

Distance vectors in Costas arrays

Konstantinos Drakakis, Rod Gow
School of Mathematics and CASL
University College Dublin
Belfield, Dublin 4
Ireland

Email: {Konstantinos.Drakakis, Rod.Gow}@ucd.ie

Scott Rickard
School of Electrical, Electronic &
Mechanical Engineering and UCD CASL
University College Dublin
Belfield, Dublin 4
Ireland

Email: Scott.Rickard@ucd.ie

Abstract—We investigate the distance vectors contained in individual and in pairs of Costas arrays, and prove some rigorous results in the case of the algebraically constructed ones. Overall, it appears that the set with the property that every Costas array has a distance vector therein, or that every pair of Costas arrays with a common vector have a common vector therein, is in both cases surprisingly small.

I. INTRODUCTION

Costas arrays/permutations [1], [2], [3] have numerous applications in RADAR and SONAR systems, time synchronization etc. They have been the object of active research for more than 40 years now [1], but, on the theoretical front, there has been a stalemate for the last 20 years or so, ever since the publication of the known algebraic construction methods by Golomb et al. in 1984 [6]. Among the various semi-empirical methods suggested for the construction of new Costas arrays was “interlacing” 2 Costas arrays of the same order to produce a Costas array of order twice as high; it was shown [5], however, that any 2 Costas arrays of equal orders have a distance vector in common (except for orders of 3 or less), implying that the interlaced array would never be Costas. The same result (except again for very small orders) holds for any 2 Costas arrays of orders differing by 1, where interlacing is still technically possible.

For 2 Costas arrays of orders differing by 2 or more it is not possible to extend the interlacing method, at least in an obvious way. It still makes sense, however, to investigate whether it remains true that any such pair of Costas arrays have a vector in common; experimental evidence strongly suggests this is the case most of the time. What would be then the smallest set of distance vectors with the property that any pair of Costas arrays with a distance vector in common have a common vector lying in that set? Similarly, what is the smallest set of distance vectors with the property that any Costas array has a distance vector lying in this set?

The closest 2 dots of a Costas array can lie is in adjacent rows and columns, hence the shortest distance vectors possible are $(1, 1)$ and $(1, -1)$, of length $\sqrt{2}$. As they can potentially exist in all Costas arrays of order larger than 1, we would expect them to be contained in the sets mentioned above, and perhaps very nearly essentially “be” the sets by themselves, in the sense that most pairs of Costas arrays with a vector in common will have one of these 2 vectors in common, and that most Costas arrays will contain one of these 2 vectors.

II. BASICS

Simply put, a Costas array is a square arrangement of dots and blanks, such that there is exactly one dot per row and

column, and such that all vectors between dots are distinct.

Definition 1. Let $f : [n] \rightarrow [n]$, where $[n] = \{1, \dots, n\}$, $n \in \mathbb{N}$, be a bijection; then f has the *Costas property* iff the collection of vectors $\{(i - j, f(i) - f(j)) : 1 \leq j < i \leq n\}$, called the distance vectors, are all distinct, in which case it is called a *Costas permutation*. The corresponding *Costas array* is the square array $n \times n$ where the elements at $(f(i), i)$, $i \in [n]$ are equal to 1 (dots), while the remaining elements are equal to 0 (blanks).

Remark 1. The operations of horizontal flip, vertical flip, and transposition on a Costas array result to a Costas array as well; hence, out of a Costas array 8 can be created, or 4 if the particular Costas array is symmetric.

In the sequel we will make no distinction between the Costas array and the corresponding permutation.

Definition 2. Let $f : [n] \rightarrow [n]$ be a permutation; its *difference triangle* $T(f)$ is the collection of multisets $t_i(f) = \{f(k) - f(i + k) : k \in [n - i]\}$, $i \in [n - 1]$, called the *rows* of the triangle.

Remark 2. The Costas property is equivalent to the fact that no row of the difference triangle contains a given entry more than once; in other words, the rows are sets rather than multisets. The proof is simple: row i contains the second coordinates of those distance vectors whose first coordinate is equal to $i \in [n - 1]$, hence a duplicate entry in a row would immediately imply the existence of 2 equal distance vectors, in violation of the Costas property.

There are essentially 2 construction methods for Costas arrays, based on the algebraic theory of finite fields, each of which has a number of possible extensions, some applicable systematically and some haphazardly. Let us see them without proof:

Theorem 1 (Welch exponential construction W_1). Let p be prime and g a primitive root of the field $\mathbb{F}(p)$; for $c \in \{0, \dots, p - 2\}$ constant, the permutation

$$f(i) = g^{i-1+c} \pmod{p}, \quad i = 1, \dots, p - 1$$

has the Costas property and corresponds to a Costas array of order $p - 1$.

- When $c = 0$, $f(1) = 1$: then, by removing $f(1)$, and, setting $h(i) = f(i + 1) - 1$, $i \in [p - 2]$, we create a new Costas permutation h . This is method W_2 and is always applicable.

- If, in addition, we use $g = 2$ (this is not always possible), then $h(1) = f(2) = 2$, and, setting $s(i) = h(i + 1) - 1$, $i \in [p - 3]$, we create a new Costas permutation s . This is method W_3 .
- It can be shown [4] that the set of exponential Welch arrays created by method W_1 is closed under horizontal and vertical flips; however, the set of the transposes of these arrays is completely disjoint from the original set if $p > 5$: the transposes are called *logarithmic Welch arrays*.

Theorem 2 (Golomb construction G_2). Let p be a prime, $m \in \mathbb{N}$, $q = p^m$ and a, b primitive roots of the field $\mathbb{F}(q)$; we build the permutation f such that

$$a^i + b^{f(i)} = 1, \quad i = 1, \dots, q - 2$$

corresponding to a Costas array of order $q - 2$.

- It can be shown that in every finite field there exist 2 primitive roots a and b such that $a + b = 1$, in which case G_2 yields $f(1) = 1$, and setting $h(i) = f(i + 1) - 1$, $i \in [q - 3]$, we create a new Costas permutation h . This is method G_3 and is always applicable.
- When the characteristic of the field is 2 ($p = 2$), $a + b = 1 \Rightarrow 1 = (a + b)^2 = a^2 + b^2 \Rightarrow f(2) = 2$, and setting $s(i) = h(i + 1) - 1$, $i \in [q - 4]$, we create a new Costas permutation s . This is method G_4 .
- In the special case where $a = b$ (Lempel case), it may be possible to find a primitive root a such that $a^2 + a = 1$, in which case G_2 yields $f(1) = 2$ and $f(2) = 1$, so setting $t(i) = f(i + 2) - 2$, $i \in [q - 4]$, we create a new Costas permutation t . This is method T_4 .

Costas arrays not constructed by the 2 algebraic methods or their derived methods are commonly referred to as *sporadic*.

III. COMMON VECTORS

We wish to find (at least partial) answers to the following problems:

Problem 1. Is it true that there exists a $n \in \mathbb{N}$, such that for all $n_1, n_2 \geq n$, any 2 Costas arrays, one of order n_1 and one of order n_2 , have a distance vector in common?

Problem 2. What is the smallest set S of distance vectors with the property that any pair of Costas arrays (of any, possibly not the same, order) with a distance vector in common have a common distance vector lying in S ?

Problem 3. What is the smallest set S of distance vectors with the property that any Costas array of order larger than 1 has a distance vector lying in S ?

We ran an exhaustive search on the database of all known Costas arrays up to order 26 to find pairs without common vectors. Let us denote by $C(i, j)$, $i, j \in [26]$ the number of pairs of Costas arrays without common vectors when one array is of order i and the other of order j ; obviously, $C(i, j) = C(j, i)$, so we can assume that $i \leq j$. The experiment was coded in Matlab and needed approximately 27.8 hours to complete on a Core 2 Duo 6600 (2.4 GHz) PC with 2 GB of memory. The results were as follows:

- When $i = 1$, $C(1, j)$ is trivially the total number of Costas arrays of order j , as 1 contains no distance vectors whatsoever!

Order	# arrays	# symmetric arrays	# arrays by T_4
1	1	1	1
2	0	0	0
3	0	0	0
4	0	0	0
5	4	2	4
6	4	2	0
7	4	2	4
8	12	2	0
9	16	0	0
10	44	2	0
11	60	2	0
12	272	0	0
13	416	8	0
14	524	10	0
15	428	10	4
16	584	8	0
17	432	8	0
18	256	4	0
19	224	4	0
20	160	0	0
21	96	0	0
22	40	0	0
23	32	0	0
24	0	0	0
25	0	0	0
26	0	0	0

TABLE II
NUMBER OF ARRAYS THAT CONTAIN NEITHER $\{1, 1\}$ NOR $\{1, -1\}$ PER ORDER. THE COLUMNS OF THE TABLE ARE, FROM LEFT TO RIGHT: ORDER; TOTAL NUMBER OF ARRAYS; NUMBER OF SYMMETRIC ARRAYS; NUMBER OF ARRAYS PRODUCED BY T_4 .

Order	Costas array
14	8 13 3 6 10 2 14 5 11 7 1 12 9 4
15	15 8 13 3 6 10 2 14 5 11 7 1 12 9 4

TABLE III
REPRESENTATIVES OF THE 2 FAMILIES OF SYMMETRIC SPORADIC ARRAYS AT ORDERS 14 AND 15 THAT CONTAIN NONE OF THE VECTORS IN $\{(1, -1), (1, 1), (1, -2), (1, 2), (2, -1), (2, 1)\}$; THE REPRESENTATIVES ARE CLEARLY RELATED THROUGH THE ADDITION OF A CORNER DOT.

- When $i = 2$ or $i = 3$, the results are given in Table I.
- When $i = 4$, $C(4, j) = 0$, $j \in [26], j \geq 4, j \neq 13, 17$, while $C(4, 13) = 8$ and $C(4, 17) = 16$.
- When $5 \leq i \leq j$, $C(i, j) = 0$.

This result allows us to formulate a conjecture regarding Problem 1:

Conjecture 1. Problem 1 can be answered in the affirmative with $n = 5$.

Let us now turn our attention to Problem 3 for Costas arrays of order $n \in [26]$, $n \geq 2$. Again, exhaustive search reveals that:

- When $S = \{(1, -1), (1, 1)\}$, the arrays that contain no distance vector in S are shown in Table II for the various orders $n \leq 26$.
- When $S = \{(1, -1), (1, 1), (1, -2), (1, 2), (2, -1), (2, 1)\}$, there exist Costas arrays that contain no distance vectors in S , but they are extremely few: our exhaustive search revealed 4 in each of the orders 14 and 15. In both cases they correspond to the families of a symmetric but sporadic Costas array, and actually the one at order 15 can be obtained from the one at order 14 by the addition of a corner dot. They are shown in Table III.
- Finally, when $S = \{(1, -1), (1, 1), (1, -2), (1, 2), (2, -1), (2, 1), (2, -2), (2, 2)\}$, all Costas arrays of order at most 26 register at least one distance vector in S .

We can formulate then the following conjecture:

Conjecture 2. The set mentioned in Problem 3 is $S =$

		j															
		2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
i	2	2	4	8	28	68	104	236	304	856	1900	3236	5076	6484	7320	7824	6688
	3		8	0	0	0	8	8	8	80	208	176	240	336	432	424	320
		j															
		18	19	20	21	22	23	24	25	26							
i	2	5344	3552	2196	1208	656	288	32	16	24							
	3	200	136	160	80	16	8	0	0	0							

TABLE I
 $C(i, j)$, AS DEFINED IN SECTION III, FOR $i = 2, 3$ AND $j = 2, \dots, 26$

$\{(1, -1), (1, 1), (1, -2), (1, 2), (2, -1), (2, 1), (2, -2), (2, 2)\}$.

An exhaustive search for the set S mentioned in Problem 2, similar to the search for Problem 1, on all arrays of order $n \in [26]$, shows that $S = \{(x, y) \in \mathbb{Z}^2 : x \in [3], y \in -[3] \cup [3], (x, y) \neq (3, 3), (3, -3)\}$. Hence, the appropriate conjecture is:

Conjecture 3. The set mentioned in Problem 2 is $S = \{(x, y) \in \mathbb{Z}^2 : x \in [3], y \in -[3] \cup [3], (x, y) \neq (3, 3), (3, -3)\}$.

IV. COMMON VECTORS BETWEEN GOLOMB AND WELCH COSTAS ARRAYS

In the previous section we exhaustively searched the database of known Costas arrays, in those orders for which *all* Costas arrays are known today, for common vectors between pairs and formulated conjectures. In this section we will attempt to formulate and prove rigorously similar results for Golomb and Welch Costas arrays.

A. Golomb Costas arrays

The following lemma is here of paramount importance:

Lemma 1. In the notation of Theorem 2, the distance vector (u, v) , $|v| < q - 2, 0 < u < q - 2$ is not contained in the Golomb Costas array generated by the primitive roots a and b if $a^u = b^v$ in $\mathbb{F}(q)$.

Proof: We wish to solve the system of equations:

$$a^i + b^j = 1, \quad a^{i+u} + b^{j+v} = 1;$$

by multiplying the first equation by a^u , then b^v , and in each case subtracting them, we obtain the solution:

$$b^j = \frac{a^u - 1}{a^u - b^v}, \quad a^i = \frac{b^v - 1}{b^v - a^u}$$

When clearly $a^u \neq 1$ for the given range of values of u , so $a^u = b^v$ leads to no solution; otherwise, a unique solution exists.

Remark 3. The existence of a unique solution in the lemma above when $a^u \neq b^v$ should *not* be taken to imply that the vector (u, v) is physically contained in the array: beware of the possibilities $i < q - 1 \leq i + u$ or $j < q - 1 \leq j + v$, in which case the vectors are interrupted by a boundary of the array: the Golomb equation really considers the array as a torus! Additional conditions will be needed to guarantee that the vector actually lies *within* the array.

Theorem 3. Consider the Golomb array generated by the primitive roots $a, b \in \mathbb{F}(q)$; then,

- 1) unless $a = b$, the vector $(1, 1)$ lies in the array;
- 2) unless $a = b^{-1}$, the vector $(1, -1)$ lies in the array;

- 3) unless $b = a^2$ or $a + b = 0$, the vector $(2, 1)$ lies in the array;
- 4) unless $b^{-1} = a^2$ or $a + b^{-1} = 0$, the vector $(2, -1)$ lies in the array;
- 5) unless $a = b^2$ or $a + b = 0$, the vector $(1, 2)$ lies in the array;
- 6) unless $a = b^{-2}$ or $a + b^{-1} = 0$, the vector $(1, -2)$ lies in the array;
- 7) unless $a^2 = b^2 \Leftrightarrow a = \pm b$ or $a^2 + b = 0$ or $a + b^2 = 0$, the vector $(2, 2)$ lies in the array;
- 8) unless $a^2 = b^{-2} \Leftrightarrow a = \pm b^{-1}$ or $a^2 + b^{-1} = 0$ or $a + b^{-2} = 0$, the vector $(2, -2)$ lies in the array;
- 9) unless $a^3 = b$ or $a^3 + ab - b - a = 0$ or $a^3 + a^2b - a^2 - b = 0$, the vector $(3, 1)$ lies in the array;
- 10) unless $a^3 = b^{-1}$ or $a^3 + ab^{-1} - b^{-1} - a = 0$ or $a^3 + a^2b^{-1} - a^2 - b^{-1} = 0$, the vector $(3, -1)$ lies in the array;
- 11) unless $b^3 = a$ or $b^3 + ab - b - a = 0$ or $b^3 + b^2a - b^2 - a = 0$, the vector $(1, 3)$ lies in the array;
- 12) unless $b^{-3} = a$ or $b^{-3} + ab^{-1} - b^{-1} - a = 0$ or $b^{-3} + b^{-2}a - b^{-2} - a = 0$, the vector $(1, -3)$ lies in the array;

Proof: The proof is inescapably quite repetitive in nature and consists of checking all possible cases:

- 1) If $a \neq b$, the only possibility for $(1, 1)$ not lying within the array is either $i = q - 2 = -1$ or $j = q - 2 = -1$; the first equation in Lemma 1 in this case becomes:

$$\frac{1}{b} = \frac{a - 1}{a - b} \Leftrightarrow a - b = ab - b \Leftrightarrow a = 0 \text{ or } b = 1$$

which is impossible, while the second equation is the symmetric expression by swapping a and b , hence also impossible.

- 2) In view of the previous result, flip the array vertically; this is equivalent to substituting b with b^{-1} , hence with negating the second coordinate of distance vectors.
- 3) If $b \neq a^2$, $(2, 1)$ will fail to be in the array only if it gets interrupted by the boundary; this would occur if $i = q - 2 = -1$ or $i = q - 3 = -2$ or $j = q - 2 = -1$, leading to the equations:

$$\frac{1}{a} = \frac{b - 1}{b - a^2}, \quad \frac{1}{a^2} = \frac{b - 1}{b - a^2}, \quad \frac{1}{b} = \frac{a^2 - 1}{a^2 - b}$$

Among these, the second and the third lead to the trivial solutions $b = 0$ or $a^2 = 1$, and $a = 0$ or $b = 1$, respectively, while the first yields the condition:

$$b - a^2 = ab - a \Leftrightarrow a^2 + ab - a - b = 0 \Leftrightarrow (a - 1)(a + b) = 0 \Leftrightarrow a + b = 0$$

- given that $a \neq 1$ as a primitive root.
- 4) Use the previous result and flip vertically.

- 5) Use the result for (2, 1) and transpose the array: transposition is equivalent to swapping the primitive roots; however, as the condition $a + b = 0$ is symmetric in a and b , it remains unchanged.
- 6) Use the previous result and flip vertically.
- 7) If $a^2 \neq b^2 \Leftrightarrow a \neq \pm b$, (2, 2) will lie within the array unless i or j is equal to $q - 2 = -1$ or $q - 3 = -2$. The corresponding equations are:

$$\frac{1}{a} = \frac{b^2 - 1}{b^2 - a^2}, \quad \frac{1}{a^2} = \frac{b^2 - 1}{b^2 - a^2},$$

$$\frac{1}{b} = \frac{a^2 - 1}{a^2 - b^2}, \quad \frac{1}{b^2} = \frac{a^2 - 1}{a^2 - b^2}$$

Among these, the second and the fourth lead to the trivial solutions $b = 0$ or $a^2 = 1$, and $a = 0$ or $b^2 = 1$, respectively, while the first gives:

$$b^2 - a^2 = b^2 a - a \Leftrightarrow ab^2 - b^2 + a^2 - a = 0 \Leftrightarrow (a - 1)(b^2 + a) = 0 \Leftrightarrow b^2 + a = 0$$

and the fourth the symmetric result in a and b , namely $a^2 + b = 0$.

- 8) Use the previous result and flip vertically.
- 9) If $a^3 \neq b$, (3, 1) will lie within the array unless $i = -1, -2, -3$ or $j = -1$. The corresponding equations are:

$$\frac{1}{a} = \frac{b - 1}{b - a^3}, \quad \frac{1}{a^2} = \frac{b - 1}{b - a^3},$$

$$\frac{1}{a^3} = \frac{b - 1}{b - a^3}, \quad \frac{1}{b} = \frac{a^3 - 1}{a^3 - b}$$

Among these, the third and the fourth equation lead to the trivial solutions $b = 0$ or $a^3 = 1$ and $a = 0$ or $b = 1$, respectively, while the first gives:

$$b - a^3 = ab - a \Leftrightarrow a^3 + ab - a - b = 0$$

and similarly the second gives: $a^3 + a^2 b - a^2 - b = 0$.

- 10) Use the previous result and flip vertically.
- 11) Use the result for (3, 1) and transpose the array.
- 12) Use the previous result and flip vertically.

The large number of cases analyzed above allows us now to prove the following important theorem:

Theorem 4. Any 2 Golomb Costas arrays having a distance vector in common have at least one of the following distance vectors in common: (1, 1), (1, -1), (2, 1), (2, -1), (3, 1), (3, -1), (3, 2).

Proof: Consider 2 Golomb Costas arrays with a distance vector in common; if they both contain either (1, 1) or (1, -1) the proof is complete. Assume then that the first array, generated by some primitive roots a and b in some $\mathbb{F}(q)$, does not contain (1, 1), and that the second array, generated by some primitive roots α and β in some $\mathbb{F}(q')$, does not contain (1, -1). It follows, in accordance with Theorem 3, that $a = b$ and that $\alpha\beta = 1$.

Can the 2 arrays contain both the distance vector (2, 1)? The first would not if either $a^2 = a$ or $2a = 0$; the former is impossible, as a is a primitive root, while the second is impossible unless $q = 2^m$. The second, in turn, would not if either $\alpha^{-1} = \alpha^2 \Leftrightarrow \alpha^3 = 1$ or $\alpha + \alpha^{-1} = 0 \Leftrightarrow \alpha^2 =$

$-1 \Leftrightarrow \alpha^4 = 1$; the former excludes only the case $q' = 3$ and the latter only the case $q' = 4$, in which (2, 1) would not fit anyway. So, unless $q = 2^m$, (2, 1) is a common vector.

Assume now that for the first array it holds true that $a = b$ and $q = 2^m$; then, according to Theorem 3, this array cannot contain (1, 1), (2, 1), (1, 2), and (2, 2). Can both arrays contain (2, -1)? The second will unless $\alpha^2 = \alpha$, which is impossible, or $2\alpha = 0$, which is impossible unless $q' = 2^m$. Assuming then that q' is not a power of 2, (2, -1) is a common vector.

Assuming, in addition, that $q' = 2^m$, however, the second array cannot contain (1, -1), (2, -1), (1, -2), and (2, -2). Hence, we need to investigate the possibility that (3, 1) be a common distance vector. The first array will contain it iff none of the following equations hold: $a^3 = a$, $a^3 + a^2 = 0$, and $a^2 + a = 0$, which are clearly impossible as a is a primitive root. The second array will contain it iff none of the following equations hold: $a^4 = 1$, $a^3 + 1 + a^{-1} + a = 0 \Leftrightarrow a^4 + a^2 + a + 1 = 0 \Leftrightarrow a^3 = a^2 + 1$, $a^3 + a + a^2 + a^{-1} = 0 \Leftrightarrow a^4 + a^3 + a^2 + 1 = 0 \Leftrightarrow a^3 = a + 1$. The first of these equations excludes Golomb arrays of order 3, which are too small to contain (3, 1) anyway, while the other two describe 2 Golomb Costas arrays in $\mathbb{F}(8)$, one being the rotation by 180° of the other: their permutations can be readily found to be 245163 and 416235, and it can also be seen that they both contain the distance vector (3, -1).

Can then (3, -1) be a common vector? It will, unless the first array satisfies the corresponding equations stated in Theorem 3. When is this the case? We could proceed as above, but we can use the result above as a shortcut: as the 2 arrays we found contain (3, 1) but not (3, -1), their vertical flips will contain (3, -1) but not (3, 1). Their corresponding permutations are then 532614 and 361542. We observe that all 4 of these arrays contain (3, 2) (as well as (3, -2)), and the proof is complete.

B. Welch Costas arrays

Consider the Welch Costas permutation generated by the primitive root $g \in \mathbb{F}(p)$, p prime, and the fixed constant $c \in [p - 1] - 1$: $j = f(i) = g^{i-1+c} \pmod p$, $i \in [p - 1]$. If we want the distance vector (u, v) to appear in the array, we need to make sure the following system can be solved for i and j :

$$j = g^{i-1+c} \pmod p, \quad j + v = g^{i+u-1+c} \pmod p$$

Let us first seek a solution to the very similar in appearance but very different system:

$$j \equiv g^{i-1+c} \pmod p, \quad j + v \equiv g^{i+u-1+c} \pmod p$$

Multiplying the first equation by g^u and subtracting, we obtain:

$$j \equiv \frac{v}{g^u - 1} \pmod p, \quad g^{i-1+c} \equiv \frac{v}{g^u - 1} \pmod p \quad (1)$$

Therefore, a unique solution exists for every distance vector. We just need to make sure the vector actually lies within the array. We formulate now the counterpart of Theorem 3 for Welch arrays.

Theorem 5. Consider the Welch Costas permutation generated by the primitive root $g \in \mathbb{F}(p)$, p prime, and the fixed constant $c \in [p - 1] - 1$: $j = f(i) = g^{i-1+c} \pmod p$, $i \in [p - 1]$. Then:

- 1) unless $g^c - g^{c-1} \equiv 1 \pmod p$, the vector (1, 1) lies in the array;

- 2) unless $g^c - g^{c-1} \equiv -1 \pmod{p}$, the vector $(1, -1)$ lies in the array;
- 3) unless $g^c - g^{c-1} \equiv 2 \pmod{p}$, the vector $(1, 2)$ lies in the array;
- 4) unless $g^c - g^{c-1} \equiv -2 \pmod{p}$, the vector $(1, -2)$ lies in the array;
- 5) unless $g^c - g^{c-2} \equiv 1 \pmod{p}$ or $g^{c+1} - g^{c-1} \equiv 1 \pmod{p}$, $(2, 1)$ lies in the array;
- 6) unless $g^c - g^{c-2} \equiv -1 \pmod{p}$ or $g^{c+1} - g^{c-1} \equiv -1 \pmod{p}$, $(2, -1)$ lies in the array;
- 7) unless $g^c - g^{c-2} \equiv 2 \pmod{p}$, $g^{c+1} - g^{c-1} \equiv 2 \pmod{p}$, or $g^4 \equiv 1 \pmod{p}$, $(2, 2)$ lies in the array;
- 8) unless $g^c - g^{c-2} \equiv -2 \pmod{p}$, $g^{c+1} - g^{c-1} \equiv -2 \pmod{p}$, or $g^4 \equiv 1 \pmod{p}$, $(2, -2)$ lies in the array.

Proof:

- 1) This vector will fail to lie within the array iff its starting point is on the bottom or the right border of the array, namely iff $i = p-1$ or $j = p-1$. Setting $(u, v) = (1, 1)$ in (1), we obtain $j \equiv \frac{1}{g-1} \pmod{p}$, $g^{i-1+c} \equiv \frac{1}{g-1} \pmod{p}$. Setting $j = p-1$, we obtain $g \equiv 0 \pmod{p}$, which is impossible, while setting $i = p-1$ we obtain $g^c - g^{c-1} \equiv 1 \pmod{p}$.
- 2) This vector will fail to lie within the array iff its starting point is on the top or the right border of the array, namely iff $i = p-1$ or $j = 1$. Setting $(u, v) = (1, -1)$ in (1), we obtain $j \equiv -\frac{1}{g-1} \pmod{p}$, $g^{i-1+c} \equiv -\frac{1}{g-1} \pmod{p}$. Setting $j = 1$, we obtain $g \equiv 0 \pmod{p}$, which is impossible, while setting $i = p-1$ we obtain $g^c - g^{c-1} \equiv -1 \pmod{p}$.
- 3) This vector will fail to lie within the array iff $i = p-1$, $j = p-2$, or $j = p-1$. Setting $(u, v) = (1, 2)$ in (1), we obtain $j \equiv \frac{2}{g-1} \pmod{p}$, $g^{i-1+c} \equiv \frac{2}{g-1} \pmod{p}$. Setting $j = p-2$, we obtain $g \equiv 0 \pmod{p}$, which is impossible; setting $j = p-1$, we obtain $g \equiv -1 \pmod{p}$, which is impossible; finally, setting $i = p-1$ we obtain $g^c - g^{c-1} \equiv 2 \pmod{p}$.
- 4) Repeat the derivation above with $v = -2$.
- 5) This vector will fail to lie within the array iff its starting point (i, j) satisfies $i = p-1$, $i = p-2$, or $j = p-1$. The first equation leads to $\frac{1}{g^2-1} \equiv g^{c-1} \pmod{p} \Leftrightarrow g^{c+1} - g^{c-1} \equiv 1 \pmod{p}$; the second to $\frac{1}{g^2-1} \equiv g^{c-2} \pmod{p} \Leftrightarrow g^c - g^{c-2} \equiv 1 \pmod{p}$; and the third to $-1 \equiv \frac{1}{g^2-1} \pmod{p} \Leftrightarrow g \equiv 0 \pmod{p}$ which is impossible.
- 6) Repeat the derivation above with $v = -1$.
- 7) This vector will fail to lie within the array iff either i or j is equal to $p-1$ or $p-2$. These conditions lead to the 4 equations:

$$\begin{aligned} -1 &\equiv \frac{2}{g^2-1} \pmod{p}, & -2 &\equiv \frac{2}{g^2-1} \pmod{p}, \\ g^{c-1} &\equiv \frac{2}{g^2-1} \pmod{p}, & g^{c-2} &\equiv \frac{2}{g^2-1} \pmod{p} \end{aligned}$$

The first leads to $g^2 \equiv -1 \pmod{p} \Rightarrow g^4 \equiv 1 \pmod{p}$; the second to $g \equiv 0 \pmod{p}$ which is impossible; the

third to $g^{c+1} - g^{c-1} \equiv 2 \pmod{p}$; and the fourth to $g^c - g^{c-2} \equiv 2 \pmod{p}$.

- 8) Repeat the derivation above with $v = -1$.

As in the Golomb case, the large number of cases analyzed above allows us now to prove the following important theorem:

Theorem 6. Any 2 Welch Costas arrays, as defined in Theorem 1, having a distance vector in common have at least one of the following distance vectors in common: $(1, 1)$, $(1, -1)$, $(1, 2)$, $(2, 1)$, $(2, -1)$, $(2, 2)$.

Proof: Consider 2 Welch Costas arrays with a distance vector in common; if they both contain either $(1, 1)$ or $(1, -1)$ the proof is complete. Assume then that the first array, generated by some primitive root $g \in \mathbb{F}(p)$, does not contain $(1, 1)$, and that the second array, generated by some primitive root $h \in \mathbb{F}(q)$, does not contain $(1, -1)$.

Note that it is impossible for a Welch Costas array to contain neither of $(1, 1)$ and $(2, 1)$, or neither of $(1, -1)$ and $(2, -1)$. Let us focus on the first case, as the second follows from a verbatim repetition of the argument for the first: if it were possible for neither of the vectors to be present, the array would need to satisfy, according to Theorem 5, both $g^c - g^{c-1} \equiv 1 \pmod{p}$ and one of $g^c - g^{c-2} \equiv 1 \pmod{p}$, $g^{c+1} - g^{c-1} \equiv 1 \pmod{p}$. Either choice, however, leads to the trivial solution $g = 0$ or $g = 1$, which is impossible.

We are actually assuming then that the first array contains neither $(1, 1)$ nor $(2, -1)$, while the second array contains neither $(1, -1)$ nor $(2, 1)$. Would it be possible for both not to contain $(2, 2)$? Once more, let us focus on the first array, as the equations for the second are almost the same. If the first array contains none of $(1, 1)$, $(2, -1)$, and $(2, 2)$, it should satisfy

$$\begin{aligned} &g^c - g^{c-1} \equiv 1 \pmod{p} \quad (1), \\ \text{one of } &\begin{cases} g^c - g^{c-2} \equiv -1 \pmod{p} & (a) \\ g^{c+1} - g^{c-1} \equiv -1 \pmod{p} & (b) \end{cases} \\ \text{and one of } &\begin{cases} g^c - g^{c-2} \equiv 2 \pmod{p} & (A), \\ g^{c+1} - g^{c-1} \equiv 2 \pmod{p} & (B), \\ g^4 \equiv 1 \pmod{p} & (C) \end{cases} \end{aligned}$$

There are then 6 possible scenarios in total:

- 1aA Impossible, unless $-1 \equiv 2 \pmod{p}$, which implies $p = 3$.
- 1aB Summing (1) and (a) we get $2g^2 - g - 1 \equiv 0 \pmod{p} \Rightarrow g \equiv -2^{-1} \pmod{p}$, $g \equiv 1 \pmod{p}$, while (a) and (B) give $g \equiv -2 \pmod{p}$; this is impossible unless $2^{-1} \equiv 2 \pmod{p} \Rightarrow p = 3$.
- 1aC Summing (1) and (a) we get $2g^2 - g - 1 \equiv 0 \pmod{p} \Rightarrow g \equiv -2^{-1} \pmod{p}$, $g \equiv 1 \pmod{p}$, the latter being impossible. (C) implies $p = 5$, in which case $g \equiv -2^{-1} \equiv 2 \pmod{5}$, and indeed $g^4 \equiv 1 \pmod{5}$. Now, (1) yields $2^{c-1} \equiv 1 \pmod{5}$, namely $c = 1$. To sum up, the equations are compatible and specify the array 2431.
- 1bA Summing (1) and (b) we get $g^2 + g - 2 \equiv 0 \pmod{p} \Rightarrow g \equiv -2 \pmod{p}$, $g \equiv 1 \pmod{p}$, while (b) and (A) give $g \equiv -2^{-1} \pmod{p}$; this is impossible unless $2^{-1} \equiv 2 \pmod{p} \Rightarrow p = 3$.
- 1bB Impossible, unless $-1 \equiv 2 \pmod{p}$, which implies $p = 3$.

1bC Summing (1) and (b) we get $g^2 + g - 2 \equiv 0 \pmod p \Rightarrow g \equiv -2 \pmod p, g \equiv 1 \pmod p$, the latter being impossible. (C) implies $p = 5$, in which case $g \equiv 3 \pmod 5$, and indeed $g^4 \equiv 1 \pmod 5$. Now, (1) yields $3^{c-1} \equiv \frac{1}{2} \equiv 3 \pmod 5$, namely $c = 2$. To sum up, the equations are compatible and specify the array 4213, which is the rotation by 180° of 2431.

For the second array, we similarly end up with the 2 arrays 3124 and 1342, the vertical flips of the 2 arrays found above, which are also the rotation by 180° of each other. So, all pairs of Welch Costas arrays with a vector in common, except for 4 pairs of Welch arrays of order 4, have a common vector in $(1, 1), (1, -1), (2, 1), (2, -1), (2, 2)$; and in those 4 pairs, we observe that $(1, 2)$ and $(1, -2)$ are always common vectors.

We are not done yet with Welch arrays, however: the transposition of a Welch array cannot be generated by the general equation in Theorem 1, in contrast to the case of Golomb arrays. If we expand the family of Welch arrays to include transpositions as well, we need to check for common vectors pairs of transposed arrays as well as mixed pairs.

Theorem 7. Any pair of Costas arrays consisting of a Welch array and a transposed Welch array with a common vector have a common vector in $(1, 1), (1, -1), (2, 1)$.

Proof: Assume the first array corresponds to the primitive root $g \in \mathbb{F}(p)$ and the parameter c , and that the second is the transposition of the array corresponding to the primitive root $h \in \mathbb{F}(q)$ and the parameter d . Assume further that the first array does not contain $(1, 1)$, while the second does not contain $(1, -1)$; according to Theorem 5, the first must then contain $(2, 1)$, unless it is of order 2. Is it possible for the second not to contain $(1, 2)$? In such a case the second array should satisfy the equations $h^d - h^{d-1} \equiv -1 \pmod p$ and $h^d - h^{d-1} \equiv 2 \pmod p$, implying that $p = 3$.

Obviously, the common vectors between transposed Welch Costas arrays must lie within the transposed set of vectors of Theorem 6. Putting everything together, we obtain:

Theorem 8. Any 2 Welch Costas arrays with a common distance vector have one of the following vectors in common: $(1, 1), (1, -1), (1, 2), (2, 1), (2, -1), (1, -2), (2, 2)$.

C. Mixed pairs

What can we say about common vectors between a Golomb Costas array and a Welch Costas array? With all the results we have already obtained, the answer is quite simple to obtain:

Theorem 9. A Welch and a Golomb Costas array with a vector in common always have a common vector among: $\{(1, 1), (1, -1), (1, 2), (1, -2), (2, 1), (2, -1)\}$.

Proof: Assuming $(1, 1)$ or $(1, -1)$ is a common vector, the proof is complete. Hence, let us assume that the Welch array, corresponding to the primitive root $g \in \mathbb{F}(p)$ and the parameter c , does not contain $(1, 1)$, while the Golomb array, corresponding to the primitive roots $a, b \in \mathbb{F}(q)$, does not contain $(1, -1)$. It follows by Theorems 3 and 5 that $(2, 1)$ is contained in the Welch array, and that $a = b^{-1}$. If the Golomb array does not contain $(2, 1)$, either $b = a^2$ or $a + b = 0$; it follows that either $a^3 = 1$ or $a^2 = -1 \Rightarrow a^4 = 1$, implying that the Golomb array must be of order 2 or 3. There are only

2 Costas arrays that do not contain $(1, 1)$, namely 312 and 231, and they both contain $(2, -1)$ and $(1, -2)$; now, Theorem 5 shows that any Welch array not containing $(1, 1)$ contains $(1, -2)$, and this completes this case.

If we assume the symmetric scenario, namely that the Welch array does not contain $(1, -1)$ and the Golomb array does not contain $(1, 1)$, flipping both arrays we are back in the previous case; therefore, the common vectors here are the previous ones with the sign of the second coordinate changed. This completes the proof.

D. A general theorem

Combining all of the results in this section, we get a general result on common vectors between Golomb and Welch arrays:

Theorem 10. The smallest set of common vectors, closed under flips and transposition, with the property that any pair of Costas arrays, chosen among Golomb and Welch arrays only, having a common vector has a vector in this set, is: $\{(1, 1), (1, -1), (1, 2), (2, 1), (2, -1), (1, -2), (2, 2), (2, -2), (3, 1), (3, -1), (1, 3), (1, -3), (2, 3), (2, -3), (3, 2), (3, -2)\}$. This the same set as in Conjecture 3.

V. CONCLUSION AND FUTURE DIRECTION

We investigated the distance vectors in individual Costas arrays (of various categories), and in pairs of Costas arrays. We offered general results by simulation, and rigorous results for algebraically constructed arrays. We were especially interested in pairs of Costas arrays with no distance vector in common (“orthogonal” pairs of Costas arrays), and the evidence we discovered seems to suggest that such pairs do not exist if the order of the arrays is large enough (5 or higher).

Our results constitute little progress towards the general problem itself of the distance vectors present within a Costas array. The (tedious and repetitive) methods used above can be extended to the derived algebraic constructions (such as W_2 or T_4), but the biggest problem we will still be facing is the classification of the distance vectors of the sporadic arrays: this task clearly requires some understanding of the way in which the constraining equations of the Costas property shape the distance vectors, and we feel that such an understanding is currently eluding us.

REFERENCES

- [1] J. P. Costas. “Medium constraints on sonar design and performance.” Technical Report Class 1 Rep. R65EMH33, GE Co., 1965
- [2] J. P. Costas. “A study of detection waveforms having nearly ideal range-doppler ambiguity properties.” Proceedings of the IEEE, 72(8), pp. 996-1009, August 1984
- [3] K. Drakakis. “A review of Costas arrays.” Journal of Applied Mathematics, Volume 2006 (2006)
- [4] K. Drakakis. “On some properties of Costas arrays generated via finite fields.” IEEE CISS 2006
- [5] A. Freedman, N. Levanon. “Any two $N \times N$ Costas signals must have at least one common ambiguity sidelobe if $N > 3$ —A proof.” Proceedings of the IEEE, Volume 73, No. 10, October 1985, pp. 1530-1531
- [6] S. Golomb. “Algebraic Constructions For Costas Arrays.” Journal Of Combinatorial Theory Series A, Volume 37(1), pp. 13-21, 1984.