IEICE TRANS. FUNDAMENTALS, VOL.E106–A, NO.12 DECEMBER 2023

PAPER *Special Section on Signal Design and Its Applications in Communications*

A New Transformation for Costas Arrays

Ali ARDALANI[†a)] ***and*** **Alexander POTT**[†b)]**,** ***Nonmembers***

SUMMARY A Costas array of size n is an $n \times n$ binary matrix such that no two of the $\binom{n}{2}$ line segments connecting 1s have the same length and slope. Costas arrays are found by finite-field-based construction methods and their manipulations (systematically constructed) and exhaustive search methods. The arrays found exhaustively, which are of completely unknown origin, are called sporadic. Most studies in Costas arrays have tended to focus on systematically constructed Costas arrays rather than sporadic ones, which reveals the hardness of examining a link between systematically constructed Costas arrays and sporadic ones. This paper introduces a new transformation that preserves the Costas property for some Costas arrays, but not all. We observed that this transformation could transform some systematically constructed Costas arrays to sporadic ones and vice versa. Moreover, we introduce a family of arrays with the property that the auto-correlation of each array and the cross-correlation between any two arrays in this family is bounded above by two.

key words: *Costas arrays, auto-correlation, cross-correlation, almost Costas arrays*

1. Introduction

In 1965 in the context of sonar detection, J. P. Costas studied a particular class of permutations of n elements to improve the poor performance of radar and sonar systems [1]. These classes are now known as Costas arrays. A Costas array of size n is an $n \times n$ binary matrix such that there is precisely a single 1 per each row and each column (i.e., it is a permutation matrix) and such that the line segments formed by joining pairs of 1s are all distinct.

There are two basic approaches currently being adopted to study Costas arrays. One is the finite field-based construction approach, and the other is computer search. In their investigation into algebraic construction for Costas arrays, L. R. Welch and A. Lempel found constructions and applications for them, and Solomon W. Golomb provided both the first proofs of the validity of the Welch and Lempel constructions and also a new construction [2], [3]. After discovering these two main algebraic techniques, together with some construction techniques obtained by manipulating these constructions [4], there have been no further discoveries of new algebraic methods.

Although extensive research has been carried out on Costas arrays, many fundamental questions are not yet answered, especially, do Costas arrays exist for all sizes? This question was raised for the first time in a paper by S. Golomb and H. Taylor in 1984, and it is still open [2]. According to the two main constructions for Costas arrays, they can be generated for infinitely many but not for all sizes. To the best of our knowledge, since 1984, the smallest sizes for which no Costas array is currently known are 32 and 33. Referring to such difficulties, some authors have mainly been interested in computer search for Costas arrays [4]–[8]. A computer search for Costas arrays has provided a significant opportunity to enhance our understanding of the possible existence pattern for Costas arrays. However, the generalisability of these methods is subject to certain limitations. Notably, all Costas arrays have been found through exhaustive search up to size 29, while many of them are sporadic [9]. Sporadic Costas arrays for sizes $6 \leq n \leq 27$ exist, and the enumeration of sizes 28 and 29 showed no sporadic Costas array for these sizes. Therefore, there is this possibility that sporadic Costas arrays will not exist from a specific size onwards [9].

In this study, we took advantage of a database of all known Costas arrays up to size $n = 1030$, provided by James K. Beard. It is also uploaded to IEEE DataPort [10]. The database root folder contains the subfolders \searches and \generated. The \generated subfolder contains all systematically constructed Costas arrays, and we mean by non-generated the Costas arrays in the \searches subfolder, which are not in the \generated subfolder. The primary purpose of this paper is to introduce a new transformation with the property that, after applying this transformation on the existing Costas arrays, we always obtain permutation matrices with the maximum auto-correlation functions value of two. Surprisingly, this transformation leaves the Costas property invariant for most of the generated Costas arrays and some non-generated ones. There are examples of generated Costas arrays with the property that the transformed matrices are non-generated.

Families of arrays with good auto and cross-correlation have practical applications in digital watermarking [11]. As we will see, our new transformation has the potential to turn a single permutation into a family of permutations. Using our transformation, we construct a family of permutation arrays constructed by applying the transformation on the inverse mapping over a finite field with p elements. We will see that this family contains arrays with aperiodic auto-correlation and the pairwise aperiodic cross-correlation of

Manuscript received February 6, 2023.
Manuscript revised June 26, 2023.
Manuscript publicized August 24, 2023.

[†]The authors are with the Faculty of Mathematics, Institute of Algebra and Geometry, Otto von Guericke University Magdeburg, Germany.
a) E-mail: ali.ardalani@ovgu.de
b) E-mail: Pottalexander.pott@ovgu.de

DOI: 10.1587/transfun.2023SDP0005

any two arrays of this family bounded above by two.

This paper is divided into four sections, starting with the introductory section. Within the introduction, there will be a subsection that provides a review of the relevant definitions and theorems used in this study. Section 2 will present the formal definition of the new transformation and also explore its application to Welch and Lempel-Golomb Costas arrays. Moving forward, Section 3 will delve into the impact of the transformation on non-generated Costas arrays. Finally, the last section will be dedicated to discussing the family of inverse permutations.

1.1 Costas Arrays Definitions and Construction Techniques

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

Definition 1: Let $f : [n] \to [n]$, $n \in \mathbb{N}$ be a bijection, that is a permutation of n elements, which we denote by $[f(1), f(2), \ldots, f(n)]$. Then the corresponding permutation matrix of f, say $A_f = (a_{i,j})$, $i,j \in [n]$, is an $n \times n$ matrix where the entries are given by

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

Sometimes it will be more convenient to consider permutations as permutation matrices. Definition 1 also tells us how to recover a permutation from a given permutation matrix.

Let $A = (a_{i,j})$, $i,j \in [n]$, be a permutation matrix of size n. Then each column has a unique element equal to 1 and 0's elsewhere. Now we can construct a permutation $\sigma_A : [n] \to [n]$, $n \in \mathbb{N}$, $\sigma_A(j) = i$, if $a_{i,j} = 1$. This means that each element of the permutation indicates the position of the 1 in the corresponding column of the matrix. The following remark will explicate the relation between a permutation matrix and its corresponding permutation.

Remark 1: There is a bijection $\sigma : P_n \to \{f : f \textit{ is a bijection on } n \textit{ elements}\}$, where P_n is the set of all permutation matrices of size n. More precisely, $\sigma_A = [f(1), \ldots, f(n)]$, where $f(i)$ is the position of the nonzero entry in the ith column of A, counting from top to bottom. It means $f^{-1}(i) = j \Leftrightarrow a_{i,j} = 1$.

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

Note 1: Throughout this paper, the terms "permutation matrix" and "permutation" will be used interchangeably, and we will not distinguish between A and σ_A.

Definition 2 (Displacement vectors): Consider the permutation matrix $A = (a_{i,j})$, $i,j \in [n]$, and let a_{i_1,j_1} and a_{i_2,j_2}, be two nonzero entries of A. Then if $j_1 < j_2$ we call the vector $(j_2 - j_1, i_2 - i_1)$ the displacement vector between a_{i_1,j_1} and a_{i_2,j_2}.

Definition 3 (First definition of Costas array [2]): Let $A = (a_{i,j})$, $i,j \in [n]$, be a permutation matrix of size n. Then $A = (a_{i,j})$ is a Costas array if and only if all displacement vectors of the form $\{(j_2 - j_1,\ i_2 - i_1),\ j_1 < j_2,\ j_1, j_2 \in [n]\}$ are distinct.

Let us provide a brief overview of a finite field's leading properties, which will be required to define the systematic constructions. A finite (Galois) field with q elements, $GF(q)$, exists if and only if q is a prime power. The multiplicative group of a finite field, $GF^\star(q)$, is cyclic, and a generator of $GF^\star(q)$ is called a primitive element, and every finite field has a primitive element. For more details on the finite field's theory, one can refer to the literature [12].

Lemma 1 ([12]): If α is a primitive element of $GF(q)$ then α^t is a primitive element of $GF(q)$ if and only if $gcd(t, q-1) = 1$.

Theorem 1 (Exponential Welch Construction [2]): Let α be a primitive element of $GF(p)$, with p a prime, and let c be an element of the set $[p-1]-1$. Then the $(p-1)\times(p-1)$ permutation matrix with $a_{i,j} = 1$ if and only if $i \equiv \alpha^{j+c} \pmod p$, where $1 \le i \le p-1$, $0 \le j \le p-2$, is a Costas array.

Theorem 2 (Logarithmic Welch array [13]): Let α be a primitive element of $GF(p)$, with p a prime and c be an element of the set $[p-1]-1$. Then the $(p-1)\times(p-1)$ permutation matrix with $a_{i,j} = 1$ if and only if $i \equiv c + \log_\alpha j \pmod{p-1}$, where $1 \le j \le p-1$, $0 \le i \le p-2$, is a Costas array.

Note 2: One can easily verify that the transposed of an exponential Welch Costas array is a logarithmic Welch array.

Theorem 3 (Lempel-Golomb Construction [2]): Let α and β be two primitive elements of $GF(q)$ with $q > 2$. Then the $(q-2)\times(q-2)$ permutation matrix with $a_{i,j} = 1$ if and only if $\alpha^i + \beta^j = 1$, $1 \le i,j \le q-2$, is a Costas array.

The difference triangle table provides an easy way to check whether a given permutation is a Costas array.

Definition 4 (Difference Triangle Table): Let $\sigma_A = [f(1), \ldots, f(n)]$, where A is a permutation matrix of size n and $[f(1), \ldots, f(n)]$, $n \in \mathbb{N}$, be its corresponding permutation (according to remark 1). Then the ith row of the difference triangle table, for $1 \le i \le n-1$, contains the following $n-i$ elements:

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

Definition 5 (Second definition of Costas array): Let A be a permutation matrix of size n, $n \in \mathbb{N}$, with the corresponding permutation $[f(1), \ldots, f(n)]$. Then, A is a Costas array if the entries of row i, for $1 \le i \le n-1$, of the difference triangle table, as defined in Definition 4, are pairwise distinct.

1.2 Auto-Correlation Property

Definition 6 (cross-correlation function [14], [15]): For a

binary matrix $A = (a_{i,j})$ and $B = (b_{i,j})$, with $1 \le i, j \le n$, for $i, j \in \mathbb{Z}$ let

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

and

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

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

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

Equivalently, the cross-correlation can be defined on permutations. Let $f, g : [n] \longrightarrow [n]$ be the corresponding permutations of the arrays A and B, respectively. Then, we define

$$C_{f,g}(r,s) = |\{i \in [n] : i + r \in [n], f(i) + s = g(i + r)\}|.$$

We regard the auto-correlation function of a given array A as the cross-correlation of A with itself, and we denote it by C_A.

Definition 7 ([15]): Let $\mathcal{F}$ be a family of permutation arrays of size n. We define the maximal cross-correlation of the family $\mathcal{F}$, denoted by $C(\mathcal{F})$, as follows

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

where the first maximum is taken over all possible shifts $(r, s) \in \mathbb{Z}^2$.

Definition 8: (Third definition of Costas array) Let A be a permutation matrix of size n, where $n \in \mathbb{N}$. Then A is a Costas array if for any pairs of integers $(r, s) \neq (0, 0)$, the aperiodic auto-correlation function of A satisfies

$$C_A(r,s) \le 1.$$

It can be observed that the three definitions of Costas arrays are equivalent [14]. One can provide a relaxation of the Costas property by allowing the occurrence of displacement vectors with the same length and slope in a permutation matrix of at most twice. These types of permutation matrices can be referred to as "Almost Costas arrays".

Definition 9: (Almost Costas array) Let A be a permutation matrix of size n, where $n \in \mathbb{N}$. Then A is an Almost Costas array if for any pairs of integers $(r, s) \neq (0, 0)$, the aperiodic auto-correlation function of A satisfies

$$C_A(r,s) \le 2.$$

To gain insights into the prevalence of Almost Costas arrays, we conducted an exhaustive search to determine the total number of such arrays among all permutation matrices of a given size $n \le 13$. Table 1 presents the result of this computation.

Table 1 Total number of Almost Costas arrays up to size 13. $\mathcal{AC}_n$ denotes the total number of Almost Costas arrays of size n. The last column shows the density of Almost Costas arrays among all permutation matrices of size n.

Size n	$\mathcal{AC}_n$	Density
2	0	0
3	6	1
4	22	0.916
5	102	0.850
6	548	0.761
7	3262	0.647
8	23082	0.572
9	173402	0.477
10	1417736	0.390
11	12417078	0.311
12	115250636	0.240
13	1133465160	0.182

2. A New Transformation

We introduce a new transformation, which enables us to apply this transformation to an existing Costas array to obtain Almost Costas arrays, as defined in Definition 9. What follows is the definition of our new transformation, and we will explain how this transformation is beneficial to construct a Costas array from a given one in some cases.

Let $X = [f(1), f(2), \ldots, f(n)]$ be a Costas array of size n. We plan to construct another bijection g from f and then examine the correlation properties of its corresponding permutation matrix. Suppose that k is a positive integer such that $gcd(k, n + 1) = 1$. We define $g : [n] \longrightarrow [n]$, by

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

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

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

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

$$ki_1 \bmod (n + 1) = ki_2 \bmod (n + 1).$$

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

Definition 10: Let $X = [f(1), f(2), \ldots, f(n)]$ represent a permutation matrix of size n, where $n \in \mathbb{N}$, and k is a positive integer such that $gcd(k, n + 1) = 1$. We define a bijection $g : [n] \longrightarrow [n]$, by

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

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

Let us mention that the transformation $\mathcal{A}_k$ is reversible. This can be demonstrated by considering the fact that the inverse transformation can be obtained as $\mathcal{A}_{k^{-1}}$, where k^{-1} represents the multiplicative inverse of k in $\mathbb{Z}_{n+1}$.

Example 1: Consider a Costas array $X = [1,7,4,8,2,3,6,5]$ of size 8. Since $gcd(2,9) = gcd(4,9) = 1$, we can construct $\mathcal{A}_2(X)$ and $\mathcal{A}_4(X)$. Then, we have

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

Similarly, $\mathcal{A}_4(X) = [8,5,4,6,7,3,1,2]$. One can easily check that $\mathcal{A}_2(X)$ is Costas array, but $\mathcal{A}_4(X)$ is not.

Let us define the concept of **transferable** arrays as follows:

Definition 11: Let X be a Costas array of size n. We refer to X as a transferable array if there exists an integer k such that $gcd(k, n+1) = 1$, and the application of the transformation $\mathcal{A}_k$ to X, denoted as $\mathcal{A}_k(X)$, yields another Costas array.

Assume that C_n is the set of all Costas arrays of size n. It is well-known that the dihedral group D_8 (the group of symmetries of a square) acts on C_n. Thus the orbit of D_8 partitions C_n. Therefore, the equivalence class of a Costas array X is the orbit of X under the action of D_8, then this equivalence class contains either eight Costas arrays or four Costas arrays if the array is symmetric. We observed that if an array is transferable, then some of the elements of its equivalence class are also transferable, but not all.

Theorem 4: Let X be a transferable Costas array of size n. Then the vertical reflection, horizontal reflection and 180° rotation of X are transferable.

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

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

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

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

We already know that $[f(ki \ mod\ n+1)]$ for $1 \le i \le n$ is a Costas array. Thus X_h is transferable. Similarly, we can verify that 180° rotation of X is also transferable. The 180° rotation of X is given by $X_r = [n+1-f(n+1-i)]$ for $1 \le i \le n$. Let us take $t = -k$, then we have

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

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

Corollary 1: Assume that X and its transpose, X^T, are transferable. Then all the elements of the equivalence class of X are transferable.

Proof: The proof is straightforward. □

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

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

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

Proof: By way of contradiction, we can assume that the aperiodic auto-correlation function of $\mathcal{A}_k(X)$ for a non-zero shift has a value of at least 3, meaning there is a row l in the difference triangle table of $\mathcal{A}_k(X)$ in which there are at least three equal entries, say $g(i_1+l) - g(i_1)$, $g(i_2+l) - g(i_2)$, and $g(i_3+l) - g(i_3)$, where $1 \le i_1, i_2, i_3, i_1+l, i_2+l, i_3+l \le n$, and i_1, i_2, and i_3 are all distinct. As in Definition 10, for $t = 1,2,3$, $g(i_t+l) - g(i_t)$ is equal to

$$f((ki_t + kl) \ mod\ n+1)) - f(ki_t \ mod\ n+1). \tag{1}$$

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

$$g(i_t+l) - g(i_t) = f((i'_t + l') \ mod\ n+1) - f(i'_t). \tag{2}$$

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

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

Case 1. According to (2), we have

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

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

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

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

$$\begin{aligned} f(i'_1 + l' - n - 1) - f(i'_1) &= f(i'_2 + l' - n - 1) - f(i'_2) \\ &= f(i'_3 + l' - n - 1) - f(i'_3). \end{aligned}$$

It follows that

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

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

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

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

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

Theorem 6: Let X be a logarithmic Welch Costas array. Then $\mathcal{A}_k(X)$, where $\mathcal{A}_k$ is the transformation introduced in Definition 10, is also a logarithmic Welch Costas array, obtained by a cyclic shift of the rows of X.

Proof: Assume that X is a logarithmic Welch Costas array, as in Definition 2. Then $X = [c + \log_\alpha j \ mod \ p - 1]$ for $1 \leq j \leq p - 1$. We know that the non-zero elements in $GF(p)$ form a cyclic group with respect to multiplication. Moreover, according to the discrete logarithm's definition, if we have a cyclic group G of order n, then for any $g_1, g_2 \in G$ and a generator x we have

$$\log_x(g_1 g_2) = \left(\log_x g_1 + \log_x g_2\right) \ mod \ n.$$

Therefore, we can conclude that

$$\log_\alpha(kj \ mod \ p) = (\log_\alpha k + \log_\alpha j) \ mod \ p - 1 \qquad (3)$$

Table 2 Exponential Welch arrays' parameters and integer k for which $\mathcal{A}_k$ gives a non-generated Costas array.

GF(q)	Exponential Welch information and k
11	$\alpha = 2, c = 3, k = 5$
11	$\alpha = 2, c = 3, k = 6$
11	$\alpha = 6, c = 8, k = 5$
11	$\alpha = 6, c = 8, k = 6$
23	$\alpha = 5, c = 5, k = 2$
23	$\alpha = 5, c = 5, k = 21$
23	$\alpha = 5, c = 16, k = 2$
23	$\alpha = 5, c = 16, k = 21$

It is known that a cyclic shift of the rows of a logarithmic Welch Costas array is also a Costas array. Now, if we take a look at the $\mathcal{A}_k(X)$ permutation, we can see

$$\mathcal{A}_k(X) = \left[\left(c + \log_\alpha(kj \ mod \ p)\right) \ mod \ p - 1\right].$$

Thus, equality (3) shows that

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

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

It is worthwhile to mention that exponential Costas arrays are not always transferable. In fact, what is surprising is that in a few examples of exponential Welch Costas arrays, after applying $\mathcal{A}_k$, we obtain non-generated Costas arrays. We did hope that we might find transferable exponential Welch Costas arrays of size greater than or equal to 30, for which we do not have a complete search to see whether we find a new Costas array. We checked for all exponential Welch Costas arrays up to size 1030 while none of them was transferable, except a few cases of small sizes, collected in Table 2. Let us discuss the transformation $\mathcal{A}_k$'s effect on Lempel-Golomb Costas arrays.

Theorem 7: Let X be a Lempel-Golomb Costas array of size $q - 2$, where q is a prime power, see Definition 3. Suppose that $\mathcal{A}_k$ is the transformation introduced in Definition 10. Then $\mathcal{A}_k(X)$ is again a Lempel-Golomb Costas array.

Proof: Since X is a Lempel or Golomb Costas array, there are primitive elements α and β of $GF(q)$ such that in the array X there is a dot at position (i, j) if and only if $\alpha^i + \beta^j = 1$, $1 \leq i, j \leq q-2$. It follows that in the matrix $\mathcal{A}_k(X)$, there is a dot at position $(ki \ mod \ q-1, j)$ if and only if $\alpha^{ki \ mod \ q-1} + \beta^j = 1$, $1 \leq i, j \leq q - 2$. According to the Lemma 1 and the fact that $gcd(k, q - 1) = 1$, we can conclude that $\mathcal{A}_k(X)$ is again a Lempel or Golomb Costas array because α^k is a primitive element as well. □

We have investigated the transferability of Costas arrays and examined the values of k for which this transferability holds. Our findings indicate that logarithmic Welch and Lempel-Golomb Costas arrays exhibit transferability for all possible k, while other transferable Costas arrays do not demonstrate

the same property. It should be noted that the transferability of a Costas array does not guarantee transferability for all values of k. We have encountered cases where applying the transformation $\mathcal{A}_k$ for some values of k yields another Costas array, while the same array with different k values may not result in another Costas array. These observations highlight the need for further investigation into the properties of transferable Costas arrays to determine the conditions under which a Costas array is transferable.

3. Non-Generated Costas Arrays

Although a considerable amount of literature has been published on Costas arrays, most of these studies have only focused on systematically constructed Costas arrays. Not much has been discovered about non-generated Costas arrays' properties, which indicates the difficulties of finding any common property between generated Costas arrays and non-generated ones [8].

Turning now to the experimental evidence, we went through the database to identify transferable Costas arrays up to size 29. Independent analyses were carried out on generated and non-generated Costas arrays. Table 3 contains all information about the number of transferable Costas arrays of each size up to size 29. The previous section showed that logarithmic Welch and Lempel-Golomb Costas arrays are transferable. Therefore, we have infinitely many transferable Costas arrays because we have infinitely many logarithmic Welch and Lempel-Golomb Costas arrays. Another interesting observation is that, in some cases, we can obtain a non-generated Costas array by transforming a generated one. We saw examples of this type in Table 2. The last column of Table 3 illustrates the total number of transferable generated Costas arrays with the property that the transformed permutations are non-generated Costas arrays.

Let us mention, as experimental evidence, that we have extensively examined all known Costas arrays ranging in size from 30 up to 500. During our investigation, we specifically checked whether applying the transformation $\mathcal{A}_k$ would yield new Costas arrays. However, we found no instances of transferable Costas arrays within this range, except for the logarithmic Welch and Lempel-Golomb Costas arrays.

Table 3 The total number of transferable Costas arrays per class up to size 29. C_n stands for the total number of Costas arrays of size n; GT and NGT stand for generated transferable Costas arrays and non-generated transferable Costas arrays, respectively.

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

4. Family of Inverse Permutations

For a prime $p \geq 5$, let $f(x) = x^{-1}$ be the inverse mapping over $GF(p)$ and k be an integer relatively prime to p. We define the family of $\mathcal{I}_p$ of inverse permutations of $[p-1]$, by

$$\mathcal{I}_p = \left\{ \left[(kx)^{-1} \right] : x \in GF(p) \setminus \{0\} \text{ and } gcd(k,p) = 1 \right\}.$$

Then, the size of the family $\mathcal{I}_p$ is $p-1$, where ϕ is the Euler's toitient function. It can be seen that the family $\mathcal{I}_p$ is obtained by applying the transformation $\mathcal{A}_k$ on a given inverse mapping over $GF(p)$.

Theorem 8: For a prime $p \geq 5$, let $\mathcal{I}_p$ be the family of inverse permutations. Then, we have $C(\mathcal{I}_p) \leq 2$.

Proof: Consider two inverse permutations f_1 and f_2 in $\mathcal{I}_p$, generated by $f_1(x) = (k_1 x)^{-1}$ and $f_2(x) = (k_2 x)^{-1}$ in $GF(p)$, where k_1 and k_2 are not necessarily distinct integers relatively prime to p. To compute the cross-correlation at $(r,s) \in \mathbb{Z}^2$ between f_1 and f_2, we need to estimate the number of solutions of the equation

$$\left((k_1 x)^{-1} \bmod p \right) + s = \left((k_2 (x+r))^{-1} \bmod p \right). \tag{4}$$

We perform all computations in $GF(p)$ and keep in mind that we compute the aperiodic correlation, which means that x and $x+r$ will never be 0. We obtain an upper bound for the number of solutions of the following equation

$$\left((k_1 x)^{-1} \right) + s = (k_2 (x+r))^{-1}. \tag{5}$$

Multiplying both sides of (5) by $k_2 x(x+r)$ yields

$$k_1^{-1} k_2 (x+r) + s k_2 x^2 + s k_2 r x = x. \tag{6}$$

Equivalently, we have

$$s k_2 x^2 + \left(k_1^{-1} k_2 + s k_2 r - 1 \right) x + k_1^{-1} k_2 r = 0. \tag{7}$$

Since (7) is a polynomial of degree 2 in $GF(p)$, it can admit

at most two solutions. Since k_1 and k_2 are not necessarily distinct, we can conclude that both auto-correlation of each member of the family $\mathcal{I}_p$ and the cross-correlation of any two distinct elements of $\mathcal{I}_p$ is at most two, which completes the proof. □

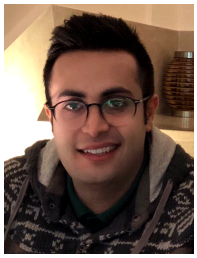
Let us note that if we consider the inverse mapping $f(x) = x^{-1}$ in $GF(p)$, taking element 0 into account may increase the aperiodic auto-correlation by 1. In other words, an inverse permutation f over $GF(p)$ produces a permutation on elements $\{0, 1, \ldots, p-1\}$ of size p with the property that its corresponding $p \times p$ permutation array has the aperiodic auto-correlation of at most three.

Acknowledgments

The author gratefully acknowledges the many helpful suggestions and valuable advice of Dr Yuri Santos Rego (OVGU, Institute of Algebra and Geometry) during the preparation of the paper. This study is based upon works supported by the Deutsche Forchungsgemeinschaft (314838170, GRK 2297, MathCoRe).

References

[1] J.P. Costas, "Medium constraints on sonar design and performance," Technical Report Class 1. Rep. R65EMH33, GE Co., 1965.
[2] S. Golomb, "Algebraic constructions for Costas arrays," Journal Of Combinatorial Theory Series A, vol.37, no.1, pp.13–21, 1984.
[3] S. Golomb and H. Taylor, "Two-dimensional synchronization patterns for minimum ambiguity," IEEE Trans. Inf. Theory, vol.IT-28, no.4, pp.600–604, 1982.
[4] J.K. Beard, J.C. Russo, K.G. Erickson, M.C. Monteleone, and M.T. Wright, "Costas arrays generation and search methodology," IEEE Trans. Aerosp. Electron. Syst., vol.43, no.2, pp.522–538, 2007.
[5] S. Rickard, "Searching for Costas arrays using periodicity properties," IMA International Conference on Mathematics in Signal Processing at The Royal Agricultural College, Cirencester, UK, 2004.
[6] K. Drakakis, S. Rickard, J. Beard, R. Caballero, F. Iorio, G. O'Brien, and J. Walsh, "Results of the enumeration of Costas arrays of order 27," IEEE Trans. Inf. Theory, vol.54, no.10, pp.4684–4687, Oct. 2008.
[7] K. Drakakis, F. Iorio, and S. Rickard, "The enumeration of Costas arrays of order 28 and its consequences," Advances in Mathematics of Communications, vol.5, no.1, pp.69–86, 2011.
[8] K. Drakakis, F. Iorio, S. Rickard, and J. Walsh, "Results of the enumeration of Costas arrays of order 29," Advances in Mathematics of Communications, vol.5, no.3, 547–553, 2011.
[9] K. Drakakis, "Open problems in Costas arrays," [Online]. Available: http://arxiv.org/abs/1102.5727
[10] James Beard, April 6, 2017, "Costas arrays and enumeration to order 1030," IEEE Dataport, doi: 10.21227/H21P42.
[11] S. Blake, O. Moreno, and A.Z. Tirkel, "Families of 3D arrays for video watermarking," Sequences and Their Applications-SETA 2014: 8th International Conference, Melbourne, VIC, Australia, Nov. 2014, Proceedings 8, pp.134–145, 2014.
[12] R. Lidl and H. Niederreiter, Introduction to Finite Fields and their Applications, Cambridge University Press, 1994.
[13] K. Drakakis, R. Gow, and G. McGuire, "APN permutations on $\mathbb{Z}_n$ and Costas arrays," Discrete Applied Mathematics, vol.157, no.15, pp.3320–3326, 2009.
[14] J.L. Wodlinger, "Costas arrays, Golomb rulers and wavelength isolation sequence pairs," Ph.D. thesis, Department of Mathematics, 2012.
[15] K. Drakakis and S. Rickard, "Cross-correlation of Costas arrays: The current status," Proc. 19th Int. Symp. Math. Theory Networks Syst. (MTNS), 2010.



Ali Ardalani received his Ph.D. degree from the Otto von Guericke University Magdeburg in 2023.

Alexander Pott received his Ph.D. degree from the Justus Liebig University Gießen in 1988. Since 1998 he is full professor at the Otto von Guericke University Magdeburg.