

The Status of Costas Array Construction

Solomon W. Golomb
Department of Electrical Engineering
University of Southern California
Los Angeles, CA 90089-2565
Email: milly@usc.edu
Telephone: (213) 740-7333
Fax: (213) 740-8729

Abstract—To date, two approaches have been followed to identify Costas arrays. One has been exhaustive search, by computer, to find all $n \times n$ Costas arrays, which has currently been completed for $n \leq 26$. [1] [2] [3]. The other has been the discovery of specific constructions which provide examples of Costas arrays for many different values of n [4] [5] [6]. All the specific construction methods which have been found are related to primitive roots in finite fields, or involve the opportunistic adjoining of an extra “dot”, usually at a corner, to go from an example of size n to one of size $n + 1$. For many years, $n = 32$ and $n = 33$ have been the smallest values for which no Costas arrays are known [4]. The last publication that described new specific constructions appeared in 1992 [6]. If there are as yet undiscovered specific constructions, one possible way to identify them may be to look at examples found by exhaustive computer search that do not arise from any of the known constructions, and attempt to identify patterns in their formation.

keywords: Costas arrays, systematic constructions, primitive roots

I. KNOWN SYSTEMATIC CONSTRUCTIONS

A. The Welch Construction

For every prime $p > 2$, let g be any one of the $\phi(p - 1)$ primitive roots mod p , where ϕ is Euler’s phi-function. Then the pairs (j, g^j) for $1 \leq j \leq p - 1$ are the coordinates of the points in an order $(p - 1)$ Costas array.

Since $(p - 1, g^{p-1}) = (p - 1, 1)$ is a “corner dot” of the foregoing Costas array, the row and column of this corner dot can be removed to obtain an order $(p - 2)$ Costas array. Finally, if $g = 2$ is primitive mod p , which is believed (by Artin’s conjecture) to occur for a positive percentage of all prime numbers, $(1, 2)$ becomes a corner dot after the removal of the row and column of $(p - 1, 1)$, which may be removed (along with its row and column) to obtain an order $(p - 3)$ Costas array.

B. The Lempel Construction

For every finite field of $q > 2$ elements (where $q = p^k$, for all primes p and all positive integers k , such that $q > 2$), let α be any one of the $\phi(q - 1)$ primitive elements (i.e. generators of the multiplicative group) of $GF(q)$. Then the pairs (i, j) with $1 \leq i, j \leq q - 2$ such that $\alpha^i + \alpha^j = 1$ are the coordinates of the points in an order $(q - 2)$ Costas array. (Note that this Costas array is symmetric relative to the $i = j$ diagonal.)

When $q = p > 2$ is a prime, with the primitive root $\alpha = 2$, then $(i, j) = (q - 2, q - 2)$ is a corner dot which (together with its row and column) can be removed to give an order $(p - 3)$ Costas array, which is still symmetric relative to the $i = j$ diagonal. It is therefore distinct from the order $(p - 3)$ Costas array obtained from the Welch construction for the same prime p with primitive root 2.

C. The Golomb Construction

This is a generalization of the Lempel construction. Let α and β be any two primitive elements in the field $GF(q)$, and use the pairs (i, j) with $1 \leq i, j \leq q - 2$ as the coordinates of points in a Costas array whenever $\alpha^i + \beta^j = 1$. This gives an order $(q - 2)$ Costas array for all $q > 2$, which is the Lempel construction if and only if $\alpha = \beta$. (It is a rotation of the Lempel construction if $\alpha = \beta^{-1}$.) In general it is not symmetric.

By a theorem of O. Moreno et al. [7], proving a conjecture of Golomb [5], for every $q > 2$ it is possible to find primitive elements α and β in $GF(q)$ such that $\alpha + \beta = 1$. (Here α and β are not necessarily distinct.) In the Golomb construction, this yields an order $(q - 2)$ Costas array with $(1, 1)$ as a corner dot. Removing this corner dot, with its row and column, produces an order $(q - 3)$ Costas array for every $q > 2$ where $q = p^k$, p prime and $k \geq 1$. In the special case $q = 2^k$, $k > 1$, from $\alpha + \beta = 1$ we also have $\alpha^2 + \beta^2 = 1$, so that $(2, 2)$ is also a point of the Costas array, which becomes a corner dot after $(1, 1)$, together with its row and column, is removed. When also $(2, 2)$, along with its row and column, is removed, a Costas array of order $(2^k - 4)$ results.

Proofs of the validity of the Welch, Lempel, and Golomb constructions are given in [5].

D. Taylor’s T_4 Construction

If, in the field $GF(q)$, there is a primitive element α with $\alpha + \alpha^2 = 1$, then in the Lempel construction both $(1, 2)$ and $(2, 1)$ are points of the Costas array of order $q - 2$. Removing the two rows, and two columns, containing $(1, 2)$ and $(2, 1)$, an order $(q - 4)$ Costas array results.

In [6] it is shown that this situation arises for $q = 4$, $q = 5$, $q = 9$, and for those prime values of $q = p \equiv \pm 1 \pmod{10}$

where at least one of the roots of $x^2 + x - 1$ is a primitive root modulo p .

Note that $\alpha + \beta^2 = 1$, $\alpha^2 + \beta = 1$, with $\alpha \neq \beta$ leads to $\alpha - \beta = \alpha^2 - \beta^2$, $1 = \alpha + \beta$, hence $\alpha = \alpha^2$ and $\beta = \beta^2$, so α and β cannot be primitive modulo p for any prime p . (This rules out a possible generalization of the T_4 construction.)

E. The G_4 and G_5 Constructions

In the field $GF(q)$, if there are two primitive roots α and β with $\alpha + \beta = 1$ and $\alpha^2 + \beta^{-1} = 1$, then also $\alpha^{-1} + \beta^2 = 1$, as shown in [6]. When this occurs, using the Golomb construction, since $\alpha^1 + \beta^1 = 1$, $(1, 1)$ is a corner dot which can be removed (together with its row and column), so that $(2, -1) = (2, q - 2)$ becomes a corner dot which can be similarly removed. Also, $(-1, 2) = (q - 2, 2)$ is now a corner dot, which can also be similarly removed. This process yields Costas arrays of successive orders $q - 2$, $q - 3$, $q - 4$ and $q - 5$. The values of q for which this construction occurs are $q = 4$, $q = 5$, $q = 9$, and those primes p for which the T_4 construction occurs which satisfy either $p \equiv 1 \pmod{20}$ or $p \equiv 9 \pmod{20}$, as shown in [6].

F. A Construction of Very Limited Use

Another possible way to go from $n = q - 2$ successively to $n = q - 3$ and $n = q - 4$, for $n \times n$ Costas arrays, is to find two primitive roots α and β in $GF(q)$ where both $\alpha + \beta = 1$ and $\alpha^{-1} + \beta^{-1} = 1$, which would give dots at the diametrically opposite corners $(1, 1)$ and $(-1, -1) = (q - 2, q - 2)$. This actually occurs for $q = 7$, with $\alpha = 3$ and $\beta = 5$. (Here $\alpha^{-1} = 5$ and $\beta^{-1} = 3$, so that $\alpha + \beta \equiv \alpha^{-1} + \beta^{-1} \equiv 1 \pmod{7}$). However, this cannot work for any $q > 7$ for the following reason. From $\alpha + \beta = 1$ and $\alpha^{-1} + \beta^{-1} = 1$, we have $\beta = 1 - \alpha$, $\alpha^{-1} + (1 - \alpha)^{-1} = 1$, $\alpha^{-1}(1 - \alpha) + 1 = 1 - \alpha$, $\alpha^{-1} = 1 - \alpha$, and $\alpha^2 - \alpha + 1 = 0$. Thus α is a root of $x^2 - x + 1$, which is a factor of $x^6 - 1$, so that $\alpha^6 = 1$. Given that α must be primitive, $q - 1 \leq 6$ and $q \leq 7$.

Essentially the same argument shows that if two primitive elements α and β in $GF(q)$ satisfy both $\alpha + \beta^{-1} = 1$ and $\alpha^{-1} + \beta = 1$ giving corner dots at $(1, q - 2)$ and $(q - 2, 1)$, then again $\alpha^2 - \alpha + 1 = 0$, $\alpha^6 = 1$, and α cannot be primitive for $q > 7$.

II. ON THE ABUNDANCE OF COSTAS ARRAYS

A. Do Costas Arrays Become Extinct?

In [8], Silverman et al. presented a probabilistic argument to suggest that $C(n)$, the number of $n \times n$ Costas arrays, should go to 0 for large n . Indeed, as seen in the table of values of $C(n)$ for $2 \leq n \leq 26$ ([9], p. 417), the value of $C(n)$ increases monotonically from $C(2) = 2$ to $C(16) = 21,104$, beyond which it decreases monotonically down to $C(26) = 56$. The reduced number, $c(n)$, of $n \times n$ Costas arrays when patterns which differ only by symmetries of the square are not considered distinct, exhibits similar behavior, from $C(2) = 1$ up to $c(16) = 2,648$ and then down to $c(26) = 8$. However, from Section 1, we know that there are systematic

constructions for $n \times n$ Costas arrays for arbitrarily large values of n , since the sequence of the prime numbers is infinite. The pessimistic assumption would be that for large n , only the examples obtained from these known constructions exist. By this reasoning, quite possibly $C(32) = C(33) = 0$.

B. $\limsup C(n) = \infty$ as $n \rightarrow \infty$

While it is possible, as just discussed, that $\liminf C(n) = 0$ as $n \rightarrow \infty$, it is provable that $\limsup C(n) = \infty$ as $n \rightarrow \infty$. Specifically, using only the Welch construction when $n = p - 1$, where p is prime, there are $\phi(p - 1)$ different primitive roots mod p , so that $C(p - 1) \geq \phi(p - 1)$ for every prime p . It is well-known (see [10]) that $\phi(m) > m^{1-\epsilon}$ for all $m > m_0(\epsilon)$. Hence the value of $C(n)$ becomes arbitrarily large as n takes the successive values $p_j - 1$, where p_j is the j^{th} prime number.

C. Specific Large Values of $C(n)$

At $p = 65,537 = 2^{16} + 1$, the largest known Fermat prime, we have $p - 1 = 2^{16}$ and $\phi(p - 1) = 2^{15}$. Thus, from the Welch construction alone, $C(2^{16}) \geq 2^{15} = 32,768$, an even larger number than $C(16) = 21,104$. However, we can find a much bigger lower bound for $C(2^{16} - 1) = C(65,535)$. Specifically, there are still 2^{15} Costas arrays from the Welch construction at $p - 2$. In addition, from the Lempel and Golomb constructions, the number of ways to pick two primitive roots α and β , not necessarily distinct, from the set of 2^{15} such roots, is $\binom{2^{15} + 1}{2} = 2^{14}(2^{15} + 1) = 536,887,296$, a lower bound for $C(65,535)$. As large as this number seems, it is microscopic in comparison with $65,535!$, the total number of permutation matrices of order $n = 65,535$.

D. General Large Values of $C(n)$

As already observed, since there are infinitely many primes, we can get $C(n) > x$ for any preassigned value of x by finding a prime p with $\phi(p - 1) > x$, and using the Welch construction for $n = p - 1$.

It is widely believed, though not yet proved, that there are infinitely many *twin primes*, integers p and $r = p + 2$ that are both prime. Using the Golomb construction on the $\phi(r - 1)$ primitive roots modulo r to get order $r - 3 = p - 1$ Costas arrays, these will be distinct from the $\phi(p - 1)$ Welch constructions for order $p - 1$ Costas arrays. (The combined number depends on the number of pairs of primitive roots α and β , modulo r , with $\alpha + \beta = 1$.)

Generally, the largest contribution to $C(n)$ from systematic constructions occurs when $n = q - 2$ (where q is any power of any prime) using the Golomb construction with any two primitive roots α and β from the multiplicative group of $GF(q)$.

III. SEARCHING FOR OTHER SYSTEMATIC CONSTRUCTIONS

A. One Specific Possibility

The pairs (a, a^2) modulo p , for $1 \leq a \leq \frac{p-1}{2}$, for all primes $p > 2$, have the property that when plotted on a

