.$$

Proof. In order to compute the crosscorrelation between f and g at shift $(r,0)$, we need to discuss the number of solutions of Equation 5.15. As we explained briefly at the early of this chapter, the number of solutions of this equation is

$$\tfrac{1}{p-1} \sum_{\chi} \sum_{x \in \mathbb{F}_p^\star \setminus \{-r\}} \chi\left((x+r)^{d_2}\right) \overline{\chi}(x^{d_1}), \tag{5.16}$$

where the first sum runs through all multiplicative characters of $\mathbb{F}_p$. Let us denote the number of solutions of 5.16 by N. The contribution of the trivial character is $\frac{p-2}{p-1}$. So that from 5.16 and the Weil bound in Theorem 5.8, we obtain

$$\begin{aligned} N &= \tfrac{p-2}{p-1} + \tfrac{1}{p-1} \sum_{\chi \neq \chi_0} \sum_{x \in \mathbb{F}_p^\star} \chi\left((x+r)^{d_2}\right) \overline{\chi}(x^{d_1}) \\ &\leq \tfrac{p-2}{p-1} + \tfrac{p-2}{p-1} \max_{r \in \mathbb{F}_p^\star} \max_{\chi \neq \chi_0} \left| \sum_{x \in \mathbb{F}_p^\star} \chi\left((x+r)^{d_2} x^{p-1-d_1}\right) \right| \\ &\leq \left\lceil \tfrac{p-2}{p-1}\left(1+\sqrt{p}\right) \right\rceil. \end{aligned}$$

Note that we can use the Weil bound because

$$gcd(d_2, p-1) = gcd(p-1-d_1, p-1) = 1$$

and the order m of any multiplicative character χ is a divisor of $p-1$. □

It is also worth noting that we cannot use this method for estimating $C^a_{f,g}(r,s)$, where both r and s are non-zero because the Weil bound becomes trivial. In other words, to estimate $C^a_{f,g}(r,s)$, where f and g are power mappings over $\mathbb{F}_p$, we need to study the number of solutions of the form

$$x^{d_1} + s \equiv (x+r)^{d_2} \bmod p. \tag{5.17}$$

Since the Weil bound depends on the number of roots of the polynomial $(x^{d_1}+s)\,(x+r)^{p-1-d_2}$ over the splitting field and the fact that this polynomial over the splitting field can have at most d_1+1 roots, the Weil bound becomes trivial.

5.3 Crosscorrelation of exponential Welch and power mappings

The previous section discussed how the two families of power mappings and exponential Welch Costas arrays are closely related. So, it would be interesting to extend the family of exponential Welch with the family of power mappings and examine its crosscorrelation properties. The family that we considered is

$$\mathcal{PW}_p = \{f : f \in \mathcal{W}_p \vee f \in \mathcal{P}_p \text{ over } \mathbb{F}_p\}.$$

Let $f(x) = x^d$, $x \in \mathbb{F}_p \setminus \{0\}$ and $gcd(d, p-1) = 1$, be a power mapping over $\mathbb{F}_p$, and let $g = W_1^{exp}(p, \alpha, 0)$ be an exponential Welch Costas array as in Definition 2.34. Then, to compute $C^a_{f,g}(r,s)$, we need to solve the following equation

$$x^d \bmod p + s = \alpha^{x-1+r} \bmod p \text{ for } x \in \mathbb{F}_p \setminus \{0\}. \tag{5.18}$$

It can be seen that estimating the number of solutions for Equation (5.18) could be challenging. Even where $r = s = 0$ (at the origin), studying Equation (5.18) could be tricky.

From the computational experiments' point of view, we exhaustively computed the value of the maximal crosscorrelation between any two elements of the family $\mathcal{PW}_p$ for primes $5 \leq p \leq 271$. The results of this computation are collected in table 5.4 in which, in order to avoid overwriting, we point out that the maximal crosscorrelation for non-safe primes occurs between either two exponential Welch Costas arrays or two power mappings as well as safe primes 47, 59, 83, 167 and 263, for which the results is already included in Table 5.3 and Appendix 6. Then, in table 5.4, we just collected the results for safe primes where the maximal value occurs between an exponential Welch Costas array and a power mapping over $\mathbb{F}_p$.

Overall, the provided information in this section shows how the maximal crosscorrelation of the three families, $\mathcal{W}_p$, $\mathcal{P}_p$, and $\mathcal{PW}_p$, are closely related. The size of the family $\mathcal{PW}_p$ equals $\phi^2(p-1) - \phi(p-1)$, indicating a family of size larger than both exponential Welch and power mappings still have almost the same crosscorrelation properties, which is indeed noticeable.

5.4 The family of inverse permutations

Oscar Moreno et al. in [84, 92] discussed how it is essential to introduce new families of binary arrays with low auto- and crosscorrelation properties.

TABLE 5.4: Value of the maximum crosscorrelation between two pairs of the family $\mathcal{PW}_p$: the second column shows the value of d's and α's, for which the maximum occurs, and the third column illustrates the responsible shifts (r, s). The last column depicts $\mathcal{C}(\mathcal{PW}_p)$.

p	Power mappings and Welch arrays parameters	Shifts (r, s)	$\mathcal{C}(\mathcal{PW}_p)$
11	[d=3, α=2]	(2, 0)	4
11	[d=7, α=2]	(1, 1), (4, 0)	4
11	[d=7, α=6]	(2, 0), (5, -1)	4
11	[d=7, α=8]	(0, 1)	4
11	[d=9 α=2]	(4, 4)	4
11	[d=9, α=8]	(2, 0)	4
23	[d=21, α=11]	(0, -1)	6
107	[d=15, α=98]	(5, 14)	10
179	[d=117, α=115]	(24, 1)	11
227	[d=5, α=178]	(-50, 35), (176, 35)	10
227	[d=175, α=151]	(11, 5)	10
227	[d=189, α=184]	(-21, 2), (205, 2)	10
227	[d=191, α=216]	(11, -6)	10

Such families of binary arrays have actual applications in watermarking. As explained in Section 4.4, inverse functions over a finite field have periodic autocorrelation 2. We realized that applying the transformation $\mathcal{A}_k$, as in Definition 3.12, allows us to construct a family of binary arrays with aperiodic auto and crosscorrelation 2.

Let us consider a permutation matrix X defined as $X = [f(1), f(2), \ldots, f(p-1)]$, where $f(i) = i^{-1}$, and i belongs to the finite field $\mathbb{F}_p \setminus \{0\}$, where p is a prime. Now, we apply the transformation $\mathcal{A}_k$, as defined in Definition 3.12, to X, where k is an integer that is relatively prime to the size of the permutation matrix plus one, denoted as $gcd(k, p) = 1$. This results in $\mathcal{A}_k(X) = [f(k \cdot 1 \bmod p), f(k \cdot 2 \bmod p), \ldots, f(k \cdot (p-1) \bmod p)]$. Now, we can provide the definition of this family obtained through the transformation. For convenience, we call a permutation an inverse permutation if it is generated by the inverse function over a finite field. The family that we consider is as follows.

• **Family of inverse permutations**: For a prime p, we define the family $\mathcal{I}_p$ of inverse permutations of $\{1, \ldots, p-1\}$, by

$$\mathcal{I}_p = \left\{ \left[(kx)^{p-2} \right] : x \in \mathbb{F}_p \setminus \{0\} \text{ and } gcd(k, p) = 1 \right\}.$$

Then we have $|\mathcal{I}_p| = p - 1$.

We will now investigate the crosscorrelation properties of the family $\mathcal{I}_p$ by stating the following theorem.

Theorem 5.10. *For a prime p, the maximal aperiodic auto and crosscorrelation of the family of inverse permutations $\mathcal{I}_p$ of $\{1, \ldots, p-1\}$ satisfies $\mathcal{C}(\mathcal{I}_p) = 2$.*

Proof. Consider two inverse permutations f_1 and f_2, generated by $f_1(x) = (k_1x)^{-1}$ and $f_2(x) = (k_2x)^{-1}$ in $\mathbb{F}_p \setminus \{0\}$, where k_1 and k_2 are not necessarily distinct integers relatively prime to p. In order to compute the crosscorrelation at $(r, s) \in \mathbb{Z}^2$ between f_1 and f_2, we need to estimate the number of solutions of the equation

$$\left((k_1x)^{-1} \bmod p\right) + s = (k_2(x+r))^{-1} \bmod p. \tag{5.19}$$

The main idea of the proof is to show that any solution of (5.19) is also a solution to a quadratic equation over $\mathbb{F}_p$, which can admit at most two solutions, leading to $\mathcal{C}(\mathcal{I}_p) \leq 2$. By following the subsequent sequence of steps, while considering that we are calculating the aperiodic correlation (where x and $x + r$ are never equal to 0), we will demonstrate the equivalence of (5.19) to a quadratic equation.

$$\begin{aligned} &\left((k_1x)^{-1} \bmod p\right) + s = (k_2(x+r))^{-1} \bmod p \\ \Longleftrightarrow &\left(k_1^{-1}x^{-1} \bmod p\right) + s = \left(k_2^{-1} \bmod p\right) \cdot \left((x+r)^{-1} \bmod p\right) \end{aligned}$$

Multiplying both sides of the above equation by $(x + r)^{-1} \bmod p$ yields

$$\begin{aligned} &\left(k_1^{-1}x^{-1} \bmod p\right) \cdot ((x+r) \bmod p) + s\,((x+r) \bmod p) = k_2^{-1} \\ \Longleftrightarrow &\left(k_1^{-1} + rk_1^{-1}x^{-1} + sx + sr\right) \bmod p = k_2^{-1} \end{aligned}$$

Multiplying now both sides of the above equation by k_2 gives

$$\left(k_1^{-1}k_2 + rk_1^{-1}k_2x^{-1} + k_2sx + k_2sr\right) \bmod p = 1.$$

We multiply both sides of the above equation by $(x \bmod p)$ to obtain

$$\begin{aligned} &\left(k_1^{-1}k_2x + rk_1^{-1}k_2 + k_2sx^2 + k_2srx\right) \bmod p = x \bmod p \\ \Longleftrightarrow &\left(k_1^{-1}k_2x + rk_1^{-1}k_2 + k_2sx^2 + k_2srx - x\right) \equiv 0 \bmod p. \end{aligned}$$

It follows that since $k_2sx^2 + \left(k_1^{-1}k_2 + k_2sr - 1\right)x + rk_1^{-1}k_2$ is a polynomial of degree 2 in $\mathbb{F}_p$, it can have at most two solutions. This observation completes the proof by considering the fact that, since k_1 and k_2 are not necessarily distinct, both the aperiodic autocorrelation and aperiodic crosscorrelation of any two members of this family are two. □

One application of transformation $\mathcal{A}_k$ is that it turns a single permutation into a family of permutations. Therefore, there is ample room for further investigation into finding permutations with good autocorrelation properties, for which applying transformation $\mathcal{A}_k$ might construct a family of permutations with suitable crosscorrelation properties.

Chapter 6

Appendix

Computational results on the maximal crosscorrelation of the family of power mappings

Value of the maximum Crosscorrelation between pairs of power mappings is shown in the following table: the second column shows the value of d_1 and d_2, not necessarily distinct, for which the maximal crosscorrelation occurs, and the third column illustrates the responsible shifts (r, s) for the maximal value. The last column depicts $\mathcal{C}(\mathcal{P}_p)$.

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
5	[3, 3]	(1, -1), (1, -3), (2, 2), (3, -1), (4, -2), (-1, 1), (-1, 3), (-2, -2), (-3, 1), (-4, 2)	2
7	[5, 5]	(1, -2), (2, -1), (-1, 2), (-2, 1)	2
11	[3, 9]	(-2, -4), (2, 4)	3
11	[7, 9]	(-4, -2), (4, 2)	3
13	[5,11]	(0, 0)	6
17	[3, 11], [5, 13], [7, 15]	(0,0)	8
19	[5, 11], [5, 17], [7, 13], [11, 17]	(0, 0)	6
23	[7, 19]	(4, -4), (-1, -1), (1, 1), (-4, 4)	6
29	[3, 17], [5, 19], [9, 23], [11, 25], [13, 27]	(0, 0)	14
31	[7, 17], [13, 23], [19, 29]	(0, 0)	10
37	[5, 23], [7, 25], [11, 29], [13, 31], [17, 35]	(0, 0)	18
41	[3, 23], [7, 27], [9, 29], [11, 31], [13, 33], [17, 37], [19, 39]	(0, 0)	20
43	[5, 19], [11, 25], [13, 41], [17, 31], [23, 37]	(0, 0)	14
47	[11, 11]	(-2, -23), (3, -14), (-4,-10), (6, -2), (-6, 2), (4, 10), (-3, 14), (2,23)	8

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
47	[17, 17]	(-9, -5), (6, -4), (2, -2), (-15, -1), (15, 1), (-2, 2), (-6, 4), (9, 5)	8
47	[19, 19]	(-1, -15), (-5, -9), (4, -6), (2, -2), (-2, 2), (-4, 6), (5, 9), (1, 15)	8
47	[21, 21]	(2, -6), (-10, -4), (14, -3), (-23, -2), (23, 2), (-14, 3), (10, 4), (-2, 6)	8
53	[3, 29], [5, 31], [7, 33], [9, 35], [11, 37], [15, 41], [17, 43], [19, 45], [21, 47], [23, 49], [25, 51]	(0, 0)	26
59	[17, 17]	(-8, -6), (-1, -1), (1, 1), (8, 6)	12
59	[41, 41]	(-6, -8), (-1, -1), (1, 1), (6, 8)	12
61	[7, 37], [11, 41], [13, 43], [17, 47], [19, 49], [23, 53], [29, 59]	(0, 0)	30
67	[5, 49], [7, 29], [13, 35], [17, 61], [19, 41], [25, 47], [31, 53], [37, 59], [43, 65]	(0, 0)	22
71	[3, 17], [3, 31], [3, 59], [9, 23], [9, 37], [9, 51], [11, 39], [11, 53], [11, 67], [13, 27], [13, 41], [13, 69], [17, 31], [17, 59], [19, 33], [19, 47], [19, 61], [23, 37], [23, 51], [27, 41], [27, 69], [29, 43], [29, 57], [31, 59], [33, 47], [33, 61], [37, 51], [39, 53], [39, 67], [41, 69], [43, 57], [47, 61], [53, 67]	(0, 0)	14
73	[5, 41], [7, 43], [11, 47], [13, 49], [17, 53], [19, 55], [23, 59], [25, 61], [29, 65], [31, 67], [35, 71]	(0, 0)	36
79	[5, 31], [7, 59], [11, 37], [17, 43], [19, 71], [23, 49], [25, 77], [29, 55], [35, 61], [41, 67], [47, 73]	(0, 0)	26
83	[63, 71]	(-1, -11), (1, 11)	9
83	[67, 69]	(-11, -1), (11, 1)	9

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
89	[3, 47], [5, 49], [7, 51], [9, 53], [13, 57], [15, 59], [17, 61], [19, 63], [21, 65], [23, 67], [25, 69], [29, 73], [31, 75], [35, 79], [37, 81], [39, 83], [41, 85], [43, 87]	(0, 0)	44
97	[5, 53], [7, 55], [11, 59], [17, 65], [19, 67], [23, 71], [25, 73], [29, 77], [31, 79], [35, 83], [37, 85], [41, 89], [43, 91], [47, 95	(0, 0)	48
101	[3, 53], [7, 57], [9, 59], [11, 61], [13, 63], [17, 67], [19, 69], [21, 71], [23, 73], [27, 77], [29, 79], [31, 81], [33, 83], [37, 87], [39, 89], [41, 91], [43, 93], [47, 97], [49, 99]	(0, 0)	50
103	[5, 73],[7, 41],[11, 79],[13, 47],[19, 53],[23, 91],[25, 59],[29, 97],[31, 65],[37, 71],[43, 77],[49, 83],[55, 89],[61, 95],[67, 101]	(0, 0)	34
107	[21, 21]	(-2, -45), (7, -23), (31, -14), (6, -13), (30, -5), (18, -1), (-18, 1), (-30, 5), (-6, 13), (-31, 14), (-7, 23), (2, 45)	10
107	[101, 101]	(14, -31), (5, -30), (1, -18), (23, -7), (13, -6), (-45, -2), (45, 2), (-13, 6), (-23, 7), (-1, 18), (-5, 30), (-14, 31)]	10
109	[5, 59], [7, 61], [11, 65], [13, 67], [17, 71], [19, 73], [23, 77], [25, 79], [29, 83], [31, 85], [35, 89], [37, 91], [41, 95], [43, 97], [47, 101], [49, 103], [53, 107]	(0, 0)	54

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
113	[3, 59], [5, 61], [9, 65], [11, 67], [13, 69], [15, 71], [17, 73], [19, 75], [23, 79], [25, 81], [27, 83], [29, 85], [31, 87], [33, 89], [37, 93], [39, 95], [41, 97], [43, 99], [45, 101], [47, 103], [51, 107], [53, 109], [55, 111]	(0, 0)	56
127	[5, 47], [11, 53], [11, 95], [13, 55], [13, 97], [17, 59], [17, 101], [19, 61], [19, 103], [23, 65], [23, 107], [25, 67], [25, 109], [29, 71], [29, 113], [31, 73], [31, 115], [37, 79], [37, 121], [41, 83], [41, 125], [43, 85], [47, 89], [55, 97], [59, 101], [61, 103], [65, 107], [67, 109], [71, 113], [73, 115], [79, 121], [83, 125]	(0, 0)	42
131	[3, 29], [3, 81], [3, 107], [7, 33], [7, 111], [9, 61], [9, 87], [9, 113], [11, 37], [11, 63], [11, 89], [17, 43], [17, 69], [17, 121], [19, 71], [19, 97], [19, 123], [21, 47], [21, 73], [21, 99], [23, 49], [23, 101], [23, 127], [27, 53], [27, 79], [29, 81], [29, 107], [31, 57], [31, 83], [31, 109], [33, 59], [33, 111], [37, 89], [41, 67], [41, 119],[43, 69], [43, 121], [47, 73], [47, 99], [49, 101], [49, 127], [51, 77], [51, 129], [53, 79], [57, 83], [57, 109], [59, 111], [61, 87], [61, 113], [63, 89], [67, 93],	(0, 0)	26

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
131	[67, 119], [69, 121], [71, 97], [71, 123], [73, 99], [77, 103], [77, 129], [81, 107], [83, 109], [87, 113], [93, 119], [97, 123], [101, 127], [103, 129]	(0, 0)	26
137	[3, 71],[5, 73],[7, 75],[9, 77],[11, 79],[13, 81],[15, 83],[19, 87],[21, 89],[23, 91],[25, 93],[27, 95],[29, 97],[31, 99],[33, 101],[35, 103],[37, 105],[39, 107],[41, 109],[43, 111],[45, 113],[47, 115],[49, 117],[53, 121],[55, 123],[57, 125],[59, 127],[61, 129],[63, 131],[65, 133],[67, 135]	(0, 0)	68
139	[5, 97],[7, 53],[11, 103],[13, 59],[17, 109],[19, 65],[25, 71],[29, 121],[31, 77],[35, 127],[37, 83],[41, 133],[43, 89],[49, 95],[55, 101],[61, 107],[67, 113],[73, 119],[79, 125],[85, 131],[91, 137]	(0, 0)	46
149	[3, 77],[5, 79],[7, 81],[9, 83],[11, 85],[13, 87],[15, 89],[17, 91],[19, 93],[21, 95],[23, 97],[25, 99],[27, 101],[29, 103],[31, 105],[33, 107],[35, 109],[39, 113],[41, 115],[43, 117],[45, 119],[47, 121],[49, 123],[51, 125],[53, 127],[55, 129],[57, 131],[59, 133],[61, 135],[63, 137],[65, 139],[67, 141],[69, 143],[71, 145],[73, 147]	(0, 0)	74

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
151	[7, 107],[11, 61],[13, 113],[17, 67],[19, 119],[23, 73],[29, 79],[31, 131],[37, 137],[41, 91],[43, 143],[47, 97],[49, 149],[53, 103],[59, 109],[71, 121],[77, 127],[83, 133],[89, 139]	(0,0)	50
157	[5, 83],[7, 85],[11, 89],[17, 95],[19, 97],[23, 101],[25, 103],[29, 107],[31, 109],[35, 113],[37, 115],[41, 119],[43, 121],[47, 125],[49, 127],[53, 131],[55, 133],[59, 137],[61, 139],[67, 145],[71, 149],[73, 151],[77, 155]	(0, 0)	78
163	[5, 59],[5, 113],[7, 61],[7, 115],[11, 65],[11, 119],[13, 67],[13, 121],[17, 71],[17, 125],[19, 73],[19, 127],[23, 77],[23, 131],[25, 79],[25, 133],[29, 83],[29, 137],[31, 85],[31, 139],[35, 89],[35, 143],[37, 91],[37, 145],[41, 95],[41, 149],[43, 97],[43, 151],[47, 101],[47, 155],[49, 103],[49, 157],[53, 107],[53, 161],[55, 109],[59, 113],[61, 115],[65, 119],[67, 121],[71, 125],[73, 127],[77, 131],[79, 133],[83, 137],[85, 139],[89, 143],[91, 145],[95, 149],[97, 151],[101, 155],[103, 157],[107, 161]	(0, 0)	54

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
167	[69, 69]	(-15, -69), (-47, -31), (30, -24), (-38, -22), (-6, -18), (3, -10), (-50, -9), (-32, -6), (25, -5), (-12, -1), (12, 1), (-25, 5), (32, 6), (50, 9), (-3, 10), (6, 18), (38, 22), (-30, 24), (47, 31), (15, 69)	12
167	[77, 77]	(-9, -50), (-31, -47), (-22, -38), (-6, -32), (24, -30), (5, -25), (-69, -15), (-1, -12), (-18, -6), (10, -3), (-10, 3), (18, 6), (1, 12), (69, 15), (-5, 25), (-24, 30), (6, 32), (22, 38), (31, 47), (9, 50)	12
167	[131, 131]	(45, -44), (5, -24), (35, -22), (26, -19), (-29, -18), (56, -17), (7, -13), (-4, -9), (-2, -3), (-1, -1), (1, 1), (2, 3), (4, 9), (-7, 13), (-56, 17), (29, 18), (-26, 19), (-35, 22), (-5, 24), (-45, 44)	12
167	[147, 147]	(17, -56), (44, -45), (22, -35), (-18, -29), (19, -26), (13, -7), (24, -5), (-9, -4), (-3, -2), (-1, -1), (1, 1), (3, 2), (9, 4), (-24, 5), (-13, 7), (-19, 26), (18, 29), (-22, 35), (-44, 45), (-17, 56)	12
173	[3, 89],[5, 91],[7, 93],[9, 95],[11, 97],[13, 99],[15, 101],[17, 103],[19, 105],[21, 107],[23, 109],[25, 111],[27, 113],[29, 115],[31, 117],[33, 119],[35, 121],[37, 123],[39, 125],[41, 127],[45, 131],[47, 133],[49, 135],[51, 137],[53, 139],[55, 141],[57, 143],[59, 145],[61, 147],[63, 149],[65, 151],[67, 153],[69, 155],[71, 157],[73, 159],[75, 161],[77, 163],[79, 165],[81, 167],[83, 169],[85, 171]	(0, 0)	86

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
179	[47, 47]	(11, -50), (84, -40), (-42, -32), (-4, -24), (-41, -16), (-3, -6), (-28, -5), (14, -4), (-14, 4), (28, 5), (3, 6), (41, 16), (4, 24), (42, 32), (-84, 40), (-11, 50)	10
179	[125, 125]	(40, -84), (-32, -42), (-16, -41), (-5, -28), (4, -14), (50, -11), (-24, -4), (-6, -3), (6, 3), (24, 4), (-50, 11), (-4, 14), (5, 28), (16, 41), (32, 42), (-40, 84)	10
181	[7, 97],[11, 101],[13, 103],[17, 107],[19, 109],[23, 113],[29, 119],[31, 121],[37, 127],[41, 131],[43, 133],[47, 137],[49, 139],[53, 143],[59, 149],[61, 151],[67, 157],[71, 161],[73, 163],[77, 167],[79, 169],[83, 173],[89, 179]	(0, 0)	90
191	[3, 41],[3, 79],[3, 117],[7, 83],[7, 121],[7, 159],[9, 47],[9, 123],[9, 161],[11, 49],[11, 87],[11, 163],[13, 51],[13, 89],[13, 127],[17, 93],[17, 131],[17, 169],[21, 59],[21, 97],[21, 173],[23, 61],[23, 99],[23, 137],[27, 103],[27, 141],[27, 179],[29, 67],[29, 143],[29, 181],[31, 69],[31, 107],[31, 183],[33, 71],[33, 109],[33, 147],[37, 113],[37, 151],[37, 189],[39, 77],[39, 153],[41, 79],[41, 117],[43, 81],[43, 119],[43, 157],[47, 123],[47, 161],[49, 87],[49, 163],[51, 89],[51, 127],[53, 91],[53, 129],[53, 167],[59, 97],[59, 173],[61, 99],[61, 137],[63, 101]	(0, 0)	38

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
191	[63, 139],[63, 177],[67, 143],[67, 181],[69, 107],[69, 183],[71, 109],[71, 147],[73, 111],[73, 149],[73, 187],[77, 153],[79, 117],[81, 119],[81, 157],[83, 121],[83, 159],[87, 163],[89, 127],[91, 129],[91, 167],[93, 131],[93, 169],[97, 173],[99, 137],[101, 139],[101, 177],[103, 141],[103, 179],[107, 183],[109, 147],[111, 149],[111, 187],[113, 151],[113, 189],[119, 157],[121, 159],[123, 161],[129, 167],[131, 169],[139, 177],[141, 179],[143, 181],[149, 187],[151, 189]	(0, 0)	38
193	[5, 101],[7, 103],[11, 107],[13, 109],[17, 113],[19, 115],[23, 119],[25, 121],[29, 125],[31, 127],[35, 131],[37, 133],[41, 137],[43, 139],[47, 143],[49, 145],[53, 149],[55, 151],[59, 155],[61, 157],[65, 161],[67, 163],[71, 167],[73, 169],[77, 173],[79, 175],[83, 179],[85, 181],[89, 185],[91, 187],[95, 191]	(0, 0)	96

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
197	[3, 101],[5, 103],[9, 107],[11, 109],[13, 111],[15, 113],[17, 115],[19, 117],[23, 121],[25, 123],[27, 125],[29, 127],[31, 129],[33, 131],[37, 135],[39, 137],[41, 139],[43, 141],[45, 143],[47, 145],[51, 149],[53, 151],[55, 153],[57, 155],[59, 157],[61, 159],[65, 163],[67, 165],[69, 167],[71, 169],[73, 171],[75, 173],[79, 177],[81, 179],[83, 181],[85, 183],[87, 185],[89, 187],[93, 191],[95, 193],[97, 195]	(0, 0)	98
199	[5, 71],[5, 137],[7, 73],[7, 139],[13, 79],[13, 145],[17, 83],[17, 149],[19, 85],[19, 151],[23, 89],[23, 155],[25, 91],[25, 157],[29, 95],[29, 161],[31, 97],[31, 163],[35, 101],[35, 167],[37, 103],[37, 169],[41, 107],[41, 173],[43, 109],[43, 175],[47, 113],[47, 179],[49, 115],[49, 181],[53, 119],[53, 185],[59, 125],[59, 191],[61, 127],[61, 193],[65, 131],[65, 197], [67, 133],[71, 137],[73, 139],[79, 145],[83, 149],[85, 151],	(0, 0)	66

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
199	[89, 155],[91, 157],[95, 161],[97, 163],[101, 167],[103, 169],[107, 173],[109, 175],[113, 179],[115, 181],[119, 185],[125, 191],[127, 193],[131, 197]	(0, 0)	66
211	[11, 151],[13, 83],[17, 157],[19, 89],[23, 163],[29, 169],[31, 101],[37, 107],[41, 181],[43, 113],[47, 187],[53, 193],[59, 199],[61, 131],[67, 137],[73, 143],[79, 149],[97, 167],[103, 173],[109, 179],[121, 191],[127, 197],[139, 209]	(0, 0)	70
223	[5, 79],[7, 155],[11, 85],[13, 161],[17, 91],[19, 167],[23, 97],[25, 173],[29, 103],[31, 179],[35, 109],[41, 115],[43, 191],[47, 121],[49, 197],[53, 127],[55, 203],[59, 133],[61, 209], [65, 139],[67, 215],[71, 145],[73, 221],[77, 151],[83, 157],[89, 163],[95, 169],[101, 175],[107, 181],[113, 187],[119, 193],[125, 199],[131, 205],[137, 211],[143, 217]	(0, 0)	74
227	[29, 29]	(-46, -109), (-21, -93), (-7, -55), (17, -54), (-41, -48), (-95, -43), (23, -26), (-9, -24), (56, -20), (-1, -18), (-19, -15), (-32, -10), (76, -4), (-42, -3), (-11, -2), (11, 2), (42, 3), (-76, 4), (32, 10), (19, 15), (1, 18), (-56, 20), (9, 24), (-23, 26), (95, 43), (41, 48), (-17, 54), (7, 55), (21, 93), (46, 109)	10

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
227	[39, 39]	(-43, -95), (4, -76), (20, -56), (-109, -46), (-3, -42), (-48, -41), (-10, -32), (26, -23), (-93, -21), (-15, -19), (54, -17), (-2, -11), (-24, -9), (-55, -7), (-18, -1), (18, 1), (55, 7), (24, 9), (2, 11), (-54, 17), (15, 19), (93, 21), (-26, 23), (10, 32), (48, 41), (3, 42), (109, 46), (-20, 56), (-4, 76), (43, 95)	10
227	[93, 93]	(-46, -59), (14, -52), (30, -49), (64, -47), (38, -46), (28, -28), (-60, -26), (-53, -22), (-2, -9), (42, -6), (-42, 6), (2, 9), (53, 22), (60, 26), (-28, 28), (-38, 46), (-64, 47), (-30, 49), (-14, 52), (46, 59)	10
227	[209, 209]	(47, -64), (-26, -60), (-22, -53), (-59, -46), (6, -42), (46, -38), (49, -30), (28, -28), (52, -14), (-9, -2), (9, 2), (-52, 14), (-28, 28), (-49, 30), (-46, 38), (-6, 42), (59, 46), (22, 53), (26, 60), (-47, 64)	10
229	[5, 119],[7, 121],[11, 125],[13, 127],[17, 131],[23, 137],[25, 139],[29, 143],[31, 145],[35, 149],[37, 151],[41, 155],[43, 157],[47, 161],[49, 163],[53, 167],[55, 169],[59, 173],[61, 175],[65, 179],[67, 181],[71, 185],[73, 187],[77, 191],[79, 193],[83, 197],[85, 199],[89, 203],[91, 205],[97, 211],[101, 215],[103, 217],[107, 221],[109, 223],[113, 227]	(0, 0)	114

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
233	[3, 119],[5, 121],[7, 123],[9, 125],[11, 127],[13, 129],[15, 131],[17, 133],[19, 135],[21, 137],[23, 139],[25, 141],[27, 143],[31, 147],[33, 149],[35, 151],[37, 153],[39, 155],[41, 157],[43, 159],[45, 161],[47, 163],[49, 165],[51, 167],[53, 169],[55, 171],[57, 173],[59, 175],[61, 177],[63, 179],[65, 181],[67, 183], [69, 185],[71, 187],[73, 189],[75, 191],[77, 193],[79, 195],[81, 197],[83, 199],[85, 201],[89, 205],[91, 207],[93, 209],[95, 211],[97, 213],[99, 215],[101, 217],[103, 219],[105, 221],[107, 223],[109, 225],[111, 227],[113, 229],[115, 231]	(0, 0)	116
239	[3, 37],[3, 71],[3, 139],[3, 173],[3, 207],[5, 39],[5, 73],[5, 107],[5, 141],[5, 209],[9, 43],[9, 111],[9, 145],[9, 179],[9, 213],[11, 45],[11, 79],[11, 113],[11, 181],[11, 215],[13, 47],[13, 81],[13, 115],[13, 149],[13, 183],[15, 83],[15, 117],[15, 151],[15, 185],[15, 219],[19, 53],[19, 87],[19, 121],[19, 155],[19, 223],[23, 57],[23, 125],[23, 159],[23, 193],[23, 227],	(0, 0)	34

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
239	[25, 59],[25, 93],[25, 127],[25, 195],[25, 229],[27, 61],[27, 95],[27, 129],[27, 163],[27, 197],[29, 97],[29, 131],[29, 165], [29, 199],[29, 233],[31, 65],[31, 99],[31, 167],[31, 201],[31, 235],[33, 67],[33, 101], [33, 135],[33, 169],[33, 237],[37, 71],[37, 139],[37, 173],[37, 207],[39, 73],[39, 107],[39, 141],[39, 209],[41, 75],[41, 109], [41, 143],[41, 177],[41, 211],[43, 111],[43, 145],[43, 179],[43, 213],[45, 79],[45, 113],[45, 181],[45, 215],[47, 81],[47, 115],[47, 149],[47, 183],[53, 87],[53, 121],[53, 155],[53, 223], [55, 89],[55, 123],[55, 157],[55, 191],[55, 225],[57, 125],[57, 159],[57, 193],[57, 227],[59, 93],[59, 127],[59, 195],[59, 229],[61, 95],[61, 129],[61, 163],[61, 197],[65, 99], [65, 167],[65, 201],[65, 235],[67, 101],[67, 135],[67, 169],[67, 237],[69, 103],[69, 137],[69, 171],[69, 205],[71, 139],[71, 173],[71, 207],[73, 107],[73, 141],[73, 209],[75, 109],[75, 143],[75, 177],[75, 211],[79, 113],[79, 181],[79, 215],[81, 115],[81, 149],[81, 183],[83, 117],[83, 151],[83, 185],[83, 219],[87, 121],	(0, 0)	34

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
239	[87, 155],[87, 223],[89, 123],[89, 157],[89, 191],[89, 225],[93, 127],[93, 195],[93, 229],[95, 129],[95, 163],[95, 197],[97, 131],[97, 165],[97, 199],[97, 233],[99, 167],[99, 201],[99, 235],[101, 135],[101, 169],[101, 237],[103, 137],[103, 171],[103, 205],[107, 141],[107, 209],[109, 143],[109, 177],[109, 211],[111, 145],[111, 179],[111, 213],[113, 181],[113, 215],[115, 149],[115, 183],[117, 151],[117, 185],[117, 219], [121, 155],[121, 223],[123, 157],[123, 191],[123, 225],[125, 159],[125, 193],[125, 227],[127, 195],[127, 229],[129, 163],[129, 197],[131, 165],[131, 199],[131, 233],[135, 169],[135, 237],[137, 171],[137, 205],[139, 173],[139, 207],[141, 209],[143, 177],[143, 211],[145, 179],[145, 213],[149, 183],[151, 185],[151, 219],[155, 223], [157, 191],[157, 225],[159, 193],[159, 227],[163, 197],[165, 199],[165, 233],[167, 201],[167, 235],[169, 237],[171, 205],[173, 207],[177, 211],[179, 213],[181, 215],[185, 219],[191, 225],[193, 227],[195, 229],[199, 233],[201, 235]	(0, 0)	34

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
241	[7, 127],[11, 131],[13, 133],[17, 137],[19, 139],[23, 143],[29, 149],[31, 151],[37, 157],[41, 161],[43, 163],[47, 167],[49, 169],[53, 173],[59, 179],[61, 181],[67, 187],[71, 191],[73, 193],[77, 197],[79, 199],[83, 203],[89, 209],[91, 211],[97, 217],[101, 221],[103, 223],[107, 227],[109, 229],[113, 233],[119, 239]	(0, 0)	120
251	[3, 53],[3, 103],[3, 153],[3, 203],[7, 57],[7, 107],[7, 157],[7, 207],[9, 59],[9, 109],[9, 159],[9, 209],[11, 61],[11, 111],[11, 161],[11, 211],[13, 63],[13, 113],[13, 163],[13, 213],[17, 67],[17, 117],[17, 167],[17, 217],[19, 69],[19, 119],[19, 169],[19, 219],[21, 71],[21, 121],[21, 171],[21, 221],[23, 73],[23, 123],[23, 173],[23, 223],[27, 77],[27, 127],[27, 177], [27, 227],[29, 79],[29, 129],[29, 179],[29, 229],[31, 81],[31, 131],[31, 181],[31, 231],[33, 83],[33, 133],[33, 183],[33, 233], [37, 87],[37, 137],[37, 187], [37, 237],[39, 89],[39, 139],[39, 189],[39, 239],[41, 91],[41, 141],[41, 191],[41, 241],	(0, 0)	50

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
251	[43, 93],[43, 143],[43, 193],[43, 243],[47, 97],[47, 147],[47, 197],[47, 247],[49, 99],[49, 149],[49, 199],[49, 249],[51, 101],[51, 151], [51, 201],[53, 103],[53, 153],[53, 203],[57, 107],[57, 157],[57, 207], [59, 109],[59, 159],[59, 209],[61, 111],[61, 161],[61, 211],[63, 113],[63, 163],[63, 213],[67, 117],[67, 167],[67, 217],[69, 119],[69, 169],[69, 219], [71, 121],[71, 171],[71, 221],[73, 123],[73, 173],[73, 223],[77, 127],[77, 177],[77, 227],[79, 129],[79, 179],[79, 229],[81, 131],[81, 181],[81, 231],[83, 133],[83, 183],[83, 233],[87, 137],[87, 187],[87, 237],[89, 139],[89, 189],[89, 239],[91, 141],[91, 191],[91, 241],[93, 143],[93, 193],[93, 243],[97, 147],[97, 197],[97, 247],[99, 149],[99, 199],[99, 249],[101, 151],[101, 201],[103, 153],[103, 203], [107, 157],[107, 207],[109, 159],[109, 209],[111, 161],[111, 211],[113, 163],[113, 213],[117, 167],[117, 217],[119, 169],[119, 219],[121, 171],[121, 221],[123, 173],[123, 223],[127, 177],[127, 227],[129, 179],[129, 229],[131, 181],[131, 231],[133, 183],[133, 233],	(0, 0)	50

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
251	[137, 187],[137, 237],[139, 189], [139, 239],[141, 191],[141, 241],[143, 193],[143, 243],[147, 197],[147, 247],[149, 199],[149, 249],[151, 201],[153, 203],[157, 207],[159, 209],[161, 211],[163, 213],[167, 217],[169, 219],[171, 221],[173, 223],[177, 227],[179, 229],[181, 231],[183, 233],[187, 237],[189, 239],[191, 241],[193, 243],[197, 247],[199, 249]	(0, 0)	50
257	[3, 131],[5, 133],[7, 135],[9, 137],[11, 139],[13, 141],[15, 143],[17, 145],[19, 147],[21, 149],[23, 151],[25, 153],[27, 155],[29, 157],[31, 159],[33, 161],[35, 163],[37, 165],[39, 167],[41, 169],[43, 171],[45, 173],[47, 175],[49, 177],[51, 179],[53, 181],[55, 183],[57, 185],[59, 187], [61, 189],[63, 191],[65, 193],[67, 195],[69, 197],[71, 199],[73, 201],[75, 203],[77, 205],[79, 207],[81, 209],[83, 211],[85, 213],[87, 215],[89, 217],[91, 219], [93, 221], [95, 223],[97, 225],[99, 227],[101, 229],[103, 231],[105, 233],[107, 235],[109, 237],[111, 239],[113, 241],[115, 243],[117, 245],[119, 247],[121, 249],[123, 251],[125, 253],[127, 255]	(0, 0)	128

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
263	[41, 41]	(-52, -95), (-78, -89), (-8, -75), (-6, -72), (-16, -68), (21, -52), (-3, -33), (-35, -31), (59, -25), (32, -19), (-93, -18), (15, -17), (-89, -12), (-18, -9), (-34, -4), (-49, -2), (-1, -1), (1, 1), (49, 2), (34, 4), (18, 9), (89, 12), (-15, 17), (93, 18), (-32, 19), (-59, 25), (35, 31), (3, 33), (-21, 52), (16, 68), (6, 72), (8, 75), (78, 89), (52, 95)	12
263	[147, 147]	(-18, -93), (-12, -89), (-89, -78), (25, -59), (-95, -52), (-2, -49), (-31, -35), (-4, -34), (19, -32), (52, -21), (-9, -18), (-68, -16), (17, -15), (-75, -8), (-72, -6), (-33, -3), (-1, -1), (1, 1), (33, 3), (72, 6), (75, 8), (-17, 15), (68, 16), (9, 18), (-52, 21), (-19, 32), (4, 34), (31, 35), (2, 49), (95, 52), (-25, 59), (89, 78), (12, 89), (18, 93)	12
269	[3, 137],[5, 139],[7, 141],[9, 143],[11, 145],[13, 147],[15, 149],[17, 151],[19, 153],[21, 155],[23, 157],[25, 159],[27, 161],[29, 163],[31, 165],[33, 167],[35, 169],[37, 171],[39, 173],[41, 175],[43, 177],[45, 179],[47, 181],[49, 183],[51, 185],[53, 187],[55, 189],[57, 191],[59, 193],[61, 195],[63, 197],[65, 199],[69, 203],[71, 205],[73, 207],[75, 209], [77, 211],[79, 213],[81, 215],[83, 217],[85, 219],[87, 221],[89, 223],[91, 225],[93, 227],	(0, 0)	134

p	$[d_1, d_2]$	Shifts (r, s)	$\mathcal{C}(\mathcal{P}_p)$
269	[95, 229],[97, 231],[99, 233],[101, 235],[103, 237],[105, 239],[107, 241],[109, 243],[111, 245],[113, 247],[115, 249],[117, 251],[119, 253],[121, 255],[123, 257],[125, 259],[127, 261],[129, 263],[131, 265],[133, 267]	(0, 0)	134
271	[7, 97],[7, 187],[11, 101],[11, 191],[13, 103],[13, 193],[17, 107],[17, 197],[19, 109],[19, 199],[23, 113],[23, 203],[29, 119],[29, 209],[31, 121],[31, 211],[37, 127],[37, 217],[41, 131],[41, 221],[43, 133],[43, 223],[47, 137],[47, 227],[49, 139],[49, 229],[53, 143],[53, 233],[59, 149],[59, 239],[61, 151], [61, 241],[67, 157],[67, 247],[71, 161],[71, 251],[73, 163],[73, 253],[77, 167],[77, 257],[79, 169],[79, 259],[83, 173],[83, 263],[89, 179],[89, 269],[91, 181],[97, 187],[101, 191], [103, 193],[107, 197],[109, 199],[113, 203],[119, 209],[121, 211],[127, 217],[131, 221],[133, 223],[137, 227],[139, 229],[143, 233],[149, 239],[151, 241],[157, 247],[161, 251],[163, 253],[167, 257],[169, 259],[173, 263],[179, 269]	(0, 0)	90

Bibliography

[1] Erkan Afacan, *A new search method for costas arrays by using difference triangle analysis*, 2017 progress in electromagnetics research symposium-spring (piers), 2017, pp. 456–461.

[2] KT Arasu, *Sequences and arrays with desirable correlation properties*, Information security, coding theory and related combinatorics, 2011, pp. 136–171.

[3] KT Arasu, Cunsheng Ding, Tor Helleseth, P Vijay Kumar, and Halvard M Martinsen, *Almost difference sets and their sequences with optimal autocorrelation*, IEEE transactions on information theory **47** (2001), no. 7, 2934–2943.

[4] Alejandro Arbelaez and Philippe Codognet, *A gpu implementation of parallel constraint-based local search*, 2014 22nd euromicro international conference on parallel, distributed, and network-based processing, 2014, pp. 648–655.

[5] Ali Ardalani and Alexander Pott, *A new transformation for costas arrays*, 2022 10th international workshop on signal design and its applications in communications (iwsda), 2022, pp. 1–5.

[6] Simeon Ball and Michael Zieve, *Symplectic spreads and permutation polynomials*, International conference on finite fields and applications, 2003, pp. 79–88.

[7] Lionel Barker, Konstantinos Drakakis, and Scott Rickard, *On the complexity of the verification of the costas property*, Proceedings of the IEEE **97** (2009), no. 3, 586–593.

[8] Daniele Bartoli and Marco Calderini, *On construction and (non) existence of c-(almost) perfect nonlinear functions*, Finite Fields and Their Applications **72** (2021), 101835.

[9] J. K. Beard, J. C. Russo, K. G. Erickson, M. C. Monteleone, and M. T. Wright, *Costas array generation and search methodology*, IEEE Transactions on Aerospace and Electronic Systems **43** (2007), no. 2, 522–538.

[10] James Beard, *Costas arrays and enumeration to order 1030*, IEEE Dataport (2017), available at `https://dx.doi.org/10.21227/H21P42`.

[11] James Beard, Keith Erickson, M. Monteleone, M. Wright, and Jon Russo, *Combinatoric collaboration on costas arrays and radar applications*, 200405, pp. 260 –265.

[12] Céline Blondeau, Anne Canteaut, and Pascale Charpin, *Differential properties of power functions*, International Journal of Information and Coding Theory **1** (2010), no. 2, 149–170.

[13] Leopold Bomer and Markus Antweiler, *Binary and biphase sequences and arrays with low periodic autocorrelation sidelobes*, International conference on acoustics, speech, and signal processing, 1990, pp. 1663–1666.

[14] Carl Bracken and Gregor Leander, *A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree*, Finite Fields and Their Applications **16** (2010), no. 4, 231–242.

[15] Kevin Byard, *Synthesis of binary arrays with perfect correlation properties—coded aperture imaging*, Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment **336** (1993), no. 1-2, 262–268.

[16] Domenick Calabro and Jack K Wolf, *On the synthesis of two-dimensional arrays with desirable correlation properties*, Information and Control **11** (1967), no. 5-6, 537–560.

[17] Yves Caniou, Philippe Codognet, Florian Richoux, Daniel Diaz, and Salvador Abreu, *Large-scale parallelism for constraint-based local search: the costas array case study*, Constraints **20** (2015), no. 1, 30–56.

[18] Weita Chang, *A remark on the definition of costas arrays*, Proceedings of the IEEE **75** (1987), no. 4, 522–523.

[19] Wensong Chu, *Permutation polynomials, tuscan-k arrays and costas sequences* (2003), 7–16 pp., available at https://doi.org/10.1007/978-1-4615-0304-0_2.

[20] Philippe Codognet, *Modeling the costas array problem in qubo for quantum annealing*, European conference on evolutionary computation in combinatorial optimization (part of evostar), 2022, pp. 143–158.

[21] Stephen D Cohen and Gary L Mullen, *Primitive elements in finite fields and costas arrays*, Applicable Algebra in Engineering, Communication and Computing **2** (1991), no. 1, 45–53.

[22] Bill Correll, *The density of costas arrays and three-free permutations*, 2012 ieee statistical signal processing workshop (ssp), 2012, pp. 492–495.

[23] ______, *A new structural property of Costas arrays*, 2018 ieee radar conference (radarconf18), 2018, pp. 0748–0753.

[24] ______, *More new structural properties of Costas arrays*, 2019 ieee radar conference (radarconf), 2019, pp. 1–6.

[25] J. P. Costas, *Medium constraints on sonar design and performance*, Technical Report Class 1 Rep. R65EMH33 (1965November).

[26] John P Costas, *A study of a class of detection waveforms having nearly ideal range—doppler ambiguity properties*, Proceedings of the IEEE **72** (1984), no. 8, 996–1009.

[27] J.P. Costas, *A study of a class of detection waveforms having nearly ideal range—doppler ambiguity properties*, Proceedings of the IEEE **72** (1984), no. 8, 996–1009.

[28] D Huw Davies, *On the density of costas arrays*, IEEE Transactions on Information Theory (1989).

[29] Daniel Diaz, Florian Richoux, Yves Caniou, Philippe Codognet, and Salvador Abreu, *Parallel local search for the costas array problem*, 2012 ieee 26th international parallel and distributed processing symposium workshops & phd forum, 2012, pp. 1793–1802.

[30] Daniel Diaz, Florian Richoux, Philippe Codognet, Yves Caniou, and Salvador Abreu, *Constraint-based local search for the costas array problem*, International conference on learning and intelligent optimization, 2012, pp. 378–383.

[31] H. Dobbertin, *Almost perfect nonlinear power functions on $GF(2^n)$: the welch case*, IEEE Transactions on Information Theory **45** (1999), no. 4, 1271–1275.

[32] Xiang dong Hou, *Permutation polynomials over finite fields — a survey of recent advances*, Finite Fields and Their Applications **32** (2015), 82–119. Special Issue : Second Decade of FFA.

[33] Konstantinos Drakakis, *A review of costas arrays*, Journal of Applied Mathematics (2006).

[34] ______, *Some results on the degrees of freedom of costas arrays*, 2010 44th annual conference on information sciences and systems (ciss), 2010, pp. 1–5.

[35] ______, *Open problems in Costas arrays*, arXiv preprint arXiv:1102.5727 (2011).

[36] Konstantinos Drakakis, Rod Gow, John Healy, and Scott Rickard, *Cross-correlation properties of costas arrays and their images under horizontal and vertical flips*, Mathematical Problems in Engineering (2008).

[37] Konstantinos Drakakis, Rod Gow, and Gary McGuire, *APN permutations on $\mathbb{Z}_n$ and Costas arrays*, Discrete Applied Mathematics **157** (2009), no. 15, 3320–3326.

[38] Konstantinos Drakakis, Roderick Gow, and Scott Rickard, *Common distance vectors between costas arrays*, Advances in Mathematics of Communications **3** (2009), no. 1, 35.

[39] Konstantinos Drakakis, Roderick Gow, Scott Rickard, John Sheekey, and Ken Taylor, *On the maximal cross-correlation of algebraically constructed costas arrays*, IEEE Transactions on Information Theory **57** (2011), no. 7, 4612–4621.

[40] Konstantinos Drakakis, Francesco Iorio, and Scott Rickard, *The enumeration of Costas arrays of order* 28, 2010 ieee information theory workshop, 2010, pp. 1–5.

[41] Konstantinos Drakakis, Francesco Iorio, Scott Rickard, and John Walsh, *Results of the enumeration of Costas arrays of order* 29, Advances in Mathematics of Communications **5** (2011), no. 3, 547.

[42] Konstantinos Drakakis, Verónica Requena, and Gary McGuire, *On the nonlinearity of exponential welch costas functions*, IEEE Transactions on information theory **56** (2010), no. 3, 1230–1238.

[43] Konstantinos Drakakis, Scott Rickard, James K Beard, Rodrigo Caballero, Francesco Iorio, Gareth O'Brien, and John Walsh, *Results of the enumeration of Costas arrays of order* 27, IEEE Transactions on Information Theory **54** (2008), no. 10, 4684–4687.

[44] David Mark Drumheller and Edward L Titlebaum, *Cross-correlation properties of algebraically constructed costas arrays*, IEEE Transactions on Aerospace and Electronic Systems **27** (1991), no. 1, 2–10.

[45] David Steven Dummit and Richard M Foote, *Abstract algebra*, Vol. 3, Wiley Hoboken, 2004.

[46] Yves Edel, Gohar Kyureghyan, and Alexander Pott, *A new apn function which is not equivalent to a power mapping*, IEEE Transactions on Information Theory **52** (2006), no. 2, 744–747.

[47] Tuvi Etzion, *Combinatorial designs derived from costas arrays*, Sequences, 1990, pp. 208–227.

[48] Pingzhi Z Fan and Michael Darnell, *The synthesis of perfect sequences*, Ima international conference on cryptography and coding, 1995, pp. 63–73.

[49] Patrick Felke, *The multivariate method strikes again: New power functions with low differential uniformity in odd characteristic*, Cryptography and Communications **12** (2020), no. 5, 841–857.

[50] Avraham Freedman and Nadav Levanon, *Any two $n\times n$ costas signals must have at least one common ambiguity sidelobe if $n>3$—a proof*, Proceedings of the IEEE **73** (1985), no. 10, 1530–1531.

[51] Michael J Ganley, *Direct product difference sets*, Journal of Combinatorial Theory, Series A **23** (1977), no. 3, 321 –332, available at https://doi.org/10.1016/0097-3165(77)90023-1.

[52] Gagan Garg, Tor Helleseth, and P. Vijay Kumar, *Recent advances in low-correlation sequences* (Vahid Tarokh, ed.), Springer US, Boston, MA, 2009.

[53] E. N. Gilbert, *Latin squares which contain no repeated digrams*, SIAM Review **7** (1965), no. 2, 189–198, available at https://doi.org/10.1137/1007035.

[54] Solomon Golomb and Herbert Taylor, *Two-dimensional synchronization patterns for minimum ambiguity*, IEEE Transactions on Information Theory **28** (1982), no. 4, 600–604.

[55] Solomon W Golomb, *Algebraic constructions for Costas arrays*, Journal of Combinatorial Theory, Series A **37** (1984), no. 1, 13–21.

[56] Solomon W. Golomb and Guang Gong, *Signal design for good correlation: For wireless communication, cryptography, and radar*, Cambridge University Press, 2005.

[57] ———, *The status of costas arrays*, IEEE Transactions on Information Theory **53** (2007), no. 11, 4260–4265.

[58] Solomon W Golomb and Guang Gong, *The status of Costas arrays*, IEEE Transactions on Information Theory **53** (2007), no. 11, 4260–4265.

[59] S.W. Golomb, *The T_4 and G_4 constructions for costas arrays*, IEEE Transactions on Information Theory **38** (1992), no. 4, 1404–1406.

[60] S.W. Golomb and H. Taylor, *Constructions and properties of costas arrays*, Proceedings of the IEEE **72** (1984), no. 9, 1143–1163.

[61] DH Green and SK Amarasinghe, *Families of sequences and arrays with good periodic correlation properties*, IEE Proceedings E (Computers and Digital Techniques) **138** (1991), no. 4, 260–268.

[62] Domingo Gómez-Pérez and Arne Winterhof, *A note on the cross-correlation of costas permutations*, IEEE Transactions on Information Theory **66** (2020), no. 12, 7724–7727.

[63] Hao He, Jian Li, and Petre Stoica, *Waveform design for active sensing systems: a computational approach*, Cambridge University Press, 2012.

[64] Hao He, Petre Stoica, and Jian Li, *Designing unimodular sequence sets with good correlations—including an application to mimo radar*, IEEE Transactions on Signal Processing **57** (2009), no. 11, 4391–4405.

[65] T. Helleseth, C. Rong, and D. Sandberg, *New families of almost perfect nonlinear power mappings*, IEEE Transactions on Information Theory **45** (1999), no. 2, 475–485.

[66] Tor Helleseth, Chunming Rong, and Daniel Sandberg, *New families of almost perfect nonlinear power mappings*, IEEE transactions on Information Theory **45** (1999), no. 2, 475–485.

[67] Tor Helleseth and Daniel Sandberg, *Some power mappings with low differential uniformity*, Applicable Algebra in Engineering, Communication and Computing **8** (1997), no. 5, 363–370.

[68] Xiang-dong Hou, *Determination of a type of permutation trinomials over finite fields, ii*, Finite Fields and Their Applications **35** (2015), 16–35.

[69] Jonathan Jedwab and Jane Wodlinger, *Structural properties of Costas arrays.*, Adv. Math. Commun. **8** (2014), no. 3, 241–256.

[70] Jonathan Jedwab and Kayo Yoshida, *The peak sidelobe level of families of binary sequences*, IEEE transactions on information theory **52** (2006), no. 5, 2247–2254.

[71] WenJie Jia, XiangYong Zeng, ChunLei Li, Tor Helleseth, and Lei Hu, *Permutation polynomials with low differential uniformity over finite fields of odd characteristic*, Science China Mathematics **56** (2013), no. 7, 1429–1440.

[72] Dieter Jungnickel and Alexander Pott, *Perfect and almost perfect sequences*, Discrete Applied Mathematics **95** (1999), no. 1-3, 331–359.

[73] Sükrü Ekin Kocabas and Abdullah Atalar, *Binary sequences with low aperiodic autocorrelation for synchronization purposes*, IEEE Communications Letters **7** (2003), no. 1, 36–38.

[74] P. Vijay Kumar, *On the existence of square dot-matrix patterns having a specific three-valued periodic-correlation function*, IEEE transactions on information theory **34** (1988), no. 2, 271–277.

[75] Nadav Levanon, *Radar*, Encyclopedia of physical science and technology (third edition), 2003, pp. 497–510.

[76] Nian Li, Yanan Wu, Xiangyong Zeng, and Xiaohu Tang, *On the differential spectrum of a class of power functions over finite fields*, CoRR **abs/2012.04316** (2020), available at 2012.04316.

[77] Rudolf Lidl and Harald Niederreiter, *Introduction to finite fields and their applications*, Cambridge university press, 1994.

[78] Hans Dieter Luke, *Sequences and arrays with perfect periodic correlation*, IEEE Transactions on Aerospace and Electronic Systems **24** (1988), no. 3, 287–294.

[79] SV Maric, Ivan Seskar, and Edward L Titlebaum, *On cross-ambiguity properties of welch-costas arrays*, IEEE Transactions on Aerospace and Electronic Systems **30** (1994), no. 4, 1063–1071.

[80] Oscar Moreno, *Survey on Costas arrays and their generalizations*, Mathematical properties of sequences and other combinatorial structures, 2003, pp. 55–64.

[81] Oscar Moreno, Reza Omrani, and Svctislav V Maric, *A new construction of multiple target sonar and extended costas arrays with perfect correlation*, 2006 40th annual conference on information sciences and systems, 2006, pp. 512–517.

[82] Oscar Moreno and Jose Ortiz-Ubarri, *Double periodic arrays with good correlation for applications in watermarking*, 2007 3rd international workshop on signal design and its applications in communications, 2007, pp. 214–218.

[83] Oscar Moreno and José Ortiz-Ubarri, *A new method to construct double periodic arrays with optimal correlation*, 2009 ieee information theory workshop, 2009, pp. 364–368.

[84] Oscar Moreno and Andrew Tirkel, *Multi-dimensional arrays for watermarking*, 2011 ieee international symposium on information theory proceedings, 2011, pp. 2691–2695.

[85] Oscar Moreno et al., *Survey of results on signal patterns for locating one or multiple targets*, Nato adv. sci. inst. ser. c, math. phys. sci., ser. difference sets, sequences and their correlation properties, 1999.

[86] Gary L Mullen and Daniel Panario, *Handbook of finite fields*, Vol. 17, CRC Press Boca Raton, 2013.

[87] Amela Muratovic-Ribic, Alexander Pott, David Thomson, and Qiang Wang, *On the characterization of a semi-multiplicative analogue of planar functions over finite fields*, Topics in finite fields, Amer. Math. Soc., Providence, RI **632** (2015), 317–325.

[88] Jong-Seon No, Hong-Yeop Song, Tor Helleseth, and P Vijay Kumar, *Mathematical properties of sequences and other combinatorial structures*, Vol. 726, Springer Science & Business Media, 2012.

[89] Kaisa Nyberg, *Perfect nonlinear s-boxes*, Workshop on the theory and application of of cryptographic techniques, 1991, pp. 378–386.

[90] ———, *Differentially uniform mappings for cryptography*, Workshop on the theory and application of of cryptographic techniques, 1993, pp. 55–64.

[91] Kaisa Nyberg and Lars Ramkilde Knudsen, *Provable security against differential cryptanalysis*, Annual international cryptology conference, 1992, pp. 566–574.

[92] Anatol Zygmunt Tirkel Oscar Moreno De Ayala, *"digital watermarking," us patent application, docket no: Us8934663b2, 2015-01-13.*

[93] Daniel Panario, Amin Sakzad, Brett Stevens, and Qiang Wang, *Two new measures for permutations: ambiguity and deficiency*, IEEE transactions on information theory **57** (2011), no. 11, 7648–7657.

[94] Daniel Panario, Brett Stevens, and Qiang Wang, *Ambiguity and deficiency in costas arrays and apn permutations*, Latin 2010: Theoretical informatics, 2010, pp. 397–406.

[95] Matthew G Parker and Alexander Pott, *On boolean functions which are bent and negabent*, Sequences, subsequences, and consequences, 2007, pp. 9–23.

[96] Alexander Pott, *Group algebras and correlation immune functions*, International conference on sequences and their applications, 2004, pp. 437–450.

[97] ______, *Nonlinear functions in abelian groups and relative difference sets*, Discrete Applied Mathematics **138** (2004), no. 1-2, 177–193.

[98] Alexander Pott, Qi Wang, and Yue Zhou, *Sequences and functions derived from projective planes and their difference sets*, International workshop on the arithmetic of finite fields, 2012, pp. 64–80.

[99] Scott Rickard, *Searching for Costas arrays using periodicity properties*, Ima international conference on mathematics in signal processing, the royal agricultural college, cirencester, 2004.

[100] Harvey E Rose, *A course on finite groups*, Springer Science & Business Media, 2009.

[101] H Rosen Kenneth, *Elementary number theory and its applications*, Addison-Weley Publishing Company, 1984.

[102] Ivelisse Rubio and Jaziel Torres, *Circular costas maps: a multidimensional analog of circular costas sequences*, arXiv preprint arXiv:2210.16661 (2022).

[103] Joseph J Rushanan, *Weil sequences: A family of binary sequences with good correlation properties*, 2006 ieee international symposium on information theory, 2006, pp. 1648–1652.

[104] D.V. Sarwate and M.B. Pursley, *Crosscorrelation properties of pseudorandom and related sequences*, Proceedings of the IEEE **68** (1980), no. 5, 593–619.

[105] D Shedd and D Sarwate, *Construction of sequences with good correlation properties (corresp.)*, IEEE Transactions on Information Theory **25** (1979), no. 1, 94–97.

[106] J. Silverman, V.E. Vickers, and J.M. Mooney, *On the number of costas arrays as a function of array size*, Proceedings of the IEEE **76** (1988), no. 7, 851–853.

[107] Mojtaba Soltanalian and Petre Stoica, *Computational design of sequences with good correlation properties*, IEEE Transactions on Signal processing **60** (2012), no. 5, 2180–2193.

[108] Mojtaba Soltanalian, Petre Stoica, and Jian Li, *Search for costas arrays via sparse representation*, 2014 22nd european signal processing conference (eusipco), 2014, pp. 2235–2239.

[109] Junxiao Song, Prabhu Babu, and Daniel P Palomar, *Sequence set design with good correlation properties via majorization-minimization*, IEEE Transactions on Signal Processing **64** (2016), no. 11, 2866–2879.

[110] Petre Stoica, Hao He, and Jian Li, *New algorithms for designing unimodular sequences with good correlation properties*, IEEE Transactions on Signal Processing **57** (2009), no. 4, 1415–1425.

[111] Imants D Svalbe and Andrew Z Tirkel, *Extended families of 2d arrays with near optimal auto and low cross-correlation*, EURASIP Journal on Advances in Signal Processing **2017** (2017), no. 1, 1–19.

[112] Christopher N. Swanson, Bill Correll, and Randy W. Ho, *Enumeration of parallelograms in permutation matrices for improved bounds on the density of costas arrays*, Electron. J. Comb. **23** (2016), no. 1, P1.44.

[113] Nima Tabatabaei, *Matched-filter thermography*, Applied Sciences **8** (2018), no. 4.

[114] Ken Taylor, Konstantinos Drakakis, and Scott Rickard, *Generated, emergent, and sporadic costas arrays*, Ima international conference on mathematics in signal processing at the royal agricultural college," cirencester, uk, 2008.

[115] E.L. Titlebaum and S.V. Maric, *Multiuser sonar properties for costas array frequency hop coded signals*, International conference on acoustics, speech, and signal processing, 1990, pp. 2727–2730.

[116] David Vulakh and Raphael Finkel, *Parallel m-dimensional relative ant colony optimization (mdraco) for the costas-array problem*, Soft Computing **26** (2022), no. 12, 5765–5772.

[117] S Wang, *Efficient heuristic method of search for binary sequences with good aperiodic autocorrelations*, Electronics Letters **44** (2008), no. 12, 731–732.

[118] Lutz Warnke, Bill Correll, and Christopher N. Swanson, *The density of costas arrays decays exponentially*, IEEE Transactions on Information Theory **69** (2023), no. 1, 575–581.

[119] Jane Louise Wodlinger, *Costas arrays, golomb rulers and wavelength isolation sequence pairs*, Master's Thesis, 2012.

[120] Yongbo Xia, Xianglai Zhang, Chunlei Li, and Tor Helleseth, *The differential spectrum of a ternary power mapping*, Finite Fields and Their Applications **64** (2020), 101660.

[121] Yin Xinchun and Liu Tao, *Searching for costas arrays using general particle swarm optimization*, Tencon 2006-2006 ieee region 10 conference, 2006, pp. 1–3.

[122] Guangkui Xu, Xiwang Cao, and Shanding Xu, *Several classes of polynomials with low differential uniformity over finite fields of odd characteristic*, Applicable Algebra in Engineering, Communication and Computing **27** (2016), no. 2, 91–103.

[123] Haode Yan and Dongchun Han, *New ternary power mapping with differential uniformity $\triangle_f \leq 3$ and related optimal cyclic codes*, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences **102** (2019), no. 6, 849–853.

[124] Haode Yan and Zhengchun Zhou, *Power functions over finite fields with low c-differential uniformity*, CoRR **abs/2003.13019** (2020), available at `2003.13019`.

[125] Haode Yan, Zhengchun Zhou, Jian Weng, Jinming Wen, Tor Helleseth, and Qi Wang, *Differential spectrum of kasami power permutations over odd characteristic finite fields*, IEEE Transactions on Information Theory **65** (2019), no. 10, 6819–6826.

[126] Zhengbang Zha and Lei Hu, *Some classes of power functions with low c-differential uniformity over finite fields*, Designs, Codes and Cryptography **89** (2021), no. 6, 1193–1210.