UNIVERSITY OF PUERTO RICO
RÍO PIEDRAS CAMPUS
FACULTY OF NATURAL SCIENCES
DEPARTMENT OF MATHEMATICS

MULTIDIMENSIONAL COSTAS ARRAYS AND PERIODIC PROPERTIES

By

Jaziel Torres Fuentes

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCES IN MATHEMATICS
AT THE UNIVERSITY OF PUERTO RICO

May 5th, 2022

© 2022. All rights reserved.

APPROVED BY THE MASTER OF SCIENCE ADVISORY COMMITTEE

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTER OF SCIENCE IN MATHEMATICS

AT THE UNIVERSITY OF PUERTO RICO

ADVISOR:

Ivelisse M. Rubio Canabal, Ph.D.

University of Puerto Rico, Río Piedras

Department of Computer Sciences

READERS:

Rafael A. Arce Nazario, Ph.D.

University of Puerto Rico, Río Piedras

Department of Computer Sciences

Raúl F. Figueroa Guerrero, Ph.D.

University of Puerto Rico, Río Piedras

Department of Mathematics

José R. Ortiz Ubarri, Ph.D.

University of Puerto Rico, Río Piedras

Department of Computer Sciences

ABSTRACT

Costas arrays were first introduced for SONAR detection applications, but later became an interesting object of mathematical research. Several generalizations of Costas arrays to multiple dimensions have been proposed. In this thesis, we lay the ground for the study of multidimensional Costas arrays by proposing concepts and showing results that extend into the higher-dimensional realm most of what is known about the periodicity of two-dimensional Costas arrays. Among the most important results is, for large classes of arrays, the non-existence of multidimensional Costas arrays that preserve the Costas property in every commensurate window when extended periodically in all directions. We also extend to higher-dimensions the Golomb-Moreno Conjecture that asserts all circular Costas maps are those from the Welch construction, which had been proved in the two-dimensional case. We prove a weaker version of this conjecture in the higher-dimensional context.

Para mi abuelo Nelson Torres y en memoria de mi abuelo Lucas Fuentes,

que hubiesen sido mejores matemáticos de lo que yo jamás pudiera ser.

ACKNOWLEDGEMENTS

The research work that culminates with the present document was funded by "Fondos Institucionales para la Investigación" (FIPI) under the project 2020–2022 Multidimensional Periodic Arrays.

I apologize to those of you reading these pages that do not understand Spanish. Those I want to gratefully acknowledge deserve some words written in my mother tongue.

Entre tantos a los que pudiera agradecer, quiero ser puntual en reconocer aquellos que, de no haber sido parte de estas andanzas a las que llamo vida, esta tesis jamás habría sido escrita. Primeramente, quiero agradecer a la mujer que me regaló la vida: mi madre, Ivette. Gracias por escuchar con tanta atención y paciencia todas las veces que, con desproporcionada emoción, te relataba el problema matemático que al momento me fascinaba o atribulaba. Gracias a Miguel Frau, Maritza Martínez y Juan Mulero, maestros formidables de escuela elemental y superior, que me inspiraron amor por las matemáticas. Un abrazo desmedido a Nunila Dávila, que por tantos años me ha regalado una amistad a la que le debo poco menos que la vida. Mención honorífica se merece mi camarada y secuaz en todas las aventuras matemáticas subgraduadas, Luis Quiñones. Mi más profundo agradecimiento al profesor Heeralal Janwa, por ser mi primer mentor; a quien debo gran parte lo que soy hoy como matemático. Gracias a los miembros del comité de tesis por sus constructivos y puntuales comentarios, que mejoraron grandemente esta tesis.

Finalmente, el mayor de todos mis agradecimientos va para quien he logrado considerar como una segunda madre; mi jefa, consejera y mentora, Ivelisse Rubio. Gracias por todo el tiempo, por la gran confianza depositada en mí, por los consejos, y por ser partícipe y arquitecta de las grandes experiencias matemáticas que perimitieron la escritura de esta tesis, y las que ahora me abren puertas para continuar mi carrera en matemáticas. A todos los muchos que se me quedan: gracias.

Contents

List of Figures **vii**

List of Symbols **viii**

Historical Introduction **1**

Structure and Contributions 8

1 Costas Arrays in Two Dimensions **10**

1.1 Arrays 10

1.2 Difference and Toroidal Vectors 13

1.3 Costas Arrays 25

1.4 Algebraic Constructions 29

1.5 Periodicity of Costas Arrays 31

1.6 Circular Costas 40

1.6.1 Characterizing circular Costas as Welch arrays 51

Summary 54

2 Multidimensional Costas Arrays **55**

2.1 Multidimensional Arrays 56

2.2 Difference and Toridal Vectors 57

2.3 Multidimensional Costas Arrays 59

2.3.1 Previous definitions in the literature 61

2.4 Periodicity of Multidimensional Costas Arrays 64

Summary 82

3 Multidimensional Circular Costas Arrays **83**

3.1 Circular Costas Maps 84

3.2 Costas Polynomials 92

3.3 Counting Costas Polynomials 98

3.4 Shifting Costas Polynomials 102

Summary 107

Epilogue **109**

Some Open Questions 111

Bibliography **113**

List of Figures

1 A Costas array of order 4 corresponding to the sequence $2, 4, 3, 1$. . . 3

1.1 A 3×4 array defined by $A(i, j) = A_{ij}$ as in the first quadrant of the Cartesian plane. 11

1.2 A 6×4 binary array written with '0' and '1', and equivalently with blanks and dots. Its set of dots is $\{(1, 1),\ (1, 4),\ (3, 2),\ (4, 3),\ (6, 2)\}$. 13

1.3 Coincidences between a binary array and a shifted version of itself. . 28

1.4 Three 4×4 binary arrays 29

1.5 Coincidences between a binary array and a shifted version of itself considered as in the plane (b) and as in the torus (c). 32

1.6 The periodic extension of two inequivalent Costas arrays of order $n = 4$, where none is periodic Costas. The original array is shaded in gray, and a 4×4 window with a repeated difference vector has a bold border. 37

2.1 Costas array in Example 1.10 67

2.2 Frequency of toroidal vectors for the array in Figure 2.1 67

2.3 A three-dimensional periodic Costas array 81

3.1 Asymptotic behavior of $R(p, 3)$ 102

List of Symbols

A	multidimensional array; matrix
m	dimension of multidimensional array; degree of a circular Costas map
n	order of a Costas array
Λ	index set of a multidimensional array
$[n]$	set of integers from 1 to n; $\{1, 2, \ldots, n\}$
φ	function defining a Costas array
p	prime number
q	power of a prime
$\mathbb{A}$	periodic extension of multidimensional array
$\mathbb{F}_q$	finite field with q elements
$\mathbb{Z}$	ring of integers
$\mathbb{Z}_n$	ring of integers modulo n
( )	used to write dots of a Costas array

$\langle\ \rangle$	used to write difference and toroidal vectors
α	initial dot of a difference/toroidal vector; primitive root of finite field
ω	end dot of a difference/toroidal vector
$\mathcal{T}_A$	multiset of toroidal vectors occurring in A
$\mathcal{H}_A$	multisubset of $\mathcal{T}_A$ with a component half the length of the array in the corresponding direction
T_Λ	value set of toroidal vectors for arrays with index set Λ
H_Λ	subset of T_Λ with a component half the length of the array in the corresponding direction
G	group
$\mathrm{Aut}(G)$	group of automorphisms of G
$L(x)$	linearized permutation polynomial over a finite field

Historical Introduction

El mundo era tan reciente que muchas cosas carecían de nombre, y para mencionarlas había que señalarlas con el dedo.

—Gabriel García Márquez, *Cien años de soledad*

To detect the distance and velocity of a moving target using active SONAR detection, the observer sends a signal that bounces off the object and is received back by the observer. The signal consist of a series of pulses at frequencies chosen from a set of available frequencies $\{f_1, f_2, \ldots, f_m\}$ that are emitted at each consecutive time intervals $\{t_1, t_2, \ldots, t_n\}$. The round-trip time delay or time shift determines the distance, and the frequency shift of the signal determines the velocity. For practical reasons, it is best to consider the case where $m = n$. In this case, the signal can be represented by an $n \times n$ matrix $A = [a_{ij}]$, where the rows correspond to the frequencies and the columns to the time intervals; a dot is placed in entry a_{ij} if frequency f_i is transmitted at time t_j. Otherwise, a_{ij} is left blank. The observer has to detect the number of coincidences between the sent and the received signal, which is, under ideal conditions, a two-dimensional shift of the original signal. Let $C(r, s)$ denote the number of coincidences between dots from a signal matrix A and A', a shifted version of A, which is shifted r units to the right (to the left if $r < 0$) and s units upward (downward if $s < 0$). It is straightforward to see that

(i) $0 \leqslant C(r, s) \leqslant n$,

(ii) $C(r, s) = n$ if and only if $r = s = 0$, and

(iii) $C(r,s) = 0$ if $|r| > n$ or $|s| > n$.

In the quest to improve the performance of SONAR detection, in a 1965 technical report for the General Electric Company [**2**], John P. Costas concluded that the best signals are those whose number of coincidences for any non-trivial shift is at most one. For hardware constraints, it is best to consider signals consisting of a single pulse at each time interval. A synopsis of the original report was presented in the 1975 Electronics and Aerospace Systems Convention [**3**] and later published in 1984 as a journal article [**4**]. Arrays satisfying the above conditions were originally called *constellation arrays* (see [**1**, Section I; **16**, Section II]), but later acquired the name for which they are known today: *Costas arrays.*

Definition 0.1. A **Costas array** is an $n \times n$ permutation matrix A, i.e., a matrix of blanks and dots such that each row contains exactly one dot, as does each column, satisfying

$$C(r,s) \leqslant 1, \quad \text{for all } (r,s) \in \mathbb{Z}^2 \setminus \{(0,0)\} \tag{0.1}$$

Condition (0.1) is known as the *Costas property.* If $C(r,s) = 1$, there are only two dots in the array for which the vector connecting one dot to the other is equal to $\langle r,s \rangle$. The converse is also true: if there are only two dots at "distance" $\langle r,s \rangle$, then $C(r,s) = 1$. Similarly, $C(r,s) \geqslant 2$ if and only if there are at least two pairs of dots that are at "distance" $\langle r,s \rangle$ of each other: the dots that account for the coincidences between those from the array A and those from the superimposed copy of A shifted r units horizontally and s units vertically. As a consequence, the Costas property (0.1) can be equivalently expressed as:

All the vectors connecting two dots from the array are distinct as vectors (no two are equal in both length and slope). (0.2)

A permutation matrix of order n naturally defines a bijection

$$\varphi : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\},$$

where $\varphi(i) = j$ if and only if there is a dot in position (i, j). Given such bijection, one can consider the sequence of images $\varphi(1), \varphi(2), \ldots, \varphi(n)$. Thus J. P. Costas' problem of finding permutation matrices with $C(r, s) \leqslant 1$ can be equivalently expressed in terms of sequences. For it, there must be a translation of the Costas property (0.1), or equivalently (0.2), to sequences.

Definition 0.2. A sequence $a_0, a_1, \ldots, a_{n-1}$ which is a permutation of the integers $1, 2, \ldots, n$ is a **Costas sequence** if it satisfies: for any $k \in \{1, 2, \ldots, n-1\}$,

$$a_{i+k} - a_i = a_{j+k} - a_j \implies i = j \tag{0.3}$$

for all i, j with $0 \leqslant i, j \leqslant n - 1 - k$.

Condition (0.3) is called the *distinct difference property.* It is straightforward to verify that a permutation sequence has the distinct difference property if and only if it defines a Costas array.

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

Figure 1: A Costas array of order 4 corresponding to the sequence $2, 4, 3, 1$.

One can verify the distinct difference property, and hence that a sequence is Costas, if every row in the sequence's difference triangle has no repeated terms. The first row of the difference triangle is filled by taking differences between adjacent terms. The second row is filled with differences between next-to-adjacent terms and so on. In symbols, the k-th row of the difference triangle contains $a_{i+k} - a_i$ for

k	**2**	**4**	**3**	**1**
1	2	-1	-2	
2	1	-3		
3	-1			

Table 1: Difference triangle for the Costas sequence $2, 4, 3, 1$.

$i = 0, 1, \ldots, n-1-k$, where $1 \leqslant k \leqslant n-1$. In each row, the differences must be unique; otherwise, the sequence is not Costas.

Although originally studied solely for application purposes, Costas arrays became an interesting object of mathematical research. As J. P. Costas recounted in [**4**, Section II], in a private correspondence that took place at least before 1982[I], Solomon W. Golomb affirmed that sequences as in Definition 0.2 had apparently not been studied and gave three conjectures regarding Costas sequences[II]:

1. *Costas sequences exist for every natural n.*
2. *The number of Costas sequences will grow with n.*
3. *The density of Costas sequences among permutations will go to zero as n goes to infinity.*

As of today, the first conjecture of Golomb is still open. The second conjecture was proven false by computation in 1988 [**29**]. In the late 1980's, the third one was proven true independently by Benjamin Weiss, Victor Reiner, and D. Huw Davies[III].

The first systematic procedures to construct Costas arrays, known at least since 1982, rely on primitive elements of finite fields and are due to Lloyd R. Welch,

[I] Costas mentions the correspondence with Golomb in the 1984 article [**4**], but the correspondence is also mentioned by Golomb in [**16**, Section II], published in 1982.

[II] In addition to the recount given in [**4**, Section II], these conjectures are formally stated in [**17**, Section II] as open problems #1, #2, and #5, respectively.

[III] We were not able to find the original sources. Nonetheless, the work by Weiss and Reiner is acknowledged by Golomb in [**13**, Appendices p. 14] while the work by Davies is acknowledged by Konstantinos Drakakis in [**6**, Section 4.2] and [**8**, Section 4.2]. Interestingly, in the recent preprint [**31**], the authors proved that the density of Costas arrays decays exponentially.

Abraham Lempel, and Solomon W. Golomb [**12**]. As of today, all Costas arrays constructed systematically are obtained from those three constructions or particular modifications of them, mainly removing or adding dots. In this thesis, we only discuss the three main constructions in Section 1.4; for the modifications see [**17**, Section II].

In a 1984 article, Solomon W. Golomb and Herbert Taylor [**17**, Section III.A] considered some periodic properties of Costas arrays. In particular, they mentioned:

> Repeating the 2×2 Costas array in both directions over the entire plane gives a doubly periodic checkerboard pattern with a Costas array in every 2×2 window. For any $n > 2$, however, there does not exist a doubly periodic pattern with a Costas array in every $n \times n$ window. [**17**, p. 1154]

The above result was proven by Herbert Taylor in 1984 [**30**].

On the other hand, singly periodical patterns do exist. That is, repeating an $n \times n$ array horizontally to obtain an array with n rows and infinite columns such that every $n \times n$ window is a Costas array. However, the only known arrays producing singly periodical patterns are those obtained from the Welch construction, which leads Golomb and Taylor to conjecture that those are indeed the only ones (problem #8 in [**17**, Section V]). This conjecture, published in 1984, is still open:

Conjecture 0.3 (Golomb & Taylor [**17**])**.** *A Costas array is singly periodical if and only if it is Welch.*

Making progress towards Conjecture 0.3, in 1992, Oscar Moreno [**21**] proved that a condition he called the *shifting property*, which is stronger than single periodicity, characterizes the Welch construction. It is defined as follows: for a Costas sequence $a_0, a_1, \ldots, a_{n-1}$, consider the circular differences

$$a_{0+k} - a_0, \quad a_{1+k} - a_1, \quad \ldots, \quad a_{n-1+k} - a_{n-1}, \tag{0.4}$$

where the indices $i+k$ are considered modulo n. The Costas sequence is said to have the shifting property if, for each $k = 1, 2, \ldots, n-1$, the circular differences in (0.4) considered modulo $n+1$ are a shift of the original sequence.

Four years later, in 1996, Golomb and Moreno presented a weaker version of Conjecture 0.3 using a condition called *circular*, which lies between single periodicity and the shifting property [**15**, Conjecture 1]. That is, the condition of being circular is stronger than single periodicity, yet weaker than the shifting property, or, using implication arrows:

$$\textit{shifting property} \implies \textit{circular} \implies \textit{singly periodic.}$$

A Costas sequence $a_0, a_1, \ldots, a_{n-1}$ is said to be *circular* if the circular differences in (0.4) are distinct modulo $n+1$, for each $k = 1, 2, \ldots, n-1$.

Conjecture 0.4 (Golomb & Moreno [**15**])**.** *A Costas sequence is circular if and only if it is Welch.*

It is easy to verify that the Welch construction yields circular Costas sequences, all of length $p-1$, where p is a prime. In the same 1996 article, Golomb and Moreno showed that if a Costas sequence is circular, it must be of length $p-1$ [**15**, Theorem 1], which is consistent with the length of the Welch sequences, thus making progress towards Conjecture 0.4. Nevertheless, a complete proof remained elusive for many years.

Several generalizations of the Welch construction have been proposed throughout the years, which yield generalized analogs of Costas arrays. For example, Golomb and Gong in 2007 [**14**, Construction A]; Drakakis in 2008 [**7**, Theorem 2]; Moreno and Tirkel in 2011 [**22**, Secton III.B]. In 2013, José Ortiz Ubarri, together with Oscar Moreno, Andrew Z. Tirkel, Rafael A. Arce, and Solomon W. Golomb [**24**], gave a definition of multidimensional periodic Costas arrays over finite abelian groups that is a higher-dimensional generalization of the circular property defined by Golomb and

Moreno for two-dimensional Costas arrays. Moreover, they showed that a multidimensional analog of the Welch construction yields Costas arrays having the higher-dimensional circular property.

In April 2013, Ortiz Ubarri and Moreno went to the International Workshop on Finite Fields Constructions of Combinatorial Arrays, held in Florianópolis, Brazil, where they presented their research set forth in [**24**]. Their conjecture sparked the interest of several researchers attending the workshop. The interest triggered discussions on different approaches to the conjecture, later called by the attendees "the Florianópolis problem". One approach was translating the problem from Costas arrays to difference sets and using character theory to tackle it. This approach was successful as, in 2015, a group of researchers, some of who attended the workshop at Florianópolis, finally solved Conjecture 0.4 affirmatively [**23**, Theorem 3.4].

To summarize, these are, to the best of our knowledge, the main results regarding periodic properties of Costas arrays:

1. For $n > 2$, there are no doubly periodic patterns having a Costas array in every $n \times n$ window [**30**, Theorem B].
2. There are three instances of periodicity of Costas arrays: singly periodical, circular, and those with the shifting property, where

$$\text{shifting property} \implies \text{circular} \implies \text{singly periodical.}$$

3. All arrays with the shifting property are Welch arrays [**21**, Theorem].
4. All circular Costas arrays are Welch arrays [**23**, Theorem 3.4].
5. All singly periodic patters are conjectured to be Welch arrays [**17**, Unsolved problem 8, p. 1161].

Can the definition of a Costas array be extended to higher dimensions? What

happens with the periodic properties of those higher-dimensional Costas arrays? Do the results summarized above extend? Which do not and why? These questions started a research endeavor culminating with the present document.

Structure and Contributions

At large, this thesis provides a suitable definition for higher-dimensional Costas arrays. It establishes a framework for studying the periodic properties of multidimensional Costas arrays that is consistent with what is known for (two-dimensional) Costas arrays. We follow the trail left by J. P. Costas, S. W. Golomb, O. Moreno, H. Taylor, and many others who studied Costas arrays before us.

The structure of the thesis is as follows. We already gave a historical introduction narrating the main developments in the study of Costas arrays and their periodic properties; we introduced and showed the path we want to walk once more, but for higher-dimensional Costas arrays. Nonetheless, some definitions and proofs do not generalize straightforwardly. In Chapter 1, the theory of two-dimensional Costas arrays is revisited, and some of the original definitions are rewritten in equivalent ways that are easier to extend into higher dimensions. The last sections of Chapter 1 are devoted to studying two types of periodicity of Costas arrays: integral and modular periodicity. These periodic properties have been studied, but not much emphasis has been given in the literature. The study of higher-dimensional Costas arrays starts in Chapter 2, where multidimensional Costas arrays are defined and some of the results on integral periodicity are presented. Chapter 3 is dedicated to multidimensional circular Costas arrays, a type of multidimensional Costas arrays exhibiting a particular modular periodicity. The thesis ends with an Epilogue, synthesizing the main results.

The main contribution of this thesis is a framework of definitions and results for the further study of multidimensional Costas arrays. We where able to combine in

a cohesive and coherent narrative the definitions for *permutation Costas hypercubes* [**7**], *multidimensional periodic Costas arrays* [**24**], and *Costas polynomials* over extension fields [**23**]; independent and apparently unrelated higher-dimensional analogs of Costas arrays. In addition to the survey-like framework, this thesis contributes to the study of Costas arrays with the following original concepts and results:

1. A new proof for the result of Taylor [**30**] stating that periodic Costas arrays must have order 2; Theorem 1.32.

2. A novel definition for multidimensional Costas arrays; Definition 2.13.

3. Multidimensional modular Costas arrays do not exist; Theorem 2.25.

4. Multidimensional Costas arrays of odd order are not periodic Costas; Theorem 2.27.

5. "Large" multidimensional Costas arrays of even order and one-dimensional image are not periodic Costas; Theorem 2.30.

6. Three-dimensional periodic Costas arrays must have order 4; Theorem 2.32. This is a three-dimensional analog of Taylor's theorem [**30**].

7. A definition of a higher-dimensional analog of circular Costas arrays; Definition 3.1.

8. The establishment of two conjectures and the partial solution of a third conjecture by Ortiz-Ubarri et al. [**24**]; Theorem 3.12, Corollary 3.29, and Proposition 3.30, respectively.

9. The characterization of shifting Costas polynomials as multidimensional Welch; Theorem 3.34. This proves a weaker version of the higher-dimensional analog of the Golomb-Moreno Conjecture [**15**].

Chapter 1

Costas Arrays in Two Dimensions

Yes, he said, there is a remarkable charm in them. But I do not clearly understand the change in the order. First you began with a geometry of plane surfaces? Yes, I said.

—Plato, *Republic*

In this chapter, we present the foundation upon which we will build, in later chapters, a multidimensional theory of Costas arrays and their periodic properties. Assuming the calculated risk of stating the obvious, several concepts discussed in the Introduction are redefined in slightly different terms, making the definitions and results easy to extend into higher dimensions.

1.1 Arrays

Definition 1.1. For positive integers n_1 and n_2, an **array** of size $n_1 \times n_2$ over a set X is a function $A : \Lambda \to X$, where Λ is the rectangular subset of $\mathbb{N}^2$ given by

$$\Lambda = \big\{(a_1, a_2) \in \mathbb{N}^2 \,:\, a_1 \leqslant n_1 \text{ and } a_2 \leqslant n_2\big\}.$$

We say that Λ is the **index set** for the array A.

With the usual notation $[n] = \{1, 2, \ldots, n\}$, the index set of an $n_1 \times n_2$ array is the Cartesian product $\Lambda = [n_1] \times [n_2]$. An array is nothing more than a table or a matrix, but we make the following distinction for convenience: n_1 is the number of columns, and n_2 is the number of rows; matrices use the opposite convention. The reason for us not to use the matrix convention is because we see arrays as finite and rectangular subsets of the integer lattice living in the first quadrant of the Euclidean plane $\mathbb{R}^2$, so we will label the entries as coordinates of the first quadrant of the plane.

$$A = \begin{array}{|c|c|c|} \hline A_{14} & A_{24} & A_{34} \\ \hline A_{13} & A_{23} & A_{33} \\ \hline A_{12} & A_{22} & A_{32} \\ \hline A_{11} & A_{21} & A_{31} \\ \hline \end{array}$$

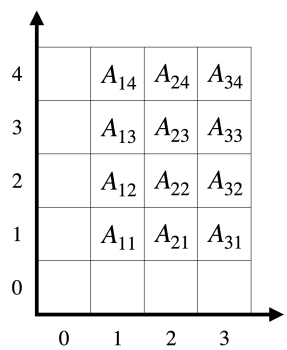


Figure 1.1: A 3×4 array defined by $A(i, j) = A_{ij}$ as in the first quadrant of the Cartesian plane.

Definition 1.2. Let A be an $n_1 \times n_2$ array with index set $\Lambda = [n_1] \times [n_2]$. For $\alpha = (a_1, a_2) \in \mathbb{Z}^2$, define $\alpha_\Lambda = (a_1', a_2') \in \Lambda$ to be the unique tuple in Λ for which

$$a_1' \equiv a_1 \pmod{n_1}, \quad \text{and} \quad a_2' \equiv a_2 \pmod{n_2}.$$

We want to emphasize that α_Λ must be an element of Λ, so $a_1' \neq 0$ and $a_2' \neq 0$. For example, if A is a 6×5 array and $\alpha = (8, 10)$, then $\alpha_\Lambda = (2, 5)$. In other words, to obtain α_Λ we reduce the i-th coordinate of α modulo n_i, but mapping 0 to n_i. We can define a_1' and a_2' in the definition above equivalently with the expressions

$$a_1' = (a_1 - 1 \bmod n_1) + 1 \quad \text{and} \quad a_2' = (a_2 - 1 \bmod n_2) + 1,$$

where $a_i - 1 \bmod n_i$ is the reminder of $a_i - 1$ when divided by n_i, hence an integer

between 0 and n_i.

Remark 1.3. Throughout this thesis, we primarily use the expression "$x \bmod n$" to represent the remainder of x when divided by n. Hence, "$x \bmod n$" is an integer between 0 and $n-1$, including both. Nonetheless, we write $y \equiv x \pmod{n}$ to indicate that x and y have the same residue when divided by n (see Definition 1.2 above and the proof of Lemma 1.11 below). Our rule of thumb: "$x \bmod n$" is the reminder itself unless we use the symbol "$\equiv$" and the modulo in parenthesis, in which case we are comparing reminders.

Definition 1.4. Let A be an $n_1 \times n_2$ array over a set X with index set $\Lambda = [n_1] \times [n_2]$. The **periodic extension** of A is the infinite array $\mathbb{A} : \mathbb{Z}^2 \to X$ defined by

$$\mathbb{A}(\alpha) = A(\alpha_\Lambda) \qquad \forall \alpha \in \mathbb{Z}^2.$$

For an $n_1 \times n_2$ array A, its periodic extension $\mathbb{A}$ contains at most $n_1 n_2$ distinct windows[I] of size $n_1 \times n_2$, and these windows are repeated infinitely and periodically in the whole plane. One set of these possibly distinct windows of $\mathbb{A}$ is the set of arrays with index set

$$\{\Lambda + (x, y) \,:\, 0 \leqslant x \leqslant n_1 - 1 \text{ and } 0 \leqslant y \leqslant n_2 - 1\},$$

where $\Lambda + (x, y) = \{(a_1 + x, a_2 + y) \in \mathbb{Z}^2 \,:\, (a_1, a_2) \in \Lambda\}$.

We will only focus on binary arrays: arrays for which $X = \{0, 1\}$. Binary arrays are usually represented as arrays of blanks and dots, where a blank represents '0' and a dot represents '1'. Our object of study is a particular type of binary array, called Costas arrays, defined in due course, which has a lot more blanks than dots. Knowing what awaits on the horizon, we will only care about the positions in which

[I] By a "window" we mean a subarray of $\mathbb{A}$, that is, the restriction of the domain of $\mathbb{A}$ to a rectangular subset of $\mathbb{Z}^2$. However, we will stick to the noun "window" for it is visually intuitive.

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

4	●					
3				●		
2			●			●
1	●					
	1	2	3	4	5	6

Figure 1.2: A 6×4 binary array written with '0' and '1', and equivalently with blanks and dots. Its set of dots is $\{(1,1),\ (1,4),\ (3,2),\ (4,3),\ (6,2)\}$.

the binary array has a dot, thus the following definition.

Definition 1.5. Let A be a binary array with index set Λ. An element $\alpha \in \Lambda$ is called a **dot of** A if $A(\alpha) = 1$.

We can know the whole map defining a binary array if we know its index set, i.e., its size, and its set of dots, because dots are mapped to '1,' and the remaining coordinates are mapped to '0'. In this context we will abuse notation and, for a binary array $A : \Lambda \to \{0,1\}$ and $\alpha \in \mathbb{Z}^2$, we write $\alpha \in A$ if α is a dot of A. Notice that using our convention, if $A(\alpha) = 0$, then $\alpha \notin A$, even when $\alpha \in \Lambda$. To dissipate any confusion, we reinstate our notation.

Definition 1.6. Let $A : \Lambda \to \{0,1\}$ be a binary array, and let $\alpha \in \mathbb{Z}^2$. We say that α is **in** A or that α **belongs to** A, and write $\alpha \in A$, if and only if $A(\alpha) = 1$.

1.2 Difference and Toroidal Vectors

In this section, we consider binary arrays for generality. Still, we care about these results only because they can be applied to Costas arrays, formally defined in due course. Nevertheless, such generality will prove helpful in our ultimate quest of generalizing to higher dimensions various results that are known for Costas arrays in two dimensions.

Definition 1.7. For two distinct dots $\alpha = (a_1, a_2)$ and $\omega = (w_1, w_2)$ in a binary array A, the **difference vector** from α to ω is the vector

$$\langle w_1 - a_1,\ w_2 - a_2 \rangle.$$

To avoid confusion, we will write ordered pairs (and later m-tuples) with parenthesis ( ), and vectors with angled brackets $\langle\ \rangle$.

For each pair of dots in a binary array, we have two, possibly distinct, difference vectors joining them: from α to ω and vice versa. Hence, the number of difference vectors occurring in a binary array with n dots is $2\binom{n}{2} = n(n-1)$. In an arbitrary binary array A of size $n_1 \times n_2$, all difference vectors $\langle h_1, h_2 \rangle$ must satisfy

$$-(n_1 - 1) \leqslant h_1 \leqslant n_1 - 1 \quad \text{and} \quad -(n_2 - 1) \leqslant h_2 \leqslant n_2 - 1.$$

For permutation arrays, and in particular, Costas arrays, since there are no two dots in the same column nor two dots in the same row, the difference vectors must have $h_1 \neq 0$ and $h_2 \neq 0$.

When considering periodic extensions, a modular version of difference vectors is extremely helpful.

Definition 1.8 ([**18**, Definition 1.5])**.** Let A be an $n_1 \times n_2$ binary array. The **toroidal vector** from the dot $\alpha = (a_1, a_2) \in A$ to the dot $\omega = (w_1, w_2) \in A$, is the vector

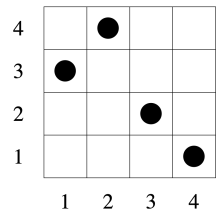
$$\langle w_1 - a_1 \bmod n_1,\ w_2 - a_2 \bmod n_2 \rangle.$$

Remark 1.9. To avoid degenerate cases, we assume the dots α and ω in Definitions 1.7 and 1.8 are distinct, i.e., $\alpha \neq \omega$.

Toroidal vectors are just difference vectors taken modulo the size of the array. That is, we let the vectors wrap around as if the array is written on the surface of

a torus. As with difference vectors, for a binary array with n dots, the number of toroidal vectors is $n(n-1)$, counting repetitions.

Example 1.10. Consider the 4×4 binary array:



It has four dots, $\{(1,3),\ (2,4),\ (3,2),\ (4,1)\}$. There are $4(4-1) = 12$ difference vectors and 12 toroidal vectors. All the difference vectors are

$$\langle 1,1\rangle \quad \langle 2,-1\rangle \quad \langle 3,-2\rangle \quad \langle -1,-1\rangle \quad \langle 1,-2\rangle \quad \langle 2,-3\rangle$$

$$\langle -2,1\rangle \quad \langle -1,2\rangle \quad \langle 1,-1\rangle \quad \langle -3,2\rangle \quad \langle -2,3\rangle \quad \langle -1,1\rangle.$$

The toroidal vectors are

$$\langle 1,1\rangle\ \langle 2,3\rangle\ \langle 3,2\rangle\ \langle 3,3\rangle\ \langle 1,2\rangle\ \langle 2,1\rangle\ \langle 2,1\rangle\ \langle 3,2\rangle\ \langle 1,3\rangle\ \langle 1,2\rangle\ \langle 2,3\rangle\ \langle 3,1\rangle.$$

The periodic extension of a binary array is defined by taking the coordinates modulo the size of the array, so it is natural to explore the relationship between toroidal vectors of a binary array and its periodic extension.

Lemma 1.11. *Let A be an $n_1 \times n_2$ binary array and $\mathbb{A}$ its periodic extension to $\mathbb{Z}^2$. If S is an $n_1 \times n_2$ window of $\mathbb{A}$, A and S have the same multiset of toroidal vectors.*

Proof. Let A be an $n_1 \times n_2$ binary array with index set $\Lambda = [n_1] \times [n_2]$ and S an $n_1 \times n_2$ window of the periodic extension of A, $\mathbb{A} : \mathbb{Z}^2 \to \{0,1\}$. Then, for some $(k_1, k_2) \in \mathbb{Z}^2$, S is the restriction of the domain of $\mathbb{A}$ to the set

$$D = \big\{(d_1, d_2) \in \mathbb{Z}^2 \,:\, k_1 \leqslant d_1 \leqslant k_1 + n_1 - 1 \text{ and } k_2 \leqslant d_2 \leqslant k_2 + n_2 - 1\big\}.$$

Define

$$\varphi_1 : [n_1] \to \{k_1,\ k_1+1,\ \ldots,\ k_1+n_1-1\}$$

and

$$\varphi_2 : [n_2] \to \{k_2,\ k_2+1,\ \ldots,\ k_2+n_2-1\},$$

by the rule

$$\varphi_1(a_1) = a_1' \iff a_1' \equiv a_1 \pmod{n_1} \quad \text{and} \quad \varphi_2(a_2) = a_2' \iff a_2' \equiv a_2 \pmod{n_2}.$$

Clearly φ_1 and φ_2 are bijections. Set $\varphi : \Lambda \to D,\ (a_1, a_2) \mapsto (\varphi_1(a_1), \varphi_2(a_2))$. By the definition of periodic extension, for $\alpha \in \Lambda$, $A(\alpha) = 1$ if and only if $\mathbb{A}(\varphi(\alpha)) = 1$, so φ is a bijection between the dots of A and the dots of S. Therefore, $\omega - \alpha$ is a difference vector in A if and only if $\varphi(\omega) - \varphi(\alpha)$ is a difference vector in S. By the definition of φ_1 and φ_2, the toroidal vector from α to ω is equal to the toroidal vector from $\varphi(\alpha)$ to $\varphi(\omega)$. This shows that A and S have the same multiset of toroidal vectors. □

Proposition 1.12. *Let A be an $n_1 \times n_2$ binary array and $\mathbb{A}$ its periodic extension to $\mathbb{Z}^2$. If an $n_1 \times n_2$ window of $\mathbb{A}$ has a repeated difference vector, then A has a repeated toroidal vector.*

Proof. Let S be a window of $\mathbb{A}$ with size $n_1 \times n_2$ with repeated difference vector $\langle h_1, h_2 \rangle \in \mathbb{Z}^2$. Then $\langle h_1 \bmod n_1,\ h_2 \bmod n_2 \rangle$ is a repeated toroidal vector of S hence, by Lemma 1.11, a repeated toroidal vector of A. □

For the implication in the opposite direction of Proposition 1.12, we need an additional condition.

Proposition 1.13. *Let A be an $n_1 \times n_2$ binary array and $\mathbb{A}$ its periodic extension to $\mathbb{Z}^2$. If A has a repeated toroidal vector $\langle h_1, h_2 \rangle$ with $h_1 \neq n_1/2$ and $h_2 \neq n_2/2$, there is an $n_1 \times n_2$ window of $\mathbb{A}$ having a repeated difference vector.*

The idea for the proof is the following. We will construct two equal difference vectors component by component. The repeated toroidal vectors yield two difference vectors that may not be equal, but are equal after taking modulo. First, we consider the horizontal (first) component of those difference vectors; that is, their projection onto the x-axis. The original vectors are in A, so those components are already in a window of width n_1. Therefore, if both are equal, we use those same components for the difference vectors. Otherwise, the components point in opposite directions, and in such case we need to "flip" one of the components by changing the starting or finishing point; we do that by adding or subtracting n_1. Which component to flip and whether to change the starting or the finishing point depends on the configuration, because we want to keep both components in a window of width n_1. After choosing the suitable horizontal components, we do the same for the vertical components. After the proof, we go through the procedure with an example, hoping to clarify the imbroglio of inequalities. Now the proof.

Proof of Proposition 1.13. Let A be a binary array with index set $\Lambda = [n_1] \times [n_2]$, and let $\mathbb{A}$ be its periodic extension to $\mathbb{Z}^2$. Assume that $\langle h_1, h_2 \rangle$ appears (at least) twice as a toroidal vector of A, with $0 \leqslant h_1 \leqslant n_1 - 1$ and $0 \leqslant h_2 \leqslant n_2 - 1$. Then, we have two distinct pairs of distinct dots of A,

$$\alpha_1 = (a_{11},\ a_{12}),\ \omega_1 = (w_{11},\ w_{12}) \quad \text{and} \quad \alpha_2 = (a_{21},\ a_{22}),\ \omega_2 = (w_{21},\ w_{22})$$

such that

$$\begin{aligned}\langle w_{11} - a_{11} \bmod n_1,\ w_{12} - a_{12} \bmod n_2 \rangle &= \langle w_{21} - a_{21} \bmod n_1,\ w_{22} - a_{22} \bmod n_2 \rangle \\ &= \langle h_1,\ h_2 \rangle.\end{aligned}$$

We need to show that there are two distinct pairs of distinct dots of $\mathbb{A}$

$$\alpha_1' = (a_{11}',\ a_{12}'),\ \omega_1' = (w_{11}',\ w_{12}') \quad \text{and} \quad \alpha_2' = (a_{21}',\ a_{22}'),\ \omega_2' = (w_{21}',\ w_{22}')$$

satisfying

(i) $w_{1i}' - a_{1i}' = w_{2i}' - a_{2i}'$, and

(ii) $k_i \leqslant a_{1i}', w_{1i}', a_{2i}', w_{2i}' \leqslant k_i + n_i - 1$, for some $k_i \in \mathbb{Z}$.

If, for $i = 1$ and $i = 2$, we can show that it is possible to pick four values satisfying (i) and (ii), then we are done, making sure that at the end we have four dots of $\mathbb{A}$.

Let us focus on the first coordinates. Notice that $\alpha_1, \omega_1 \in \Lambda$, hence $-(n_1-1) \leqslant w_{11} - a_{11} \leqslant n_1 - 1$. Therefore, $h_1 = (w_{11} - a_{11}) \bmod n_1$ implies $w_{11} - a_{11} = h_1$ or $w_{11} - a_{11} = h_1 - n_1$. Similarly, $w_{21} - a_{21} = h_1$ or $w_{21} - a_{21} = h_1 - n_1$. If $w_{11} - a_{11} = w_{21} - a_{21}$, we set

$$a_{11}' = a_{11}, \quad w_{11}' = w_{11}, \quad a_{21}' = a_{21}, \quad \text{and} \quad w_{21}' = w_{21}. \tag{1.1}$$

These four values satisfy (i) and (ii) with $k_1 = 0$.

Otherwise, $w_{11} - a_{11} \neq w_{21} - a_{21}$ so one difference is equal to h_1 and the other one is equal to $h_1 - n_1$. Notice that if $h_1 = 0$, we must have $w_{11} - a_{11} = w_{21} - a_{21} = 0$, thus we suppose $h_1 > 0$. Without loss of generality, we may assume $w_{11} - a_{11} = h_1 - n_1$ and $w_{21} - a_{21} = h_1$. Hence

$$w_{11} - a_{11} < 0 \implies w_{11} \leqslant a_{11} - 1, \quad \text{and} \tag{1.2}$$

$$w_{21} - a_{21} > 0 \implies a_{21} \leqslant w_{21} - 1. \tag{1.3}$$

There are three cases: $a_{11} \leqslant w_{21} - 1$, $w_{21} \leqslant a_{11} - 1$ or $a_{11} = w_{21}$.

Case 1. If $a_{11} \leqslant w_{21} - 1$, we set

$$a'_{11} = a_{11}, \quad w'_{11} = w_{11}, \quad a'_{21} = a_{21}, \quad \text{and} \quad w'_{21} = w_{21} - n_1 \leqslant 0.$$

Notice that $w'_{11} - a'_{11} = w'_{21} - a'_{21} = h_1 - n_1$, so (i) is satisfied. We claim that (ii) is satisfied with $k_1 = w'_{21}$. Indeed, by inequality (1.3) and the assumption $a_{11} \leqslant w_{21} - 1$, we have

$$a'_{11},\ a'_{21} \leqslant w_{21} - 1 = w'_{21} + (n_1 - 1)$$

By the above and (1.2), we also have $w'_{11} \leqslant w'_{21} + (n_1 - 1)$. Therefore,

$$w'_{21} \leqslant a'_{11}, w'_{11}, a'_{21}, w'_{21} \leqslant w'_{21} + n_1 - 1,$$

proving the claim.

Case 2. If $w_{21} \leqslant a_{11} - 1$, we set

$$a'_{11} = a_{11} - n_1 \leqslant 0, \quad w'_{11} = w_{11}, \quad a'_{21} = a_{21}, \quad \text{and} \quad w'_{21} = w_{21}. \tag{1.4}$$

In this case, $w'_{11} - a'_{11} = w'_{21} - a'_{21} = h_1$, so that (i) is satisfied. With an argument analogous to the one in Case 1 we can show that these values satisfy (ii) with $k_1 = a'_{11}$.

Case 3. If $w_{21} = a_{11}$ we have to consider two different cases: $h_1 < n_1/2$ or $n - h_1 < n_1/2$ (the case $h_1 = n_1/2$ does not happen by hypothesis).

Case 3a. If $h_1 < n_1/2$, we set

$$a'_{11} = a_{11}, \quad w'_{11} = w_{11} + n_1, \quad a'_{21} = a_{21}, \quad \text{and} \quad w'_{21} = w_{21}.$$

Condition (i) is satisfied because $w'_{11} - a'_{11} = w'_{21} - a'_{21} = h_1$. To see condition (ii),

we note that $w_{21} = a_{11}$, and (1.3) imply

$$a_{21} < w_{21} = a_{11} < w_{11} + n_1.$$

We have

$$w'_{11} - a'_{21} = (w'_{11} - a'_{11}) + (a'_{11} - a'_{21}) = (w'_{11} - a'_{11}) + (w'_{21} - a'_{21}) = h_1 + h_1.$$

Therefore, $w'_{11} - a'_{21} \geqslant 0$, hence $a'_{21} \leqslant w'_{11}$. On the other hand, $w'_{11} - a'_{21} = h_1 + h_1 < n_1$ so that $w'_{11} < a'_{21} + n_1$. Using (1.3) we conclude

$$a'_{21} \leqslant a'_{11}, w'_{11}, a'_{21}, w'_{21} \leqslant a'_{21} + n_1 - 1,$$

and (ii) is satisfied with $k_1 = a'_{21}$.

Case 3b. If $n_1 - h_1 < n_1/2$ we set

$$a'_{11} = a_{11}, \quad w'_{11} = w_{11}, \quad a'_{21} = a_{21} + n_1, \quad \text{and} \quad w'_{21} = w_{21}.$$

Condition (i) is satisfied because $w'_{11} - a'_{11} = w'_{21} - a'_{21} = h_1 - n_1$. As in Case 3a, we have

$$w_{11} < a_{11} = w_{21} < a_{21} + n_1.$$

Also $a'_{21} - w'_{11} = (a'_{21} - w'_{21}) + (a'_{11} - w'_{11}) = (n_1 - h_1) + (n_1 - h_1) < n_1$, implying $w'_{11} \leqslant a'_{21}$ and $a'_{21} < w'_{11} + n_1$. Hence

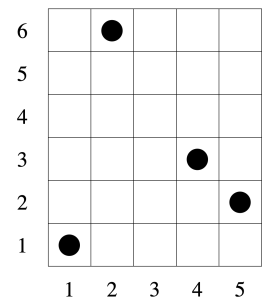
$$w'_{11} \leqslant a'_{11}, w'_{11}, a'_{21}, w'_{21} \leqslant w'_{11} + n_1 - 1,$$

and (ii) is satisfied with $k_1 = w'_{11}$.

In a similar fashion we choose the second coordinates. At the end, by adding

or subtracting n_i to one of the i-th coordinates of the original points in A, namely α_1, ω_1 and α_2, ω_2, we obtained four dots α_1', ω_1' and α_2', ω_2' in $\mathbb{A}$ with equal difference vectors, and both vectors fitting in an $n_1 \times n_2$ window. This finishes the proof. $\square$

The procedure in the above proof is far more simple and intuitive than what it appears. We go through it with an example. Consider the following binary array.



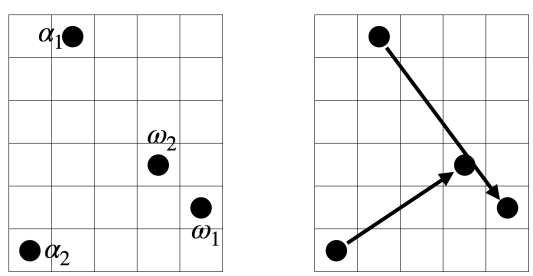
This is a 5×6 array with dots

$$(1,1) \quad (2,6) \quad (4,3) \quad (5,2).$$

All the 12 toroidal vectors (counting multiplicities) occurring in the array are:

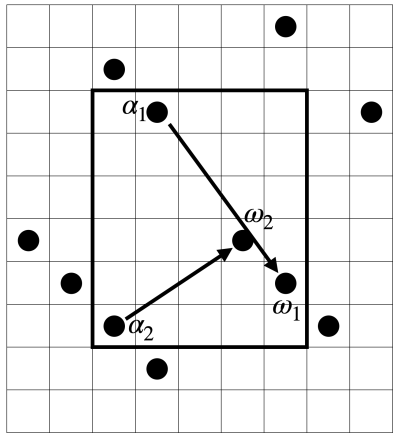
$$\langle 1,5\rangle \ \langle 3,2\rangle \ \langle 4,1\rangle \ \langle 4,1\rangle \ \langle 2,3\rangle \ \langle 3,2\rangle \ \langle 2,4\rangle \ \langle 3,3\rangle \ \langle 1,5\rangle \ \langle 1,5\rangle \ \langle 2,4\rangle \ \langle 4,1\rangle.$$

Notice that the vector $\langle 3,2\rangle$ is repeated. Two difference vectors producing the same toroidal vector $\langle 3,2\rangle$ are the following:



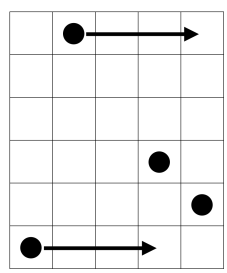
We will find a 5×6 window in the periodic extension of the array with a repeated difference vector. That is, we will find four dots in the periodic extension corresponding to the two starting and two finishing dots defining the same difference vector, all

four fitting in a 5×6 window. Here a part of the periodic extension and the original array window:

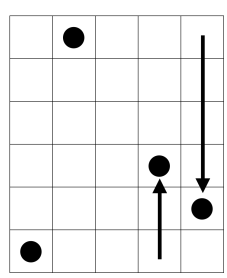


Our candidate dots are the four dots $\alpha_1, \alpha_2, \omega_1, \omega_2$. Of course these dots do not produce a repeated difference vector because $\omega_1 - \alpha_1 \neq \omega_2 - \alpha_2$. We have to "flip" one of the dots horizontally or vertically to produce two equal difference vectors.

Consider the horizontal components:

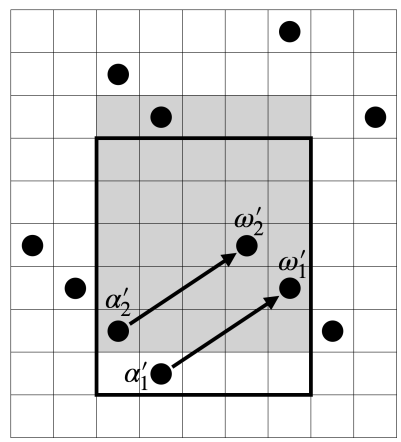


We do nothing since the horizontal components are equal (as vectors). In the proof, all the first coordinates of the candidate points are equal to the original points; see (1.1). Now consider the vertical components:



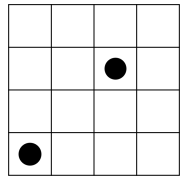
Those are pointing in opposite directions, so we have to flip one of them. Which vector to flip depends on the configuration and hence the cases in the proof. This

configuration corresponds to Case 2: the starting point of the first vector (second coordinate of α_1, which is 6) is greater than the finishing point of the second vector (second coordinate of ω_2, which is 3). In this case, we flip the first vector by changing the starting dot to the corresponding dot in the periodic copy of the array below the original array. We do it by subtracting n to the second coordinate of α_1, so that $\alpha_1' = (1, 0)$ (see (1.4)). Finally, a 5×6 window with a repeated difference vector is the original window shifted down so that the dot α_1' is at the bottom. In this case, the original array window is shifted down one unit (the original array window appears in gray for reference).

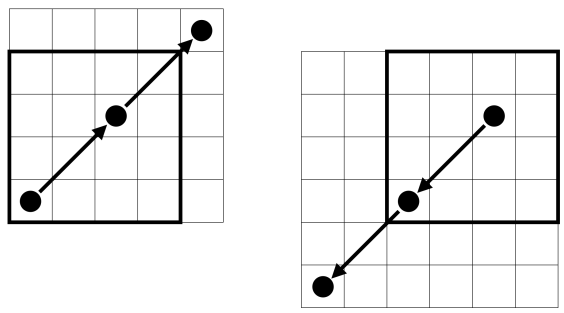


Why the assumption $h_i \neq n_i/2$ is necessary? Notice that the assumption is only used in Case 3. Recall the context of that case. For $i = 1$ we have the following assumptions: $w_{11} - a_{11} = h_1 - n_1$, $w_{21} - a_{21} = h_1$, and $a_{11} = w_{21}$. That is, we have two difference vectors, whose projection onto the x-axis (if $i = 2$, then we consider the projection onto the y-axis) are two vectors pointing in opposite directions and sharing one point, i.e., the starting point of one of the vector projections is the same as the finishing point for the other vector projection. Now, if $h_1 = n_1/2$, then $h_1 - n_1 = -n_1/2$, so both projections have the same magnitude. If we try to flip any of these projections (adding or subtracting n_1), we obtain again two projected vectors pointing in the same direction and sharing one point, with a combined length of n_1, so one point is always out of a window of width n_1. Take, for example, this

4×4 binary array



It only has two difference vectors: $\langle 2, 2\rangle$ and $\langle -2, -2\rangle$. If one tries to flip any of the vectors by choosing points in the periodic extension in order to obtain two equal difference vectors, the vectors do not fit in a 4×4 window.



Since the assumption $h_i \neq n_i/2$ is only used in Case 3, if a binary array A has a repeated toroidal vector $\langle h_1, h_2\rangle$ not falling under that particular case, we can follow the proof of Proposition 1.13 word for word to obtain the same conclusion, even when $h_i = n_i/2$ for some $i \in \{1, 2\}$. This shows the following corollary:

Corollary 1.14. *Let A be an $n_1 \times n_2$ binary array and $\mathbb{A}$ its periodic extension to $\mathbb{Z}^2$. Assume A has two difference vectors $\omega_1 - \alpha_1$ and $\omega_2 - \alpha_2$ that are equal as toroidal vectors to $\langle h_1, h_2\rangle$, where $\alpha_1 = (a_{11}, a_{12})$, $\omega_1 = (w_{11}, w_{12})$, $\alpha_2 = (a_{21}, a_{22})$, $\omega_2 = (w_{21}, w_{22})$ are dots of A. If for $i = 1, 2$,*

$$h_i = \frac{n_i}{2} \implies w_{1i} - a_{1i} = w_{2i} - a_{2i}, \quad \text{or} \quad a_{1i} \neq w_{2i} \text{ and } a_{2i} \neq w_{1i}, \tag{1.5}$$

then there is an $n_1 \times n_2$ window of $\mathbb{A}$ having a repeated difference vector.

Corollary 1.14 will be used to give an alternative proof of an important theorem (Theorem 1.32) regarding a periodic property of Costas arrays.

1.3 Costas Arrays

Before giving a formal definition of Costas arrays, the following proposition is a well-known fact that describes, in equivalent ways, one of the critical properties of Costas arrays. A formal proof is always delightful, even when something is known to be true, so we shall give one.

Proposition 1.15. *Let $A : \Lambda \to \{0,1\}$ be a binary array, $\Lambda = [n_1] \times [n_2]$, and assume there is a function $\varphi : [n_1] \to [n_2]$ such that $A(i,j) = 1$ if and only if $\varphi(i) = j$. The following are equivalent:*

(i) For any $\lambda \in \mathbb{Z}^2 \setminus \{(0,0)\}$,

$$\sum_{\alpha \in (\Lambda - \lambda) \cap \Lambda} A(\alpha)A(\alpha + \lambda) \leqslant 1, \tag{1.6}$$

where $\Lambda - \lambda = \{\alpha - \lambda \in \mathbb{Z}^2 \,:\, \alpha \in \Lambda\}$.

(ii) A has no repeated difference vectors.

(iii) For any $k \in [n_1 - 1]$,

$$\varphi(i+k) - \varphi(i) = \varphi(j+k) - \varphi(j) \implies i = j, \tag{1.7}$$

for all $i, j \in [n_1]$ for which $i + k, j + k \in [n_1]$.

Proof. We will show *not (i)* $\implies$ *not (ii)* $\implies$ *not (iii)* $\implies$ *not (i)*.

Not (i) $\implies$ not (ii). Assume there exists $\lambda \in \mathbb{Z}^2 \setminus \{(0,0)\}$ for which

$$\sum_{\alpha \in (\Lambda - \lambda) \cap \Lambda} A(\alpha)A(\alpha + \lambda) \geqslant 2.$$

Then there exist distinct $\alpha_1, \alpha_2 \in (\Lambda - \lambda) \cap \Lambda$ such that $A(\alpha_1)A(\alpha_1 + \lambda) = 1$ and

$A(\alpha_2)A(\alpha_2+\lambda)=1$. Since A is a binary array we must have

$$A(\alpha_1)=A(\alpha_1+\lambda)=A(\alpha_2)=A(\alpha_2+\lambda)=1.$$

Then α_1, $\alpha_1+\lambda$, α_2, $\alpha_2+\lambda$ are all dots of A and λ is a repeated difference vector in A.

Not (ii) $\implies$ not (iii). Assume A has a repeated difference vector $\langle k,h\rangle$. Notice that, if $\lambda\in\mathbb{Z}^2$ is a difference vector in A, then $-\lambda$ is also a difference vector in A, so we may assume $k\geqslant 0$. Then we have two distinct pairs of distinct dots[II] α_1,ω_1 and α_2,ω_2 in A such that

$$\omega_1-\alpha_1=\omega_2-\alpha_2=\langle k,h\rangle.$$

Since φ defines the dots in A, we may assume $\alpha_1=(i,\varphi(i)),\ \alpha_2=(j,\varphi(j))$ for some $i,j\in[n_1],\ i\neq j$. Then

$$\omega_1=(i+k,\varphi(i)+h),\quad \omega_2=(j+k,\varphi(j)+h).$$

We see that $k\leqslant n_1-1$ because, otherwise, $i+k>n_1$ would be out of the index set of A and ω could not be a dot of A. However, since ω_1 and ω_2 are dots of A, $\varphi(i)+h=\varphi(i+k)$ and $\varphi(j)+h=\varphi(j+k)$. From here we see that $k\neq 0$ because, otherwise, $\omega_1=\alpha_1$ and $\omega_2=\alpha_2$, contradicting our assumption that those are distinct dots. Therefore, there is some $k\in[n_1-1]$ for which

$$\varphi(i+k)-\varphi(i)=h=\varphi(j+k)-\varphi(j)$$

[II]We will use the phrase *two distinct pairs of distinct dots* repeatedly through this thesis. This means that we have four dots $\alpha_1,\alpha_2,\omega_1,\omega_2\in A$ such that $(\alpha_1,\omega_1)\neq(\alpha_2,\omega_2)$ —here the part *distinct pairs*— and $\alpha_1\neq\omega_1,\ \alpha_2\neq\omega_2$ —here the part *distinct dots*—. This is to avoid taking the same difference vector twice (same starting and finishing dots) when we actually want difference vectors with distinct starting or finishing dots, and to avoid taking the zero vector as a difference vector.

and $i \neq j$.

Not (iii) $\implies$ not (i). Assume $\exists k \in [n_1 - 1]$ such that $\varphi(i+k) - \varphi(i) = \varphi(j+k) - \varphi(j)$, for some $i, j \in [n_1]$, $i \neq j$. Take

$$\alpha_1 = (i, \varphi(i)),\ \omega_1 = (i+k, \varphi(i+k)) \quad \text{and} \quad \alpha_2 = (j, \varphi(j)),\ \omega_2 = (j+k, \varphi(j+k)).$$

Clearly $\alpha_1, \omega_1, \alpha_2, \omega_2$ are all dots of A and $\omega_1 - \alpha_1 = \omega_2 - \alpha_2$. Set $\lambda = \omega_1 - \alpha_1$. Of course $\alpha_1 \in \Lambda$. Moreover, $\alpha_1 + \lambda = \omega_1 \in \Lambda$, hence $\alpha_1 \in (\Lambda - \lambda) \cap \Lambda$. Similarly, $\alpha_2 \in \Lambda$ and $\alpha_2 + \lambda = \omega_2 \in \Lambda$ implying $\alpha_2 \in (\Lambda - \lambda) \cap \Lambda$. Therefore

$$\begin{aligned}
\sum_{\alpha \in (\Lambda - \lambda) \cap \Lambda} A(\alpha)A(\alpha+\lambda) &\geqslant A(\alpha_1)A(\alpha_1+\lambda) + A(\alpha_2)A(\alpha_2+\lambda) \\
&= A(\alpha_1)A(\omega_1) + A(\alpha_2)A(\omega_2) \\
&= 1 \cdot 1 + 1 \cdot 1 = 2.
\end{aligned}$$

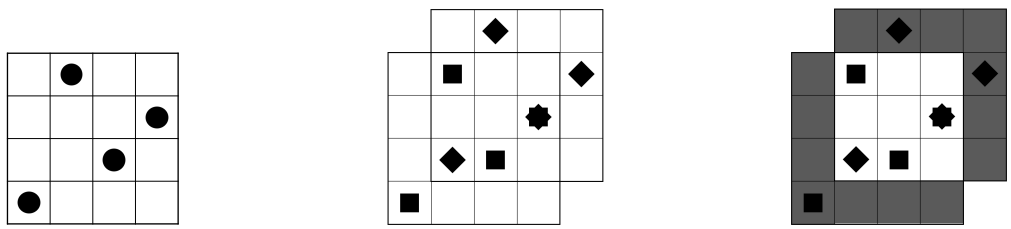
This completes the proof. □

Remark 1.16. If for some $\lambda \in \mathbb{Z}^2 \setminus \{(0,0)\}$, $(\Lambda - \lambda) \cap \Lambda = \emptyset$, the sum in (1.6) is defined to be zero.

All of the three equivalent properties in Proposition 1.15 are known as the **Costas property**. The reader is encouraged to compare (1.6) with the property (0.1) in Definition 0.1, given in the Introduction. The sum in (1.6) is a formal mathematical formulation of what we defined as $C(r,s)$. Take $\lambda = (r,s) \in \mathbb{Z}^2 \setminus \{(0,0)\}$, so the sum counts the coincidences between the original array A and the shifted version of A, corresponding to the factors $A(\alpha)$ and $A(\alpha+\lambda)$, respectively. Property 1.15(ii) in particular is known as the **distinct difference property**.

We want to reiterate that for the Costas property to be satisfied, the number of dots coinciding in the array A and any shifted version of A, A', must be at most

one; thus, we only care about the dots in the intersection of A and A'. Any dot not in the intersection of A and A' is ignored. This is illustrated in Figure 1.3. Figure 1.3(a) is the binary array A. Figure 1.3(b) shows the superposition of A, with square dots, and A', with diamond dots, where A' is the array A shifted one unit to the right and one unit up; i.e., shifted by $\lambda = (1, 1)$. Every dot not in the intersection of A and A' is ignored, so in this case, all dots in the gray shaded area of Figure 1.3(c) are ignored. Since there is only one coincidence in the white area of Figure 1.3(c), for $\lambda = (1, 1)$, $\sum_{\alpha \in (\Lambda - \lambda) \cap \Lambda} A(\alpha)A(\alpha + \lambda) = 1$.



(a) (b) (c)

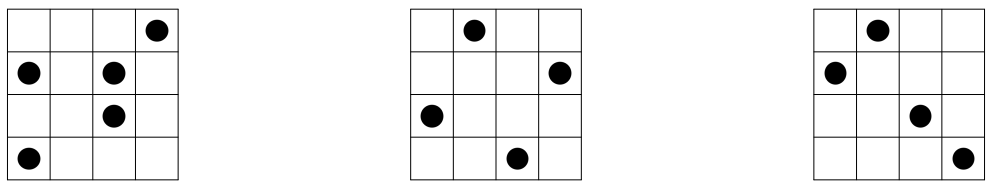
Figure 1.3: Coincidences between a binary array and a shifted version of itself.

And now, a trumpet fanfare announcing the moment in which we hereby define, with all due formality, the subject matter of this thesis.

Definition 1.17. A **Costas array** of order n is a binary array $A : [n] \times [n] \to \{0, 1\}$ having no repeated difference vectors and for which there is a bijection $\varphi : [n] \to [n]$, such that $\varphi(i) = j$ if and only if $A(i, j) = 1$.

The existence of a bijection $\varphi : [n] \to [n]$ which defines the dots of the array, implies that a Costas array has the structure of a permutation matrix. That is to say: there is exactly one dot per row and per column. Hence, binary arrays whose dots are defined by a bijection are called **permutation arrays**. In short, a Costas array is a permutation array satisfying the Costas property. Figure 1.4(c) is an example of a Costas array of order 4. It has exactly one dot per column and one dot per row, and in Example 1.10, we checked that it has no repeated difference vectors.

It is clear that a rotation or a reflection of a Costas array is still a Costas array. Therefore, the set of Costas arrays of order n can be partitioned in equivalent classes under the action of the symmetries of the square, that is, the dihedral group D_8.



(a) Not a permutation array (b) Permutation array, not Costas (c) Costas array

Figure 1.4: Three 4×4 binary arrays

1.4 Algebraic Constructions

This section discusses the three main algebraic methods for constructing Costas arrays, which are due to L. R. Welch, A. Lempel, and S. W. Golomb. We omit the proofs that, in effect, the constructions yield Costas arrays; for it, see [**12**].

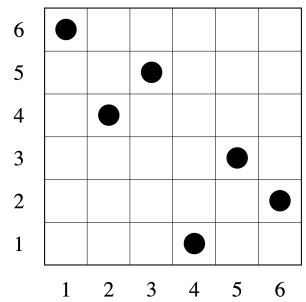
Proposition 1.18 (**Welch Construction**). *Let α be a primitive element in $\mathbb{F}_p$, with p prime, and $c \in \mathbb{Z}$. The array $A : [p-1] \times [p-1] \to \{0,1\}$, where $A(i,j) = 1$ if and only if $\alpha^{i+c} = j$, is a Costas array.*

The above is known in the literature as the exponential Welch construction since the array is defined by the function $\varphi(i) = \alpha^{i+c}$, which can be interpreted as a bijection $\varphi : [p-1] \to [p-1]$. The inverse permutation, i.e., the transpose of an exponential Welch array, is called a logarithmic Welch array. In this thesis, we only consider exponential, not logarithmic Welch arrays. Thus we will drop the adjective "exponential".

Example 1.19. Let $p = 7$, $\alpha = 3$ and $c = 2$. The array below is the Welch array

with those parameters, which has size 6×6, and set of dots

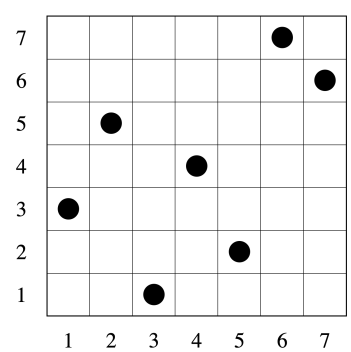
$$\left\{(i,j) \in [6] \times [6] \,:\, j = 3^{i+2} \bmod 7\right\} = \{(1,6),\ (2,4),\ (3,5),\ (4,1),\ (5,3),\ (6,2)\}.$$



Proposition 1.20 (**Lempel Construction**). *Let α be a primitive element in $\mathbb{F}_q$, with $q > 2$ a prime power. The array $A : [q-2] \times [q-2] \to \{0,1\}$, where $A(i,j) = 1$ if and only if $\alpha^i + \alpha^j = 1$ is a Costas array.*

Example 1.21. Let $q = 3^2$, and let α be the root of the primitive polynomial $x^2 + 2x + 2 \in \mathbb{F}_9[x]$. The array below is the Lempel array with those parameters, which has size 7×7, and set of dots

$$\left\{(i,j) \in [7] \times [7] \,:\, \alpha^i + \alpha^j = 1\right\} = \{(1,3),\ (2,5),\ (3,1),\ (4,4),\ (5,2),\ (6,7),\ (7,6)\}.$$

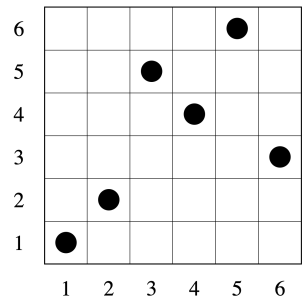


Proposition 1.22 (**Golomb Construction**). *Let α and β be primitive elements in $\mathbb{F}_q$, with $q > 2$ a prime power. The array $A : [q-2] \times [q-2] \to \{0,1\}$, where $A(i,j) = 1$ if and only if $\alpha^i + \beta^j = 1$ is a Costas array.*

The Golomb construction reduces to the one by Lempel when $\alpha = \beta$.

Example 1.23. Let $q = 2^3$, α be the root of the primitive polynomial $x^3 + x + 1 \in \mathbb{F}_8[x]$, and $\beta = \alpha^3$. The array below is the Golomb array with those parameters, which has size 6×6, and set of dots

$$\big\{(i,j) \in [6] \times [6] \,:\, \alpha^i + \beta^j = 1\big\} = \{(1,1),\ (2,2),\ (3,5),\ (4,4),\ (5,6),\ (6,3)\}.$$

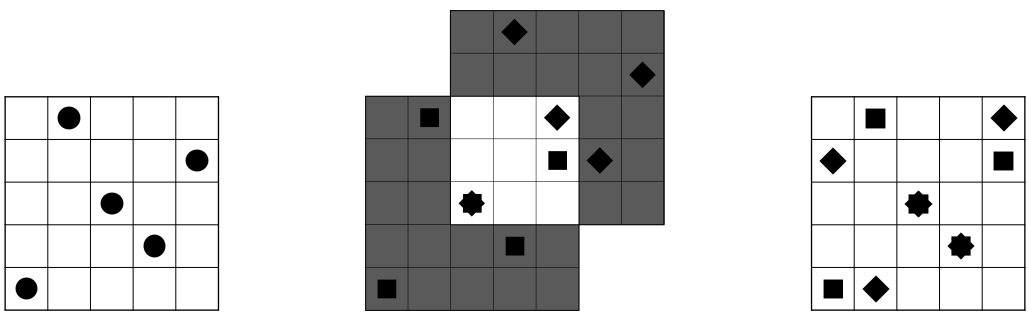


1.5 Periodicity of Costas Arrays

Any array can be extended periodically into the whole plane by repeating the same pattern in both the vertical and horizontal directions. But what happens to the Costas property when a Costas array is extended periodically? In this section, we explore that question.

Let A be a Costas array of order n, and let $\mathbb{A}$ be its periodic extension to $\mathbb{Z}^2$. It is natural to consider two forms in which the Costas property could extend periodically into $\mathbb{A}$. The first and most natural way is to request every $n \times n$ window in $\mathbb{A}$ to be a Costas array. But we have to be careful and, for each window, only consider the difference vectors among dots inside the window; all dots outside the window must be ignored. Since all the component-wise differences are carried out in $\mathbb{Z}$, we call this type of periodicity **integral periodicity**. Integral periodicity was considered in [**17**, Section III.A] and [**30**].

The second type of periodicity that we consider is stronger than integral periodicity. Imagine writing the array on the surface of a torus so that the left-most and right-most columns are glued together, as well as the top and bottom rows. Now we may consider the coincidences between the dots in the array A and the dots in a shifted version of A, A', where A' is shifted on the surface of the torus. Notice that, in this case, there could be coincidences that do not occur when both arrays A and A' are written in the plane. As illustrated in Figure 1.5(b), the farthest A' is shifted away from A, the smaller the area where the coincidences can occur. This does not happen when the array is written in the torus, as shifting A' in one direction brings the dots back over A from the other side.



(a) (b) (c)

Figure 1.5: Coincidences between a binary array and a shifted version of itself considered as in the plane (b) and as in the torus (c).

We can "write" a Costas array over a torus by considering the index set $\Lambda' = \mathbb{Z}_n \times \mathbb{Z}_n$ and take all differences in $\mathbb{Z}_n$, instead of considering the index set $\Lambda = [n] \times [n]$ and taking differences in $\mathbb{Z}$. Thus, this context considers toroidal vectors instead of difference vectors. The second type of periodicity is achieved when the Costas array has distinct toroidal vectors, so when the array is shifted in the torus, either all dots coincide or at most one coincides.

Equivalently, we can "write" a Costas array over a torus by mapping the bijection $\varphi : [n] \to [n]$ that defines the array to a bijection $\varphi' : \mathbb{Z}_n \to \mathbb{Z}_n$ satisfying

the distinct modular difference property: for any $k \in \mathbb{Z}_n$, $k \neq 0$,

$$\varphi'(i+k) - \varphi'(i) = \varphi'(j+k) - \varphi'(j) \implies i = j, \tag{1.8}$$

for all $i, j \in \mathbb{Z}_n$, where the addition, differences and the equality are taken in $\mathbb{Z}_n$. Notice that (1.8) is the same as requiring the difference map

$$\Delta_{\varphi',k} : \mathbb{Z}_n \to \mathbb{Z}_n, \quad i \mapsto \varphi'(i+k) - \varphi'(i)$$

to be injective. In fact, a bijection $\varphi' : \mathbb{Z}_n \to \mathbb{Z}_n$ with injective difference map is defined in [**9**, Definition 2] as a perfect non-linear permutation.

For obvious reasons, we call the second type of periodicity **modular periodicity**. However, hope for the existence of Costas arrays with modular periodicity is short-lived because we already know that a Costas array of order n has at least $n-1$ repeated toroidal vectors. In terms of functions, perfect non-linear permutation does not exist [**9**, Theorem 1].

To formalize and summarize:

Definition 1.24. A Costas array of order n is **periodic Costas** if any $n \times n$ window of its periodic extension is a Costas array.

Definition 1.25. A Costas array of order n is **modular Costas** if it has no repeated toroidal vectors.

Remark 1.26. A modular Costas array of order n is equivalent to a bijective map $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n$ for which the difference map $\Delta_{\varphi,k}(i) = \varphi(i+k) - \varphi(i)$ is injective for all $k \in \mathbb{Z}_n, k \neq 0$.

Proposition 1.27. *If an array is modular Costas, it is periodic Costas.*

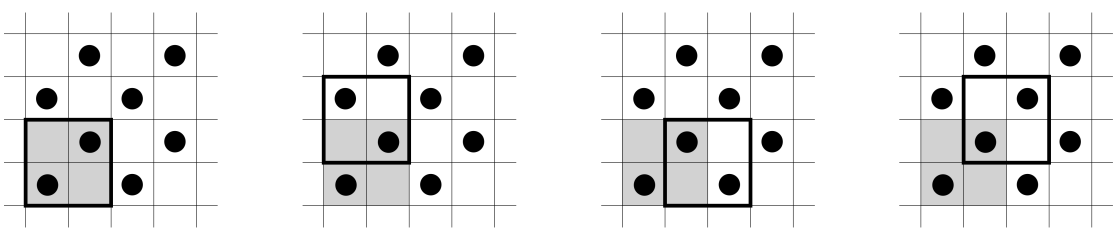
Theorem 1.28 (cf. Theorem 1 in [**9**])**.** *Modular Costas arrays do not exist.*

For the remainder of this section, all efforts are directed toward showing the non-existence of Costas arrays with integral periodicity, i.e., the non-existence of periodic Costas arrays. This fact was proven by Taylor [**30**].

Remark 1.29. The property of being periodic Costas is preserved under the action of the symmetries of the square. Hence, in an equivalence class of Costas arrays, either all arrays are periodic Costas or none is.

Example 1.30. Consider the following 2×2 array:

It is a Costas array as it has only two difference vectors, $\langle 1, 1\rangle$ and $\langle -1, -1\rangle$, which are distinct. There are (at most) 4 distinct 2×2 windows in its periodic extension, including the original array, which are repeated throughout the whole plane. Those are:



The original array appears in gray, and the four windows with a bold border. Since each window is a Costas array, it is periodic Costas.

As shown in the example above, to check whether a Costas array of order n is periodic Costas, it is necessary to check that all the possibly distinct n^2 windows in its periodic extension are Costas arrays. That is a lot of computation. But as we mentioned earlier, there is a clear connection between the periodic extension of a Costas array and its toroidal vectors: both are defined modulo the size of the array. We will utilize toroidal vectors to determine when an array is not periodic Costas. The best-case scenario would be to have the implication *repeated toroidal vectors*

implies not periodic Costas, but Example 1.30 is a counterexample to such implication. Nonetheless, we will show in Theorem 1.32 that this is the only counterexample[III]. The following lemma, mentioned without proof in the proof of [**18**, Theorem 1.7], is a step in that direction. For completeness, we will provide a proof.

Lemma 1.31. *Let $A : \Lambda \to \{0,1\}$ be an $n \times n$ permutation array. For a fixed $x \in [n-1]$, there are exactly n toroidal vectors (counting multiplicities) of the form $\langle x, h_1 \rangle$ occurring in A, with $h_1 \in [n-1]$. Analogously, there are exactly n toroidal vectors (counting multiplicities) of the form $\langle h_2, x \rangle$ occurring in A, with $h_2 \in [n-1]$.*

Proof. Since A is a permutation array of order n, there is a bijection $\varphi : [n] \to [n]$ such that $\varphi(i) = j$ if and only if $A(i,j) = 1$. Notice that if $\langle h, k \rangle$ is a toroidal vector in A, then $0 \leqslant h, k < n$ because they are reminders when divided by n. Moreover, $h \neq 0$ because there are no two dots in the same row. Similarly, $k \neq 0$ because A does not have two dots in the same column. Therefore, the toroidal vectors occurring in A are drawn from the set $[n-1] \times [n-1]$.

Fix $x \in [n-1]$. For $a \in [n]$, take $w = (a + x - 1 \bmod n) + 1$. Notice that $a \neq w$ (otherwise $x = 0$) and w is the only value from 1 to n satisfying $x = w - a \bmod n$. Then $(a, \varphi(a))$, $(w, \varphi(w)) \in A$, and

$$\begin{aligned}
&\langle w - a \bmod n,\ \varphi(w) - \varphi(a) \bmod n \rangle \\
&\qquad = \langle (a + x - 1 + 1) - a \bmod n,\ \varphi(w) - \varphi(a) \bmod n \rangle \\
&\qquad = \langle x, h_1 \rangle
\end{aligned}$$

for $h_1 = \varphi(w) - \varphi(a) \bmod n$.

On the other hand, since φ is a bijection and $a \in [n]$, $(\varphi^{-1}(a), a) \in A$ and, similarly, $(\varphi^{-1}(w), w) \in A$. If we set $h_2 = \varphi^{-1}(w) - \varphi^{-1}(a) \bmod n$, we obtain a

[III]There are only two permutation arrays of order 2, and each is a Costas array. However, they are equivalent arrays under the action of the symmetries of the square, so they are essentially the same array.

toroidal vector

$$\langle h_2,\ w - a \bmod n\rangle = \langle h_2, x\rangle.$$

For each $a \in [n]$ we found exactly one toroidal vector occurring in A with the form $\langle x, h_1\rangle$, and exactly one with the form $\langle h_2, x\rangle$, as w is unique for each a. Therefore, there are n toroidal vectors of each form, one for each choice of a. $\square$

Theorem 1.32 ([**30**, Theorem B])**.** *Costas arrays of order $n > 2$ are not periodic Costas.*

Proof. Let A be a Costas array of order $n > 2$ and $\mathbb{A}$ its periodic extension. A has a total of $n(n-1)$ toroidal vectors (counting multiplicities) out of $(n-1)(n-1)$ possible toroidal vectors, so there are at least $n-1$ repeated toroidal vectors. If n is odd, no toroidal vector can have a component equal to $n/2$, as $n/2 \notin \mathbb{Z}$. Since we have repeated toroidal vectors, none with component equal to $n/2$, by Proposition 1.13, $\mathbb{A}$ has an $n \times n$ window containing repeated difference vectors. Therefore, A is not a periodic Costas array.

If n is even, by Lemma 1.31, A has at most $2n$ toroidal vectors with at least one component equal to $n/2$. Hence, A has at least $n(n-1) - 2n$ toroidal vectors with no component equal to $n/2$. The number of possible toroidal vectors without an $n/2$ component is $(n-2)(n-2)$. If $n > 4$ we have

$$\begin{aligned} n > 4 \quad \Longrightarrow \quad & n^2 + n > n^2 + 4 \\ \Longrightarrow \quad & n^2 - 3n > n^2 - 4n + 4 \\ \Longrightarrow \quad & n(n-1) - 2n > (n-2)(n-2). \end{aligned}$$

By the pigeonhole principle, there is a repeated toroidal vector with none of its components equal to $n/2$. Once again by Proposition 1.13, $\mathbb{A}$ has an $n \times n$ window

containing repeated difference vectors, so it is not a periodic Costas array. For $n = 4$, we know from [**16**, Figure 12] there are only two inequivalent classes of Costas arrays, and none is periodic Costas (see Figure 1.6). This completes the proof. $\square$

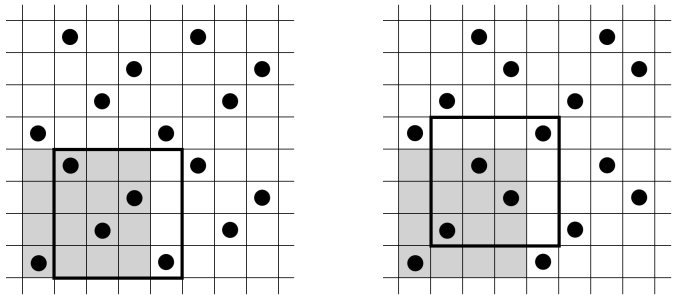


Figure 1.6: The periodic extension of two inequivalent Costas arrays of order $n = 4$, where none is periodic Costas. The original array is shaded in gray, and a 4×4 window with a repeated difference vector has a bold border.

Herbert Taylor proved the above result in [**30**]. The ideas behind Taylor's proof and ours are more or less the same. Still, Taylor's is more visual, and precisely because of that, it is more complicated to apply the proof in the context of higher-dimensional arrays. Our proof, albeit less visual, generalizes straightforwardly to higher dimensions (see Chapter 2). Moreover, our approach is more general than Taylor's as the key result in our proof is Proposition 1.13, which is proved for binary arrays instead of the particular case of Costas arrays.

The idea driving the proof of Theorem 1.32 is simple. To avoid verbose phrases, for an order n Costas array A, let $\mathcal{H}_A$ be the multiset of toroidal vectors $\langle h_1, h_2 \rangle$ in A such that $h_1 = n/2$ or $h_2 = n/2$. This is the approach: A has at least $n - 1$ repeated toroidal vectors. Thus, if the number of repeated toroidal vectors in $\mathcal{H}_A$ is at most $n-2$, there must be a repeated toroidal vector not in $\mathcal{H}_A$, so we apply Proposition 1.13 to obtain the result. Assuming we have higher-dimensional generalizations for the necessary definitions, if we want to use this approach to obtain a result along the lines of *multidimensional Costas arrays are not periodic Costas*, these are the three essential ingredients:

1. A higher-dimensional analog of Proposition 1.13.
2. A lower bound on the number of repeated toroidal vectors in a multidimensional Costas array.
3. An upper bound on the number of repeated toroidal vectors in $\mathcal{H}_A$.

Using this recipe, we will show (Corollary 2.31 in Chapter 2) that almost all three-dimensional Costas arrays are not periodic Costas, except for an infinite family of particular sizes and another few solitary arrays. To tackle the infinite family, we will use a slightly different approach, which uses Corollary 1.14.

Hereinafter we present the new approach with an alternative proof of Theorem 1.32, but first, we need an auxiliary lemma.

Lemma 1.33. *Let A be a Costas array of order n. Assume A has two distinct pairs of distinct dots $\alpha_1 = (a_{11}, a_{12})$, $\omega_1 = (w_{11}, w_{12})$ and $\alpha_2 = (a_{21}, a_{22})$, $\omega_2 = (w_{21}, w_{22})$ for which $\omega_1 - \alpha_1$ and $\omega_2 - \alpha_2$ are equal as toroidal vectors to $\langle h_1, h_2 \rangle$. If the implication* (1.5) *in Corollary 1.14 is false for $i = 1$, that is,*

$$h_1 = \frac{n_1}{2}, \quad w_{11} - a_{11} \neq w_{21} - a_{21}, \quad \text{and} \quad a_{11} = w_{21} \text{ or } a_{21} = w_{11},$$

then $h_2 = \dfrac{n}{2}$. Similarly, if the implication (1.5) *in Corollary 1.14 is false for $i = 2$, that is,*

$$h_2 = \frac{n_2}{2}, \quad w_{12} - a_{12} \neq w_{22} - a_{22}, \quad \text{and} \quad a_{12} = w_{22} \text{ or } a_{22} = w_{12},$$

then $h_1 = \dfrac{n}{2}$. In particular, a Costas array has at most two pairs of difference vectors with the assumptions of Corollary 1.14 that do not satisfy (1.5).

Proof. Let A be a Costas array of order n. Recall the implication in (1.5):

$$h_i = \frac{n_i}{2} \implies w_{1i} - a_{1i} = w_{2i} - a_{2i}, \quad \text{or} \quad a_{1i} \neq w_{2i} \text{ and } a_{2i} \neq w_{1i}. \tag{2.5}$$

Notice that if n is odd, $n/2 \notin \mathbb{Z}$, so (1.5) is trivially satisfied.

Let n be even. Assume A has two difference vectors $\omega_1 - \alpha_1$ and $\omega_2 - \alpha_2$ that are equal as toroidal vectors to $\langle h_1, h_2 \rangle$, where $\alpha_1 = (a_{11},\, a_{12}),\ \omega_1 = (w_{11},\, w_{12}),\ \alpha_2 = (a_{21},\, a_{22}),\ \omega_2 = (w_{21},\, w_{22})$ are dots of A. Assume further that (1.5) is false for $i = 1$ (the case $i = 2$ is analogous). That is, $h_1 = n/2$, $w_{11} - a_{11} \neq w_{21} - a_{21}$ and

$$a_{11} = w_{21} \quad \text{or} \quad a_{22} = w_{12}.$$

Without loss of generality, assume $a_{11} = w_{21}$.

Given that $w_{11} - a_{11}$ and $w_{21} - a_{21}$ are equal to $h_1 = n/2$ after reducing modulo n, and that $a_{11}, a_{21}, w_{11}, w_{21} \in [n]$, we have

$$w_{11} - a_{11} = -(w_{21} - a_{21}). \tag{1.9}$$

But $a_{11} = w_{21}$ and (1.9) imply $w_{11} = a_{21}$. A has only one dot per column and one dot per row, so

$$a_{11} = w_{21} \implies \alpha_1 = \omega_2 \quad \text{and} \quad w_{11} = a_{21} \implies \omega_1 = \alpha_2.$$

We are assuming that $\omega_1 - \alpha_1$ and $\omega_2 - \alpha_2 = \alpha_1 - \omega_1$ are equal as toroidal vectors, hence

$$\begin{aligned} w_{21} - a_{21} \equiv a_{21} - w_{21} \pmod{n} \qquad &\implies \qquad 2(w_{21} - a_{21}) \equiv 0 \pmod{n} \\ &\implies \qquad w_{21} - a_{21} \equiv \frac{n}{2} \pmod{n}. \end{aligned}$$

Then $h_1 = h_2 = n/2$. Since A is a Costas array, $\omega_1 - \alpha_1 \neq \omega_2 - \alpha_2$, and this leaves

only two possible pairs of difference vectors satisfying the assumptions:

$$\left\langle \frac{n}{2}, \frac{n}{2} \right\rangle, \left\langle -\frac{n}{2}, -\frac{n}{2} \right\rangle \quad \text{and} \quad \left\langle -\frac{n}{2}, \frac{n}{2} \right\rangle, \left\langle \frac{n}{2}, -\frac{n}{2} \right\rangle.$$

□

Alternative proof for Theorem 1.32. Let A be a Costas array of order $n > 2$. By the same arguments given in the proof of Theorem 1.32, if n is odd, A is not periodic Costas. Assume n is even, thus $n \geqslant 4$. As discussed also in the proof of Theorem 1.32, A has at least $n - 1$ repeated toroidal vectors. Therefore, by Lemma 1.33, at most two of these repeated toroidal vectors do not satisfy (1.5). But $n - 1 - 2 \geqslant 1$, so there is at least one repeated toroidal vector satisfying (1.5). By Corollary 1.14, the periodic extension $\mathbb{A}$ has an $n \times n$ window containing repeated difference vectors, so A is not a periodic Costas array. □

1.6 Circular Costas

In Section 1.5 we showed that, when we extend any Costas array of order $n > 2$ periodically to the whole plane, that is, repeating the same pattern in both the vertical and horizontal directions, the Costas property is not preserved; there is an $n \times n$ window which is not a Costas array. Similarly, modular periodic Costas arrays do not exist, even for $n = 2$. The conditions required for a binary array to be Costas are simply too strong to allow even the weakest type of periodicity. The natural road ahead is to relax any of the two conditions on a Costas array: relax the structure of a permutation matrix or relax the number of coincidences. Since modular periodicity implies integral periodicity, we focus on finding objects "close" to being modular periodic Costas.

Recall from Remark 1.26 that a modular periodic Costas array of order n

is equivalent to a bijection $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n$ such that, for every $k \in \mathbb{Z}_n, k \neq 0$, the difference map $\Delta_{\varphi,k}(i) = \varphi(i+k) - \varphi(i)$ is injective. In this modular context, to obtain a modular periodic Costas array, we could relax the condition of φ being a bijection or the condition of $\Delta_{\varphi,k}$ being injective. The latter, i.e., studying bijective functions between finite abelian groups for which the difference map is "close" to be injective, is studied in [**9**, **25**, **26**]. Particularly, in [**25**, **26**], the authors define a measure called *ambiguity* that measures how close a difference maps between finite abelian groups is to be injective.

Let us relax the condition of φ being a bijection. As the reader may see in many proofs, we have been using the injectivity of the Costas maps far more often than the surjectivity, so we relax the latter. The closest we can get to a bijective function while sacrificing surjectivity is an injective function whose image is the whole codomain, except for a single element. Thus we give the following definition.

Definition 1.34 (cf. [**15**, p. 2252])**.** A **circular Costas array** of order n is a binary array

$$A : \mathbb{Z}_n \times \mathbb{Z}_{n+1} \to \{0, 1\}$$

defined by an injective function $\varphi : \mathbb{Z}_n \to \mathbb{Z}_{n+1}$, such that, for all $k \in \mathbb{Z}_n$, $k \neq 0$, the difference map

$$\Delta_{\varphi,k} : \mathbb{Z}_n \to \mathbb{Z}_{n+1}, \quad i \mapsto \varphi(i+k) - \varphi(i) \tag{1.10}$$

is injective.

There is a subtlety between regular Costas arrays and circular Costas arrays (or, more generally, modular Costas arrays) that we are sweeping under the carpet. Under full mathematical rigor, the array $A : \mathbb{Z}_n \times \mathbb{Z}_{n+1} \to \{0, 1\}$, and hence the map $\varphi : \mathbb{Z}_n \to \mathbb{Z}_{n+1}$ defining it, looses all its geometric interpretation since, technically, the elements of $\mathbb{Z}_n$ are cosets of $\mathbb{Z}$. What does it mean to make a "shift" of $\lambda = (a, b) \in \mathbb{Z}_n \times \mathbb{Z}_{n+1}$? How to move the array "a units to the right" if a is a coset? But

of course, we can make the usual identification

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\} \subset \mathbb{Z},$$

so that the index set of A, $\mathbb{Z}_n \times \mathbb{Z}_{n+1}$ can be viewed as

$$\{0, \ldots, n-1\} \times \{0, \ldots, n\}.$$

In turn, A can be interpreted as a regular array living in $\mathbb{Z}^2$, with the only distinction that it is indexed starting from zero, instead of one, as defined in Definition 1.1, way back at the beginning of the chapter. In this way, A acquires its geometric interpretation of shifts and difference vectors.

Remark 1.35. All the geometric aspects of circular Costas arrays discussed in this section are "geometric" in the aforementioned sense.

Remark 1.36. Throughout this thesis, whenever we use an element of $\mathbb{Z}_n$ in a context where only integers make sense, e.g., sequence indices and exponents, we are implicitly making the identification $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ and using these integers as representative of their class in $\mathbb{Z}_n$.

In this geometric sense, circular Costas arrays are Costas arrays with the addition of an empty row. The empty row corresponds to the element in the codomain of φ with no preimage. It is clear that if $\varphi : \mathbb{Z}_n \to \mathbb{Z}_{n+1}$ defines a circular Costas array, $i \mapsto \varphi(i) - c$ also defines a circular Costas array, for any constant $c \in \mathbb{Z}_{n+1}$. Hence, by choosing a suitable constant c, we may assume that $\mathrm{Im}(\varphi) = \mathbb{Z}_{n+1} \setminus \{0\}$. That is, we can "shift" the circular Costas array so that the empty row is at the bottom, thus making 0 the only element with no preimage under φ. A circular Costas array will be called **standard** if $\mathrm{Im}(\varphi) = \mathbb{Z}_{n+1} \setminus \{0\}$. We will use the notation X^* to denote $X \setminus \{0\}$.

We will see shortly that standard circular Costas arrays are equivalent to circular Costas sequences, the latter defined by Golomb and Moreno [**15**]. We decided to respect the established precedence and call the arrays in Definition 1.34 "circular". Here is their definition.

Definition 1.37 ([**15**, Section I.D])**.** A sequence $a_0, a_1, \ldots, a_{n-1}$ which is a permutation of the integers $1, 2, \ldots n$ is a **circular Costas sequence**, if for $k = 1, 2, \ldots, n-1$, the circular differences

$$a_{0+k} - a_0, \quad a_{1+k} - a_1, \quad \ldots, \quad a_{n-1+k} - a_{n-1}$$

are distinct modulo $n+1$. The indices $i+k$ are taken modulo n.

To see that circular Costas arrays in their standard form are equivalent to circular Costas sequences, make the identification $\mathbb{Z}_{n+1} = \{0, 1, \ldots, n\} \subset \mathbb{Z}$. Let $\varphi : \mathbb{Z}_n \to \mathbb{Z}_{n+1}$ define a circular Costas array in standard form. Then, for any $i \in \mathbb{Z}_n$, $\varphi(i) \neq 0$. Define the sequence required in Definition 1.37 by

$$a_0 = \varphi(0), \quad a_1 = \varphi(1), \quad \ldots\ , \quad a_{n-1} = \varphi(n-1). \tag{1.11}$$

Then the sequence $\{a_i\}_{i=0}^{n-1}$ is a permutation of the integers $1, 2, \ldots, n$, and for $k = 1, 2, \ldots, n-1$, that is, $k \in \mathbb{Z}_n^*$, the differences

$$a_{i+k} - a_i = \varphi(i+k) - \varphi(i)$$

are all distinct modulo $n+1$ because, by definition, the difference map (1.10) is injective. By making the same identification in (1.11), a circular Costas sequence defines a standard circular Costas array. This shows that φ defines a standard circular Costas array if and only if the sequence (1.11) is a circular Costas sequence, thus Definition 1.34 (restricted to standard maps) is equivalent to Definition 1.37.

A circular Costas array, although having the adjective "Costas array" in its name, is not a Costas array as defined in Definition 1.17. First of all, it is not a square array as it has n columns and $n+1$ rows, so it cannot be a permutation array. Yet, it is almost a permutation array: every column has exactly one dot, given that φ is injective, and every row has exactly one dot except for a single empty row. Hence, since no two dots are in the same column nor in the same row, in a circular Costas array of order n, the toroidal vectors are drawn from $\mathbb{Z}_n^* \times \mathbb{Z}_{n+1}^*$.

It is clear from the definitions of difference and toroidal vectors that if all toroidal vectors in a binary array are distinct, all its difference vectors are also distinct. That is to say, having no repeated toroidal vectors is a sufficient condition for the array to satisfy the Costas property. As we will see in the next proposition, circular Costas arrays have no repeated toroidal vectors, so they satisfy the Costas property.

Proposition 1.38. *In a circular Costas array of order n, every element of $\mathbb{Z}_n^* \times \mathbb{Z}_{n+1}^*$ occurs exactly once as a toroidal vector. In particular, a circular Costas array has no repeated toroidal vectors.*

Proof. Let $\langle k, h\rangle$ be a toroidal vector in the circular Costas array A defined by $\varphi : \mathbb{Z}_n \to \mathbb{Z}_{n+1}$. First, notice that $k \neq 0$ and $h \neq 0$ because A does not have two dots in the same column nor two dots in the same row. That is, $\langle k, h\rangle \in \mathbb{Z}_n^* \times \mathbb{Z}_{n+1}^*$. There must be $i, j \in \mathbb{Z}_n$ such that the toroidal vector from the dot $(i, \varphi(i))$ to the dot $(j, \varphi(j))$ is $\langle k, h\rangle$. Therefore $j - i = k$ and $\varphi(j) - \varphi(i) = h$. By the distinct modular difference property of φ, there is a unique i for which $\varphi(i+k) - \varphi(i) = h$. Since k is fixed, j is also unique. This shows there is a unique pair of dots producing the toroidal vector $\langle k, h\rangle$. Since this toroidal vector was arbitrary, we conclude that every element in $\mathbb{Z}_n^* \times \mathbb{Z}_{n+1}^*$ occurs exactly once as a toroidal vector in A. $\square$

Notice the contrapositive statement of Proposition 1.12: *if an $n_1 \times n_2$ binary array has no repeated toroidal vectors, then any window of size $n_1 \times n_2$ in its periodic*

extension has no repeated difference vectors. Therefore, circular Costas arrays are the closest we can get to a periodic Costas array. In a circular Costas array, we obtain an "almost" permutation array that preserves the Costas property periodically throughout the whole plane. More specifically, any $n \times (n+1)$ window in the periodic extension of a circular Costas array has:

(1) no repeated difference vectors,

(2) one dot per column, and

(3) one dot per row, except for a single row which is empty.

Proposition 1.38 provides a manifest connection between circular Costas arrays and a particular type of difference set called *direct product difference sets.* Difference sets are related to many mathematical objects, but in particular, they have been extremely useful in the study of finite projective planes. Direct product difference sets were introduced by Ganley in [**11**], and their connection to circular Costas arrays was identified in [**23**]. With this connection, we can utilize all the results and mathematical machinery developed for the study of finite projective planes to answer questions regarding circular Costas arrays.

Definition 1.39 (cf. [**11**])**.** Let $G = A \times B$ be the direct product of two groups A and B (written additively), with $|A| = n - 1$ and $|B| = n$, where $n \geqslant 3$. Let $D \subseteq G$ be such that every element of $G \setminus \{(A \times \{0\}) \cup (\{0\} \times B)\}$ can be uniquely represented in the form $d_j - d_i$, where $d_i, d_j \in D$. Furthermore, suppose that no nonidentity element of $(A \times \{0\}) \cup (\{0\} \times B)$ can be so represented. Then we call D a **direct product difference set** in G of order n.

Notice that, in a direct product difference set D in the group $G = A \times B$, if $(a_1, b_1) \in D$ and $(a_2, b_2) \in D$ are distinct, then $a_1 \neq a_2$ and $b_1 \neq b_2$. Otherwise, an element of $(A \times \{0\}) \cup (\{0\} \times B)$ could be represented as the difference of elements

in D. By the previous observation, a simple count gives that, if $D \subseteq G$ is a direct product difference set of order n, $|D| = n - 1$.

Example 1.40. Let $G = \mathbb{Z}_4 \times \mathbb{Z}_5$. Consider the subset

$$D = \{(0,2),\ (1,4),\ (2,3),\ (3,1)\} \subseteq G$$

Take all the differences between distinct elements of D:

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

Since every element of $\mathbb{Z}_4^* \times \mathbb{Z}_5^*$ appears exactly once, and no element of $(\mathbb{Z}_4 \times \{0\}) \cup (\{0\} \times \mathbb{Z}_5)$ appears as difference for elements in D, we conclude that D is a direct product difference set in G. Since $|D| = 4$, D is a direct product difference set of order 5.

Definition 1.41 ([**23**, p. 321; **27**, p. 186])**.** Two direct product difference sets D_1 and D_2 in the group $G = A \times B$ are **equivalent** if there is an element $(a,b) \in G$ and a group automorphism $\psi \in \mathrm{Aut}(G)$, such that $D_2 = (a,b) \cdot \psi(D_1)$.[IV]

Jungnickel and de Resmini [**20**] proved this remarkable result about direct product difference sets.

[IV] As usual, we write $(a,b) \cdot D$ for the set $\{(a+x, b+x) : (x,y) \in D\}$, where $G = A \times B$ is a group, $D \subseteq G$, and $(a,b) \in G$.

Proposition 1.42 ([**20**, Theorem 1])**.** *Let D be an order n direct product difference set in the abelian group $G = A \times B$, where $|A| = n - 1$ and $|B| = n$. The order n must be a prime power and the group B is elementary abelian.*[V]

As teased before Definition 1.39, circular Costas arrays are related to direct product difference sets.

Theorem 1.43. *A is a circular Costas array of order n if and only if the set of dots of A is a direct product difference set of order $n + 1$ in the group $\mathbb{Z}_n \times \mathbb{Z}_{n+1}$.*

Proof. Let A be a circular Costas array defined by $\varphi : \mathbb{Z}_n \to \mathbb{Z}_{n+1}$. Let $G = \mathbb{Z}_n \times \mathbb{Z}_{n+1}$ and define $D \subseteq G$ as the set of dots of A. That is,

$$D = \{(i, \varphi(i)) \,:\, i \in \mathbb{Z}_n\}.$$

Let $d_i = (i, \varphi(i))$ and $d_j = (j, \varphi(j))$ be elements of D, and consider the difference $d_j - d_i = (j - i, \varphi(j) - \varphi(i))$. If $j - i = 0$, then $j = i$ and $d_j - d_i = (0, 0)$. On the other hand, if $\varphi(j) - \varphi(i) = 0$, then $\varphi(j) = \varphi(i)$, which implies $j = i$ because φ is injective, thus $d_j - d_i = (0, 0)$. Therefore, except for the identity, no element of $\mathbb{Z}_n \times \{0\}$ or $\{0\} \times \mathbb{Z}_{n+1}$ can be represented as a difference from elements in D. By Proposition 1.38 every element of $G \setminus \{(\mathbb{Z}_n \times \{0\}) \cup (\{0\} \times \mathbb{Z}_{n+1})\}$ has unique representation as a difference from elements in D. We conclude that D is a direct product difference set in G.

Conversely, assume $D \subseteq G$ is a direct product difference set of order $n + 1$. Define $\varphi : \mathbb{Z}_n \to \mathbb{Z}_{n+1}$ by setting $\varphi(i) = i'$ if and only if $(i, i') \in D$. This function is well defined because, for any two distinct elements in a direct product difference set, their second components must differ. Let $(i, \varphi(i)),\ (j, \varphi(j)) \in D$, where $j = i + k$ for

[V] Theorem 1 in [**20**] is not stated in terms of direct product difference sets, but rather in terms of collineation groups of finite projective planes.

some $k \in \mathbb{Z}_n$. To avoid the subgroup $\mathbb{Z}_n \times \{0\}$,

$$\varphi(j) - \varphi(i) = \varphi(i+k) - \varphi(i) \neq 0$$

for any $i, k \in \mathbb{Z}_n$ with $k \neq 0$. Hence, φ is injective. Since D is a direct product difference set, the difference map $\Delta_{\varphi,k}(i) = \varphi(i+k) - \varphi(i)$ must map to every element in $\mathbb{Z}_{n+1}^*$. Therefore, the difference map is also injective. We conclude that φ defines a circular Costas array of order n. □

Remark 1.44. The statement and the proof of Theorem 1.43 are analogous to Lemma 3.3 in [**23**]. However, their statement is in terms of Costas polynomials, which we define later in this section.

The following result was proved by Golomb and Moreno [**15**] using several results regarding Tuscan-k squares. We present a new proof using a completely different approach.

Corollary 1.45 ([**15**, Theorem 1])**.** *A circular Costas array has order $p-1$ for some prime number p.*

Proof. Let A be a circular Costas array defined by $\varphi : \mathbb{Z}_n \to \mathbb{Z}_{n+1}$. Let $G = \mathbb{Z}_n \times \mathbb{Z}_{n+1}$ and define $D \subseteq G$ as the set of dots of A. Since D is a direct product difference set of order $n+1$, Proposition 1.42 tells us that $n+1$ is a power of a prime and, moreover, that $\mathbb{Z}_{n+1}$ is elementary abelian. Then $n+1$ is a prime number. □

Based on Corollary 1.45, if φ defines a circular Costas array, the domain of φ is $\mathbb{Z}_{p-1}$ and the codomian of φ is $\mathbb{Z}_p$, for some prime p. Since $\mathbb{Z}_{p-1} \cong (\mathbb{F}_p^*, \times)$ and $\mathbb{Z}_p \cong (\mathbb{F}_p, +)$, we may consider a circular Costas map as an injection

$$f : \mathbb{F}_p^* \to \mathbb{F}_p.$$

But we must be cautious. Notice that this map f uses multiplicative notation in the domain. Up to now, we have been using additive notation. If, in particular, we consider the circular Costas array defined by φ to be standard, $\mathrm{Im}(\varphi) = \mathbb{Z}_p \setminus \{0\}$, therefore $\mathrm{Im}(f) = \mathbb{F}_p \setminus \{0\}$. We can extend the domain and the image of f by setting $f(0) = 0$. Then, by Lagrange interpolation, f can be defined as a unique polynomial function with degree at most $p-1$ and coefficients in $\mathbb{F}_p$. In fact, f is a permutation polynomial. Since for each $k \neq 0$, $i \mapsto \varphi(i+k) - \varphi(i)$ is injective, the map

$$\mathbb{F}_p^* \to \mathbb{F}_p, \qquad x \mapsto f(dx) - f(x)$$

is also injective for $d \in \mathbb{F}_p^*, d \neq 1$. But f is injective as a polynomial function over $\mathbb{F}_p$; hence, $f(dx) - f(x) \neq 0$ for $x \in \mathbb{F}_p^*$. However, if $x = 0$, $f(dx) - f(x) = 0$, so the polynomial $f(dx) - f(x)$ is also a permutation of $\mathbb{F}_p$ for any $d \in \mathbb{F}_p^*$, $d \neq 1$. Moreover, if $d = 0$,

$$f(dx) - f(x) = f(0) - f(x) = -f(x)$$

is a permutation of $\mathbb{F}_p$, because $f(x)$ is a permutation. Therefore, $f(dx) - f(x)$ is a permutation of $\mathbb{F}_p$ for any $d \in \mathbb{F}_p$, $d \neq 1$.

Circular Costas maps defined as polynomial functions are handy, so they have a special name.

Definition 1.46 ([**23**, Definition 2.4])**.** A **Costas polynomial** is a polynomial $f \in \mathbb{F}_p[x]$ for which $f(0) = 0$ and $f(dx) - f(x)$ is a permutation for all $d \in \mathbb{F}_p, d \neq 1$.

Remark 1.47. Based on the discussion before Definition 1.46, Costas polynomials are equivalent to standard circular Costas arrays.

It is well known that two distinct polynomials over a finite field $\mathbb{F}_p$ may define the same map, and this happens if and only if those polynomials correspond to the same element in the quotient ring $\mathbb{F}_p[x]/(x^p - x)$. We want a unique polynomial for

each map; thus, for the remainder of the section, we will consider Costas polynomials to be taken modulo $x^p - x$.

We want to clarify that the connection between circular Costas maps and permutation polynomials was known before [**23**]. The connection was established by Golomb and Moreno in [**15**, Section III], although they did not give a name to polynomials satisfying the conditions in Definition 1.46. To the best of our knowledge, the name "Costas polynomials" is due to Muratović-Rubić et al. [**23**].

To move from Costas maps (additive notation) to Costas polynomials (multiplicative domain) is easy. We need an isomorphism $\psi : \mathbb{Z}_{p-1} \to \mathbb{F}_p^*$, and $\psi(i) = \alpha^i$ does the trick, for some primitive element $\alpha \in \mathbb{F}_p^*$. Then, for a standard circular Costas map $\varphi : \mathbb{Z}_{p-1} \to \mathbb{Z}_p$, define $f \in \mathbb{F}_p[x]$ by setting $f(\alpha^i) = \varphi(i)$ and interpolating. This interponlant polynomial f is a Costas polynomial. The converse is also true: if $f \in \mathbb{F}_p[x]$ is a Costas polynomial and $\varphi : \mathbb{Z}_{p-1} \to \mathbb{Z}_p$ is defined by $\varphi(i) = f(\alpha^i)$, φ is a standard circular Costas map. Making this distinction is important, because one might be tempted to construct a binary array with a Costas polynomial f by defining the set of dots as $\big\{(x, f(x)) : x \in \mathbb{F}_p^*\big\}$. However, this does not produce a Costas array, as one can see in the example below.

Example 1.48. It is easy to verify that $f(x) = x$ is a Costas polynomial in $\mathbb{F}_p[x]$, for any prime p. However, if we construct a binary array with dots $\big\{(x, f(x)) : x \in \mathbb{F}_p^*\big\}$, $p \geqslant 3$, this array is <u>not</u> a circular Costas array (it has all dots in diagonal, so there are repeated difference vectors). On the other hand, the array defined by the dots

$$\big\{(i, f(\alpha^i)) : i \in \mathbb{Z}_{p-1}\big\}, \tag{1.12}$$

for some primitive $\alpha \in \mathbb{F}_p$, is circular Costas. In fact, the array with dots as in (1.12) is a Welch array, as we will see shortly.

1.6.1 Characterizing circular Costas as Welch arrays

Let $\alpha \in \mathbb{F}_p$ be a primitive element. Recall that Welch arrays are the arrays $A : [p-1] \times [p-1] \to \{0,1\}$ with set of dots $\{(i, \alpha^{i+c}) : i \in [p-1]\}$, for some constant c. Of course, $\alpha^{i+c} \in \mathbb{F}_p^*$, so we do the usual identification $\mathbb{F}_p^* = [p-1]$. Now define $\varphi : \mathbb{Z}_{p-1} \to \mathbb{Z}_p (= \mathbb{F}_p)$ by $\varphi(i) = \alpha^{i+c}$. In fact, the difference map with respect to φ is injective since, for any $k \in \mathbb{Z}_{p-1}^*$,

$$\begin{aligned}
\varphi(i+k) - \varphi(i) = \varphi(j+k) - \varphi(j) &\implies \alpha^i\alpha^c\alpha^k - \alpha^i\alpha^c = \alpha^j\alpha^c\alpha^k - \alpha^j\alpha^c \\
&\implies \alpha^i\alpha^c(\alpha^k - 1) = \alpha^j\alpha^c(\alpha^k - 1) \\
&\implies \alpha^i = \alpha^j \\
&\implies i = j.
\end{aligned}$$

The third implication holds given that $k \neq 0$ and $\alpha^c \neq 0$, so $\alpha^c(\alpha^k - 1) \neq 0$. Therefore, the array $A : \mathbb{Z}_{p-1} \times \mathbb{Z}_p \to \{0,1\}$ whose set of dots is $\{(i, \varphi(i)) : i \in \mathbb{Z}_p\}$ is a circular Costas array. But this array is exactly a Welch array, except that it has an additional row at the bottom. This row corresponds to the tuples $(i, 0)$, and the row has no dots because 0 is not in the image of φ. This shows that Welch arrays, with the addition of an empty row at the bottom, are circular Costas arrays. Golomb and Moreno conjectured that the only circular Costas arrays are those obtained from the Welch construction [**15**, Conjecture 1] (in this thesis, Conjecture 0.4).

As discussed at the end of the previous section, from a circular Costas map $\varphi : \mathbb{Z}_{p-1} \to \mathbb{Z}_p$ we obtain a Costas polynomial $f \in \mathbb{F}_p[x]$ by setting $f(\alpha^i) = \varphi(i)$, for some primitive element $\alpha \in \mathbb{F}_p$. For Welch arrays, $\varphi(i) = \beta^{i+c}$, for some primitive element $\beta \in \mathbb{F}_p$ and $c \in \mathbb{Z}$. We can write $\beta = \alpha^s$ for some s with $\gcd(s, p-1) = 1$. Hence, for Welch arrays,

$$f(\alpha^i) = (\alpha^s)^{i+c} = \alpha^c(\alpha^i)^s.$$

This shows that Costas polynomials corresponding to Welch arrays are monomials of the form ax^s, for some nonzero coefficient $a \in \mathbb{F}_p$ and some positive integer $s < p-1$ with $\gcd(s, p-1) = 1$. Therefore, Conjecture 0.4 can be equivalently expressed in terms of Costas polynomials:

Conjecture 1.49 ([**15**, Conjecture 2])**.** *If $f \in \mathbb{F}_p[x]$ is a Costas polynomial of degree at most $p-1$, then $f(x) = ax^s$ for some integer $s < p-1$ satisfying $\gcd(s, p-1) = 1$, and some nonzero constant $a \in \mathbb{F}_p$.*

Thanks to Muratović-Rubić, Pott, Thompson, and Wang, the above statement changed its status from "conjecture" to "theorem" [**23**]. We state it in the equivalent form:

Theorem 1.50 ([**23**, Theorem 3.4])**.** *A Costas array is circular if and only if it is Welch.*

Yet, almost 20 years before the publication of [**23**] where Conjecture 1.49 was finally solved, Moreno [**21**] proved a weaker version of Conjecture 1.49 by considering the following condition.

Definition 1.51 ([**21**, p. 158])**.** A sequence $a_0, a_1, \ldots, a_{n-1}$ which is a permutation of the integers $1, 2, \ldots n$ has the **shifting property** if for each $k \neq 0$, the sequence of circular differences

$$a_{0+k} - a_0, \quad a_{1+k} - a_1, \quad \ldots, \quad a_{n-1+k} - a_{n-1},$$

considered modulo $n+1$, is a circular permutation of the original sequence. The indices $i+k$ are taken modulo n.

Notice that if a sequence has the shifting property, the circular differences are all distinct modulo $n+1$ because the original sequence is a permutation of the integers from 1 to n. Therefore, if a sequence has the shifting property, it must be a circular

Costas sequence. Based on this observation, the following result, due to Moreno [**21**], is a weaker version of Conjecture 0.4.

Theorem 1.52 ([**21**, Theorem])**.** *A sequence has the shifting property if and only if it is Welch.*

Theorem 1.52 is a remarkable result. Together with Theorem 1.50, it shows that every circular Costas sequence has the shifting property. We state it as a corollary.

Corollary 1.53. *A Costas sequence is circular if and only if it has the shifting property.*

Since Costas sequences satisfying the shifting property are circular Costas, we end this chapter by expressing the shifting property as an additional condition on Costas polynomials. Let A be a standard circular Costas array of order n defined by an injective $\varphi : \mathbb{Z}_n \to \mathbb{Z}_{n+1}$. Notice that $\varphi(i) \neq 0$ for any $i \in \mathbb{Z}_n$. We already established that the sequence $\varphi(0),\ \varphi(1),\ \ldots,\ \varphi(n-1)$ is a circular Costas sequence. Hence, it satisfies the shifting property if, for each $k \in \mathbb{Z}_n^*$, there is some $h \in \mathbb{Z}_n$ for which

$$\varphi(i+k) - \varphi(i) = \varphi(i+h), \quad \forall i \in \mathbb{Z}_n.$$

In terms of Costas polynomials, this translates into (using multiplicative notation in the domain)

$$f(dx) - f(x) = f(ax).$$

Definition 1.54. A shifting Costas polynomial is a Costas polynomial $f \in \mathbb{F}_p[x]$ for which, for any $d \neq 1$, there exist $a \in \mathbb{F}_p$ such that $f(dx) - f(x) = f(ax)$.

Hence, we can express Theorem 1.52 in terms of Costas polynomials.

Theorem 1.55 (Equivalent to Theorem 1.52)**.** *A monic polynomial $f \in \mathbb{F}_p[x]$ is a shifting Costas polynomial if and only if $f(x) = x^s$ with* $\gcd(s, p-1) = 1$.

Summary

In this Chapter 1, we start building up our framework for the upcoming development of a multidimensional Costas theory. We define an arbitrary two-dimensional array (Definition 1.1), and for binary arrays we define their difference and toroidal vectors [**18**] (Definitions 1.7 and 1.8, respectively). We define Costas arrays as binary arrays defined by a bijection with no repeated difference vectors (Definition 1.17). Also, we discuss the three main algebraic constructions for Costas arrays: the Welch, the Lempel, and the Golomb constructions [**17**] (Propositions 1.18, 1.20, and 1.22, respectively). The chapter finishes with a deep dive into the periodic properties of Costas arrays.

Two types of periodicity are introduced: periodic Costas arrays (Definition 1.24) and modular Costas arrays (Definition 1.25), where modular Costas implies periodic Costas (Proposition 1.27). However, we show that modular Costas arrays do not exist (Theorem 1.28) and a theorem by Taylor told us that periodic Costas arrays exist only of order 2 [**30**] (Theorem 1.32). We give two new proofs for the latter fact (p. 36 and p. 40). Finally, a special type of modular periodicity is introduced in circular Costas arrays [**15**] (Definition 1.34). These circular Costas arrays can be conveniently expressed in terms of Costas polynomials, a special type of permutation polynomials [**15**, **23**] (Definition 1.46). Golomb and Moreno [**15**] conjectured that all circular Costas maps are Welch, and this was proven true by Muratović-Rubić et al. [**23**] (Theorem 1.50), by connecting Costas polynomials, and hence circular Costas arrays, with direct product difference sets. The last main result we present in the chapter is a theorem by Moreno [**21**] that established a weaker version of the conjecture by Golomb and Moreno, where the Welch construction characterizes all circular Costas maps with a shifting property (Theorem 1.52).

Now we are ready to introduce a multidimensional theory of Costas arrays.

Chapter 2

Multidimensional Costas Arrays

We set sail on this new sea because there is new knowledge to be gained, and new rights to be won, and they must be won and used for the progress of all people.

—John F. Kennedy

After introducing the theory of two-dimensional Costas arrays with definitions and notations whose higher-dimensional generalizations are straightforward, the glorious moment we give such conception has arrived. After defining multidimensional Costas arrays, the ultimate goal of this chapter is to show that multidimensional periodic Costas arrays do not exist for a large family of arrays sizes. For it, we need to obtain three main ingredients:

1. A higher-dimensional analog of Proposition 1.13.
2. A lower bound on the number of repeated toroidal vectors in a multidimensional Costas array.
3. An upper bound on the number of repeated toroidal vectors in the multiset $\mathcal{H}_A$ of toroidal vectors having a component half the length of the array in the corresponding dimension.

These three ingredients are beautifully connected in Lemma 2.26.

But first, we have to set up the stage. All necessary notations and definitions are established in the opening sections. Also, we discuss previous higher-dimensional analogs of Costas arrays, all of which influenced, in one way or another, the work presented in this thesis. Multidimensional periodic Costas arrays, the pinnacle of the chapter, are discussed last.

To make completely evident the parallelism between the higher-dimensional generalizations of this chapter and all that was developed for two dimensions in Chapter 1, to every definition and result that applies, the corresponding reference for its two-dimensional analog is provided.

2.1 Multidimensional Arrays

Brace yourselves for the coming bombardment of definitions. Adding more comments instead would be reckless as these are straightforward higher-dimensional analogs of the definitions and results given in Chapter 1.

Definition 2.1 (cf. Definition 1.1)**.** An **array of dimension** m over a set X is a function $A : \Lambda \to X$ where Λ is the hyper-rectangular subset of $\mathbb{N}^m$ given by

$$\Lambda = \{(a_1, a_2, \ldots, a_m) \in \mathbb{N}^m \,:\, a_k \leqslant n_k, \quad k = 1, 2, \ldots, m\},$$

for some natural numbers $n_1, n_2, \ldots, n_m$. Equivalently, $\Lambda = [n_1] \times [n_2] \times \cdots \times [n_m]$. We say that Λ is the **index set** for the array A, and that A has size $n_1 \times n_2 \times \cdots \times n_m$.

If, in the definition above, $n_i = 1$ for some i, the i-th dimension would be trivial, so we avoid those cases. Hence, whenever we consider an m-dimensional array, we implicitly assume that the size in each dimension is at least 2.

Definition 2.2 (cf. Definition 1.2)**.** Let A be an m-dimensional array of size $n_1 \times \cdots \times n_m$, with index set $\Lambda = [n_1] \times [n_2] \times \cdots \times [n_m]$. For $\alpha = (a_1, \ldots, a_m) \in \mathbb{Z}^m$,

define $\alpha_\Lambda = (a'_1, \ldots, a'_m)$, where a'_i is the unique integer in $[n_i]$ which is congruent to $a_i \bmod n_i$.

Definition 2.3 (cf. Definition 1.4)**.** Let A be an m-dimensional array of size $n_1 \times \cdots \times n_m$, with index set Λ. The **periodic extension of** A, denoted by $\mathbb{A}$ is the infinite array defined by

$$\mathbb{A}(\alpha) = A(\alpha_\Lambda) \qquad \forall \alpha \in \mathbb{Z}^m.$$

Definition 2.4 (cf. Definition 1.5)**.** Let A be an m-dimensional binary array with index set Λ. A **dot of** A is an element of the set

$$\{\alpha \in \Lambda \,:\, A(\alpha) = 1\}.$$

As done for two-dimensional binary arrays, we only consider the set of m-tuples (coordinates) where the array has an entry of '1' instead of considering the whole array. Also, as for two-dimensional binary arrays, we say that α *is in* A or that it *belongs to* A, and write $\alpha \in A$, if and only if α is a dot of A, i.e., $A(\alpha) = 1$.

2.2 Difference and Toridal Vectors

Definition 2.5 (cf. Definition 1.7)**.** For two distinct dots $\alpha = (a_1, \ldots, a_m)$ and $\omega = (w_1, \ldots, w_m)$ in a binary m-dimensional array A, the **difference vector** from α to ω is the vector

$$\langle w_1 - a_1,\ w_2 - a_2,\ \ldots,\ w_m - a_m \rangle \in \mathbb{Z}^m.$$

Definition 2.6 (cf. Definition 1.8)**.** Let A be an $n_1 \times \cdots \times n_m$ binary array. The **toroidal vector** from the dot $\alpha = (a_1, \ldots, a_m) \in A$ to the dot $\omega = (w_1, \ldots, w_m) \in A$

is the vector

$$\langle w_1 - a_1 \bmod n_1,\ w_2 - a_2 \bmod n_2,\ \ldots,\ w_m - a_m \bmod n_m \rangle.$$

Remark 2.7. To avoid degenerate cases, we assume the dots α and ω in Definitions 2.5 and 2.6 are distinct, i.e., $\alpha \neq \omega$.

As for two-dimensional arrays, for each pair of dots in a binary array, we have two, possibly distinct, difference vectors joining them: from α to ω and vice versa. Hence, the number of difference vectors occurring in a binary array with n dots is $2\binom{n}{2} = n(n-1)$, counting repetitions. Similarly, the number of toroidal vectors is $n(n-1)$, again counting repetitions.

Definition 2.8. For an m-dimensional binary array A of size $n_1 \times \cdots \times n_m$, define the following multisets:

- $\mathcal{T}_A$ is the multiset of toroidal vectors occurring in A.
- $\mathcal{H}_A$ is the multiset of toroidal vectors $\langle h_1, \ldots, h_m \rangle$ occurring in A for which $h_i = n_i/2$ for some $i \in [m]$.

We use the letter "H" because a toroidal vector belongs to $\mathcal{H}_A$ if it has a component that is *half* the length of the array in the corresponding direction. As discussed before Definition 2.8, for a binary array A with n dots, $|\mathcal{T}_A| = n(n-1)$.

Lemma 2.9 (cf. Lemma 1.11)**.** *Let A be an m-dimensional binary array of size $n_1 \times \cdots \times n_m$ and $\mathbb{A}$ its periodic extension to $\mathbb{Z}^m$. If S is an $n_1 \times \cdots \times n_m$ window of $\mathbb{A}$, then A and S have the same multiset of toroidal vectors. That is, $\mathcal{T}_S = \mathcal{T}_A$.*

Proof. Similar to the one in Lemma 1.11, adjusting for the dimension. □

Proposition 2.10 (cf. Proposition 1.12)**.** *Let A be an m-dimensional binary array of size $n_1 \times \cdots \times n_m$ and $\mathbb{A}$ its periodic extension to $\mathbb{Z}^m$. If an $n_1 \times \cdots \times n_m$ window of $\mathbb{A}$ has a repeated difference vector, then A has a repeated toroidal vector.*

Proof. Similar to the one in Proposition 1.12, adjusting for the dimension. □

Proposition 2.11 (cf. Proposition 1.13)**.** *Let A be an m-dimensional binary array of size $n_1 \times \cdots \times n_m$ and $\mathbb{A}$ its periodic extension to $\mathbb{Z}^m$. If A has a repeated toroidal vector $\langle h_1, \ldots, h_m \rangle \notin \mathcal{H}_A$, then there is an $n_1 \times \cdots \times n_m$ window of $\mathbb{A}$ having a repeated difference vector.*[I]

Proof. Similar to the one in Proposition 1.13, adjusting for the dimension. □

Since the proof of Proposition 2.11 is essentially the same as the proof of Proposition 1.13, we obtain the corollary below. It is a refinement of Proposition 2.11, analogous to Corollary 1.14, where the repeated toroidal vectors that belong to $\mathcal{H}_A$ and fall under Case 3 (see the proof of Proposition 1.13) are excluded.

Corollary 2.12 (cf. Corollary 1.14)**.** *Let A be an m-dimensional binary array of size $n_1 \times \cdots \times n_m$ and $\mathbb{A}$ its periodic extension to $\mathbb{Z}^m$. Assume A has two difference vectors $\omega_1 - \alpha_1$ and $\omega_2 - \alpha_2$ that are equal as toroidal vectors to $\langle h_1, \ldots, h_m \rangle$, where $\alpha_1 = (a_{11}, \ldots, a_{1m})$, $\omega_1 = (w_{11}, \ldots, w_{1m})$, $\alpha_2 = (a_{21}, \ldots, a_{2m})$, $\omega_2 = (w_{21}, \ldots, w_{2m})$ are dots of A. If for $i = 1, \ldots, m$,*

$$h_i = \frac{n_i}{2} \implies w_{1i} - a_{1i} = w_{2i} - a_{2i}, \quad \text{or} \quad a_{1i} \neq w_{2i} \text{ and } a_{2i} \neq w_{1i}, \tag{2.1}$$

then there is an $n_1 \times \cdots \times n_m$ window of $\mathbb{A}$ having a repeated difference vector.

2.3 Multidimensional Costas Arrays

And now, finally, the higher-dimensional generalization of Costas arrays we announced all along.

[I] This is our ingredient #1: a higher-dimensional analog of Proposition 1.13.

Definition 2.13 (cf. Definition 1.17)**.** Let

$$\Lambda = [n_1] \times \cdots \times [n_k] \times [n_{k+1}] \times \cdots \times [n_m], \qquad 1 \leqslant k < m.$$

An m**-dimensional Costas array** of size $n_1 \times n_2 \times \cdots \times n_m$ is a binary array $A : \Lambda \to \{0, 1\}$, having no repeated difference vectors and for which there is a bijection

$$\varphi : [n_1] \times \cdots \times [n_k] \longrightarrow [n_{k+1}] \times \cdots \times [n_m],$$

such that, for $\alpha = (a_1, \ldots, a_k, a_{k+1}, \ldots, a_m) \in \Lambda$, $A(\alpha) = 1$ if and only if

$$\varphi(a_1, \ldots, a_k) = (a_{k+1}, \ldots, a_m).$$

The **order** of a Costas array, denoted n, is the number of dots in A, or equivalently, the cardinality of the domain or the cardinality of the image of φ,

$$n = n_1 n_2 \cdots n_k = n_{k+1} n_{k+2} \cdots n_m.$$

Notice that in Definition 2.13, if $m = 2$, then $k = 1$, $\Lambda = [n_1] \times [n_2]$, and φ is a bijection $\varphi : [n_1] \to [n_2]$, so $n_1 = n_2$. Therefore, when $m = 2$, Definition 2.13 is exactly the same as Definition 1.17. Therefore, Definition 2.13 is a faithful generalization of the standard definition of two-dimensional Costas arrays, Definition 1.17.

It is clear that, if a bijection $\varphi : [n_1] \times \cdots \times [n_k] \to [n_{k+1}] \times \cdots \times [n_m]$ defines an m-dimensional Costas array, the inverse map φ^{-1} is also a bijection that defines an m-dimensional Costas array, since the dots of the latter would be just a swap between the first k coordinates and the last $m - k$ coordinates of the former, so all difference vectors are going to be distinct. We consider those arrays to be equivalent. Moreover, if a bijection $\varphi : [n_1] \times \cdots \times [n_k] \to [n_{k+1}] \times \cdots \times [n_m]$ defines a Costas array, any permutation of the coordinates in the domain of φ or the image of φ will

produce another Costas array, as this only permutes the components of the difference vectors, so they are going to be, once again, distinct. We consider those arrays to be equivalent.

Example 2.14. Let A be a three-dimensional Costas array defined by a bijection $\varphi : [n_1] \times [n_2] \to [n_1 n_2]$. Then A has size $n_1 \times n_2 \times n_1 n_2$. If D_A is the set of dots of A, we can define a new array A' of size $n_2 \times n_1 \times n_1 n_2$ whose set of dots is

$$D_{A'} = \big\{(a_2, a_1, a_3) \in \mathbb{Z}^3 \,:\, (a_1, a_2, a_3) \in D_A\big\}.$$

The array A' is a three-dimensional Costas array equivalent to A.

2.3.1 Previous definitions in the literature

To the best of our knowledge, this subsection presents all the proposed definitions for higher-dimensional analogs of Costas arrays. We comment on their limitations to explain why we did not adhere to those definitions of multidimensional Costs arrays and decided to give our own.

K. Drakakis

Here we present two definitions by Drakakis [**7**].

Definition 2.15 ([**7**, Definition 5] Verbatim)**.** Let $m \in \mathbb{N}$, consider a sequence $f : \mathbb{Z}^m \to \{0, 1\}$, and suppose further that $f(i) = 0$, $i \notin [N]$, $N \in \mathbb{N}^m$, where $i = (i_1, \ldots, i_m)$, $N = (N_1, \ldots N_m)$, $[N] = [N_1] \times \cdots [N_m]$, and the vector N has the smallest possible entries (for the given sequence f). Let the autocorrelation of f be $A_f(k) = \sum_{i \in \mathbb{Z}^m} f(i) f(i+k)$, $k \in \mathbb{Z}^m$. Then, f will be a **Costas hyper-rectangle** iff $\forall k \in \mathbb{Z}^m - \{0\}$, $A_f(k) \leqslant 1$. If f is a Costas hyper-rectangle so that $N_1 = \cdots = N_m = n \in \mathbb{N}$, it is called a **Costas hypercube**; if $m = 2$ it is a Costas square, whereas if $m = 3$ it will be called a Costas cube.

Definition 2.16 ([**7**, Definition 6] Verbatim)**.** Let $m = 2s$, $s \in \mathbb{N}$, and let $g : [n]^s \to [n]^s$ be a bijection, that is a permutation on vectors in general. Let $f : \mathbb{Z}^m \to \{0, 1\}$ be a sequence such that $f(i) = 1$ iff $(i_{s+1}, \ldots, i_{2s}) = g(i_1, \ldots, i_s)$, $(i_1, \ldots, i_s) \in [n]^s$, and such that it has the Costas property, as defined in Definition 5 [here Definition 2.15]; then, f will be called a **permutation Costas hypercube** in m dimensions with side length n.

These definitions by Drakakis are not far off from the ones stated in this thesis. What he called a *Costas hyper-rectangle* is, in our case, a multidimensional array satisfying the Costas property, i.e., having distinct difference vectors. Notice the similarity between the autocorrelation function and Equation (1.6) in Proposition 1.15, which is equivalent to the property of having distinct difference vectors. However, Drakakis' Costas hyper-rectangles are not defined by bijective functions. Therefore, on the extreme side, any m-dimensional binary array with only two dots would be a Costas hyper-rectangle. This is not analogous with the definition of a Costas array, or Costas square, that is used in two dimensions, as Costas arrays must be defined by bijections.

On the other hand, his definition of a *permutation Costas hypercube* in m dimensions is a special case of an m-dimensional Costas array as defined here, with m even, $k = m/2$ and $n_1 = n_2 = \cdots = n_m$ (see Definition 2.13). Since Drakakis already used the adjective "Costas" for m-dimensional binary arrays satisfying the Costas property, he needed to add the adjective "permutation" to distinguish permutation Costas hypercubes from regular Costas hyper-rectangles. This is not consistent with the naming convention used for two-dimensional Costas arrays.[II]

Finally, we want to point out that Drakakis' generalization of Costas arrays, ie., permutation Costas hypercubes, is problematic for odd dimensions. Our definition, being more general, does not have this problem.

[II] In two dimensions, there is no such things as a *permutation Costas array*. Two-dimensional Costas arrays are, by definition, permutations.

J. Ortiz-Ubarri, et al.

The following definition was given by Ortiz-Ubarri et al. [**24**].

Definition 2.17 ([**24**, Definition 1] Verbatim)**.** A generic $(m+1)$**-dimensional periodic Costas array** over the elementary abelian group $(\mathbb{Z}_p)^m$ is a permutation function $f : ((\mathbb{Z}_p)^m)^* \to (\mathbb{Z}_{p^m-1})$, where A^* means $A - \{0\}$. This function has the distinct difference property: for any $h \neq 0$, $a, b \in (\mathbb{Z}_p)^m$, $f(a+h) - f(a) = f(b+h) - f(b)$ implies $a = b$, where the addition and subtraction operations are performed in the corresponding abelian group.

What Ortiz-Ubarri et al. called an $(m+1)$-*dimensional periodic Costas array* is a generalization of circular Costas arrays, discussed in Section 1.6. We will adopt this definition, with minor changes, in Chapter 3. In particular, we will call those arrays "circular" instead of "periodic" to maintain consistency with the established naming in the case of two-dimensional Costas arrays.

The only issue we had with Definition 2.17 is the lack of context; the authors did not define an ordinary, non-periodic, Costas array. One of the main objectives of this thesis was to give such a definition.

J. Jedwab and L. Yen

Jedwab and Yen gave the following definitions [**19**].

Definition 2.18 ([**19**, Definition 1], Verbatim)**.** The **projections** of a three-dimensional array $(d_{i,j,k})$ are Projection $A = (a_{i,j}) = (\sum_k d_{i,j,k})$, Projection $B = (b_{i,k}) = (\sum_j d_{i,j,k})$, and Projection $C = (c_{j,k}) = (\sum_i d_{i,j,k})$.

The sums in Definition 2.18 come form the fact that an array $(d_{i,j,k})$ is a function $d : \mathbb{Z}^3 \to \mathbb{Z}$, where $(i,j,k) \mapsto d_{i,j,k}$. If all the entries of an array lie in $\{0,1\}$, they say it is *an array over* $\mathbb{Z}_2$.

Definition 2.19 ([**19**, Definition 2], Verbatim)**.** An order n **Costas cube** is an $n \times n \times n$ array over $\mathbb{Z}_2$ for which Projections A, B, C are each order n Costas arrays.

The above definition of a *costas cube* is, undoubtedly, an interesting three-dimensional analog of Costas arrays. Nonetheless, we do not consider it a faithful generalization. For it to be a faithful generalization, the restriction of the definition to two dimensions must yield a two-dimensional Costas array. There is no obvious way in which Definition 2.19 could be applied to two-dimensional arrays, and even less so that it would yield an object equivalent to Costas arrays.

2.4 Periodicity of Multidimensional Costas Arrays

The existence of two-dimensional periodic Costas arrays was settled by Taylor [**30**]; in Section 1.5, we gave two (slightly) different proofs for the same result: there are no two-dimensional periodic Costas arrays of order $n > 2$ (Theorem 1.32). Does the same happen for multidimensional Costas arrays? Exploring this question is appropriate and relevant in the higher-dimensional context as there is no apparent reason why an analogous result should hold in higher dimensions.

We start by defining higher-dimensional analogs of the two types of periodicity considered in Section 1.5.

Definition 2.20 (cf. Definition 1.24)**.** An m-dimensional Costas array of size $n_1 \times \cdots \times n_m$ is **periodic Costas** if any $n_1 \times \cdots \times n_m$ window of its periodic extension is an m-dimensional Costas array.

Definition 2.21 (cf. Definition 1.25)**.** An m-dimensional Costas array is **modular Costas** if it has no repeated toroidal vectors.

Proposition 2.22 (cf. Proposition 1.27)**.** *If an m-dimensional Costas array is modular Costas, it is periodic Costas.*

Proof. Let A be an m-dimensional Costas array of size $n_1 \times \cdots \times n_m$, and $\mathbb{A}$ its periodic extension. Since A is defined by a bijection φ, by making the appropriate shift in every dimension of the domain and the image of φ, all the dots in every $n_1 \times \cdots \times n_m$ of $\mathbb{A}$ can be defined by a bijection.

Assume A is modular Costas. By Lemma 2.9, every $n_1 \times \cdots \times n_m$ window of $\mathbb{A}$ has no repeated toroidal vectors, i.e., all toroidal vectors are distinct. Since the difference between dots from A are distinct after taking modulo, they must be distinct as integers. Then, any $n_1 \times \cdots \times n_m$ window of $\mathbb{A}$ has no repeated difference vectors, so it is an m-dimensional Costas array. $\square$

To explore the periodicity properties of multidimensional Costas arrays, the sets defined next result to be quite useful.

Definition 2.23. Let $\Lambda = [n_1] \times [n_2] \times \cdots \times [n_m]$ be an index set with $n_1 \cdots n_k = n_{k+1} \cdots n_m$, for some $k < m$. We define the following sets (not allowing repetitions):

- $T_\Lambda = (Z_1 \times Z_2) \setminus (Z_1 \times \{0\} \cup \{0\} \times Z_2)$, where $Z_1 = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ and $Z_2 = \mathbb{Z}_{n_{k+1}} \times \cdots \times \mathbb{Z}_{n_m}$.
- $H_\Lambda = \{\langle h_1, \ldots, h_m \rangle \in T_\Lambda \,:\, h_i = n_i/2 \text{ for some } i \in [m]\}$.

The set T_Λ is the value set for toroidal vectors occurring in any Costas array $A : \Lambda \to \{0, 1\}$. To see this, assume

$$\varphi : [n_1] \times \cdots \times [n_k] \to [n_{k+1}] \times \cdots \times [n_m]$$

defines an m-dimensional Costas array. If $\tau = \langle h_1, \cdots, h_m \rangle$ is a toroidal vector occuring in A, it is clear that $\tau \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$. But, if τ is a toroidal vector from $\alpha = (a_1, \ldots, a_m) \in A$ to $\omega = (w_1, \ldots w_m) \in A$ with $h_1 = h_2 = \cdots = h_k = 0$, it implies

$$a_1 = w_1, \quad a_2 = w_2, \quad \cdots, \quad a_k = w_k.$$

Therefore

$$\varphi(a_1, \ldots, a_k) = \varphi(w_1, \ldots, w_k) \implies (a_{k+1}, \ldots, a_m) = (w_{k+1}, \ldots, w_m),$$

so that $\alpha = \omega$. In such case, τ is a trivial toroidal vector. Similarly, for τ to be a non-trivial toroidal vector in A, $h_{k+1} = \cdots = h_m = 0$ cannot happen. Counting out these two cases, the cardinality of the value set of toroidal vectors in a Costas array $A : \Lambda \to \{0, 1\}$ of order n is

$$|T_\Lambda| = \left(\prod_{i=1}^{k} n_k - 1\right)\left(\prod_{i=k+1}^{m} n_k - 1\right) = (n-1)^2. \tag{2.2}$$

As for two-dimensional arrays, multidimensional Costas arrays of order n have $n(n-1)$ toroidal vectors out of $(n-1)^2$ possible vectors. This proves the following lemma.

Lemma 2.24. *A multidimensional Costas array of order n has at least $n-1$ repeated toroidal vectors. In other words, $\mathcal{T}_A$ has at least $n-1$ repeated elements, counting multiplicities.*[III]

Theorem 2.25 (cf. Theorem 1.28)**.** *Multidimensional modular Costas arrays do not exist.*

Proof. Follows from Lemma 2.24. □

There is a nice picture to make sense of the multisets $\mathcal{T}_A$, $\mathcal{H}_A$ in Definition 2.8, and the sets T_Λ, H_Λ in Definition 2.23. Consider the same Costas array as in Example 1.10, which has toroidal vectors

$$\begin{aligned}\mathcal{T}_A = \{\{&\langle 1,1\rangle \quad \langle 2,3\rangle \quad \langle 3,2\rangle \quad \langle 3,3\rangle \quad \langle 1,2\rangle \quad \langle 2,1\rangle \\ &\langle 2,1\rangle \quad \langle 3,2\rangle \quad \langle 1,3\rangle \quad \langle 1,2\rangle \quad \langle 2,3\rangle \quad \langle 3,1\rangle\}\}.\end{aligned}$$

[III]This is the ingredient #2 we talk about at the beginning of the chapter: a lower bound on the number of repeated toroidal vectors in a multidimensional Costas array.

$A =$

4		●		
3	●			
2			●	
1				●
	1	2	3	4

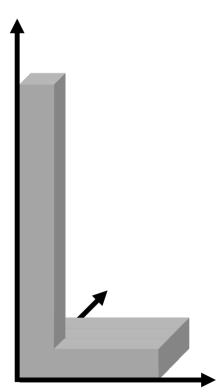
Figure 2.1: Costas array in Example 1.10

Construct a frequency array (two-dimensional in this case) such that position (x, y) contains the number of times $\langle x, y\rangle$ appears as a toroidal vector in the above Costas array: Of course, we can do this for any higher-dimensional array. The entries with

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

Figure 2.2: Frequency of toroidal vectors for the array in Figure 2.1

coordinate $(0, \cdot)$ and $(\cdot, 0)$ are obscured because, in a Costas array, we cannot have a toroidal vector with those coordinates (those are the vectors in $Z_1 \times \{0\} \cup \{0\} \times Z_2$ from Definition 2.23). In the case of a three-dimensional array of size $n_1 \times n_2 \times n_1 n_2$, the obscured entries (excluded toroidal vectors) of the frequency array are those of the form $(0, 0, \cdot)$ and $(\cdot, \cdot, 0)$; something like this:

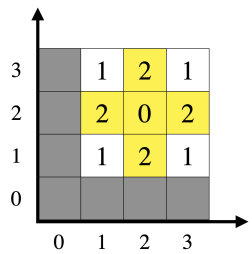


The set T_Λ is the set of all toroidal vectors corresponding to the not excluded boxes

(white boxes). For our example, shown in Figure 2.1 and Figure 2.2,

$$T_\Lambda = \{\langle 1,1\rangle,\ \langle 1,2\rangle,\ \langle 1,3\rangle,\ \langle 2,1\rangle,\ \langle 2,2\rangle,\ \langle 2,3\rangle,\ \langle 3,1\rangle,\ \langle 3,2\rangle,\ \langle 3,3\rangle\}.$$

The set H_Λ represents the boxes in the frequency array corresponding to toroidal vectors with some component half the length of the matching side of the array. We highlight those boxes in yellow. For the array A in Figure 2.1, whose order is 4, those are the toroidal vectors with a component equal to 2, so we highlight column #2 and row #2:



Therefore,

$$H_\Lambda = \{\langle 1,2\rangle,\ \langle 2,1\rangle,\ \langle 2,2\rangle,\ \langle 2,3\rangle,\ \langle 3,2\rangle\}.$$

By construction, $\mathcal{T}_A$ is the multiset of all toroidal vectors in the frequency array, each appearing repeatedly the number of times, i.e., its multiplicity, given by the number in the corresponding box. For example, the toroidal vector $\langle 1,2\rangle$ appears twice in $\mathcal{T}_A$, $\langle 3,1\rangle$ appears once, and $\langle 2,2\rangle$ does not appear in $\mathcal{T}_A$. The multiset $\mathcal{H}_A$ contains the elements of $\mathcal{T}_A$ corresponding to yellow boxes in the frequency array.

Notice that any 4×4 Costas array will have the same boxes painted yellow as the ones above. That is the reason for our notation: we put Λ as a subscript in H_Λ to emphasize that it only depends on the shape of the Costas array, not the entries, and the shape is determined by the index set Λ. On the other hand, the numbers on the array with yellow boxes do depend on the Costas array; thus, our subscript $\mathcal{H}_A$. Keeping those images in mind will be helpful when considering the existence of multidimensional periodic Costas arrays.

Using Proposition 2.11 we will show that multidimensional periodic Costas arrays do not exist for some classes of Costas arrays. This is our approach: any Costas array A with index set Λ and order n has at least $n-1$ repeated toroidal vectors; thus, if $|\mathcal{H}_A| - |H_\Lambda| < n-1$, there must be a repeated toroidal vector not in $\mathcal{H}_A$, so we can apply Proposition 2.11 to conclude that such array is not periodic Costas. We write this result as a lemma:

Lemma 2.26. *Let A be an m-dimensional Costas array of size $n_1 \times \cdots \times n_m$, index set $\Lambda = [n_1] \times \cdots \times [n_m]$, and order n. A is not a periodic Costas array if $|\mathcal{H}_A| - |H_\Lambda| < n-1$.*

Proof. We have

$$\begin{aligned} |\mathcal{H}_A| - |H_\Lambda| \quad < \quad n-1 \quad &\Longrightarrow \quad |\mathcal{H}_A| - |H_\Lambda| \quad < \quad n(n-1) - (n-1)^2 \\ &\Longrightarrow \quad (n-1)^2 - |H_\Lambda| \quad < \quad n(n-1) - |\mathcal{H}_A| \\ &\Longrightarrow \quad |T_\Lambda - H_\Lambda| \quad < \quad |\mathcal{T}_A - \mathcal{H}_A|. \end{aligned}$$

The cardinality of the multiset $|\mathcal{T}_A - \mathcal{H}_A|$ is the number of toroidal vectors not in $\mathcal{H}_A$. Since the number of toroidal vectors of A not in $\mathcal{H}_A$ is greater than the number of all possible values for toroidal vectors not in H_Λ, by the pigeonhole principle, A must have a repeated toroidal vector not in $\mathcal{H}_A$. By Proposition 2.11, an $n_1 \times \cdots \times n_m$ window of the periodic extension of A has a repeated difference vector. We conclude that A is not a periodic Costas array. □

Right away, we obtain a non-existence result for multidimensional periodic Costas arrays of odd order[IV]:

Theorem 2.27. *A multidimensional Costas array of odd order is not periodic Costas.*

[IV] Recall that, to obtain a result on the lines of *multidimensional periodic Costas arrays do not exist*, we are only missing ingredient #3: an upper bound on the number of repeated toroidal vectors in the multiset $\mathcal{H}_A$. For Costas arrays of odd order, we obtain ingredient #3 for free: it is zero.

Proof. Let A be an m-dimensional Costas array of size $n_1 \times n_2 \times \cdots \times n_m$, index set $\Lambda = [n_1] \times \cdots \times [n_m]$, and odd order n. Then, n_i is odd for $i = 1, \ldots, m$ (otherwise the order of A would be even), implying that $n_i/2$ is not an integer. Since the toroidal vectors of A have integer components, none can have the i-th component equal to $n_i/2$. That is, $\mathcal{H}_A = H_\Lambda = \emptyset$. Clearly $0 = |\mathcal{H}_A| - |H_\Lambda| < n - 1$. By Lemma 2.26, A is not periodic Costas. $\square$

To prove the non-existence of multidimensional periodic Costas arrays is more complicated for even order, at least with our approach. The problem is that with an arbitrary Costas array of even order, we do not know how to obtain a sufficiently low upper bound for $|\mathcal{H}_A|$. We illustrate the hurdle with an example.

Let A be a three-dimensional Costas array defined by a bijection $\varphi : [4] \times [6] \to [24]$, so its index set is $\Lambda = [4] \times [6] \times [24]$. A has order 24, an even number. Let us try to count the toroidal vectors in $\mathcal{H}_A$. First, we count how many toroidal vectors occurring in A may be of the form $\langle n_1/2, y, z\rangle = \langle 2, y, z\rangle$. For any $\alpha = (a_1, a_2, a_3) \in A$, take a dot of the form $\omega = (w_1, w_2, w_3)$, setting w_1 to be the unique number from 1 to 4 equivalent to $(a_1 + 2) \bmod 4$, and choosing freely $w_2 \in [6]$ and $w_3 \in [24]$. The toroidal vector from α to ω is

$$\langle 2, \quad w_2 - a_2 \bmod 6, \quad w_3 - a_3 \bmod 24\rangle,$$

which has the required form $\langle 2, y, z\rangle$.

But some caution is needed: we must ensure ω is a dot of A. For that we must set $w_3 = \varphi(w_1, w_2)$, so w_3 is not chosen freely. Since ω_1 is uniquely determined by the choice of a_1, w_3 is determined by the choice of w_2. Hence, for each $\alpha \in A$, we can find six distinct dots $\omega \in A$ (one for each w_2) for which the toroidal vector from α to one of those dots has the form $\langle 2, y, z\rangle$; a total of $6 \cdot 24 = 144$ toroidal vectors.

Similarly, the number of toroidal vectors of the form $\langle x, n_2/2, z\rangle = \langle x, 3, z\rangle$

occurring in A is $4 \cdot 24 = 96$, and of the form $\langle x, y, n_3/2\rangle = \langle x, y, 12\rangle$ is $1 \cdot 24 = 24$. Hence

$$|\mathcal{H}_A| \leqslant 144 + 96 + 24$$

Of course, we are overcounting some toroidal vectors in $\mathcal{H}_A$. For example, all toroidal vectors of the form $\langle 2, 3, z\rangle$ with same starting and finishing dots are counted twice. Thus, we subtract from $|\mathcal{H}_A|$, 24 toroidal vectors of the form $\langle 2, 3, z\rangle$, counted with an argument similar to the one given above.

What about toroidal vectors of the form $\langle 2, y, 12\rangle$? Those are also counted twice, but we have no clue how many of those can occur in A. The reason is because, for some $\alpha = (a_1, a_2, a_3) \in A$, we may use any dot $\omega = (w_1, w_2, w_3) \in A$, with w_3 being the unique integer from 1 to 24 which is congruent to $a_3 + 12$ modulo 24. But then we are forced to have $(w_1, w_2) = \varphi^{-1}(w_3)$. We have no way to know if $w_1 \equiv a_1 + 2 \pmod 4$. The same problem occurs for toroidal vectors of the form $\langle x, 3, 12\rangle$ and $\langle 2, 3, 12\rangle$. The best estimate we can get is

$$|\mathcal{H}_A| \leqslant 144 + 96 + 24 - 24 = 240.$$

For fun and completion, let us count the number of elements in H_Λ and see whether a Costas array of size $4 \times 6 \times 24$ could be periodic Costas or not. Notice that, in this case

$$T_\Lambda = \{(x, y, z) \in \Lambda \,:\, (x, y) \neq (0, 0) \text{ and } z \neq 0\},$$

and

$$H_\Lambda = \{(x, y, z) \in T_\Lambda \,:\, x = 2,\ y = 3 \text{ or } z = 12\}.$$

Therefore, by the inclusion-exclusion principle,

$$|H_\Lambda| = 6 \cdot 23 + 4 \cdot 23 + 23 - 23 - 6 - 4 + 1 = 221.$$

Since $|\mathcal{H}_A| - |H_\Lambda| \leqslant 240 - 221 = 19$, which is less than $n - 1 = 23$, applying Lemma 2.26, any Costas array of size $4 \times 6 \times 24$ is not periodic Costas. This is a particular case of Theorem 2.32, stated in due course.

The following lemma is a formalization of the counting argument given in the example above.

Lemma 2.28. *Let A be an m-dimensional Costas array of even order defined by a bijection*

$$\varphi : [n_1] \times \cdots \times [n_k] \longrightarrow [n_{k+1}] \times \cdots \times [n_m],$$

and $E \subseteq [m]$, where n_i is even for all $i \in E$. Denote $\mathcal{H}_E$ the multiset of toroidal vectors $\langle h_1, \ldots, h_m \rangle$ occurring in A for which $h_i = n_i/2$ for all $i \in E$. If $E \subseteq \{1, \ldots, k\}$ or $E \subseteq \{k+1, \ldots, m\}$, then

$$|\mathcal{H}_E| \prod_{i \in E} n_i = n^2.$$

Proof. Notice that $E \neq \emptyset$ given that A has even order. Assume $E \subseteq [k]$. After rearranging indices, we may assume $E = [t]$, for some $t \leqslant k$. For any $\alpha = (a_1, \ldots, a_m) \in A$, set w_i to be the unique number in $[n_i]$ that is equivalent to $a_i + n_i/2$ modulo n_i, for all $i \in [t]$. Choose $w_{t+1}, \ldots, w_k$ freely and set $(w_{k+1}, \ldots, w_m) = \varphi(w_1, \ldots, w_k)$. By construction, $\omega = (w_1, \ldots, w_m) \in A$, and if $\langle h_1, \ldots, h_m \rangle$ is the toroidal vector from α to ω, $h_i = n_i/2$ for all $i \in E$. Hence, for each dot $\alpha \in A$, we can choose freely $w_{t+1}, \ldots, w_k$ to obtain a toroidal vector in A with $h_i = n_i/2$, for all $i \in E$. It is easy to see that this is the only way to obtain such toroidal vectors. By simple counting

we have

$$|\mathcal{H}_E| = nn_{t+1}\cdots n_k = n\frac{\prod_{i=1}^{k} n_i}{\prod_{i\in E} n_i} = n\frac{n}{\prod_{i\in E} n_i},$$

and the result follows. The case $E \subseteq \{k+1,\ldots,m\}$ is analogous. $\square$

The next lemma provides a tidy formula for a counting done by inclusion-exclusion that will be used in Theorem 2.30 below.

Lemma 2.29. *Let $K = \{\{n_1,\ldots,n_k\}\}$ be a non-empty multiset of k natural numbers. Then,*

$$\sum_{\substack{I\subseteq[k]\\ I\neq\emptyset}} (-1)^{|I|+1}\frac{1}{\prod_{i\in I} n_i} = 1 - \prod_{i\in[k]} \frac{n_i-1}{n_i}. \tag{2.3}$$

Proof. This is a proof by induction on the cardinality of K. Let $k = 1$, i.e., $K = \{\{n_1\}\}$. Then, the left side of Equation (2.3) is

$$\sum_{\substack{I\subseteq[k]\\ I\neq\emptyset}} (-1)^{|I|+1}\frac{1}{\prod_{i\in I} n_i} = \frac{1}{n_1}.$$

On the other hand,

$$1 - \prod_{i\in[k]} \frac{n_i-1}{n_i} = 1 - \frac{n_1-1}{n_1} = \frac{1}{n_1}.$$

Hence, Equation (2.3) holds. Assume it holds for $K = \{\{n_1,\ldots,n_k\}\}$. Then

$$\begin{aligned}
&\sum_{\substack{I\subseteq[k+1]\\ I\neq\emptyset}} (-1)^{|I|+1}\frac{1}{\prod_{i\in I} n_i}\\
&= \sum_{\substack{I\subseteq[k]\\ I\neq\emptyset}} (-1)^{|I|+1}\frac{1}{\prod_{i\in I} n_i} + \frac{1}{n_{k+1}} + \sum_{\substack{I\subseteq[k]\\ I\neq\emptyset}} (-1)^{|I\cup\{k+1\}|+1}\frac{1}{n_{k+1}\prod_{i\in I} n_i}\\
&= \sum_{\substack{I\subseteq[k]\\ I\neq\emptyset}} (-1)^{|I|+1}\frac{1}{\prod_{i\in I} n_i} + \frac{1}{n_{k+1}} - \frac{1}{n_{k+1}}\sum_{\substack{I\subseteq[k]\\ I\neq\emptyset}} (-1)^{|I|+1}\frac{1}{\prod_{i\in I} n_i}
\end{aligned}$$

$$= \left(1 - \frac{1}{n_{k+1}}\right) \sum_{\substack{I \subseteq [k] \\ I \neq \emptyset}} (-1)^{|I|+1} \frac{1}{\prod_{i \in I} n_i} + \frac{1}{n_{k+1}}$$

$$= \frac{n_{k+1} - 1}{n_{k+1}} \left(1 - \prod_{i \in [k]} \frac{n_i - 1}{n_i}\right) + \frac{1}{n_{k+1}} \qquad \text{(By induction hypothesis)}$$

$$= 1 - \prod_{i \in [k+1]} \frac{n_i - 1}{n_i}$$

□

We will tackle the existence of periodic Costas arrays of even order only for arrays defined by bijections with one-dimensional image, which are equivalent, by taking the inverse, to bijections with a one-dimensional domain. We have two main reasons for it. First and foremost, the counting argument gets very convoluted for higher-dimensional image sets. Secondly, every (non-equivalent) three-dimensional Costas array must have one-dimensional image, so the three-dimensional case will be covered entirely.

Theorem 2.30. *Let A be an m-dimensional Costas array of even order n defined by a bijection*

$$\varphi : [n_1] \times \cdots \times [n_{m-1}] \longrightarrow [n_m].$$

Denote $\theta = 1 - \prod_{i \in E} \frac{n_i - 1}{n_i}$, where $E = \{i \in [m-1] : n_i \text{ is even}\}$. If $\theta < \frac{n-2}{2n}$, then A is not periodic Costas.

Proof. Let n be the order of A. That is, $n = n_1 n_2 \cdots n_{m-1} = n_m$, which is even by assumption. By Lemma 2.26, it is enough to check that $|\mathcal{H}_A| - |H_\Lambda| < n - 1$. First we count $|\mathcal{H}_A|$. For it, define the following multisets:

- $\mathcal{U}$ is the multiset of toroidal vectors $\langle h_1, \ldots, h_m \rangle \in \mathcal{H}_A$ with $h_i = n_i/2$ for some $i \in [m-1]$.

- $\mathcal{V}$ is the multiset of toroidal vectors $\langle h_1, \ldots, h_m \rangle \in \mathcal{H}_A$ with $h_m = n_m/2$.

It is clear that $|\mathcal{H}_A| = |\mathcal{U}| + |\mathcal{V}| - |\mathcal{U} \cap \mathcal{V}|$, where the intersection is in the context of multisets, i.e, including repetitions. By the inclusion-exclusion principle $|\mathcal{U}|$ is the sum of all the toroidal vectors with $h_i = n_i/2$ for one $i \in [m-1]$, minus all the toroidal vectors with $h_i = n_i/2$ for $i \in \{i_1, i_2\} \subseteq [m-1]$, plus all toroidal vectors with $i \in \{i_1, i_2, i_3\} \subseteq [m-1]$, and so on. By Lemma 2.28, for any $I \subset E$, the number of toroidal vectors with $h_i = n_i/2$ for all $i \in I$ is

$$\frac{n^2}{\prod_{i \in I} n_i}.$$

Therefore,

$$|\mathcal{U}| = \sum_{\substack{I \subseteq E \\ I \neq \emptyset}} (-1)^{|I|+1} \frac{n^2}{\prod_{i \in I} n_i}.$$

By Equation (2.3), $|\mathcal{U}| = n^2\theta$. Also, by Lemma 2.28,

$$|\mathcal{V}| = \frac{n^2}{\prod_{i \in \{m\}} n_i} = n.$$

Therefore, $|\mathcal{H}_A| \leqslant n(n\theta + 1)$.

To count $|H_\Lambda|$, define the following subsets of H_Λ:

- $U = \{\langle h_1, \ldots, h_m \rangle \in H_\Lambda \,:\, h_i = n_i/2 \text{ for some } i \in [m-1]\}$.
- $V = \{\langle h_1, \ldots, h_m \rangle \in H_\Lambda \,:\, h_m = n_m/2\}$

Then $|H_\Lambda| = |U| + |V| - |U \cap V|$. Notice that, for fixed $i \in [m-1]$, there are

$$(n-1) \prod_{\substack{j \in [m-1] \\ j \neq i}} n_j = (n-1)\frac{n}{n_i}$$

toroidal vectors $\langle h_1, \ldots, h_m \rangle \in H_\Lambda$ with $h_i = n_i/2$ (all entries are free to choose, except the i-th entry, which is fixed, and the $n-1$ factor is because h_m could be any

reminder modulo n_m except zero). It follows from the inclusion-exclusion principle and Equation (2.3) that

$$|U| = (n-1)\sum_{\substack{I\subseteq E\\ I\neq\emptyset}}(-1)^{|I|+1}\frac{n}{\prod_{i\in I} n_i} = (n-1)n\theta.$$

On the other hand, $|V| = n-1$ because, for $\langle h_1,\ldots,h_m\rangle \in V$, $h_i,\ldots,h_{m-1}$ can be chosen freely except for all zero. Finally, $|U\cap V| = \frac{|U|}{n-1} = n\theta$. Then,

$$|H_\Lambda| = (n-1)n\theta + (n-1) - n\theta = (n-1)(n\theta+1) - n\theta.$$

We conclude that

$$|\mathcal{H}_A| - |H_\Lambda| \leqslant n(n\theta+1) - (n-1)(n\theta+1) + n\theta = 2n\theta + 1.$$

By assumption, $2n\theta + 1 < n-1$, so the result follows from Lemma 2.26. □

Notice that for a Costas array of even order defined by a bijection

$$\varphi : [n_1]\times[n_2]\times\cdots\times[n_{m-1}] \longrightarrow [n_m],$$

if n_i if very large for all $i\in[m]$, then θ, as defined above, is close to zero, while $\frac{n-2}{2n}$ is close to $1/2$, so we will have $\theta < \frac{n-2}{2n}$. Therefore, "large" Costas arrays defined by a bijection with one-dimensional image or one-dimensional domain are not periodic Costas.

The proof of Theorem 2.30 reveals another reason why we considered Costas arrays defined by a bijection with one-dimensional image. Notice that the multisets $\mathcal{U}$ and $\mathcal{V}$ can be defined for arbitrary bijections, not only those having one-dimensional

image. That is, if

$$\varphi : [n_1] \times \cdots \times [n_k] \longrightarrow [n_{k+1}] \times \cdots \times [n_m]$$

defines a Costas array, define $\mathcal{U}$ as the multiset of toroidal vectors for which at least one of the first k components is half the length of the array in the corresponding direction. Similarly, define $\mathcal{V}$ as the multiset of toroidal vectors with at least one of the last $m-k$ components being half the length of the array in the corresponding direction. As in the proof of Theorem 2.30, $|\mathcal{H}_A| = |\mathcal{U}| + |\mathcal{V}| - |\mathcal{U} \cap \mathcal{V}|$. The number $|H_\Lambda|$ is easy to count using the inclusion-exclusion principle. Hence, to obtain $|\mathcal{H}_A| - |H_\Lambda| < n - 1$, the hurdle is to get a sufficiently low upper bound for $|\mathcal{H}_A|$. This can be done by obtaining a large lower bound on $|\mathcal{U} \cap \mathcal{V}|$, but, as discussed after Theorem 2.27, we have no idea how to bound it. Of course, $|\mathcal{U} \cap \mathcal{V}| \geqslant 0$ so zero is the worst possible lower bound. When the image of φ is one-dimensional, even the worst possible lower bound is good enough; zero is good enough. When the image of φ has a higher-dimensional image, zero is not in general a reasonable lower bound for $|\mathcal{U} \cap \mathcal{V}|$.

Corollary 2.31. *Let A be a three-dimensional Costas array of size $n_1 \times n_2 \times n_1 n_2$. Any of the following imply that A is not a periodic Costas array:*

(i) n_1 and n_2 are odd.

(ii) n_1 and n_2 are even, and one of them is greater than 4.

(iii) n_1 is even greater than 2 and n_2 is odd, or vice versa.

Proof. Let A be a Costas array defined by a bijection $\varphi : [n_1] \times [n_2] \to [n_1 n_2]$, so that the order of A is $n = n_1 n_2$. Notice that we are implicitly assuming $n_1, n_2 > 1$, to avoid a degenerate three-dimensional array. If (i) holds, A has odd order and by Theorem 2.27, it is not periodic Costas.

Now assume n_1 and n_2 are even. Then $\theta = 1 - \frac{(n_1-1)(n_2-1)}{n_1 n_2}$ and

$$\begin{aligned}
\theta < \frac{n_1 n_2 - 2}{2 n_1 n_2} &\iff n_1 n_2 - (n_1 - 1)(n_2 - 1) < \frac{n_1 n_2 - 2}{2} \\
&\iff n_1 + n_2 - 1 < \frac{n_1 n_2 - 2}{2} \\
&\iff 2 < \frac{n_1 n_2}{n_1 + n_2} \qquad (2.4)
\end{aligned}$$

Inequality (2.4) holds if $n_1 > 4$ or $n_2 > 4$. Hence, by Theorem 2.30, (ii) implies A is not periodic Costas.

Finally, assume n_1 is even, n_2 is odd, and $n_1 > 2$. In this case, $\theta = 1 - \frac{n_1-1}{n_1}$. Hence,

$$\begin{aligned}
\theta < \frac{n_1 n_2 - 2}{2 n_1 n_2} &\iff n_1 n_2 - n_2(n_1 - 1) < \frac{n_1 n_2 - 2}{2} \\
&\iff 2 n_2 < n_1 n_2 - 2 \\
&\iff 2 < n_2(n_1 - 2). \qquad (2.5)
\end{aligned}$$

But n_2 odd, $n_2 > 1$, and $n_1 > 2$ ensures that inequality (2.5) holds. By Theorem 2.30, A is not periodic Costas. □

With a bit more work, we can say even more than in Corollary 2.31.

Theorem 2.32 (cf. Theorem 1.32)**.** *If A is a three-dimensional periodic Costas array, it has order 4.*

Proof. Let A be a three-dimensional periodic Costas array. Without loss of generality, we assume A is defined by a bijection $\varphi : [n_1] \times [n_2] \to [n_1 n_2]$, where $n_1 n_2$ is the order of A and $n_1 \leqslant n_2$. Since A is periodic Costas, by Corollary 2.31, there are only four possibilities:

(1) $n_1 = n_2 = 2$.

(2) $n_1 = 2$ and $n_2 = 4$.

(3) $n_1 = n_2 = 4$.

(4) $n_1 = 2$ and n_2 is odd.

We must show (2)–(4) cannot happen. By exhaustive computation we checked that there are no periodic Costas arrays among all the 8! bijections $\varphi : [2] \times [4] \to [8]$ and all 16! bijections $\varphi : [4] \times [4] \to [16]$.

Now we focus on case (4). Assume A is defined by a bijection $\varphi : [2] \times [k] \to [2k]$, for k odd. Fix $(x_0, y_0) \in \mathbb{Z}_2 \times \mathbb{Z}_k$, with $(x_0, y_0) \neq (0, 0)$. Let $\alpha = (a_1, a_2, a_3) \in A$. If $\omega = (w_1, w_2, w_3) \in A$ is such that the toroidal vector from α to ω has the form $\langle x_0, y_0, z\rangle$, for some $z \in \mathbb{Z}_{2k}^*$, then

$$w_1 - a_1 \equiv x_0 \pmod 2 \qquad \text{and} \qquad w_2 - a_2 \equiv y_0 \pmod n.$$

Since $w_1 \in [2]$ and $w_2 \in [k]$, their values are unique. But A is defined by the bijection φ, so we must have $w_3 = \varphi(w_1, w_2)$. Therefore, for each $\alpha \in A$, we found a unique $\omega \in A$ such that the toroidal vector from α to ω has the from $\langle x_0, y_0, z\rangle$, for some $z \in \mathbb{Z}_{2k}^*$. We conclude that there are exactly $2k$ toroidal vectors ω of such form. However, there are only $2k - 1$ possible choices for z in a toroidal vector of the form $\langle x_0, y_0, z\rangle$. Thus, by the pigeonhole principle, for each pair $(x_0, y_0) \in (\mathbb{Z}_2 \times \mathbb{Z}_k)^*$, there must be some $z_0 \in \mathbb{Z}_{2k}^*$ such that $\langle x_0, y_0, z_0\rangle$ is a repeated toroidal vector. In particular, let $x_0 = 0$, so there is a repeated toroidal vector with the form $\langle 0, y_0, z_0\rangle$. Notice that $y_0 \neq k/2$ because k is odd. If $z_0 \neq 2k/2 = k$, by Proposition 2.11, A is not periodic Costas, and the proof would be finished.

Let $z_0 = k$. That is, assume A has a repeated toroidal vector of the form $\langle 0, y, k\rangle$, for some $y \in \mathbb{Z}_k^*$. We claim that this repeated toroidal vector will satisfy the conditions in Corollary 2.12, so A is not periodic Costas. For the sake of a

contradiction, assume A has four dots

$$\alpha_1 = (a_{11}, a_{12}, a_{13}), \qquad \omega_1 = (w_{11}, w_{12}, w_{13}),$$
$$\alpha_2 = (a_{21}, a_{22}, a_{23}), \qquad \omega_2 = (w_{21}, w_{22}, w_{23}),$$

not satisfying the conditions in Corollary 2.12 and for which $\omega_1 - \alpha_1$ and $\omega_2 - \alpha_2$ are equal as toroidal vectors to $\langle 0, y, k\rangle \in \mathbb{Z}_2 \times \mathbb{Z}_k \times \mathbb{Z}_{2k}$. Then, since $0 \neq n_1/2 = 2/2 = 1$ and also $y \neq n_2/2 = k/2$ given that k is odd, the four dots do not satisfy the conditions in Corollary 2.12, we must have $w_{13} - a_{13} = k$, $w_{23} - a_{23} = -k$, and $a_{13} = w_{23}$. Then, $w_{13} - a_{13} = -(w_{23} - a_{23}) = -(a_{13} - a_{23})$, implying $w_{13} = a_{23}$. A is defined by the bijection φ, so all the dots of A can be expressed as $(\varphi^{-1}(z), z)$, for some $z \in [2k]$. Hence, $\alpha_1 = (\varphi^{-1}(a_{13}), a_{13})$ and $\omega_2 = (\varphi^{-1}(w_{23}), w_{23})$, which implies $\alpha_1 = \omega_2$, given that $a_{13} = w_{23}$. Similarly, $\omega_1 = \alpha_2$ because $w_{13} = a_{23}$. Therefore, $\omega_1 - \alpha_1$ and $\omega_2 - \alpha_2 = \alpha_1 - \omega_1$ are both equal as toroidal vectors to $\langle 0, y, k\rangle$.

Given that $\omega_1 - \alpha_1$ and $\omega_2 - \alpha_2 = -(\omega_1 - \alpha_1)$ are both equal as toroidal vectors to $\langle 0, y, k\rangle$, $w_{12} - a_{12} \equiv y \pmod{k}$ and $-(w_{12} - a_{12}) \equiv y \pmod{k}$. Then, $2(w_{12} - a_{12}) \equiv 0 \pmod{k}$, but k is odd and $a_{12}, w_{12} \in [k]$, so $w_{12} = a_{12}$. Then we must have $y = 0$. This is a contradiction because $y \in \mathbb{Z}_k^*$. $\square$

The statement of Theorem 2.32 raises a natural question. Are there periodic Costas arrays of order 4? As the reader should expect, the answer is yes. Periodic Costas arrays of size $2 \times 2 \times 4$ do exist. There are $4! = 24$ distinct bijections

$$\varphi : \{(1,1),\ (1,2),\ (2,1),\ (2,2)\} \to \{1,2,3,4\}.$$

By exhaustive computation, we found that, out of these 24 bijections, 16 define Costas arrays, and 8 are periodic Costas.

Example 2.33. Let $A : [2] \times [2] \times [4] \to \{0, 1\}$ be the array with set of dots

$$\{(1,1,1), \quad (1,2,2), \quad (2,1,4), \quad (2,2,3)\}.$$

This array can be seen in Figure 2.3. We can verify that this is a three-dimensional Costas array by computing all the difference vectors. Moreover, although quite a task to do by hand, checking all the 16 possibly distinct windows of size $2 \times 2 \times 4$ in its periodic extension, every window is also a Costas array. Therefore, this is a periodic Costas array.

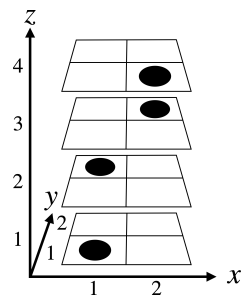


Figure 2.3: A three-dimensional periodic Costas array

Based on the above result and other computational results, we end this chapter with a conjecture.

Conjecture 2.34. *Let A be an m-dimensional Costas array of order n defined by a bijection*

$$\varphi : [n_1] \times \cdots \times [n_k] \longrightarrow [n_{k+1}] \times \cdots \times [n_m],$$

where $k \geqslant m - k$. If A is periodic Costas, $n = 2^k$. In particular, $n_1 = n_2 = \cdots = n_k = 2$.

From Theorem 1.32 and Theorem 2.32, we know the above conjecture is true for two-dimensional and three-dimensional Costas arrays. For two-dimensional arrays, the value of k as defined in Conjecture 2.34 must be 1, and it is true that all two-dimensional periodic Costas arrays have order $2^1 = 2$ (Theorem 1.32). For three-

dimensional ones, k must be 2, and yes, all three-dimensional periodic Costas arrays have order $2^2 = 4$ (Theorem 2.32).

Summary

In this Chapter 2, we start to develop our multidimensional theory of Costas arrays. We extend the definitions from Chapter 1 to define m-dimensional arrays, difference vectors, and toroidal vectors; (Definitions 2.1, 2.5 and 2.6, respectively). One of the summits of the chapter is the definition of m-dimensional Costas arrays (Definition 2.13). We also compare our definition with previous higher-dimensional analogs of Costas arrays [**7**, **19**, **24**].

We extend the definitions for two types of multidimensional periodicity: periodic Costas (Definition 2.20) and modular Costas (Definition 2.21), which are consistent with the two-dimensional definitions. However, we show that multidimensional modular Costas arrays do not exist (Theorem 2.25). On the other side of periodicity, we show that multidimensional Costas arrays of odd order are not periodic Costas (Theorem 2.27). Moreover, we show that "large" multidimensional Costas arrays of even order which are defined by a bijection with one-dimensional image, are not periodic Costas (Theorem 2.30). The latter result allow us to obtain a three-dimensional analog of Taylor's theorem [**30**]: three-dimensional periodic Costas arrays exist only of order 4, the least possible order (Theorem 2.32). We finish the chapter by conjecturing that this trend continues, i.e., the only multidimensional periodic Costas arrays have the least possible order (Conjecture 2.34).

Even though we showed the non-existence of multidimensional modular Costas arrays and the non-existence of large classes of multidimensional periodic Costas arrays, we obtain multidimensional periodicity if we relax the bijective condition on Costas arrays. This is done in the next chapter.

Chapter 3

Multidimensional Circular Costas Arrays

> **cycle** cy · cle \'sī-k əl\(noun) **1 :** an interval of time during which a sequence of a recurring succession of events or phenomena is completed **2a :** a course or series of events or operations that recur regularly and usually lead back to the starting point **2b :** one complete performance of a vibration, electric oscillation, current alternation, or other periodic process **2c :** a permutation of a set of ordered elements in which each element takes the place of the next and the last becomes first

As we saw in the previous chapter, there is not much hope for Costas arrays to preserve the Costas property when extended periodically. In particular, we showed that, for a three-dimensional Costas array to preserve the Costas property periodically, it must have order 4, the least possible order. But, as with the two-dimensional case, is there a way to obtain "almost" Costas arrays that preserve the Costas property periodically? The answer is yes. The definition of circular Costas arrays, as given in Definition 1.34, is easily generalized to produce "almost" multidimensional permu-

tation arrays preserving the Costas property periodically. As done in Section 1.6, we will construct those arrays by considering modular periodicity.

3.1 Circular Costas Maps

Recall that, in the two-dimensional case, we defined as *modular Costas maps* those bijections $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n$ satisfying the distinct modular difference property. It is natural, then, to define an *m-dimensional modular Costas map* as a bijection

$$\varphi : \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k} \longrightarrow \mathbb{Z}_{n_{k+1}} \times \mathbb{Z}_{n_{k+2}} \times \cdots \times \mathbb{Z}_{n_m},$$

satisfying the distinct modular difference property, i.e., all additions and differences taken in the corresponding group. Nonetheless, any finite abelian group is isomorphic to the direct product of cyclic groups, hence, a multidimensional modular Costas map can be more generally defined as a bijection $\varphi : G_1 \to G_2$, where G_1 and G_2 are finite abelian groups, and φ satisfies the distinct difference property: for any $k \in G_1^* = G_1 \setminus \{0\}$ and all $i, j \in G_1$,

$$\varphi(i+k) - \varphi(i) = \varphi(j+k) - \varphi(j) \implies i = j, \tag{3.1}$$

where all additions and differences are taken in the corresponding group. But, for the same reason as with $G_1 = G_2 = \mathbb{Z}_n$, for general abelian groups G_1 and G_2, bijections satisfying the distinct difference property do not exist [**9**, Theorem 1]. The reason: every m-dimensional Costas array has repeated toroidal vectors.

Walking down a road parallel to Section 1.6, we relax the conditions on Costas modularity by considering an injective function $\varphi : G_1 \to G_2$, with $\mathrm{Im}(\varphi) = G_2 \setminus \{g\}$, for some $g \in G_2$. This is an "almost" surjective function; it only misses a single element in the codomain. With this configuration, we will produce multidimensional

arrays, which are "almost" permutation arrays preserving the Costas property periodically in all directions.

As the reader will see, in this chapter, we generalize almost all the results presented in Section 1.6. Now we formally introduce the main character of this story.

Definition 3.1 (cf. Definition 1.34)**.** Let G_1 and G_2 be two finite abelian groups, $|G_1| + 1 = |G_2|$. A map $\varphi : G_1 \to G_2$ is called **circular Costas** if it is injective and if, for all $k \in G_1^*$, the difference map

$$\Delta_{\varphi,k} : G_1 \to G_2, \qquad i \mapsto \varphi(i+k) - \varphi(i)$$

is injective. If $\mathrm{Im}(\varphi) = G_2^*$, we say that φ is a **standard** circular Costas map.

Definition 3.2. Let $\varphi_1 : G_1 \to G_2$ and $\varphi_2 : H_1 \to H_2$ be circular Costas maps. We say that φ_1 and φ_2 are **isomorphic** if there exist two isomorphisms $\psi_1 : G_1 \to H_1$ and $\psi_2 : G_2 \to H_2$ such that

$$\varphi_1(x) = y \iff \varphi_2(\psi_1(x)) = \psi_2(y).$$

Although Definition 3.1 is the higher-dimensional generalization of Definition 1.34, there is slight difference between the two definitions. In Definition 1.34 we define a two-dimensional circular Costas <u>array</u> defined by an injective function, while in Definition 3.1 we do not define an array, but rather, we call the injective function "circular Costas". We did not define an m-dimensional circular Costas array because it is possible for a single circular Costas map $\varphi : G_1 \to G_2$ to define several arrays, each in different dimensions, depending on the number of factors in the chosen decomposition of G_1 and G_2 as product of cyclic groups (see Example 3.3 below). Nonetheless, the results we will present in this chapter do not depend on the particular decomposition, hence our choice towards abstraction by defining circular

Costas maps as bijections between arbitrary finite abelian groups.

Example 3.3. Let α be a primitive element in $\mathbb{F}_{25}$. Consider the map

$$\varphi : \mathbb{Z}_{24} \to (\mathbb{F}_{25}, +), \qquad i \mapsto \alpha^i.$$

This is a circular Costas map (shown in Proposition 3.5 below). Let $\psi_1 : \mathbb{Z}_{24} \to \mathbb{Z}_8 \times \mathbb{Z}_3$ and $\psi_2 : \mathbb{F}_{25} \to \mathbb{Z}_5 \times \mathbb{Z}_5$ be group isomorphisms. By making the identification $\mathbb{Z}_n = \{0, 1, \ldots, n-1\} \subset \mathbb{Z}$, the map

$$\varphi_1 : \mathbb{Z}_{24} \to \mathbb{Z}_5 \times \mathbb{Z}_5, \qquad i \mapsto \psi_2(\alpha^i),$$

defines a three-dimensional binary array preserving the Costas property periodically in all three directions. That is, any $24 \times 5 \times 5$ window of its periodic extension has no repeated toroidal vectors; hence no repeated difference vectors.

On the other hand, the map

$$\varphi_2 : \mathbb{Z}_8 \times \mathbb{Z}_3 \to \mathbb{Z}_5 \times \mathbb{Z}_5, \qquad \psi_1(i) \mapsto \psi_2(\alpha^i),\ i \in \mathbb{Z}_{24},$$

defines a 4-dimensional binary array preserving the Costas property periodically in all four directions. This means that every $8 \times 3 \times 5 \times 5$ window of its periodic extension has no repeated toroidal vectors and, therefore, no repeated difference vectors.

If we set $G_1 = \mathbb{Z}_n$ and $G_2 = \mathbb{Z}_{n+1}$, Definition 3.1 reduces to the definition given for two-dimensional circular Costas arrays (Definition 1.34). Moreover, standard circular Costas maps with $G_1 = \mathbb{Z}_{p^m-1}$ and $G_2 = \mathbb{Z}_p^m$ are exactly what Ortiz-Ubarri et al. [**24**] defined as *multidimensional periodic Costas arrays* (Definition 2.17 in this thesis). Hence, our definition of circular Costas is more general than that of Ortiz-Ubarri et al.

In the two-dimensional setting, the Welch construction yields circular Costas

maps. In fact, all two-dimensional circular Costas maps are those obtained from the Welch construction (Theorem 1.50). Once again, the narrative seems to extend to higher dimensions almost verbatim, because using [**14**, Section VI, Construction A], the Welch construction can be generalized to produce multidimensional circular Costas arrays.

Definition 3.4 (cf. [**14**])**.** Let α be a primitive element in $\mathbb{F}_q$, with q a prime power, let $L \in \mathbb{F}_q[x]$ be linearized permutation polynomial, and let $c \in \mathbb{Z}$. A **multidimensional Welch map** is any map isomorphic to

$$\varphi : \mathbb{Z}_{q-1} \to (\mathbb{F}_q, +), \qquad i \mapsto L(\alpha^{i+c}). \tag{3.2}$$

Proposition 3.5. *Multidimensional Welch maps are standard circular Costas.*

Proof. Let $\varphi : G_1 \to G_2$ be a multidimensional Welch map. Without loss of generality, we may assume φ is as in (3.2). A linearized permutation polynomial is, by definition, a bijective linear operator from $\mathbb{F}_q$ to itself. Since $\alpha \in \mathbb{F}_q$ is primitive and L is a linearized permutation polynomial, φ is injective and $0 \notin \mathrm{Im}(\varphi)$. For fixed $k \in \mathbb{Z}_{q-1}^*$, consider the difference map

$$\Delta_{\varphi,k} : \mathbb{Z}_{q-1} \to \mathbb{F}_q, \qquad i \mapsto \varphi(i+k) - \varphi(i).$$

Then,

$$\begin{aligned}
\Delta_{\varphi,k}(i) = \Delta_{\varphi,k}(j) &\implies \varphi(i+k) - \varphi(i) = \varphi(j+k) - \varphi(j) \\
&\implies L(\alpha^{i+c+k}) - L(\alpha^{i+c}) = L(\alpha^{j+c+k}) - L(\alpha^{j+c}) \\
&\implies L(\alpha^{i+c+k} - \alpha^{i+c}) = L(\alpha^{j+c+k} - \alpha^{j+c}) \\
&\implies \alpha^i \alpha^c (\alpha^k - 1) = \alpha^j \alpha^c (\alpha^k - 1) \\
&\implies \alpha^i = \alpha^j
\end{aligned}$$

$$\implies i = j.$$

Hence, the difference map is injective. We conclude that φ is a standard circular Costas map. $\square$

Remark 3.6. When q is a prime, $q = p$, the only monic linearized permutation polynomial $L \in \mathbb{F}_p$ is $L(x) = x$, which as a function is the identity. Therefore, the map φ in (3.2) has the rule $i \mapsto L(\alpha^{i+c}) = \alpha^{i+c}$, and we get back the two-dimensional Welch construction (see Proposition 1.18 and the discussion at the beginning of Section 1.6.1). If L is not monic, the non-zero leading coefficient can be expressed as a power of α, so it will be absorbed by the constant c.

In [**24**], Ortiz-Ubarri et al. gave four conjectures regarding circular Costas maps, three of which we state now. The fourth conjecture needs some context that is out of the scope of this thesis.

Conjecture 3.7 ([**24**, Conjecture 4])**.** *If $\varphi : G_1 \to G_2$ is circular Costas, G_2 is elementary abelian.*

Conjecture 3.8 ([**24**, Conjecture 2])**.** *The number of standard circular Costas maps $\varphi : \mathbb{Z}_{p^2-1} \to \mathbb{Z}_p^2$ is at least*

$$\frac{\phi(p^2-1)}{2}(p^2-p)(p^2-1), \tag{3.3}$$

where ϕ is the Euler's totient function.

Conjecture 3.9 ([**24**, Conjecture 3])**.** *For $m \geqslant 3$, the number of standard circular Costas maps $\varphi : \mathbb{Z}_{p^m-1} \to \mathbb{Z}_p^m$ is at least*

$$\frac{\phi(p^m-1)}{m}(\phi(p^m-1)-1)(p^m-1)(p-1)^{m-1}p^{m-1}, \tag{3.4}$$

where ϕ is the Euler's totient function.

A sneak peek: Conjecture 3.7 and Conjecture 3.8 will be proved towards the end of this section and in Section 3.3, respectively. On the other hand, we have reasons to believe that Conjecture 3.9 is "kind of" false. More precisely, we will show that Conjecture 3.9 is true for $m \geqslant 4$, but we think it is false for $m = 3$, and we discuss why in Section 3.3.

In this more abstract context where *circular Costas arrays* are maps between two finite abelian groups G_1 and G_2, our friendly toroidal vectors are now tuples $\langle k, h\rangle \in G_1 \times G_2$. Moreover, since the dots of the array generated by the circular Costas map $\varphi : G_1 \to G_2$ have the form $(i, \varphi(i))$, for $i \in G_1$, two distinct dots cannot be equal in their first component. Hence, if $\langle k, h\rangle$ is a toroidal vector, $k \neq 0$. Similarly, since φ is injective, two distinct dots cannot be equal in their second components, showing that $h \neq 0$. Therefore, toroidal vectors are drawn from $G_1^* \times G_2^*$. But we can say even more.

Proposition 3.10 (cf. Proposition 1.38)**.** *Let A be the array defined by the circular Costas map $\varphi : G_1 \to G_2$. Every tuple $\langle k, h\rangle \in G_1^* \times G_2^*$ occurs exactly once as a toroidal vector in A. In particular, A has no repeated toroidal vectors.*

Proof. If A is the binary array defined by the circular Costas map $\varphi : G_1 \to G_2$, the dots of A are $\{(i, \varphi(i)) : i \in G_1\}$. If $\langle k, h\rangle \in G_1^* \times G_2^*$ is a toroidal vector in A, there must be two distinct dots $(i, \varphi(i))$ and $(j, \varphi(j))$, with $i \neq j$, such that $k = j - i$ and $h = \varphi(j) - \varphi(i)$ (all operations in the corresponding group). That is,

$$h = \varphi(i + k) - \varphi(i) = \Delta_{\varphi,k}(i).$$

Hence, $\langle k, h\rangle \in G_1^* \times G_2^*$ is a toroidal vector if and only if there is some $i \in G_1$ for which $\Delta_{\varphi,k}(i) = h$. But in a circular Costas map, the difference map is injective and has image G_2^*, so such i always exists and is unique. $\square$

The following theorem is a *déjà vu* of what was already developed in Sec-

tion 1.6.

Theorem 3.11 (cf. Theorem 1.43)**.** *A map $\varphi : G_1 \to G_2$ is circular Costas if and only if the set $D = \{(i, \varphi(i)) : i \in G_1\}$ is a direct product difference set of order $n = |G_2| = |G_1| + 1$ in the abelian group $G_1 \times G_2$.*

Proof. Let $\varphi : G_1 \to G_2$ be a circular Costas map, and let $D = \{(i, \varphi(i)) : i \in G_1\}$. Notice that, if $d_i, d_j \in D$ with $d_i \neq d_j$, the difference $d_j - d_i$ is a toroidal vector in the array generated by φ. Then, by Proposition 3.10, D is a direct product difference set in $G_1 \times G_2$.

Conversely, assume $D = \{(i, \varphi(i)) : i \in G_1\}$ is a direct product difference set in $G_1 \times G_2$, for some map $\varphi : G_1 \to G_2$. To avoid the subgroup $\{0\} \times G_2$, φ must be injective. To avoid the subgroup $G_1 \times \{0\}$, $\varphi(i + k) - \varphi(i) \neq 0$ for all $i \in G_1$ and some fixed $k \in G_1^*$. Hence, the difference map $\Delta_{\varphi,k}(i) = \varphi(i + k) - \varphi(i)$ is injective. We conclude that φ is circular Costas. □

The next theorem establishes affirmatively Conjecture 3.7.

Theorem 3.12 (Conjecture 3.7)**.** *If $\varphi : G_1 \to G_2$ is circular Costas, G_2 is elementary abelian. That is, $G_2 \cong \mathbb{Z}_p^m$ for some natural m and prime p.*

Proof. Let $\varphi : G_1 \to G_2$ be circular Costas. Since φ is injective, $|G_1| + 1 = |G_2| = n$, for some natural n. By Theorem 3.11, $D = \{(i, \varphi(i)) : i \in G_1\}$ is a direct product difference set in $G_1 \times G_2$ of order n. Proposition 1.42 shows that G_2 must be elementary abelian. □

In light of Theorem 3.12, we give the following definition.

Definition 3.13. For a circular Costas map $\varphi : G_1 \to \mathbb{Z}_p^m$, the number m is called the **degree of** φ.

Remark 3.14. By Theorem 3.12, any circular Costas map has a unique degree.

Direct product difference sets were introduced by Ganley [**11**] to study finite projective planes admitting quasiregular collineation groups. In fact, a direct product difference set of order n in a group $G_1 \times G_2$ is equivalent to a projective plane of order n admitting a quasiregular collineation group isomorphic to $G_1 \times G_2$ [**11**, Theorem 4.3]. It is conjectured that projective planes that are equivalent to abelian direct product difference sets are all desarguesian [**20**, p. 216].

Conjecture 3.15 ([**20**, p. 216])**.** *Projective planes corresponding to abelian direct product difference sets are desarguesian.*

We already know from Proposition 1.42 that, if $G_1 \times G_2$ admits a direct product difference set, where G_1 and G_2 are abelian and $|G_1|+1 = |G_2|$, then G_2 is elementary abelian. In the case where the direct product difference set in the abelian group $G_1 \times G_2$ is equivalent to a desarguesian projective plane, it is known that G_1 must be cyclic [**27**, Theorem 3.4]. Hence, we set forth the following conjecture.

Conjecture 3.16. *If $\varphi : G_1 \to G_2$ is circular Costas, G_1 is cyclic.*

Finding a counterexample to Conjecture 3.16 will automatically imply the existence of a non-desarguesian finite projective plane of type (f) in the Dembowski-Piper classification [**5**] (see [**28**, Result 5.1.2] for a summarized statement). Those are the planes admitting a quasiregular collineation group isomorphic to $G_1 \times G_2$, where $|G_1| + 1 = |G_2|$.

Let us summarize what we have so far. Finite projective planes of type (f) in the Dembowski-Piper classification can be represented by direct product difference sets. Proposition 1.42 shows that, if D is a direct product difference set in the abelian group $G_1 \times G_2$ with $|G_1| + 1 = |G_2|$, then $G_2 \cong (\mathbb{F}_q, +)$. Theorem 3.11 shows that, from a direct product difference set in $G_1 \times \mathbb{F}_q$, we obtain a circular Costas map φ by setting

$$\varphi(i) = j \iff (i, j) \in D. \tag{3.5}$$

A function defined as in (3.5) is said to be **associated with the direct product difference set** D. If a finite projective plane corresponding to a direct product difference set in $G_1 \times \mathbb{F}_q$ is desarguesian, G_1 must be cyclic. For the converse, Pott [**27**] showed that another condition is required.

Proposition 3.17 ([**27**, Theorem 2.3])**.** *Let D be an abelian direct product difference set in $G \times \mathbb{F}_q$ with associated function f. The corresponding projective plane is desarguesian if and only if G is cyclic and D is equivalent to a direct product difference set whose associated function is an isomorphism onto $\mathbb{F}_q^*$.*

3.2 Costas Polynomials

In the context of Theorem 3.12, any circular Costas map φ has codomain isomorphic to $(\mathbb{F}_q, +)$ and domain G_1, for some abelian group G_1 of order $q-1$. Moreover, if Conjecture 3.16 were proven to be true, we may assume $G_1 \cong (\mathbb{F}_q^*, \times)$. Hence, by applying suitable isomorphisms (and assuming Conjecture 3.16 is true), any circular Costas map can be equivalently seen as an injective map $f : \mathbb{F}_q^* \to \mathbb{F}_q$. If, in addition, the original circular Costas map φ is standard, $\varphi(i) \neq 0$ for all $i \in G_1$, hence $f(x) \neq 0$ for all $x \in \mathbb{F}_q^*$. As we did in Section 1.6, we can extend the domain and the image of the map f by setting $f(0) = 0$. Such f is a bijection from $\mathbb{F}_q$ to itself, which can be expressed, by Lagrange interpolation, as a unique polynomial function of degree at most $q-1$. Hence, the concept of Costas polynomials over extension fields also makes sense in the context of multidimensional circular Costas maps.

Definition 3.18 ([**23**, Definition 2.4])**.** Let q be a prime power. A polynomial $f \in \mathbb{F}_q[x]$ is a **Costas polynomial** if $f(0) = 0$ and $f(dx) - f(x)$ is a permutation for all $d \in \mathbb{F}_q$, $d \neq 1$.

Notice that Definition 3.18 is the same as Definition 1.46 over extension fields.

Once again, we are extending the narrative from two dimensions into higher dimensions in a surprisingly straightforward and seamless way.

The definition of Costas polynomials over extension fields is introduced by Muratović-Rubić et al. [**23**, Definition 2.4]. However, the original concept of Costas polynomials was conceived by Golomb and Moreno [**15**, Section III], but over prime fields. Muratović-Rubić et al. extended the concept of Costas polynomials by considering the same object but over extension fields rather than prime fields. Our approach is entirely different. We started with circular Costas maps between finite abelian groups, and we ended up finding that these (standard) maps can be, if Conjecture 3.16 is true, conveniently represented as polynomial functions. For us, Costas polynomials are rediscovered in a meaningful way, not as a matter of simply changing p by q.

By how we developed the definition of Costas polynomials before Definition 3.18, the following two lemmas are quite obvious, but we state them anyway to dissipate all possible confusion.

Lemma 3.19. *Let q be a prime power. Any standard circular Costas map $\varphi : G_1 \to G_2$, with G_1 cyclic and $|G_1| = q - 1$, is isomorphic to a unique Costas polynomial $f \in \mathbb{F}_q[x]$ of degree at most $q - 1$.*

Proof. Let $\varphi : G_1 \to G_2$ be a standard circular Costas map with G_1 cyclic and $|G_1| = q - 1$. By Theorem 3.12, $G_2 \cong (\mathbb{F}_q, +)$. Then, by the definition of a circular Costas map, $|G_1| = q - 1$. Hence, $G_1 \cong (\mathbb{F}_q^*, \times)$.

Let $\psi_1 : G_1 \to (\mathbb{F}_q^*, \times)$ and $\psi_2 : G_2 \to (\mathbb{F}_q, +)$ be two group isomorphisms. Define the map $f : \mathbb{F}_q^* \to \mathbb{F}_q$, by the rule

$$\varphi(i) = j \iff f(\psi_1(i)) = \psi_2(j). \tag{3.6}$$

Notice that f is injective and $0 \notin \mathrm{Im}(f)$ because φ is standard. Extend the domain

of f from $\mathbb{F}_q^*$ to $\mathbb{F}_q$ by setting $f(0) = 0$. Evidently, f with the rule (3.6) is a Costas polynomial. Moreover, by Lagrangian interpolation, f is unique if we restrict it to have degree at most $q - 1$. $\square$

Remark 3.20. By Theorem 3.12, the codomain of any circular Costas map is a group with order a power of a prime, so $|G_2| = q$. By the definition of circular Costas map, $|G_1| = |G_2| - 1 = q - 1$; therefore, the assumption $|G_1| = q - 1$ in Lemma 3.19 is used only to establish notation, and it is not a restriction on the circular Costas map φ.

Lemma 3.21. *Let $f, g \in \mathbb{F}_q[x]$ be two polynomials for which $g \equiv f \pmod{x^q - x}$. Then, f is a Costas polynomial if and only if g is a Costas polynomial.*

Proof. If $g \equiv f \pmod{x^q - x}$, f and g are equal as functions over $\mathbb{F}_q$. The result follows. $\square$

Recall that finite projective planes corresponding to abelian direct product difference sets are conjectured to be desarguesian (Conjecture 3.15). If this conjecture is true, by Proposition 3.17, any direct product difference set D must exist in a group isomorphic to $\mathbb{F}_q^* \times \mathbb{F}_q$, and the associated function $f : \mathbb{F}_q^* \to \mathbb{F}_q$ defined by the rule

$$f(x) = y \iff (x, y) \in D,$$

must be a group automorphism of $\mathbb{F}_q^*$, so $f(x) = x^s$, for $\gcd(s, q-1) = 1$. Therefore, by Proposition 3.17 and the Definition 1.41, Conjecture 3.15 is equivalent to assuming that, if D is a direct product difference set, there exists some positive integer s with $\gcd(s, q-1) = 1$, a constant $(a, b) \in \mathbb{F}_q^* \times \mathbb{F}_q$, and $\psi = (\psi_{\mathbb{F}_q^*}, \psi_{\mathbb{F}_q}) \in \mathrm{Aut}(\mathbb{F}_q^* \times \mathbb{F}_q)$, such that $D = (a, b) \cdot \psi(D')$, where

$$D' = \left\{(x, x^s) \,:\, x \in \mathbb{F}_q^*\right\} \subseteq \mathbb{F}_q^* \times \mathbb{F}_q.$$

That is,

$$D = \left\{(a \cdot \psi_{\mathbb{F}_q^*}(x),\ b + \psi_{\mathbb{F}_q}(x^s)) \ :\ x \in \mathbb{F}_q^*\right\}.$$

But $\psi_{\mathbb{F}_q^*}(x) = x^t$ for some t with $\gcd(t, q-1) = 1$. Hence by taking $s' = st$, we have $\gcd(s', q-1) = 1$ and

$$D = \left\{(a \cdot x,\ b + \psi_{\mathbb{F}_q}(x^{s'})) \ :\ x \in \mathbb{F}_q^*\right\} = (a, b) \cdot \left\{(x, \psi_{\mathbb{F}_q}(x^{s'})) \ :\ x \in \mathbb{F}_q^*\right\}.$$

The group automorphism $\psi_{\mathbb{F}_q}$ is a linear operator on $\mathbb{F}_q$, so it can be realized as a linearized permutation polynomial $L(x) \in \mathbb{F}_q[x]$.

The above discussion proves the following proposition.

Proposition 3.22 (Equivalent to Proposition 3.17)**.** *Let D be an abelian direct product difference set in G. The projective plane corresponding to D is desarguesian if and only if $G \cong \mathbb{F}_q^* \times \mathbb{F}_q$ and there is some $s \leqslant q-1$, $\gcd(s, q-1) = 1$, a constant $(a, b) \in \mathbb{F}_q^* \times \mathbb{F}_q$, and a linearized permutation polynomial $L(x) \in \mathbb{F}_q[x]$, for which*

$$D = \left\{(a \cdot x,\ b + L(x^s)) \ :\ x \in \mathbb{F}_q^*\right\} \subseteq \mathbb{F}_q^* \times \mathbb{F}_q. \tag{3.7}$$

It is fairly straightforward to see that, for any direct product difference set $D \subseteq \mathbb{F}_q^* \times \mathbb{F}_q$ and any $\psi \in \mathrm{Aut}(\mathbb{F}_q^* \times \mathbb{F}_q)$, we can choose a suitable constant $b \in \mathbb{F}_q$ for which D is equivalent to the direct product difference set $D' = (1, b) \cdot \psi(D)$, where $(x, 0) \notin D'$ for any $x \in \mathbb{F}_q^*$. Hence, without loss of generality, we can assume that for any direct product difference set D in $\mathbb{F}_q^* \times \mathbb{F}_q$, $(x, 0) \notin D$ for any $x \in \mathbb{F}_q^*$. In other words, we may assume the function $f : \mathbb{F}_q^* \to \mathbb{F}_q$ associated to D is such that $0 \notin \mathrm{Im}(f)$. Therefore, by following the proof of Theorem 3.11, setting $G_1 = \mathbb{F}_q^*$ (with multiplicative notation, of course) and $G_2 = \mathbb{F}_q$, a set D is a direct product difference set in $\mathbb{F}_q^* \times \mathbb{F}_q$ if and only if the associated function is a Costas polynomial $f \in \mathbb{F}_q[x]$ (see a formal proof in [**23**, Lemma 3.3]).

Now consider the direct product difference set in (3.7) with (a, b) as the identity, i.e., $a = 1$ and $b = 0$. For a linearized permutation polynomial $L(x) \in \mathbb{F}_q[x]$, $L(0) = 0$. Therefore, if $L(x^s)$, with $\gcd(s, q-1) = 1$, is interpreted as a function from $\mathbb{F}_q^*$ to $\mathbb{F}_q$, $0 \notin \mathrm{Im}(L(x^s))$. Therefore, $L(x^s)$ is the associated function of the direct product difference set $D = \left\{(x, L(x^s)) : x \in \mathbb{F}_q^*\right\}$, so $L(x^s)$ must be a Costas polynomial. This class of Costas polynomials over extension fields was introduced by Muratović-Rubić et al. [**23**].

Proposition 3.23 ([**23**, Corollary 4.2])**.** *If $L(x) \in \mathbb{F}_q[x]$ is a linearized permutation polynomial and $\gcd(s, q-1) = 1$, $L(x^s)$ is a Costas polynomial.*

Proof. Let $f(x) = L(x^s)$. $L(0) = 0$, therefore $f(0) = 0$. For any $d \in \mathbb{F}_q, d \neq 1$,

$$\begin{aligned} f(dx) - f(x) &= L(d^s x^s) - L(x^s) \\ &= L((d^s - 1)x^s). \end{aligned}$$

Since $d^s \neq 1$, $L((d^s - 1)x^s)$ is the composition of permutations, thus a permutation. Then f is a Costas polynomial. □

Combining Proposition 3.23 with Proposition 3.22, an equivalent formulation of Conjecture 3.15 in terms of Costas polynomials is obtained:

Conjecture 3.24 (Conjecture 4.4 in [**23**]; equivalent to Conjecture 3.15)**.** *If $f \in \mathbb{F}_q$ is a Costas polynomial, $f(x) \equiv L(x^s) \pmod{x^q - x}$, where $L(x) \in \mathbb{F}_q[x]$ is a linearized permutation polynomial and $\gcd(s, q-1) = 1$.*

Remark 3.25. The statement in Conjecture 3.24 is my interpretation of Conjecture 4.4 in [**23**], which states: *All Costas polynomials over $\mathbb{F}_q$ are of the form given in Corollary 4.2.*[I] One could misinterpret the conjecture as the assertion that all Costas

[I] **Corollary 4.2 in [23].** *Let $q = p^e$ with $e \geq 1$ and let $f \in \mathbb{F}_q[x]$. The polynomial $f = \sum_{i=0}^{e-1} a_i x^{sp^i}$ is a Costas polynomial if $\sum_{i=0}^{e-1} a_i x^{p^i}$ is a permutation polynomial and $\gcd(s, q-1)) = 1$.*

polynomials must have the form $L(x^s)$, where $L(x) \in \mathbb{F}_q[x]$, $q = p^m$, is a linearized permutation polynomial $L(x) = \sum_{i=0}^{m-1} c_i x^{p^i}$, and where $\gcd(s, q-1) = 1$. However, as Example 3.26 below shows, that assertion is false.

Example 3.26. Let $\alpha \in \mathbb{F}_9$ be a root of the primitive polynomial $y^2+2y+2 \in \mathbb{F}_3[y]$. By computation one can verify that the polynomial $f(x) = x^7 + \alpha x^5 \in \mathbb{F}_9[x]$ is a Costas polynomial. However, f is not a polynomial of the form $L(x^s)$. Linearized permutation polynomials over $\mathbb{F}_9$ have the form $L(x) = c_1x^3 + c_0x$, and clearly there is no integer s for which $L(x^s) = c_1x^{3s} + c_0x^s$ is equal to $x^7 + \alpha x^5$. Nonetheless, for $L(x) = x^3 + \alpha x$, which is a linearized permutation polynomial,

$$x^7 + \alpha x^5 \equiv L(x^5) \pmod{x^9 - x}.$$

Lo and behold: the polynomials in Conjecture 3.24 correspond to the multidimensional Welch maps of Definition 3.4, so Conjecture 3.24 may be rephrased to assert that any circular Costas map is multidimensional Welch. For the particular case of two-dimensional arrays, this is the Golomb-Moreno conjecture! Once more, everything seems to extend into higher dimensions beautifully and surprisingly. Take a primitive element $\alpha \in \mathbb{F}_q$, a linearized permutation polynomial $L(x) \in \mathbb{F}_q[x]$, a constant $c \in \mathbb{Z}$, and consider the multidimensional Welch map

$$\varphi : \mathbb{Z}_{q-1} \to (\mathbb{F}_q, +), \qquad i \mapsto L(\alpha^{i+c}).$$

To obtain the Costas polynomial corresponding to φ, we need a group isomorphism $\psi : \mathbb{Z}_{q-1} \to \mathbb{F}_q^*$. Take $\psi(i) = \beta^i$, where β is a primitive element in $\mathbb{F}_q$. The Costas polynomial $f \in \mathbb{F}_q[x]$ corresponding to the multidimensional Welch map is the polynomial interpolating the points

$$f(\psi(i)) = \varphi(i) \implies f(\beta^i) = L(\alpha^{i+c}).$$

But $\alpha = \beta^s$, for some s with $\gcd(s, q-1) = 1$. Hence, by substituting $\alpha = \beta^s$ and taking $a = \alpha^c$, $f(x) = L(ax^s)$. Moreover, we can choose a suitable linearized permutation polynomial L' such that $L(ax) = L'(x)$. We end up with $f(x) = L'(x^s)$, where L' is a linearized permutation polynomial and $\gcd(s, q-1) = 1$. Hence, without any doubt, the polynomials in Conjecture 3.24 correspond to multidimensional Welch maps.

Conjecture 3.27 (Equivalent to Conjecture 3.15 and Conjecture 3.24)**.** *All standard circular Costas maps are multidimensional Welch.*

3.3 Counting Costas Polynomials

By Lemma 3.19, counting the number of Costas polynomials is the same as counting the number of standard circular Costas maps with cyclic domain. Of course, if Conjecture 3.24 were to be true, the number of Costas polynomials (of degree at most $q-1$) and hence the number of standard circular Costas maps with cyclic degree should be exactly the number of inequivalent Costas polynomials of the type $L(x^s)$, for $L(x) \in \mathbb{F}_q[x]$ a linearized permutation polynomial and $\gcd(s, q-1) = 1$. However, regardless of whether Conjecture 3.24 is true or not, counting the number of Costas polynomials of the type $L(x^s)$, we will obtain a lower bound on the number of standard circular Costas maps with cyclic degree and, therefore, a lower bound on general standard circular Costas maps.

Theorem 3.28. *The number of distinct Costas polynomials over $\mathbb{F}_{p^m}$ (distinct modulo $x^{p^m} - x$) of the form $L(x^s)$, for some linearized permutation polynomial $L(x) \in \mathbb{F}_{p^m}[x]$ and $\gcd(s, p^m - 1) = 1$, is*

$$\frac{\phi(p^m - 1)}{m} \prod_{k=0}^{m-1} (p^m - p^k). \tag{3.8}$$

Proof. Let $q = p^m$, p prime. The polynomials of the form $\sum_{i=0}^{m-1} c_i x^{p^i} \in \mathbb{F}_q[x]$ are linearized polynomials. Form [**32**, Theorem 2.1], there are

$$\prod_{k=0}^{m-1} (p^m - p^k)$$

distinct (modulo $x^q - x$) linearized permutation polynomials over $\mathbb{F}_q$.

Assume $L(x) = \sum_{i=0}^{m-1} c_i x^{p^i}$ is a linearized permutation polynomial. Since we will consider the polynomials modulo $x^q - x$, consider only $s < q-1$ with $\gcd(s, q-1) = 1$. There are $\phi(q-1)$ choices of s for which $L(x^s)$ is a Costas polynomial.

Now we have to count the number of distinct ways we can produce the same Costas polynomial modulo $x^q - x$. Let $L_0(x) = \sum_{i=0}^{m-1} c_i x^{p^i}$ be a linearized permutation polynomial over $\mathbb{F}_q$ and fix s_0 with $\gcd(s_0, q-1) = 1$. Assume there is a linearized permutation polynomial $L(x) = \sum_{i=0}^{m-1} b_i x^{p^i}$ and a number $s < q-1$ with $\gcd(s, q-1) = 1$, such that

$$L(x^s) \equiv L_0(x^{s_0}) \pmod{x^q - x}.$$

By comparing the powers of x, we must have $s \equiv s_0 p^k \pmod{q-1}$ for some integer k satisfying $0 \leqslant k \leqslant m-1$. Then,

$$L(x^s) \equiv L(x^{s_0 p^k}) \equiv \sum_{i=0}^{m-1} b_i x^{s_0 p^{k+i}} \equiv L_0(x^{s_0}) \pmod{x^q - x}.$$

Therefore, by comparing coefficients, $b_i = c_{i+k}$, with the index $i+k$ considered modulo m, implying $L(x^{p^k}) \equiv L_0(x)$. The converse is clearly true.

This shows that $L(x^s) \equiv L_0(x^{s_0})$ if and only if $L(x^{p^k}) \equiv L_0(x)$ and $s \equiv s_0 p^k \pmod{q-1}$, for some k, where $0 \leqslant k \leqslant m-1$. We conclude that there are exactly m distinct ways to obtain the same Costas polynomial, one for each selection of k. Equation (3.8) follows from the multiplicative principle. □

By Lemma 3.19, the number in (3.8) is a lower bound on the number of

standard circular Costas maps. Hence, Theorem 3.28 above makes all the heavy lifting required to prove Conjecture 3.8, to the point that it becomes a mere corollary.

Corollary 3.29 (Conjecture 3.8)**.** *The number of standard circular Costas maps* $\varphi : \mathbb{Z}_{p^2-1} \to \mathbb{Z}_p^2$ *is at least*

$$\frac{\phi(p^2-1)}{2}(p^2-p)(p^2-1).$$

Proof. Follows from Lemma 3.19 and Theorem 3.28 with $m = 2$. □

For $m \geqslant 3$, let us compare the lower bound on the number of standard circular Costas maps given in Theorem 3.28 with the lower bound given in Conjecture 3.9. Consider the ratio between the two lower bounds:

$$R(p,m) = \frac{\frac{\phi(p^m-1)}{m}\prod_{k=0}^{m-1}(p^m-p^k)}{\frac{\phi(p^m-1)}{m}(\phi(p^m-1)-1)(p^m-1)(p-1)^{m-1}p^{m-1}}. \tag{3.9}$$

If $R(p,m) \geqslant 1$ for any prime p and any integer $m \geqslant 3$, Conjecture 3.9 would be proved. Let us simplify the expression in (3.9). For $m \geqslant 3$, we can rewrite

$$\begin{aligned}\prod_{k=0}^{m-1}(p^m-p^k) &= (p^m-1)\prod_{k=1}^{m-1}p^k(p^{m-k}-1)\\ &= (p^m-1)p^{\sum_{k=1}^{m-1}k}\prod_{k=1}^{m-1}(p^{m-k}-1)\\ &= (p^m-1)p^{\frac{m(m-1)}{2}}(p-1)^{m-1}\prod_{k=1}^{m-1}\frac{p^{m-k}-1}{p-1}.\end{aligned} \tag{3.10}$$

Moreover, the product on the far right of (3.10) can be bounded below by

$$\prod_{k=1}^{m-1}\frac{p^{m-k}-1}{p-1} = (p+1)\prod_{\substack{k=1\\k\neq m-2}}^{m-1}\frac{p^{m-k}-1}{p-1} \geqslant p+1, \tag{3.11}$$

where equality holds only when $m = 3$. Therefore, by using (3.10), we can simplify

(3.9) to obtain

$$R(p,m) = \frac{p^{\frac{(m-1)(m-2)}{2}} \prod_{k=1}^{m-1} \frac{p^{m-k}-1}{p-1}}{\phi(p^m-1)-1}. \tag{3.12}$$

From (3.11) and (3.12), for $m \geqslant 4$,

$$R(p,m) > \frac{p^{\frac{(m-1)(m-2)}{2}}(p+1)}{\phi(p^m-1)-1} > \frac{p^m}{\phi(p^m-1)-1} > 1.$$

This shows that, for $m \geqslant 4$, the lower bound given in Theorem 3.28 for the number of standard circular Costas maps of degree m is better than the one given in Conjecture 3.9. Hence, we have shown Conjecture 3.9, except for $m = 3$.

Proposition 3.30. *For $m \geqslant 4$, the number of standard circular Costas maps $\varphi : \mathbb{Z}_{p^m-1} \to \mathbb{Z}_p^m$ is greater than*

$$\frac{\phi(p^m-1)}{m}(\phi(p^m-1)-1)(p^m-1)(p-1)^{m-1}p^{m-1},$$

where ϕ is the Euler's totient function.

The case $m = 3$ yields a different conclusion. Consider

$$R(p,3) = \frac{p(p+1)}{\phi(p^3-1)-1}.$$

It happens that $R(2,3) = 6/5 > 1$ and $R(3,3) = 12/11 > 1$. However, $R(5,3) = 30/59 < 1$. In fact, it appears that $R(p,3) < 1$ for $p \geqslant 5$ (see Figure 3.1). Thus, for $m = 3$, the lower bound given in Theorem 3.28 is almost never better than the one given in Conjecture 3.9.

If Conjecture 3.9 ought to be true for $m = 3$, it would imply that Conjecture 3.24, and hence the equivalent Conjecture 3.15, are both false. Moreover, if there is some prime power $q = p^m$ for which the number of standard circular Costas maps is greater than the number in (3.8), it would imply that Conjecture 3.24 is false.

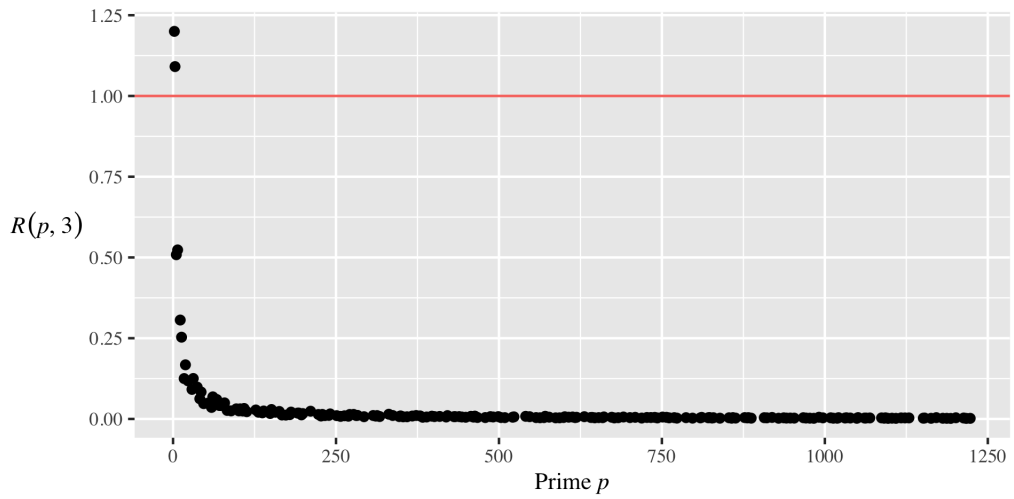


Figure 3.1: Asymptotic behavior of $R(p, 3)$

The perception of the author is that Conjecture 3.24 is true, while Conjecture 3.9 is false (for $m = 3$). The falsehood of Conjecture 3.9 could be checked computationally by constructing all the standard circular Costas maps for the smallest p for which $R(p, 3) < 1$, i.e., $p = 5$. However, the computer would need to check the Costas property for all the $(5^3 - 1)! = 124!$ possible permutation polynomials of $\mathbb{F}_{5^3}$ fixing zero. We do not have the computational resources for this computation to finish in a reasonable time.

3.4 Shifting Costas Polynomials

In this, which is the final section of the chapter and the final section of this thesis, we will prove a weaker version of the conjecture on the characterization of Costas polynomials as the composition of linearized permutation polynomials with permutation monomials, Conjecture 3.24. We do it by following the ideas carved by Moreno [**21**] in the context of two-dimensional circular Costas arrays.

Golomb and Moreno in [**15**] defined circular Costas maps, established a relationship with permutation polynomials, and conjectured that the only Costas polyno-

mials over $\mathbb{F}_p$ are permutation monomials (Conjecture 1.49). Before Muratović-Rubić et al. [**23**, Theorem 3.4] gave a proof of Conjecture 1.49, Moreno in [**21**] proved a weaker version, adding a condition on Costas polynomials. Moreno proved that a polynomial is a shifting Costas polynomial if and only if it is a permutation monomial; he added the "shifting" condition to the Costas polynomials. We want to clarify that all the Costas polynomials in the above discussion were defined over prime fields.

We shall do the same Moreno did for Costas polynomials over prime fields, but for Costas polynomials over extension fields; see Theorem 3.34 below. However, our proof is completely different to that of Moreno [**21**].

Definition 3.31 (cf. Definition 1.54)**.** Let q be a prime power. A **shifting Costas polynomial** is a permutation polynomial $f \in \mathbb{F}_q[x]$ for which $f(0) = 0$, and for any $d \neq 1$, there exist nonzero $a \in \mathbb{F}_q$ such that $f(dx) - f(x) = f(ax)$.

From a Costas polynomial $f \in \mathbb{F}_q[x]$, choose a primitive element $\alpha \in \mathbb{F}_q$ and consider the sequence

$$s_0 = f(\alpha^0), \quad s_1 = f(\alpha^1), \quad \ldots, \quad s_{q-2} = f(\alpha^{q-2}).$$

Let $d = \alpha^c$ and $x = \alpha^i$. Then $f(dx) - f(x) = s_{i+c} - s_i$, where the indices are taken modulo $q - 1$. However, if f is a shifting Costas polynomial and $a = \alpha^k$,

$$s_{i+c} - s_i = s_{i+k}.$$

Hence, the sequence of differences is a circular shift of the original sequence. This is why we call these polynomials "shifting", as they are the multidimensional generalization of the shifting property given in Definition 1.51, but expressed in terms of their Costas polynomial.

Proposition 3.32. *A shifting Costas polynomial is a Costas polynomial.*

Proof. Let $f \in \mathbb{F}_q[x]$ be a shifting Costas polynomial. If $a \in \mathbb{F}_q$ is any nonzero constant, $x \mapsto ax$ is a permutation of $\mathbb{F}_q$. The polynomial $f(ax)$ is the composition of permutations; hence, it is also a permutation of $\mathbb{F}_q$. Then, $f(dx) - f(x) = f(ax)$ is a permutation for all $d \in \mathbb{F}_q, d \neq 1$. We conclude that f is a Costas polynomial. □

Lemma 3.33. *Let $f \in \mathbb{F}_q[x]$ be a shifting Costas polynomial. The polynomial $f(x^s)$ is a shifting Costas polynomial if* $\gcd(s, q-1) = 1$.

Proof. Assume s is a positive integer with $\gcd(s, q-1) = 1$ and fix $d \in \mathbb{F}_q$, $d \neq 1$. Define $g(x) = f(x^s)$. We have $g(0) = f(0) = 0$. Moreover, $x \mapsto x^s$ is a permutation monomial, and since f is a permutation by assumption, $g(x) = f(x^s)$ is the composition of permutations, hence a permutation.

Notice that $d^s \neq 1$. Thus, since f is shifting Costas, there exists nonzero $a \in \mathbb{F}_q$ for which

$$f(d^s x) - f(x) = f(ax).$$

Since $\gcd(s, q-1) = 1$, there is some $a_0 \in \mathbb{F}_q$ such that $a_0^s = a$. Therefore,

$$g(dx) - g(x) = f(d^s x^s) - f(x^s) = f(ax^s) = g(a_0 x).$$

We conclude that $g(x) = f(x^s)$ is a shifting Costas polynomial. □

And now the main result of the section: a weaker version of Conjecture 3.24.

Theorem 3.34. *Let q be a prime power. A polynomial $f \in \mathbb{F}_q[x]$ is a shifting Costas polynomial if and only if $f(x) \equiv L(x^s) \pmod{x^q - x}$, where $L(x) \in \mathbb{F}_q[x]$ is a linearized permutation polynomial and* $\gcd(s, q-1) = 1$.

Proof. Let $f \in \mathbb{F}_q$ be a shifting Costas polynomial. Without loss of generality, assume f is reduced modulo $x^q - x$, so it has degree at most $q - 1$. Let

$$f(x) = \sum_{n=0}^{q-1} c_n x^n.$$

Since f is shifting Costas, for each $d \in \mathbb{F}_q$, $d \neq 1$, there is some $a \in \mathbb{F}_q$ such that

$$f(dx) - f(x) = f(ax).$$

Therefore, $f(x) = f(dx) - f(ax)$ and, by comparing coefficients, we must have $c_n = c_n(d^n - a^n)$, for $n = 0, 1, \ldots, q-1$. This implies

$$c_n = 0 \quad \text{or} \quad d^n - a^n = 1. \tag{3.13}$$

If for some $n \in \{0, 1, \ldots, q-1\}$, $c_n \neq 0$, we claim that $\gcd(n, q-1) = 1$.

Let us prove the claim. For the sake of a contradiction, assume that for some $n \in \{0, 1, \ldots, q-1\}$, we have $c_n \neq 0$ and $\gcd(n, q-1) > 1$. Let α be a primitive element in $\mathbb{F}_q$, and set $d = \alpha^r$, for

$$r = \frac{q-1}{\gcd(n, q-1)}.$$

Then rn is a mutiple of $q-1$, and $\alpha^{rn} = 1$. By (3.13), $c_n \neq 0$ implies $d^n - a^n = 1$. Hence

$$a^n = d^n - 1 = (\alpha^r)^n - 1 = 0,$$

implying $a = 0$. But then, $f(dx) - f(x) = f(ax) = f(0)$ is a constant map, which is impossible because, by Proposition 3.32, f is a Costas polynomial. We conclude that all the terms of f have x to the power of a number relatively prime to $q-1$.

Let $c_n x^n$ be a term of f. Then, $\gcd(n, q-1) = 1$ implying that n is a unit modulo $q-1$. Therefore, there is some s relatively prime to $q-1$ (so s is a unit), for which $ns \equiv 1 \pmod{q-1}$, implying that $f(x^s)$ has a linear term when reduced modulo $x^q - x$.

First, assume f has a linear term. Then, by (3.13), $a = d-1$. If f has another

term $a_n x^n$ for some $n > 1$, $a^n = (d-1)^n$ and (3.13) implies

$$(d-1)^n = d^n - 1. \tag{3.14}$$

Notice that, if $\mathbb{F}_q$ has odd characteristic, n must be odd because $\gcd(n, q-1) = 1$ and $q-1$ is even. Hence, in $\mathbb{F}_q$, $(-1)^n = -1$. Otherwise, if $\mathbb{F}_q$ has even characteristic, $(-1)^n = -1 = 1$ for any integer n. In either case, using (3.14), $(d-1)^n = d^n + (-1)^n$. Therefore, using the binomial formula,

$$\begin{aligned} d^n - 1 = \sum_{k=0}^{n} \binom{n}{k} (-1)^k d^{n-k} &= d^n + \sum_{k=1}^{n-1} \binom{n}{k} (-1)^k d^{n-k} + (-1)^n \\ &\implies \sum_{k=1}^{n-1} \binom{n}{k} (-1)^k d^{n-k} = 0 \quad \forall d \in \mathbb{F}_q, d \neq 1. \end{aligned}$$

That is, the polynomial $\sum_{k=1}^{n-1} \binom{n}{k} (-1)^k x^{n-k} \in \mathbb{F}_q[x]$ of degree $n-1 \leqslant q-2$ has $q-1$ zeros, so it must be the zero polynomial. Since $\mathbb{F}_q$ has characteristic p, we must have $\binom{n}{k} \equiv 0 \pmod{p}$ for $k = 1, 2, \ldots n-1$. By [**10**, Theorem 3], n has to be a power of p. We conclude that f is a linearized permutation polynomial.

If f does not have linear term, we can choose t relatively prime to $q-1$ such that $f(x^t)$ has linear term when reduced modulo $x^q - x$. Let $L(x)$ be the reduction of $f(x^t)$ modulo $x^q - x$. By Lemma 3.33, $L(x)$ is a shifting Costas polynomial, and, as shown above, it is a linearized permutation polynomial. Then, $f(x) \equiv L(x^s) \pmod{x^q - x}$, for some s such that $st \equiv 1 \pmod{q-1}$, hence $\gcd(s, q-1) = 1$.

Conversely, assume $f(x) \equiv L(x^s) \pmod{x^q - x}$ for some linearized permutation polynomial $L(x) \in \mathbb{F}_q[x]$ and for some s, $\gcd(s, q-1) = 1$. Notice that $f(x) \equiv L(x^s) \pmod{x^q - x}$ implies that f and $L(x^s)$ are equal as functions over $\mathbb{F}_q$. Hence, it is enough to show that $f(x) = L(x^s)$ is a shifting Costas polynomial.

Assume $f(x) = L(x^s)$. Clearly f is a permutation polynomial and $f(0) = 0$.

Fix $d \in \mathbb{F}_q, d \neq 1$. Then

$$\begin{aligned} f(dx) - f(x) &= L(d^s x^s) - L(x^s) \\ &= L((d^s - 1)x) \end{aligned}$$

Since $d^s - 1 \in \mathbb{F}_q$ and $d^s - 1 \neq 0$, there exists a nonzero $a \in \mathbb{F}_q$ for which $a^s = d^s - 1$. Therefore,

$$f(dx) - f(x) = L(a^s x^s) = f(ax).$$

We conclude that f is a shifting Costas polynomial, and the proof is finished. □

By following the proof of Theorem 3.34 for polynomials over prime fields, we get a completely different proof for the theorem by Moreno [**21**, p. 159] stating that a circular Costas sequence has the shifting property if and only if it is Welch (Theorem 1.52).

Summary

In this Chapter 3, we extend the definition of a circular Costas array to higher dimensions by considering circular Costas maps between finite abelian groups (Definition 3.1). These are "almost" multidimensional Costas arrays exhibiting a modular periodicity: they are defined by an injective function with only one element in the codomain, which has no preimage. We show that the codomain of a circular Costas map must be an elementary abelian group (Theorem 3.12), establishing one of the conjectures by Ortiz-Ubarri et al. [**24**]. Translating a conjecture from finite projective planes with a collineation group admitting a direct product difference set (Conjecture 3.15), we conjecture that the domain of any circular Costas maps must be a cyclic group (Conjecture 3.16).

Circular Costas maps with cyclic domain can be conveniently expressed as a

particular type of permutation polynomial over finite fields called Costas polynomials [**23**] (Definition 3.18). Muratović-Rubić et al. [**23**] defined Costas polynomials over finite fields without the notion of multidimensional circular Costas maps. We define the multidimensional Welch construction proposed by Golomb and Gong [**14**] as those circular Costas maps defined by the composition of a linearized permutation polynomial with a permutation monomial (Definition 3.4). Translating a conjecture from finite projective planes, Muratović-Rubić et al. conjectured that these are the only Costas polynomials [**23**] (Conjecture 3.24). We rewrite the conjecture using our concepts: the only circular Costas maps are multidimensional Welch (Conjecture 3.27). This is the extension of the conjecture by Golomb and Moreno [**15**] (Conjecture 0.4) to higher-dimensional circular Costas arrays.

The chapter finishes by extending Moreno's definition of the shifting property [**21**] (Definition 1.51) to higher-dimensional circular Costas and showing that, as in the two-dimensional case, a Costas polynomial has the shifting property if and only if it is multidimensional Welch (Theorem 3.34).

Epilogue

> *Sin embargo, antes de llegar al verso final ya había comprendido que no saldría jamás de ese cuarto, pues estaba previsto que la ciudad de los espejos (o los espejismos) sería arrasada por el viento y desterrada de la memoria de los hombres en el instante en que Aureliano Babilonia acabara de descifrar los pergaminos, y que todo lo escrito en ellos era irrepetible desde siempre y para siempre, porque las estirpes condenadas a cien años de soledad no tenían una segunda oportunidad sobre la tierra.*
>
> —Gabriel García Márquez, *Cien años de soledad*

The work presented in this thesis is the most recent, and hopefully not last, installment in a longstanding and strong tradition of research in Costas arrays at the University of Puerto Rico, started by a world-renowned expert in this area, Oscar Moreno. We introduce this thesis by providing a chronicle of how the study of two-dimensional Costas arrays and their periodic properties unfolded, presenting the most relevant results and conjectures.

In Chapter 1, we lay the ground for a multidimensional theory of Costas arrays and their periodic properties by rewriting concepts and results on two-dimensional Costas arrays, also providing some of our own, such that the extension of these concepts and results to higher dimensions is straightforward. Among the most important concepts and results are:

1. Definition of a Costas array [**2**]; Definition 1.17.

2. Costas arrays preserving the Costas property periodically throughout the plane must have order 2, the least possible order [**30**]; Theorem 1.32.

3. Definition of circular Costas maps as a particular type of modular periodicity [**15**]; Definition 1.34.

4. Circular Costas maps can be conveniently represented as Costas polynomials, a special type of permutation polynomial [**15**]; Definition 1.46.

5. All circular Costas maps are Welch, and vice versa [**23**]; Theorem 1.50.

These results were the roadmap for our study of the periodic properties of multidimensional Costas arrays.

Chapter 2 defines multidimensional Costas arrays (Definition 2.13) and discusses how our definition compares to other higher-dimensional analogs of Costas arrays previously proposed in the literature. We show that, when extended periodically, multidimensional Costas arrays of odd order do not preserve the Costas property (Theorem 2.27). For Costas arrays of even order, we show that "large" arrays defined by a function with one-dimensional image do not preserve the Costas property when extended periodically (Theorem 2.30). For the particular case of three-dimensional Costas arrays, those preserving the Costas property when extended periodically must have order 4, the least possible order (Theorem 2.32). We conjecture the trend continues: if a multidimensional Costas array preserves the Costas property periodically, it has the least possible order (Conjecture 2.34).

Trying to obtain an "almost" Costas array that preserves the Costas property periodically, Chapter 3 extends the definition of circular Costas maps to higher dimensions as a special type of modular periodicity (Definition 3.1). We show that circular Costas maps are equivalent to abelian direct product difference sets (Theorem 1.43), which are equivalent to finite projective planes of a certain type, which are

conjectured to be desarguesian [**20**]. The assertion that these finite projective planes are desarguesian has a two-fold consequence in terms of circular Costas maps: first, the domain must be a cyclic group (Conjecture 3.16), so all circular Costas maps can be represented as special polynomials over extension fields called Costas polynomials; and second, that those polynomials are the composition of permutation monomials with linearized permutation polynomials [**23**] (Conjecture 3.24). The last assertion is, in turn, equivalent to stating that all multidimensional circular Costas maps are multidimensional Welch and vice versa (Conjecture 3.27). This conjecture remains unsolved. However, we prove a weaker version by showing that multidimensional circular Costas maps with a shifting property are multidimensional Welch and vice versa (Theorem 3.34).

The grand synthesis of our work: a new beautiful multidimensional Costas theory in which most concepts and results regarding the periodic properties of two-dimensional Costas arrays are proven or conjectured to extend into higher dimensions.

Some Open Questions

In addition to all the conjectures presented in the thesis, this area of research still has many open questions awaiting curious minds. We are proposing a new definition for multidimensional Costas arrays, so everything known for two-dimensional Costas arrays now becomes a question in the higher-dimensional context: do the results extend? In particular, we can ask which of the higher-dimensional analogs of the three conjectures that Golomb told Costas in the private correspondence mentioned in the Introduction hold:

1. Does multidimensional Costas arrays exist for each possible size and dimension?

2. Is there a bound for the number of multidimensional Costas arrays of a particular size and dimension?

3. Does the proportion of multidimensional Costas arrays among all possible bijections go to zero as the size or the dimension increases? Is this decay exponential?

There are only three known algebraic constructions for two-dimensional Costas arrays. Is there any algebraic construction that produces multidimensional Costas arrays? Regarding the periodicity of Costas arrays, we know that the Welch construction can be generalized to produce "almost" multidimensional Costas arrays with a special type of modular periodicity. Can something similar be done for the Lempel and Golomb constructions?

In this thesis, we tackled three out of the four conjectures by Ortiz-Ubarri et al. [**24**] on circular Costas maps. The fourth conjecture is about the characterization of the group of algebraic symmetries acting over multidimensional Welch arrays. Is there a way to translate the algebraic symmetries presented in [**24**] as an action on their defining Costas polynomial? Are these symmetries related to the collineation group of finite projective planes admitting direct product difference sets?

Finally, we ask: in what applications do multidimensional Costas arrays might result useful?

Bibliography

[1] 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.

[2] John P. Costas, *Medium constraints on sonar design and performance*, Technical Report R65EMH33, General Electric Company, 1965.

[3] ———, *Medium constraints on sonar design and performance*, Electronics and Aerospace Systems Convention Record (1975), 68A–68L.

[4] ———, *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.

[5] Peter Dembowski and Frederick C. Piper, *Quasiregular collineation groups of finite projective planes*, Mathematische Zeitschrift **99** (1967), no. 1, 53–75.

[6] Konstantinos Drakakis, *A review of Costas arrays*, Journal of Applied Mathematics (2006), 4260–4265.

[7] ———, *Higher dimensional generalizations of the Costas property*, 2008 42nd annual conference on information sciences and systems, 2008, pp. 1240–1245.

[8] ———, *Open problems in Costas arrays*, 2011. arXiv Preprint arXiv:1102.5727.

[9] 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.

[10] Nathan J. Fine, *Binomial coefficients modulo a prime*, The American Mathematical Monthly **54** (1947), no. 10, 589–592.

[11] Michael J. Ganley, *Direct product difference sets*, Journal of Combinatorial Theory, Series A **23** (1977), no. 3, 321–332.

[12] Solomon W. Golomb, *Algebraic constructions for Costas arrays*, Journal of Combinatorial Theory, Series A **37** (1984), no. 1, 13–21.

[13] ———, *Discrete mathematics for communication systems*, Technical Report ADA220430, Office of Naval Research, 1990.

[14] Solomon W. Golomb and Guang Gong, *The status of Costas arrays*, IEEE Transactions on Information Theory **53** (2007), no. 11, 4260–4265.

[15] Solomon W. Golomb and Oscar Moreno, *On periodicity properties of Costas arrays and a conjecture on permutation polynomials*, IEEE Transactions on Information Theory **42** (1996), no. 6, 2252–2253.

[16] Solomon W. Golomb and Herbert Taylor, *Two-dimensional synchronization patterns for minimum ambiguity*, IEEE Transactions on Information Theory **28** (1982), no. 4, 600–604.

[17] ———, *Constructions and properties of Costas arrays*, Proceedings of the IEEE **72** (1984), no. 9, 1143–1163.

[18] Jonathan Jedwab and Jane Wodlinger, *The deficiency of Costas arrays*, IEEE Transactions on Information Theory **60** (2014), no. 12, 7947–7954.

[19] Jonathan Jedwab and Lily Yen, *Costas cubes*, IEEE Transactions on Information Theory **64** (2017), no. 4, 3144–3149.

[20] Dieter Jungnickel and Marialuisa J. de Resmini, *Another case of the prime power conjecture for finite projective planes*, Advances in Geometry **2** (2002), 215–218.

[21] Oscar Moreno, *A shifting property of some Costas sequences*, Ars Combinatoria **33** (1992), 157–160.

[22] Oscar Moreno and Andrew Z. Tirkel, *Multi-dimensional arrays for watermarking*, 2011 IEEE international symposium on information theory proceedings, 2011, pp. 2691–2695.

[23] 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 **632** (2015), 317–326.

[24] José Ortiz-Ubarri, Oscar Moreno, Andrew Z. Tirkel, Rafael A. Arce-Nazario, and Solomon W. Golomb, *Algebraic symmetries of generic* $(m+1)$*-dimensional periodic Costas arrays*, IEEE Transactions on Information Theory **59** (2013), no. 2, 1076–1081.

[25] 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.

[26] Daniel Panario, Brett Stevens, and Qiang Wang, *Ambiguity and deficiency in Costas arrays and APN permutations*, Latin american symposium on theoretical informatics, 2010, pp. 397–406.

[27] Alexander Pott, *On projective planes admitting elations and homologies*, Geometriae Dedicata **52** (1994), no. 2, 181–193.

[28] ———, *Finite geometry and character theory*, Lecture Notes in Mathematics, vol. 1601, Springer, 1995.

[29] Jerry Silverman, Virgil E. Vickers, and Jonathan M. Mooney, *On the number of Costas arrays as a function of array size*, Proceedings of the IEEE **76** (1988), no. 7, 851–853.

[30] Herbert Taylor, *Non-attacking rooks with distinct differences*, Technical Report CSI-84-03-02, Communication Sciences Institute, University of Southern California, 1984.

[31] Lutz Warnke, Bill Correll Jr., and Christopher N. Swanson, *The density of Costas arrays decays exponentially*, 2021. `https://mathweb.ucsd.edu/~lwarnke/CostasArrayExponentialDecay.pdf`.

[32] Kai Zhou, *A remark on linear permutation polynomials*, Finite Fields and Their Applications **14** (2008), no. 2, 532–536.