

Searching for Costas arrays using periodicity properties

Scott Rickard

Department of Electronic and Electrical Engineering
University College Dublin, Ireland
scott.rickard@ucd.ie

Abstract

Costas arrays are permutation matrices with ideal auto-ambiguity properties; No two of the the N choose 2 line segments between pairs of 1's in the matrix have the same slope and length. This paper presents a search technique based on the periodicity properties of the existing construction techniques which finds previously unknown Costas arrays for $N = 29$, $N = 36$, and $N = 42$. These are the first 'new' Costas arrays to be determined in nearly 20 years, excepting those found by exhaustive search for $N \leq 25$.

1 Introduction

In the 1960's, Dr. John P. Costas¹ was puzzled by the poor practical performance of sonar systems. He discovered that the rapidly time-varying channel made coherent processing inappropriate and set out to design a class of frequency-hopped waveforms and a hybrid receiver to fix the problem (Costas, 1965). His frequency-hopped waveforms had N time slots and N frequency bins and used one frequency pulse per time bin (for the noise limited case) and used all frequencies (for the clutter limited case). Most importantly, Costas was interested in waveforms with ideal thumbtack auto-ambiguity. Thus, he began searching for permutation matrices with ideal auto-ambiguity properties, that is, N -by- N arrays of dots and blanks satisfying (Costas, 1984):

1. There are N dots, one in each row and one in each column (the permutation matrix constraint), and
2. No two of the (N choose 2) line segments between pairs of dots have the same length and slope (the ideal auto-ambiguity constraint).

By hand, he found examples of such matrices of size up to $N = 12$. Unable to find one of size 13, he contacted Professor Solomon Golomb who then provided generation techniques based on the theory of finite fields for creating these matrices, dubbed *Costas arrays* (Golomb and Taylor, 1984).

The generation methods produce Costas arrays for infinitely many N , but not all N . For example, the techniques can be used to generate arrays for all $N \leq 31$, but no Costas array of size $N = 32$ or $N = 33$ has been found. Computer search has enumerated all Costas arrays of size $N \leq 25$, but the exponential growth of the search space prohibits extending these results much further with current computational capabilities. After nearly 40 years of research, the first question concerning Costas arrays remains open: Do Costas arrays exist for all N ?

Golomb conjectured in 1984 that the number of Costas arrays was monotonic increasing with N , a reasonable conjecture as the number of Costas arrays roughly doubles from N to $N + 1$ for $N = 1, \dots, 12$. Perhaps surprisingly, this conjecture was shown to be false by Silverman et al. (1988) by enumerating the number of Costas arrays up to $N \leq 17$ via computer search. There are 21104 Costas arrays of size 16-by-16, but only 18276 Costas arrays of size 17-by-17. In fact, the number of Costas arrays falls dramatically from its peak at $N = 16$, and a recent computer search has shown that there are only 88 Costas arrays of size 25-by-25 (Beard, 2004).

This paper presents a search technique based on the periodicity properties of the existing construction techniques which finds previously unknown Costas arrays for $N = 29$, $N = 36$, and $N = 42$. These are the first 'new' Costas arrays to be determined in nearly 20 years, excepting those found by exhaustive search for $N \leq 25$.

¹John Costas is famous for the invention of the Costas Loop in the 1950's.



Figure 1: Two 4-by-4 Costas arrays.

2 Costas Arrays

A Costas array can be defined:

Definition 1. An N -by- N array of dots and blanks which satisfies:

1. There are N dots, one in each row and one in each column.
2. The $\binom{N}{2}$ line segments between pairs of dots differ in length or slope.

There are many equivalent definitions, notably:

Definition 2. A permutation matrix \mathbf{A} with two-dimensional discrete auto-correlation function taking values N , 1, and 0. The two-dimensional discrete auto-correlation function can be calculated $C_{n,m} = \sum_{i=1}^{N-n} \sum_{j=1}^{N-m} A_{i,j} A_{i+n,j+m}$ where $n, m \in \{0, \dots, N\}$.

Definition 3. An ordering $\{a_1, a_2, \dots, a_N\}$ of the elements of the set $\{1, 2, \dots, N\}$ such that the difference triangle contains no repeated values on any given row. The j th row of the difference triangle contains the differences $a_{i+j} - a_i$ for all $i = 1, \dots, N - j$.

Definition 4. A permutation matrix \mathbf{A} such that if four distinct entries in the matrix $a_{i_1, j_1} = a_{i_2, j_2} = a_{i_3, j_3} = a_{i_4, j_4} = 1$, then $(i_2 - i_1, j_2 - j_1) \neq (i_4 - i_3, j_4 - j_3)$ and if three distinct entries in the matrix $a_{i_1, j_1} = a_{i_2, j_2} = a_{i_3, j_3} = 1$, then $(i_2 - i_1, j_2 - j_1) \neq (i_3 - i_1, j_3 - j_1)$.

Two example 4-by-4 Costas arrays are shown in Figure 1. In fact, all other 4-by-4 Costas arrays can be generated via rotations and reflections of the two arrays pictured in Figure 1.

Defining $C(N)$ to be the number of N -by- N Costas arrays, Golomb and Taylor (1984) conjectured that:

Conjecture 1 ((Golomb and Taylor, 1984)). $C(N) \geq 1$ for all N .

Conjecture 2 ((Golomb and Taylor, 1984)). $C(N)$ is monotonic increasing with N .

N	$C(N)$	N	$C(N)$
1	1	14	17252
2	2	15	19612
3	4	16	21104
4	12	17	18276
5	40	18	15096
6	116	19	10240
7	200	20	6464
8	444	21	3536
9	760	22	2052
10	2160	23	872
11	4368	24	200
12	7852	25	88
13	12828	26	?

Table 1: Enumeration search results: The number of Costas arrays $C(N)$ as a function of N .

Conjecture 2 seemed reasonable based on the results for $C(N)$ for $N \leq 12$ in Costas (1984). However, Silverman et al. (1988) extended the enumeration results to $N \leq 17$ and showed that the number of Costas arrays decreased from $N = 16$ to $N = 17$, demonstrating that Conjecture 2 was false. The enumeration results were extended to $N \leq 23$ by Moreno et al. (2002) and finally to $N \leq 25$ by Beard et al. (2004) and Beard (2004). A summary of the enumeration results to date are listed in Table 1.

The only two methods for systematically generating Costas arrays, aside from brute force search, are the Welch-Costas and Golomb-Costas methods, both of which are based on the theory of finite fields. We review briefly some of the main properties of finite (Galois) fields, and then describe the construction methods and some basic facts for Welch-Costas and Golomb-Costas arrays.

A finite field with q elements, $GF(q)$, exists iff $q = p^m$, where p is prime. For example, $GF(11) = \mathbb{Z}_{11}$, the integers modulo 11 under addition and multiplication. There exists at least one $\alpha \in GF(q)$ such that $\{\alpha^1, \alpha^2, \dots, \alpha^{q-1}\}$ runs through all non-zero elements of $GF(q)$. Such α are called primitive elements and satisfy $\alpha^x = \alpha^y$ in $GF(q)$ iff $x \equiv y \pmod{q-1}$. There are $\phi(q-1)$ distinct primitive elements in $GF(q)$ where $\phi(x)$ is Euler's totient function, the number of integers less than x relatively prime to x .

Definition 5 (Welch construction).

Given prime p and primitive element α , $\{\alpha^1, \alpha^2, \dots, \alpha^{p-1}\}$ is a length $N = p - 1$ Costas sequence.

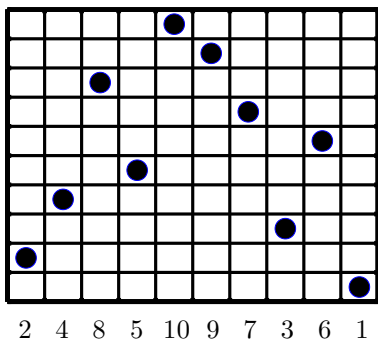


Figure 2: Welch-Costas array generated over $GF(11)$ with $\alpha = 2$.

For example, 2 is primitive in $GF(11)$. Therefore, $\{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}\} = \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$ is a Costas array; This array is shown in Figure 2. Circular shifts of Welch-Costas arrays are still Costas arrays (singly periodic). For example, 2 is primitive in $GF(5)$ leading to $2\ 4\ 3\ 1 \rightarrow 4\ 3\ 1\ 2 \rightarrow 3\ 1\ 2\ 4 \rightarrow 1\ 2\ 4\ 3$ all being Costas arrays.

Definition 6 (Golomb construction).

Given prime power $q = p^m$ and primitive elements $\alpha, \beta \in GF(q)$, $\{\log_\beta(1 - \alpha^1), \log_\beta(1 - \alpha^2), \dots, \log_\beta(1 - \alpha^{q-2})\}$ is a length $q - 2$ Costas sequence.

Here, \log over the finite field is defined: if $\beta^i = x$, then $\log_\beta x = i$. For example, using $q = 11, \alpha = \beta = 2$, and noting that: $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6$; we have $\log_2\{1 - 2^1, 1 - 2^2, 1 - 2^3, 1 - 2^4, 1 - 2^5, 1 - 2^6, 1 - 2^7, 1 - 2^8, 1 - 2^9\} = \log_2\{10, 8, 4, 7, 2, 3, 5, 9, 6\} = \{5, 3, 2, 7, 1, 8, 4, 6, 9\}$, which is a Costas array. Another way of stating the Golomb construction is: The $(q - 2)$ -by- $(q - 2)$ permutation matrix A with $a_{ij} = 1$ iff $\alpha^i + \beta^j = 1$ is a Costas array. When $\alpha = \beta$, the construction is due to Lempel and the generated matrix is symmetric (Golomb and Taylor, 1984).

Using the two generation techniques, Costas arrays of various orders can be constructed. By adding/removing corner dots (increasing/decreasing the size of the array by one) or adding/removing corner arrays, Costas arrays of all orders for $N \leq 100$ have been found except for $N = 32, 33, 43, 48, 49, 53, 54, 63, 73, 74, 83-85, 89-93, 97$ (Golomb and Taylor, 1984). Our goal is to fill these gaps.

3 Periodicity Properties

As was previously noted, the Welch-Costas arrays are singly periodic. That is, all circular shifts of the exponential sequences which generate the arrays are also Costas arrays. It is conjectured in Golomb and Taylor (1984) that single periodicity characterizes the Welch construction. The conjecture is still open but an illuminating discussion on the topic can be found in Golomb and Moreno (1996).

It has been proven that there exist no doubly periodic Costas arrays for $N > 2$ (Taylor, 1984). That is, there exists no N -by- N ($N > 2$) permutation matrix which when tiled horizontally and vertically so as to cover the entire plane has a Costas array in every N -by- N box.

However, it can be shown that both Welch-Costas and Golomb-Costas are 1-gap periodic in that if they are tiled vertically with an empty row in between adjacent arrays, every $(N + 1)$ -by- N box contains N dots which satisfy the auto-ambiguity constraint (point 2 from the definition of Costas arrays in the Introduction). Moreno et al. (2002) used this property to generate close-but-not-quite Costas arrays. We will use this property as a foundation for a constrained search for Costas arrays.

4 1-Gap Augmentation

The essential idea is to use the $(N + 1)$ -by- N box containing N dots which satisfy the auto-ambiguity constraint (from the 1-gap periodicity) as a starting point for a search. We try the two ways of adding a dot to fill the empty row and test the resulting $(N + 1)$ -by- $(N + 1)$ array to see if it is Costas. For example, starting with the Welch Costas array: 4 2 1 3. Aligning a 5-by-4 box with the top row of the array, we have the one gap array: 1 4 3 5. Filling in the missing row (2) to the left produces: 2 1 4 3 5, which, it turns out is not a Costas array. However, we can also try adding the missing row to the right which produces, 1 4 3 5 2, which it turns out is a Costas array. Of course, all possible vertical alignments of the box should be tested.

Adding one dot in this way for all Welch and Golomb Costas arrays with $N \leq 100$ produces 'new' arrays of sizes 29, 36, and 43. We define an array to be new if it has not been found by exhaustive search ($N > 25$) or by simply adding a corner dot (or dots) to a Welch or Golomb construction. The array of size 43 is pictured in Figure 3.

The technique can be generalized so as to attempt to augment the array by an arbitrary num-

method	p	N	Costas array
Welch	29	29	3 21 23 22 8 15 26 6 16 11 28 5 2 18 10 14 12 13 27 20 9 29 19 24 7 1 4 17 25
Welch	29	29	4 12 25 28 22 5 10 29 20 9 2 16 17 15 19 11 27 24 1 18 13 23 3 14 21 7 6 8 26
Golomb	37	36	2 29 33 19 21 27 32 9 1 30 17 36 16 23 14 12 24 5 31 6 26 15 18 28 22 7 25 3 11 20 8 4 35 34 13 10
Golomb	43	42	3 6 29 34 36 27 13 30 2 40 14 41 39 22 19 31 4 28 18 7 8 1 12 21 20 26 42 24 37 15 25 33 17 35 23 10 5 9 16 38 32 11

Table 2: New Costas arrays generated using the 1-gap augmentation technique. Two unique arrays were found for $N = 29$. In the $N = 36$ and $N = 42$ cases, one unique array was found. In each case, the array presented in the table is the 'minimal' array (the array from the eight in the dihedral symmetry group that come first lexicographically).

ber of dots. The $(N + 1)$ -by- N box containing N dots which satisfy the auto-ambiguity constraint serves as the starting point, and all possible ways off adding dots to fill the missing row and add rows and columns to the array to form a square array can be tested to see if the resulting permutation matrix is a Costas array. From the above example, starting with the one gap array 1 4 3 5, we would test the following to see which are Costas arrays:

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

Adding two dots or three dots in this way for all Welch and Golomb Costas arrays with $N \leq 100$ produces no new arrays. The two dot augmentation does produce Costas arrays of size 29 and 47, but these turn out to be Golomb Costas arrays of size 27 and 45 with two (opposite-corner) corner dots added. The three dot augmentation did not produce any new arrays. Table 2 contains a summary of the search results.

5 Conclusions

A search technique based on the 1-gap periodicity properties of the Welch and Golomb Costas array construction methods has been presented. The technique finds previously unknown Costas arrays for $N = 29$, $N = 36$, and $N = 42$, but fails to fill in any of the gaps for which no Costas arrays have been found.

References

- Beard, J. K. (2004). private communication.
- Beard, J. K., Russo, J. C., Erickson, K. G., Monteleone, M. C., and Wright, M. T. (2004). Combinatoric collaboration on Costas arrays and radar applications. In *IEEE Radar Conference*, Philadelphia, PA, USA.
- Costas, J. P. (1965). Medium constraints on sonar design and performance. Technical Report Class 1 Rep.

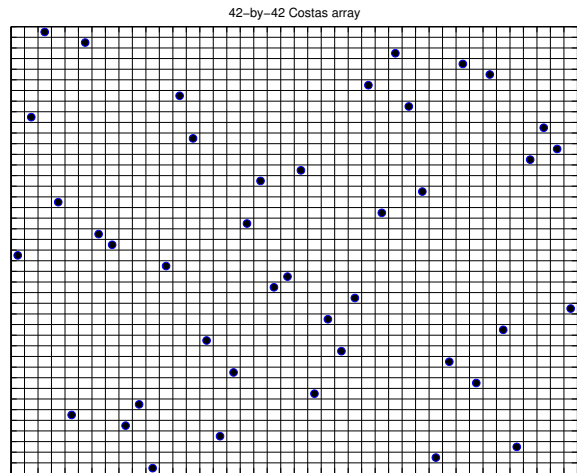


Figure 3: New Costas array generated from filling in the 1-gap shift of a Welch Costas array.

- R65EMH33, GE Co. A synopsis of this report appeared in the *Eascon. Conv. Rec.*, 1975, pp. 68A–68L.
- Costas, J. P. (1984). A study of detection waveforms having nearly ideal range-doppler ambiguity properties. *Proceedings of the IEEE*, 72(8):996–1009.
- Golomb, S. W. and Moreno, O. (1996). On periodicity properties of Costas arrays and a conjecture on permutation polynomials. *IEEE Transactions on Information Theory*, 42(6):2252–2253.
- Golomb, S. W. and Taylor, H. (1984). Constructions and properties of Costas arrays. *Proceedings of the IEEE*, 72(9):1143–1163.
- Moreno, O., Ramirez, J., Bollman, D., and Orozco, E. (2002). Faster backtracking algorithms for the generation of symmetry-invariant permutations. *Journal of Applied Mathematics*, 2(6):277–287.
- Silverman, J., Vickers, V. E., and Mooney, J. M. (1988). On the number of Costas arrays as a function of array size. *Proceedings of the IEEE*, 76(7):851–853.
- Taylor, H. (1984). Non-attacking rooks with distinct differences. Technical Report CSI-84-03-2, Univ. of Southern California.