Generating Costas Arrays to Order 200

James K. Beard, *Life Senior Member, IEEE*

***Abstract*—Number-theoretic generators of Costas arrays and generalizations in the literature and some presented here produce 526,908 of the known 663,703 known Costas arrays for orders up to 200. For orders higher than seven, there are more Costas arrays than the generators produce. A spin generalization is observed to find new Costas arrays for orders up to about 50, but none of higher order. This, and early work on the occurrence of Costas arrays, indicates that most, or all, Costas arrays are known, or are generated by known generators and their generalizations.**

***Index Terms*—Costas arrays, permutation matrices number theory, waveform design**

I. Introduction

COSTAS arrays are permutation matrices that satisfy an additional constraint: when a copy of the array is shifted by an integral number of rows and columns and overlaid on the original, no more than one "1" is superimposed on another "1". This is the Costas condition, and it makes these permutations ideal for use as frequency shift maps for sonar and radar waveforms [1] in uses where Doppler shifts equal or exceed the signal bandwidth because the ambiguity function achieved by such waveforms can approach the ideal "bed of nails" in which both range and Doppler sidelobes are an amplitude factor of N below the peak, where N is the order of the Costas array. Costas arrays are useful for frequency diversity spectrum broadening, for any communications waveforms that must achieve optimal adjacent channel rejection, and other applications such as digital watermarking in digital audio and images [2] [3]. Costas arrays are also used as a component in formulation of more complex high-performance radar waveforms [4].

Permutation matrices may be written as the sequence of the column indices in which the "1" appears in each sequential row, as in (4, 3, 1, 6, 7, 2, 5). When a Costas array (or any permutation matrix), considered as a matrix operator, is left-multiplied by a column vector whose elements are the row numbers, the resulting column vector is the column-index notation for that permutation matrix. We will use column-index notation here.

Costas arrays that are transposed, rotated, or reflected about the row or column indices produce other Costas arrays. These transformations result in sets of eight Costas arrays except in cases of symmetry about the main diagonal occurs, in which case the transformations produce sets of four. We consider any Costas array produced by such a transformation a polymorph of the other, and those that occur in sets of four as symmetrical Costas arrays.

Manuscript received January 2, 2006.

James K Beard is an independent consultant and adjunct professor for Temple University and Rowan University, (phone (609) 654-6559, e-mail jkbeard@ieee.org).

II. Generation of Costas Arrays

A. Classical Methods are Based on Finite Fields

There are three fundamental techniques known for generating Costas arrays, and several generalizations that add or subtract the first row and column when a "1" appears, or can appear, in (1,1) [5].

The number-theoretic generators are all based on the properties of finite fields [5]. These are Galois fields defined by integer arithmetic modulo a prime p or a vector extension, whose elements are vectors of k integers modulo p. We denote finite fields with the mathematical standard notation *GF(q)*, and each has q elements, and q is necessarily a prime or a power of a prime [6]. Every field has definitions of commutative and associative arithmetic operations of addition, subtraction, multiplication and division, and have an additive identity (zero) and a multiplicative identity (unity) element.

Galois fields are always characterized by *primitive elements*, sometimes called *primitive roots*. A primitive element α is characterized by the property that powers of α from zero to *q-2* steps through all the elements of *GF(q)* except the zero element, and thus represents a permutation of the sequence *{0, 1…q-1}*. Any element β of *GF(q)* has the property

$$\beta^{q-1} = 1 . \tag{2.1}$$

This is a special case of Euler's theorem. The minimum power of an element that is equal to one is the order of that element. Equation (2.1) shows that the order of every element must divide *q-1*. Elements that are of order *q-1* are the primitive elements.

The first and simplest generator is the Welch generator [5],

$$c_i + 1 = \alpha^{i+r} \bmod q \tag{2.2}$$

where here, q must be prime (i.e., a vector extension is not allowed because the left-hand side is an integer mod q). This generator produces Costas arrays of order q-1 and has the interesting property that it holds for any value of row offset r. This means that a periodic sequence of rows is produced. Every square matrix in this strip is a Costas array, so that *q-1* Costas arrays are produced by each Welch construction. The unending sequence of rows is a singly-periodic Costas array,

and all known singly-periodic Costas arrays are produced by a Welch generator [7]. The Lempel and Golomb generators [5]

$$\alpha^{i+1} + \beta^{c_i+1} = 1 \text{ in } GF(q). \quad (2.3)$$

Here, both α and β must be primitive elements. When $\alpha = \beta$, this is the Lempel generator, and when α and β are distinct this is the Golomb generator. The Lempel generator produces symmetrical Costas arrays. The Lempel-Golomb generators produce Costas arrays of order *q-2*.

Herbert Taylor has joined Lempel, Golomb, and Welch in generalizing these base generators by adding and subtracting "corner dots" or the first or last row and column when elements (1,1), (N,N), (1,N) or (N,1) have a one, or can be added while maintaining the Costas property of the augmented matrix [5]. These generators and extensions are summarized below as TABLE I.

TABLE I
NUMBER-THEORETIC GENERATORS AND EXTENSIONS FROM [5]

Generator	Remarks
Welch 0	Welch 1, add a corner dot
Welch 1	$c_i + 1 = \alpha^{i+r} \bmod q = p$, base method
Welch 2	$(1,1)$ removed
Welch 3	$(1,1)$ and $(2,2)$ removed
Taylor 0	Lempel-Golomb 2, add two corner dots
Taylor 1	Lempel-Golomb 2, add a corner dot
Lempel-Golomb 2	$\alpha^{i+1} + \beta^{c_i+1} = 1$, base method
Lempel-Golomb 3	L-G 2, $(1,1)$ removed
Lempel-Golomb 4	$(1,1)$, $(2,2)$ removed; $q = 2^k$
Taylor 4	Lempel 2, $(1,2)$ and $(2,1)$ removed
Golomb* 4	$(1,1)$, $(2,q-2)$ removed; $\alpha + \beta = 1$
Golomb* 5	Golomb* 4, $(q-2,2)$ removed
Imh. Sing. 1	L-G generalization; see [10]
Imh. Sing. S 1	L-G generalization; see [10]
Rickard Welch 0	Welch generalization; see [8]
Rickard L-G 1	L-G generalization; see [8]

B. The Base Number-Theoretic Generators Over-Constrain their Results

The *difference matrix* is a device used in many analyses of Costas arrays. This is a triangular matrix of differences between column indices of a permutation matrix. Denoting the column indices as c_i, entry at row s and column i of the difference matrix is

$$d_{s,i} = c_{i+s} - c_i. \quad (2.4)$$

For a permutation matrix of order *N,* the difference matrix has *N-1* rows, and row *s* has *N-s* elements. A condition on the difference matrix that is equivalent to the Costas property is that no row have two elements with the same value.

For the Welch generator, elements of the difference matrix are given by

$$d_{s,i} = \alpha^{i+r} \cdot (\alpha^s - 1) \bmod q. \quad (2.5)$$

The differences are seen to be unique mod *q*, which is a stronger condition than uniqueness. For the Lempel-Golomb generator, the entries in the difference matrix are given by

$$\beta^{d_{s,i}} = 1 - (1 - \alpha^s) \cdot (1 - \alpha^{-i-1}) \quad (2.6)$$

which shows that the entries in the difference matrix are unique modulo *q-1*.

C. The Base Generators are Doubly-Periodic

The Welch generator as given in (2.2) is periodic in the row with period *q-1* as we have already discussed. Since the generator equation is modulo *q*, the columns are periodic with period *q*. However, column indices that are *q-1* modulo *q* are not allowed or "forbidden" because there is no power of any element of a finite field that yields the zero element.

The Lempel-Golomb generator as given in (2.3) is periodic in both row and column indices with period *q-1*, but both rows and columns that are equal to *q-1* modulo q are forbidden because the respective power of the principal element would yield the unity element and force the power of the other principal element to the zero element; again, there is no power of any element that is the zero element.

D. Recent Generalizations Produce New Costas Arrays

Rickard [8] recently presented a focused search that adds dots in the forbidden rows of products of the Lempel-Golomb construction. This method has been shown to produce a few Costas arrays that are not otherwise found.

The current author and collaborators [9] recently showed that adding dots at the intersection of the forbidden rows and columns of products of the Lempel-Golomb construction also produces a few Costas arrays not otherwise found.

E. Other Extensions Are Presented Here

The present author implemented all of the methods in [5] as a general utility a few years ago. Additional generalizations, based on those given in [5], included trying adding and subtracting dots for all available Costas arrays of adjacent order, and a "spin" generalization. The spin generalization is implemented by rotating the products of the base and extended generators end-around in rows and columns and checking for the Costas condition. This has produced a large number of Costas arrays not otherwise found. These generalizations include, but are not limited to, the following:

- The recent additions to the generalizations mentioned in II.D above.
- Spin-add; Costas arrays of order *N-1* are spun and a dot is added at (1,1).
- Spin-drop; each dot is rotated to the (1,1) position and dropped.
- Spin-add 2; Costas arrays of order *N-2* are spun and dots are added at (1,1) and (N,N), and at (N,1) and (1,N).
- Spin-drop 2; each dot is rotated to the (1,1)

position and, if a dot is present at (N+2,N+2) then both are dropped; the corresponding operation is used to drop dots at (N+2,1) and (1,N+2).

This is personal working software. Methods are added and dropped occasionally for the purposes of experimentation. As such, the extensions presented here cannot be presented as a full set, and others may be added at any time.

III. Results

The program has been run recently for orders 2 through 200. The program, configured for using the spin generalization, produces 526,907 Costas arrays for the generalizations implemented at the time of that run. The result is shown below as Figure 1.

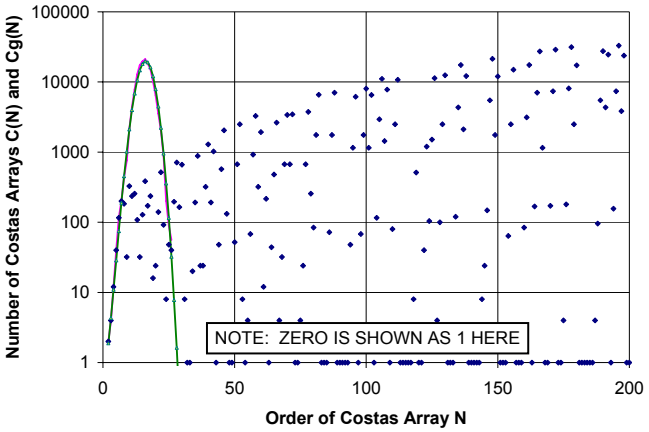

Figure 1. Numbers of Costas Arrays from Generators

The solid curve in the figure is the expected value of the number all existing Costas arrays of a given order *C(N)* from [9], but with updates for values of *C(N)* not known when [5] was written. Included are updates for orders 24 and 25 (200 and 88, respectively). The author and collaborators completed a search over order 27 in February 2005 [10] and 56 were discovered, however that value of *C(N)* does not fit the curve and was not used in the fit.

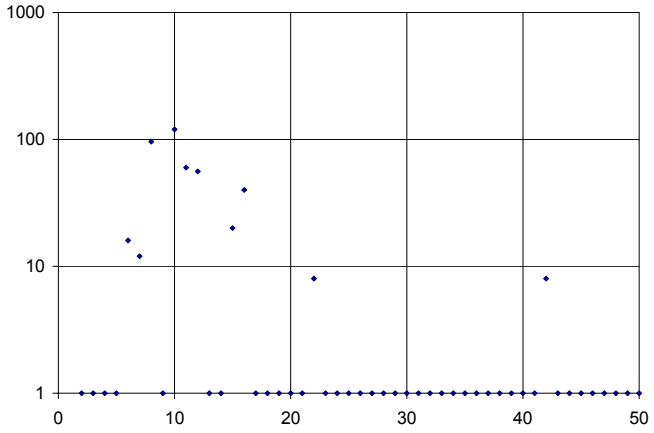

Figure 2. Additional Costas Arrays Produced by Spin

The spin generalization produces 436 Costas arrays for small and moderate orders. The number of additional Costas arrays versus order is shown as Figure 2.

The significant result is that none are produced for orders greater than 50. This is consistent with the fact that the extensions presented in [8], [10], and the spin generalizations are focused searches. These focused searches differ from exhaustive search methods in that they search over areas related to existing Costas arrays or constructs closely related to the number-theoretic generators presented in [5]. The probabilistic analysis given in [9] predicts that the likelihood of a Costas array not related to a number-theoretic generator decreases to vanishingly small levels as the order increases past about 30. Our fit of the estimation equation given in [9] predicts about 32 Costas arrays of order 26, while the generators give us 40 and 56 have been found [10]. It appears that the likelihood of Costas arrays existing that are not found by the methods and generalizations given here decreases as the order increases.

Only eight of the 436 Costas arrays found by the spin generalization but not by the classical methods and simpler generalizations is of order greater than 26, an asymmetrical Costas array of order 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) and its seven polymorphs.

A long-standing question of interest in the community is the existence of Costas arrays of order 32 and 33. The fact that the spin generalization finds one of order 42 that is not otherwise found shows that the likelihood of new Costas arrays being found by looking at areas suggested by existing methods does not become vanishingly small at orders 32 and 33. As such, we have proven here only that the issue remains open. As a matter of likelihood, however, we note that the spin generalizations don't produce very many Costas arrays from Taylor and extended Golomb 4 and Golomb 5 generalizations, and amount to moving the window around in the doubly-periodic arrays produced by the number-theoretic generators, a probabilistic fertile field that is not available for orders 32 and 33.

References

[1] John 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, August 1984..

[2] M. F. Bocko, "Data Hiding In Digital Audio Files," *IEEE Signal Processing Socitity*, Rochester chapter, March 5, 2003..

[3] Andrew Z. Tirkel, Ron G. van Schyndel, C. F. Osborne, "A Two-Dimensional Digital Watermark," *DICTA'95*, University of Queensland, Brisbane, December 5-8, 1995, pp. 378-383.

[4] Nadav Levanon and Eli Mozenson, "Orthogonal Train Of Modified Costas Pulses," *Proceedings of the IEEE 2004 Radar Conference*, April 26-29, 2004, ISBN 0-7803-8234-X, pp. 255-259.

[5] Solomon W. Golomb and Herbert Taylor, "Constructions and Properties Of Costas Arrays," *Proceedings of the IEEE Vol. 72 No. 9, pp. 1143-2263, September 1984.*.

[6] Ian Stewart, *Galois Theory*, Second Edition, Chapman & Hall/CRC (1989), ISBN 0-412-34550-1, Theorem 16.4 on p. 157.

[7] Herbert Taylor, "Singly periodic Costas arrays are equivlanet to polygonal path Vatican squares," in *Mathematical Properties of Seuences and Other Combinatorial Structures,*, Jong-Seon No, Hong-Yeop Song, Tor Helleseth, and P. Vijay Kumar, Eds., Kluwer (2003), ISBN 1-4020-7403-4, p. 45.

[8] Scott Rickard, "Searching for Costas Arrays Using Periodicity Properties," *IMA International Conference on Mathematics in Signal Processing*, the Royal Agricultural College, Cirencester UK, December 2004.

[9] J. Silverman, V. E. Vickers, and J. M. Mooney, "On the Number of Costas Arrays as a Function of Array Size," *Proceedings of the IEEE*, July 1988, pp. 851-853.

[10] J. K. Beard, J. C. Russo, M. Monteleone, and M. Wright, "Costas Array Generation and Search Methodology," to appear in *IEEE Transactions on Aerospace and Electronic Systems*.

James K. Beard (M'64–LM'04-LSM'05) became a Member (M) of IEEE in 1964, a Life Member (LM) in 2004, and a Life Senior Member in 2005. He was born in Austin, TX in 1939. He received a BS degree from the University of Texas at Austin in 1962, an MS from the University of Pittsburgh in 1963, and the Ph. D. from the University of Texas at Austin in 1968, all in electrical engineering.

Between 1959 and 2004, he worked in Government laboratories, industry, and as an individual consultant. Employers include precursors or current divisions of Northrop Grumman, Raytheon, and Lockheed Martin, most recently Lockheed Martin MS2 in Moorestown, NJ. He is currently an individual consultant based in Medford, NJ near Philadelphia. He is the author of a number of symposia papers and a book, "The FFT in the 21st Century" (Kluwer, 2003). Current research interests include system engineering solutions to homeland defense issues, estimation and decision theory, radar and communications concept and waveform design, and digital radar concepts. He is an adjunct professor at Temple University in Philadelphia and teaches graduate and undergraduate analog and digital communications.

Dr. Beard is a member of AIAA, AOC, SPIE and ACM. He was Publications Chairman for FUSION2005. He is a member of Phi Eta Sigma, Eta Kappa Nu, Tau Beta Pi, and Sigma Xi. He studied for his Ph. D. under a GSRF Fellowship (matched U. Texas Austin and Ford Foundation funding, administered by U. Texas Austin) and a NSF Fellowship.