

## *Research Article*

# **Cross-Correlation Properties of Costas Arrays and Their Images under Horizontal and Vertical Flips**

**Konstantinos Drakakis,<sup>1,2</sup> Rod Gow,<sup>2,3</sup> John Healy,<sup>1,2</sup> and Scott Rickard<sup>1,2</sup>**

<sup>1</sup> *School of Electrical, Electronic & Mechanical Engineering, University College Dublin, Belfield, Dublin 4, Ireland*

<sup>2</sup> *Claude Shannon Institute, UCD CASL, University College Dublin, Belfield, Dublin 4, Ireland*

<sup>3</sup> *School of Mathematics, University College Dublin, Belfield, Dublin 4, Ireland*

Correspondence should be addressed to Konstantinos Drakakis, [konstantinos.drakakis@ucd.ie](mailto:konstantinos.drakakis@ucd.ie)

Received 18 September 2008; Accepted 29 November 2008

Recommended by Fernando Lobo Pereira

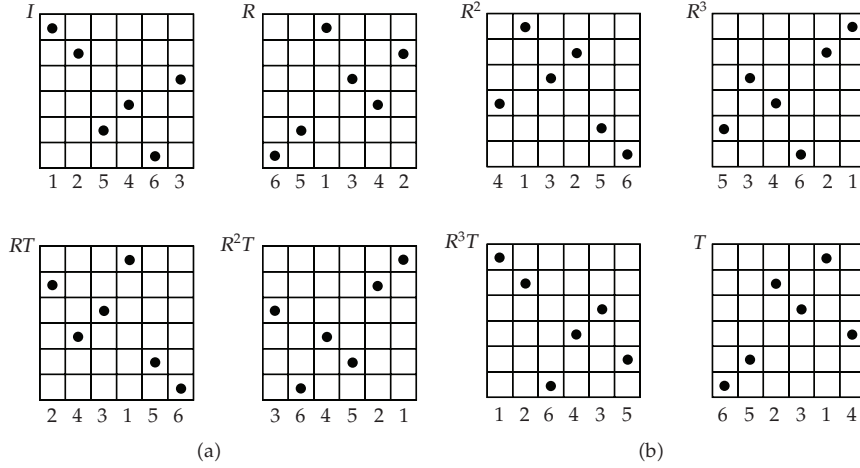
We consider the cross-correlation of a Costas array with its image under a horizontal and/or a vertical flip. We propose and prove several bounds on the maximal cross-correlation and on its value at the origin, for both general Costas arrays and for algebraically constructed ones.

Copyright © 2008 Konstantinos Drakakis et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

## **1. Introduction**

Costas arrays were introduced as frequency hopping patterns with ideal autoambiguity properties by Dr. Costas [1, 2], in an effort to improve SONAR performance. Unable to find a general construction technique himself, he approached Professor Solomon Golomb, who published [3] and proved [4] two generation techniques for Costas arrays, both based on the theory of finite fields, known as the Welch and the Golomb-Lempel methods, respectively. These are still the only general construction methods for Costas arrays available today.

In multiuser and multiplexing systems it is desirable that the signals used have low cross-correlation, in order to minimize cross-talk. While Costas arrays are known for (and, indeed, defined by) their ideal autocorrelation, they typically exhibit poor cross-correlation. Subfamilies of Costas arrays with low cross-correlation are, therefore, particularly suitable for such applications. In this paper, we examine the cross-correlation of pairs of Costas arrays related by a horizontal and/or a vertical flip, in order to identify array pairs with good cross-correlation properties. Such a small family will be sufficient in some applications, for example, when a small number of SONARs/RADARs (4 or less) operate in the same geographical area (otherwise larger families will need to be considered, but this study lies outside the scope of this paper).



**Figure 1:** Labeling of rotations and reflections of a Costas array.  $I$ , the original array;  $R$ , a  $90^\circ$  rotation CCW;  $ST = R^2$ , a  $180^\circ$  rotation;  $R^3$ , a  $270^\circ$  rotation CCW;  $RT$ , a reflection about the main antidiagonal;  $S = R^2T$ , a horizontal flip;  $R^3T$ , a reflection about the main diagonal; and  $T$ , a vertical flip.

Regarding the layout of the paper, in Section 2 we give the definition of Costas arrays and describe the construction methods available. In Section 3, we review the literature on cross-correlation properties of Costas arrays. In Section 4, we prove the reflective symmetry property of Welch Costas arrays. Section 5 states and proves bounds on the cross-correlation of pairs of Costas arrays in the same family.

## 2. Costas arrays: definition and algebraic constructions

*Definition 2.1.* Let  $[n] := \{1, \dots, n\}$ ,  $n \in \mathbb{N}$  and consider a bijection  $f : [n] \rightarrow [n]$ ;  $f$  is a Costas permutation if and only if for all  $i, j, k$  such that  $1 \leq i, j, i+k, j+k \leq n$ ,

$$f(i+k) - f(i) = f(j+k) - f(j) \implies i = j \text{ or } k = 0. \quad (2.1)$$

A Costas array  $A^f$  is the permutation array corresponding to a Costas permutation  $f$ . This correspondence is a matter of convention: we choose here the convention that the  $j$ th element of the permutation indexes the position of the (unique) 1 in the  $j$ th column of the array,  $j \in [n]$ , counting from top to bottom in the usual array convention:  $f(i) = j \Leftrightarrow a_{j,i}^f = 1$ . It is customary to refer to (and denote) the 1s of a permutation array as “dots” and to 0s as “blanks.” Definition 2.1 is equivalent to the statement that all distance vectors  $(f(i) - f(j), i - j)$ , where  $i > j$ , between pairs of dots in a Costas array are distinct (note that we take the second coordinate to be nonnegative).

An example Costas array is shown in the top left of Figure 1. Note that the image of a Costas array under rotation by  $90^\circ$ , horizontal or vertical flips, and transposition is still a Costas array: each Costas array generates a family of eight members (or four, if the array is symmetric) also shown in the figure. The notation used signifies the generation of this family using two operators:  $R$ , a  $90^\circ$  rotation counterclockwise (CCW), and  $T$ , a vertical flip. We also define for convenience  $S = R^2T$  to be the horizontal flip, in which case we also have

that  $R^2 = ST = TS$ , the double (horizontal and vertical) flip. The numbers under each array correspond to the permutation indexing it.

Every Costas array of size  $n \leq 27$  has been found by exhaustive computer search [5–7]: they add up to about 150 000 arrays in total.

The two known construction methods for Costas arrays are based on finite field techniques; each one has several submethods/variants [3, 4, 8]. In the sequel we will work exclusively with the main methods.

**Theorem 2.2** (Welch construction  $W_1(p, \alpha, c)$ ). *Let  $p$  be a prime, let  $\alpha$  be a primitive root of the finite field  $\mathbb{F}(p)$  of  $p$  elements, and let  $c \in [p - 1] - 1$  be a constant; then, the function  $f : [p - 1] \rightarrow [p - 1]$  where  $f(i) = \alpha^{i-1+c} \bmod p$  is a bijection with the Costas property.*

The reason for the presence of  $-1$  in the exponent is that when  $c = 0$ , 1 is a fixed point  $f(1) = 1$ . We refer to arrays generated with  $c \neq 0$  as circular shifts of the array generated by  $c = 0$  for the same  $p$  and  $\alpha$ . Welch Costas arrays have *antireflective symmetry* (see below, and see also [9]).

*Definition 2.3.* Let  $f : [2n] \rightarrow [2n]$ ;  $f$  has antireflective symmetry if and only if

$$f(n + i) + f(i) = 2n + 1, \quad i \in [n], \quad (2.2)$$

which means, in other words, that the right half of  $A^f$  is the vertical flip of the left half.

**Theorem 2.4** (Golomb construction  $G_2(p, m, a, b)$ ). *Let  $p$  be a prime,  $m \in \mathbb{N}$ , and let  $\alpha, \beta$  be primitive roots of the finite field  $\mathbb{F}(p^m)$  of  $q = p^m$  elements; then, the function  $f : [q - 2] \rightarrow [q - 2]$  where  $\alpha^i + \beta^{f(i)} = 1$  is a bijection with the Costas property.*

If  $\alpha = \beta$ , the array is known as a *Lempel Costas array*, and is symmetric about the main diagonal.

### 3. Cross-correlations of Costas arrays

*Definition 3.1.* Let  $f, g : [n] \rightarrow [n]$ ,  $n \in \mathbb{N}$ , and let  $u, v \in \mathbb{Z}$ ; the cross-correlation between  $f$  and  $g$  at  $(u, v)$  is defined as

$$\Psi_{f,g}(u, v) = |\{(f(i) + u, i + v) : i \in [n]\} \cap \{(g(i), i) : i \in [n]\}|. \quad (3.1)$$

In other words, in order to find the cross-correlation of two Costas arrays  $A^f$  and  $A^g$  of order  $n$  at  $(u, v)$ , we place the two arrays on top of each other, slide the first  $v$  columns horizontally and  $u$  rows vertically, and count the number of pairs of dots that overlap. We will also use the notation  $\Psi_{A^f, A^g}$  instead of  $\Psi_{f,g}$ .

There are few previous works on cross-correlations of Costas arrays in the literature. The closest to the subject of this paper is O’Carroll et al. [10] (further details about its relevance to the present work will be given in Section 5). Titlebaum and Maric [11] proved that the maximal cross-correlation of two Welch or Lempel Costas arrays generated from reciprocal primitive roots of an odd prime is 2. They also proved that the upper bound on the maximum of the cross-correlation of two Welch Costas arrays of order  $n$  is  $n/2$ , and established that primes of certain forms had good or bad cross-correlation bounds, for

example, they showed that the upper bound on the maximum of the cross-correlation of a pair of Welch Costas arrays is realized for primes equivalent to 1 modulo 4.

Drumheller and Titlebaum [12] derived upper bounds on the maximal cross-correlation of two Golomb or two Welch Costas arrays, both in terms of the relative powers of the generating primitive elements.

Rickard has previously proposed that the upper bound on the maximal cross-correlation of a pair of Golomb arrays of order  $n$ , taken over all such possible pairs of different arrays, is at most  $(n - 1)/2$  [13]. He also proposed that (a) for primes  $p$  of the form  $2r + 1$ ,  $r$  prime (known as safe or Germain primes), this quantity exhibits local minima, and that (b) the upper bound on the maximal cross-correlation of a pair of Golomb arrays of order  $p - 2$ , taken over all such possible pairs of different arrays, is one less than the corresponding quantity for pairs of Welch arrays of order  $p - 1$ , taken over all pairs of different arrays that are not circular shifts of each other, as long as  $p$  is not a safe prime.

Finally, Etzion has demonstrated that the maximum of the cross-correlation of any Costas array with its image under rotation by  $180^\circ$  is exactly 2 [14].

#### 4. A symmetry property of the Welch arrays

Welch Costas arrays, as mentioned above, have anti-reflective symmetry (see Definition 2.3), also known as *glide-reflection symmetry* (*G-symmetry*) [14]. For completeness, we present a proof of this property.

**Theorem 4.1.** *A Welch Costas array has antireflective symmetry.*

*Proof.* Consider the Welch Costas permutation  $f$  generated by  $\alpha$  in  $\mathbb{F}(p)$ ; then, for all  $i \in [(p - 1)/2]$ ,

$$f(i) + f\left(i + \frac{p-1}{2}\right) = \alpha^{i-1+c} + \alpha^{(p-1)/2+i-1+c} = \alpha^{i-1+c} + p - \alpha^{i-1+c} = p, \quad (4.1)$$

in view of the fact that  $\alpha^{(p-1)/2} \equiv -1 \pmod{p}$ . This completes the proof.  $\square$

We will make use of this property later in the paper. It should be noted that this symmetry does not characterize the Welch Costas arrays, that is, there exist non-Welch arrays with this property. Some conditions on the existence of arrays with antireflective symmetry were established in [14].

#### 5. Proof of some correlation bounds

In this section we present upper bounds on the cross-correlation values of Costas arrays related by a flip. More specifically, we divide our results in two groups: those dealing with the maximum of the cross-correlation and those dealing with the cross-correlation at the origin.

##### 5.1. Bounds on cross-correlation maximum

Freedman and Levanon [15] proved that, for  $n > 3$ , the cross-correlation between any two arrays of the same size will have at least 2 hits. We present a special case where the cross-correlation between a pair of arrays is exactly 2: the cross-correlation between any Costas array and its  $180^\circ$  rotation has a maximum value of 2.

**Theorem 5.1.** *Let  $I$  be a Costas array of order  $n > 1$ ; then  $\max_{(u,v)} \Psi_{I,R^2}(u, v) = 2$ .*

*Proof.* The key observation is that a rotation by  $180^\circ$  generates a Costas array whose distance vectors are the same as in the original array: letting two dots lie at  $A = (f(i), i)$ ,  $B = (f(j), j)$ , where  $i > j$ , their images in the rotated array lie at  $A' = (n + 1 - f(i), n + 1 - i)$ ,  $B' = (n + 1 - f(j), n + 1 - j)$ ,  $n$  being the order of the array. The distance vectors  $BA$  and  $A'B'$  are equal:  $(f(i), i) - (f(j), j) = (f(i) - f(j), i - j)$  and  $(n + 1 - f(j), n + 1 - j) - (n + 1 - f(i), n + 1 - i) = (f(i) - f(j), i - j)$ . It follows that a shift will align these pairs, whence  $\max_{(u,v)} \Psi_{I,R^2}(u, v) \geq 2$  (but note that the shift aligns  $A$  with  $B'$  and  $B$  with  $A'$ ).

Assume now that, for this given shift, a third pair of dots become aligned as well, say  $C$  and  $K$ , where  $C$  is a point in  $I$  and  $K$  a point in  $R^2$ : then  $K$  has a pre-image in  $I$ , say a point  $k$ . We claim that the points  $A, B, C$ , and  $k$  form a parallelogram, violating the Costas property: indeed, by the triple alignment we get  $A'K = BC$  and  $B'K = AC$ , while, by the observation above,  $A'K = kA$  and  $B'K = kB$ . It follows that  $BC = kA$ ,  $AC = kB$ , hence  $AkBC$  is a parallelogram and the proof is complete.  $\square$

As mentioned earlier, this result has also been derived by Etzion ([14, Theorem 2]); we chose to present it here for completeness, offering a more concise proof. O'Carroll et al. [10] sketched a proof that the maximal cross-correlation of any two amongst a Golomb array and its  $S, T$ , and  $ST$  flips is identically 2.

We now prove two bounds for Welch Costas arrays of order  $n$ : first, we show that the peak of the cross-correlation of a Welch Costas array and its vertical flip  $T$  is  $n/2$ . Then we consider the case of a Welch Costas array and its horizontal flip  $S$  which yields a rather better result.

**Theorem 5.2.** *For any antireflective Costas array  $I$  of (even) order  $n$  and its vertical flip  $T$ ,*

$$\max_{(u,v)} \Psi_{I,T}(u, v) = \frac{n}{2}. \quad (5.1)$$

*In particular, the result holds true for any Welch Costas array generated in  $\mathbb{F}(p)$  (where  $n = p - 1$ ).*

*Proof.* We prove this property by considering the form of three distinct regions of the cross-correlation. Let  $f$  be the permutation corresponding to  $i$ . Then, we show that

- (i) for all  $u$ ,  $\Psi_{I,T}(u, v) \leq 1$  when  $v \neq n/2$ ,
- (ii)  $\Psi_{I,T}(u, n/2) = 0$  when  $u \neq 0$ ,
- (iii)  $\Psi_{I,T}(0, n/2) = n/2$ .

Fixing  $u$  and  $v$ , we find the number of pairs  $(i, j)$  for which

$$(f(i), i) = (u, v) + (n + 1 - f(j), j) \implies f(v + j) = u + n + 1 - f(j) = u + f\left(j \pm \frac{n}{2}\right), \quad (5.2)$$

where “+” is chosen if  $j \leq n/2$ , and “-” otherwise.

Assuming  $v \neq n/2$ , this equation has at most one solution  $j$  because of the Costas property. Assuming  $v = n/2$ , the equation becomes  $u = 0$ , which is satisfied for no  $j$  if we choose  $u \neq 0$ , but is satisfied for all  $j \in [n/2]$ , that is  $n/2$  values of  $j$ , if we choose  $u = 0$ . This completes the proof.  $\square$

**Theorem 5.3.** For any Welch Costas array  $I$  and its horizontal flip  $S$ ,

$$\max_{(u,v)} \Psi_{I,S}(u,v) = 2. \quad (5.3)$$

*Proof.* Let  $f$  be the Welch permutation generated in  $\mathbb{F}(p)$  by the primitive root  $\alpha$  and the parameter  $c$ . For fixed values of  $u$  and  $v$ , we need to find the number of pairs  $(i, j)$  for which

$$(\alpha^{i-1+c} \bmod p, i) = (u, v) + (\alpha^{p-j-1+c} \bmod p, j) \quad (5.4)$$

whence we get the two equations

$$\alpha^{i-1+c} \bmod p = u + \alpha^{p-j-1+c} \bmod p, \quad i = v + j, \quad (5.5)$$

namely

$$\alpha^{v+j-1+c} \bmod p = u + \alpha^{p-j-1+c} \bmod p. \quad (5.6)$$

If this equation is true, it is also true mod  $p$ , whence

$$\alpha^{v+j-1+c} \equiv u + \alpha^{c-j} \bmod p \iff \alpha^{v-1+c} \alpha^{2j} - u \alpha^j - \alpha^c \equiv 0 \bmod p. \quad (5.7)$$

Setting  $\alpha^j = x$ , we obtain

$$\alpha^{v-1+c} x^2 - ux - \alpha^c \equiv 0 \bmod p. \quad (5.8)$$

This is an equation of the second degree in a field, and therefore it has at most 2 solutions for  $x$  and thus for  $j$ . Note, however, that not all solutions of this equation need actually also be solutions of (5.6). Note also that, as both  $I$  and  $S$  are Costas arrays, Freedman and Levanon's result [15] guarantees that there are two solutions for at least one pair of values of  $u$  and  $v$ .  $\square$

**Theorem 5.4.** For any Costas array  $I$  of order  $n > 1$ ,

$$\max_{(u,v)} \Psi_{I,G}(u,v) \leq \frac{n}{2} \quad \text{or} \quad \frac{n-1}{2}, \quad (5.9)$$

depending on whether  $n$  is even or odd, respectively, where  $G$  is either  $S$  or  $T$ .

*Proof.* Assume  $n$  even, and assume there exists a shift for which a subset  $A$  of  $(n/2) + 1$  dots of  $I$  can be aligned with a subset  $W$  of equally many dots of  $T$ .  $I$  also contains a subset  $B$  of  $(n/2) + 1$  dots, namely the pre-image of  $W$ : the distance vectors in  $B$  are the vertical flips of the distance vectors in  $A$ .

Observe now that, as no two dots of a Costas array lie in the same row or column, each distance vector is different from its vertical flip. Assume  $A$  contains both a vector  $x$  and

its vertical flip  $x'$ , where, without loss of generality, the starting point of  $x$  lies to the left of the starting point of  $x'$ . Then  $B$  contains both vectors as well, but now the starting point of  $x$  lies to the right of the starting point of  $x'$ . This implies that the two pairs of equal vectors cannot both be collocated, hence  $I$  contains at least two equal vectors and is not Costas, a contradiction.

It follows that distance vectors between points of  $A$  are disjoint from distance vectors between points of  $B$ . But this is absurd, since, by the pigeonhole principle,  $A$  and  $B$  have at least 2 dots in common, hence they necessarily share a common distance vector.

Assuming  $n$  odd, and considering a subset  $A$  of  $(n-1)/2+1$  dots of  $I$ , we end up, as before, with another subset  $B$  of  $(n-1)/2+1$  dots in  $I$ , so that each set contains the vertical flips of the distance vectors present in the other. But now the pigeonhole principle only guarantees the two sets have at least one dot in common, so it is necessary to count more carefully. Indeed, if we assume that the shift aligning  $A$  and  $B$  has a nonzero vertical component, say  $u \neq 0$ , it follows that  $|u| \geq 1$  dots can belong to neither  $A$  nor  $B$ , whence  $|A \cap B| \geq 2$ , that is, they share a common distance vector, which is impossible.

This implies that the shift aligning  $A$  and  $B$  is purely horizontal, so that  $A$  and  $B$  are vertical flips of each other. The only dot that could possibly lie in  $A \cap B$  then is the (unique) dot of the central row, and since at least one dot must exist in  $A \cap B$  (or else  $I$  would have at least  $n+1$  dots), we deduce that no shift is possible. Hence,  $(n-1)/2+1 = 1 \Leftrightarrow n = 1$  is the only possibility.

The argument for  $G = S$  is completely analogous. This completes the proof.  $\square$

Note that, for  $n$  even, the upper bound is actually achieved for a Welch Costas array, while, for  $n$  odd, the upper bound is again achieved for a Costas array resulting from the removal of the corner dot from a Welch Costas array generated with  $c = 0$ , in both cases due to the antireflective symmetry.

## 5.2. Bounds on origin value of cross-correlation

We now consider some of the bounds regarding the values of the cross-correlation at the origin, that is, the number of hits for perfect overlay of two arrays. The reason for our particular interest in the value of the cross-correlation at the origin is, on the one hand, practical, as it becomes the only relevant value in a multiuser system where users' clocks are synchronized, and, on the other hand, theoretical, as it is often much simpler to compute or estimate than a general value, as we are about to see.

First, we show that a Costas array of even order and its vertical or horizontal flip ( $S$  and  $T$ , resp.) do not overlap, while the corresponding result for odd orders is that they overlap at one point only. Note that we already derived and used part of this result in the proof of Theorem 5.4.

**Theorem 5.5.** *For any Costas array of order  $n$ ,*

$$\Psi_{I,B}(0,0) = n \bmod 2, \quad (5.10)$$

*when array  $B$  is either  $S$  or  $T$ .*

*Proof.* Since a Costas array contains one dot per column and row,  $\Psi_{I,T}(0,0)$  will equal the number of dots a vertical flip leaves fixed: if  $n$  is even there is no fixed dot, whereas if  $n$  is

odd exactly one dot remains fixed, namely the one lying on the central row. The horizontal flip is analogously treated. This completes the proof.  $\square$

We now sketch a proof that a symmetric Costas array of even order and its rotation by  $90^\circ$  in either direction ( $R$  and  $R^3$ ) do not overlap, while the corresponding result for odd order is that they overlap at one point only.

**Theorem 5.6.** *For any symmetric Costas array of order  $n$ ,*

$$\Psi_{I,B}(0,0) = n \bmod 2 \quad (5.11)$$

when array  $B$  is one of  $R$  or  $R^3$ .

*Proof.* We can show this by observing that a symmetric array's rotation by  $\pm 90^\circ$  is equivalent to a horizontal or vertical flip and then invoking Theorem 5.5.  $\square$

Next, we prove that if we overlay a Welch Costas array with its  $R^2$  rotation, the number of hits depends on the array order.

**Theorem 5.7.** *For any Welch Costas array  $I$ ,*

$$\Psi_{I,R^2}(0,0) = \begin{cases} 0, & \text{for } p \equiv 1 \pmod{4}, \\ 2, & \text{for } p \equiv 3 \pmod{4}. \end{cases} \quad (5.12)$$

*Proof.* A Welch Costas array of size  $n = p - 1$  contains dots at positions

$$(f(i), i), \quad i \in [p-1] \text{ where } f(i) = \alpha^{i-1+c} \bmod p \quad (5.13)$$

for prime  $p$  and a primitive element  $\alpha$  of  $\mathbb{F}(p)$ . Its  $R^2$  rotation contains dots at positions  $(p - f(j), p - j)$ ,  $j \in [p-1]$ .

The value at the origin of the cross-correlation is equal to the largest possible number of solutions of the simultaneous equations

$$f(i) = p - f(j), \quad i = p - j. \quad (5.14)$$

Substituting the latter into the former and using (5.13), we get, after some manipulation,

$$\begin{aligned} & \alpha^{i-1+c} \bmod p + \alpha^{p-i-1+c} \bmod p = p \\ \iff & \alpha^{i-1+c} + \alpha^{-i+c} \equiv 0 \pmod{p} \\ \iff & \alpha^{i-1+c} \equiv \alpha^{-i+(p-1)/2+c} \pmod{p} \\ \iff & i - 1 \equiv -i + \frac{p-1}{2} \pmod{p-1} \end{aligned}$$



$$\begin{aligned}
&\iff \text{either } i - 1 = -i + \frac{3}{2}(p - 1) \\
&\iff i = \frac{3p - 1}{4} \quad \text{or} \quad i - 1 = -i + \frac{p - 1}{2} \\
&\iff i = \frac{p + 1}{4}.
\end{aligned} \tag{5.15}$$

As  $i$  is an integer, these equations can be satisfied if and only if  $p \equiv 3 \pmod{4}$ . Therefore, when  $p$  is of this form, we have two solutions, but when  $p \equiv 1 \pmod{4}$ , there are no solutions.  $\square$

**Theorem 5.8.** For a Golomb Costas array  $I$  of order  $n$ ,

$$\Psi_{I, R^2}(0, 0) = n \pmod{3}. \tag{5.16}$$

*Proof.* A Golomb Costas array of order  $n = q - 2$  has dots at positions  $(f(i), i)$ , where

$$\alpha^i + \beta^{f(i)} = 1, \quad i \in [q - 2] \tag{5.17}$$

for  $q = p^m$ ,  $p$  prime, integer  $m$ , and primitive elements  $\alpha$  and  $\beta$ . Its  $R^2$  rotation has dots at positions  $(q - 1 - f(j), q - 1 - j)$ ,  $j \in [p - 2]$ .

The value of the cross-correlation at the origin is the number of solutions of the simultaneous equations  $f(i) + f(j) = q - 1$  and  $i + j = q - 1$ . It follows that

$$\begin{aligned}
&\alpha^j + \beta^{f(j)} = 1, \quad f(j) = q - 1 - f(i), \quad j = q - 1 - i \\
&\implies \alpha^{q-1-i} + \beta^{q-1-f(i)} = 1 \\
&\iff \alpha^{-i} + \beta^{-f(i)} = 1 \\
&\iff \frac{1}{\alpha^i} + \frac{1}{\beta^{f(i)}} = 1 \\
&\iff \frac{\alpha^i + \beta^{f(i)}}{\alpha^i \beta^{f(i)}} = 1 \\
&\iff \frac{1}{\alpha^i \beta^{f(i)}} = 1.
\end{aligned} \tag{5.18}$$

We therefore end up with two simultaneous equations:

$$\begin{aligned}
&\alpha^i \beta^{f(i)} = 1, \quad \alpha^i + \beta^{f(i)} = 1 \\
&\iff (\alpha^i)^2 - \alpha^i + 1 = 0 \beta^{f(i)} = 1 - \alpha^i.
\end{aligned} \tag{5.19}$$

Setting  $x = \alpha^i$ , we obtain the quadratic

$$x^2 - x + 1 = 0. \quad (5.20)$$

Now we consider three cases.

(i)  $n \equiv 1 \pmod{3} \Leftrightarrow q \equiv 0 \pmod{3}$ :  $q$  is a power of 3, so (5.20) becomes

$$x^2 + 2x + 1 = 0 \iff (x + 1)^2 = 0 \iff x = -1. \quad (5.21)$$

Since only solution exists,  $\Psi_{L,R^2}(0,0) = 1$ .

(ii) Otherwise,  $x$  solves  $x^2 - x + 1 = 0$  if and only if  $-x$  solves  $x^2 + x + 1 = 0 \Leftrightarrow (x^3 - 1)/(x - 1) = 0 \Leftrightarrow x^3 = 1, x \neq 1$ . This has solutions in  $\mathbb{F}(q)$  if and only if  $3 \mid q - 1 \Leftrightarrow n \equiv 2 \pmod{3}$ :

(a)  $n \equiv 2 \pmod{3}$ : (5.20) has 2 roots in  $\mathbb{F}(q)$ .

(b)  $n \equiv 0 \pmod{3}$ : (5.20) has 0 roots in  $\mathbb{F}(q)$ .

□

## 6. Conclusion

Families of Costas arrays with low cross-correlation are useful in a multiuser setting, where the necessity for ideal autoambiguity for optimal RADAR/SONAR performance is combined with the need to minimize cross-interference between different users. We focused on the special case of the cross-correlation of two Costas arrays related by a horizontal and/or a vertical flip and considered both general Costas arrays and more specific algebraically constructed subfamilies.

On many occasions the cross-correlation was found to be low (2 or less), implying that for a small number of users it is possible to use flipped variants of the same array without significant interference. Our options increase further if we tie all users to a common clock, in which case the only cross-correlation value that becomes relevant is that at the origin.

For a larger number of users, larger families of Costas arrays need to be considered; we relegate this for future work. We have also collected empirical results regarding the cross-correlation of a Costas array with its image under rotation by  $\pm 90^\circ$ , or under transposition (and flips and/or rotations thereof), but so far we have been unable to find provable formulas for these results.

## Acknowledgments

The authors would like to thank John Russo and Svetislav Maric for bringing the result stated in Theorem 5.1 to their attention. They would also like to thank the anonymous reviewers for their thorough reviews, and their detailed and insightful comments. This material is based upon works supported by the Science Foundation Ireland under Grants no. 05/YI2/I677 and no. 08/RFP/MTH1164.

## References

- [1] J. P. Costas, "Medium constraints on sonar design and performance," Tech. Rep. Class 1 Rep. R65EMH33, General Electric Company, Fairfield, CT, USA, November 1965.

- [2] J. P. Costas, "A study of a class of detection waveforms having nearly ideal range—doppler ambiguity properties," *Proceedings of the IEEE*, vol. 72, no. 8, pp. 996–1009, 1984.
- [3] S. W. Golomb, "Algebraic constructions for Costas arrays," *Journal of Combinatorial Theory, Series A*, vol. 37, no. 1, pp. 13–21, 1984.
- [4] S. W. Golomb and H. Taylor, "Constructions and properties of Costas arrays," *Proceedings of the IEEE*, vol. 72, no. 9, pp. 1143–1163, 1984.
- [5] J. K. Beard, J. C. Russo, K. G. Erickson, M. C. Monteleone, and M. T. Wright, "Costas array generation and search methodology," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 43, no. 2, pp. 522–538, 2007.
- [6] K. Drakakis, S. Rickard, J. K. Beard, et al., "Results of the enumeration of Costas arrays of order 27," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4684–4687, 2008.
- [7] S. Rickard, E. Connell, F. Duignan, B. Ladendorf, and A. Wade, "The enumeration of Costas arrays of size 26," in *Proceedings of the 40th Annual Conference on Information Sciences and Systems (CISS '07)*, pp. 815–817, Princeton, NJ, USA, March 2007.
- [8] K. Drakakis, "A review of Costas arrays," *Journal of Applied Mathematics*, vol. 2006, Article ID 26385, 32 pages, 2006.
- [9] C. P. Brown, M. Cenkci, R. A. Games, J. J. Rushanan, and O. Moreno, "New enumeration results for Costas arrays," in *Proceedings of IEEE International Symposium on Information Theory*, p. 405, San Antonio, Tex, USA, January 1993.
- [10] L. O'Carroll, D. H. Davies, C. J. Symth, J. H. Dripps, and P. M. Grant, "A study of auto- and cross-ambiguity surface performance for discretely coded waveforms," *IEE Proceedings F: Radar and Signal Processing*, vol. 137, no. 5, pp. 362–370, 1990.
- [11] E. L. Titlebaum and S. V. Maric, "Multiuser sonar properties for Costas array frequency hop coded signals," in *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '90)*, vol. 5, pp. 2727–2730, Albuquerque, NM, USA, April 1990.
- [12] D. M. Drumheller and E. L. Titlebaum, "Cross-correlation properties of algebraically constructed Costas arrays," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 27, no. 1, pp. 2–10, 1991.
- [13] S. Rickard, *Large sets of frequency hopped waveforms with nearly ideal orthogonality properties*, M.S. thesis, MIT, Cambridge, Mass, USA, 1993.
- [14] T. Etzion, "Combinatorial designs derived from Costas arrays," in *Sequences: Combinatorics, Compression, Security, and Transmission*, pp. 208–227, Springer, New York, NY, USA, 1990.
- [15] A. Freedman and 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*, vol. 73, no. 10, pp. 1530–1531, 1985.