THE DEFICIENCY OF COSTAS ARRAYS

JONATHAN JEDWAB AND JANE WODLINGER

Abstract. A Costas array is a permutation array in which the vectors joining pairs of 1s are all distinct. The toroidal vectors of a permutation array are the vectors occurring when the array is written on a torus, and the deficiency of a permutation array of order n is the number of toroidal vectors, out of the $(n-1)^2$ possible, that are missing from the array. The smallest deficiency among all permutation arrays of order $q-1$, where q is a power of a prime other than 3, is known, and it is of interest to find examples of permutation arrays attaining this minimum value. The deficiency of Costas arrays is studied computationally and theoretically. It is shown that all Welch Costas arrays of a given order have the same deficiency. It is shown that the deficiency of Golomb-Rickard Costas arrays of order $q-1$ attains the minimum value over all permutation arrays when q is a power of a prime other than 3. Computational experiments show that the deficiency distribution of Costas arrays of a given order acts as a filter that highlights the Welch Costas arrays, isolates the Golomb-Rickard Costas arrays, and gives further insights into the structure of other Costas arrays. In particular, four Costas arrays with exceptionally small deficiency are recognised, and it is asked if they could be used to identify a new algebraic construction for Costas arrays.

1. Introduction

Costas arrays were introduced in 1965 by J. P. Costas as a means of improving the performance of radar and sonar systems [3].

Definition 1.1. *A permutation array A of order n is a* Costas array *if the vectors formed by joining pairs of* 1*s in A are all distinct.*

For example, the array in Figure 1 (in which dots represent 1s and blanks represent 0s) is a Costas array of order 6. In Costas's original application, the radar or sonar frequency f_i is transmitted in time interval t_j if and only if position (i, j) of the Costas array contains a 1.

Date: 30 August 2012 (revised 13 September 2014).

J. Jedwab is with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC V5A 1S6, Canada. J. Wodlinger is with Department of Mathematics and Statistics, University of Victoria, 3800 Finnerty Road, Victoria BC V8P 5C2, Canada.

Email: jed@sfu.ca, jw@uvic.ca.

J. Jedwab is supported by an NSERC Discovery Grant. J. Wodlinger was supported by an NSERC Canada Graduate Scholarship.

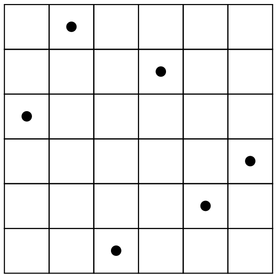


FIGURE 1. A Costas array of order 6

We use the standard labelling convention for arrays (first index downwards, second index rightwards, both indices start from 1). It is sufficient to consider only one of the vectors joining each pair of 1s in a Costas array; by convention, we choose the vector pointing rightwards. We follow other authors in also using the conflicting labelling convention for vectors (first component horizontal, second component vertical), leading to Definition 1.2.

Definition 1.2. *The vector between '1' entries $A_{i,j}$ and $A_{k,\ell}$ of a permutation array $(A_{i,j})$, where $j < \ell$, is $(\ell - j, k - i)$.*

(As a consequence of Definition 1.2, the positive direction for the second component of the vector is downwards.)

A Costas array $(A_{i,j})$ corresponds to a permutation $\alpha \in \mathcal{S}_n$, using the convention that $A_{i,j} = 1$ if and only if $\alpha(j) = i$. For example, the Costas array of Figure 1 corresponds to the permutation $\alpha = [3, 1, 6, 2, 5, 4]$. Each Costas array A belongs to an equivalence class formed by its orbit under the action of the dihedral group D_4. The equivalence class of a Costas array of order greater than 2 has size four or eight, depending on whether its elements have reflective symmetry about a diagonal.

Early research on Costas arrays led to two main algebraic construction techniques, known as the *Welch construction* and the *Golomb construction*. Both of these constructions make use of primitive elements of the finite field $\mathbb{F}_q$, and generate Costas arrays for infinitely many orders. The Welch construction was presented by L.R. Welch in 1982, but it has recently been recognised [15] that it was discovered by Gilbert [7] in 1965; as a result, Gilbert is now considered the co-inventor of Costas arrays.

Theorem 1.3 (Welch Construction $W_1(p, \phi, c)$ [7]). *Let ϕ be a primitive element of $\mathbb{F}_p$, where p is a prime, and let c be a constant. Then the permutation array $(A_{i,j})$ of order $p - 1$ with*

$$A_{i,j} = 1 \quad \text{\textit{if and only if}} \quad \phi^{j+c-1} \equiv i \pmod{p}$$

is a Costas array.

Varying the parameter c in the range $0, \dots, p-2$ corresponds to cyclically shifting the columns of A. Consequently, every $W_1(p, \phi, c)$ Welch Costas array is singly periodic: if copies of the array are placed side-by-side to form a horizontal tiling, any $p-1$ consecutive columns form a Welch Costas array.

Theorem 1.4 (Golomb construction $G_2(q, \phi, \rho)$ [8])**.** *Let ϕ and ρ be (not necessarily distinct) primitive elements of $\mathbb{F}_q$, where q is a power of a prime. Then the permutation array $(A_{i,j})$ of order $q-2$ for which*

$$A_{i,j} = 1 \quad \textit{if and only if} \quad \phi^i + \rho^j = 1$$

is a Costas array.

In addition to the algebraic constructions, there are a number of secondary construction procedures which involve modifying a known Costas array in a way that preserves the Costas property, where possible, to produce an inequivalent Costas array. Many of these procedures can be systematically applied to certain Welch or Golomb Costas arrays and are guaranteed to produce a Costas array. In other cases there is no guarantee, and one must test whether the resulting array has the Costas property. These variants are summarised in [16] and discussed in detail in [3]. We shall be interested in the Golomb-Rickard variant [14] of the Golomb construction, in which a Golomb Costas array of order $q-2$ is augmented by the inclusion of an additional lowermost row of 0s and an additional rightmost column of 0s, and the entry at the intersection of the additional row and column is set to 1. This variant construction succeeds if one or more of the cyclic row/column permutations of the resulting $(q-1) \times (q-1)$ array has the Costas property.

Costas arrays have been enumerated up to order 29 by exhaustive computer search [6]. The vast majority of these Costas arrays are not explained by any of the known construction techniques. There is no value of n for which a Costas array of order n is known not to exist; the smallest values of n for which existence is currently open are 32 and 33. Comprehensive databases of Costas arrays have been published by Beard [1] and by Rickard [13].

In this paper, we analyse the vectors joining pairs of 1s in Costas arrays when the vectors are allowed to “wrap around” both horizontally and vertically (or, equivalently, when the arrays are viewed as being written on the surface of a torus).

Definition 1.5. *Let $(A_{i,j})$ be an $m \times n$ array of* 0*s and* 1*s. The* toroidal vector *from ‘*1*’ entry $A_{i,j}$ to ‘*1*’ entry $A_{k,\ell}$ is $((\ell - j) \bmod n, (k-i) \bmod m)$.*

Each pair of 1s in a permutation array is joined by two (possibly identical) toroidal vectors, each having both components positive. For example, the 1s at positions $(3,1)$ and $(2,4)$ in the Costas array shown in Figure 1 are separated by the toroidal vector $(3,5)$ and by the toroidal vector $(3,1)$.

A permutation array of order n contains $2\binom{n}{2} = n(n-1)$ toroidal vectors drawn from the set $\{1, \ldots, n-1\}^2$. Therefore every nontrivial permutation array contains $n-1$ repeated toroidal vectors (counting multiplicity). This prompts the natural questions: are there permutation arrays of order $n > 2$ containing every possible toroidal vector $(w, h) \in \{1, \ldots, n-1\}^2$, and if not then how few of the $(n-1)^2$ possible values (w,h) can be missing? These questions were addressed by Panario, Stevens and Wang [12] (the answer to the first question being *no*), and we summarise their findings in Theorem 1.7. We present a proof of this theorem which is inspired by that of [12], but which is more visual.

Definition 1.6. *Let A be a permutation array of order n. The* deficiency *of A is the number $D(A)$ of toroidal vectors in $\{1,\dots,n-1\}^2$ missing from A.*

Theorem 1.7 ([12, Theorem 1])**.** *Let A be a permutation array of order $n>2$. Then*

$$D(A) \geq \begin{cases} n-1 & \text{for } n \text{ odd} \\ n-3 & \text{for } n \text{ even.} \end{cases}$$

Proof. Let $T=(T_{i,j})$ be the $(n-1)\times(n-1)$ array whose (w,h) entry is the number of times toroidal vector (w,h) occurs in the array A.

Suppose there is no '0' entry in row w of T. Since the sum of all entries in row w of T is n, the multiset of entries in row w of T is then $\{1,1,\dots,1,2\}$. Let the single '2' entry in this row of T occur in column $h=h(w)$, so that the multiset of heights of the toroidal vectors of width w in A is the multiset union $\{1,2,\dots,n-1\}\cup\{h\}$. Since each '1' entry of A has one toroidal vector of width w entering it and another leaving it, these heights sum to zero modulo n and so

$$0 \equiv \frac{n(n-1)}{2} + h \pmod{n}. \tag{1.1}$$

In the case that n is odd, this gives the contradiction $h\equiv 0 \pmod{n}$. We conclude that for n odd, every row w of T contains a '0' entry and therefore $D(A)\geq n-1$, as required.

Henceforth take n to be even. Equation (1.1) now gives $h=\frac{n}{2}$, and so

$$\text{if there is no '0' entry in row } w \text{ of } T \text{ then } T_{w,\frac{n}{2}}=2. \tag{1.2}$$

Consider the regions of T shown in Figure 2. For $1\leq i\leq 4$, let z_i and z_i' be the number of '0' entries in regions R_i and R_i', respectively. Since the toroidal vector (w,h) is missing from A if and only if the toroidal vector $(n-w,n-h)$ is missing, $z_i=z_i'$ for each i. Since rows $1,\dots,\frac{n}{2}-1$ of T contain exactly $z_1+z_2+z_3$ entries '0', at least $\max(0,\frac{n}{2}-1-(z_1+z_2+z_3))$ of these rows contain no '0' entry. Therefore by (1.2), at least $\max(0,\frac{n}{2}-1-(z_1+z_2+z_3))$ of the entries of R_3 are 2. Since R_3 has a total of $\frac{n}{2}-1-z_3$ nonzero entries, it follows that the sum of all entries in R_3 is at least $n-2-z_1-z_2-2z_3$.

By the same argument with rows and columns interchanged, the sum of all entries in R_4 is at least $n-2-z_1-z_2-2z_4$. Let z be 1 if $T_{\frac{n}{2},\frac{n}{2}}=0$, and 0 otherwise, so that $T_{\frac{n}{2},\frac{n}{2}}\geq 1-z$. Then comparison of the sum of all entries in column $\frac{n}{2}$ of T plus the sum of all entries in row $\frac{n}{2}$ of T, namely $2n$, with the above bounds gives

$$2n \geq 2(n-2-z_1-z_2-2z_3)+2(n-2-z_1-z_2-2z_4)+2(1-z).$$

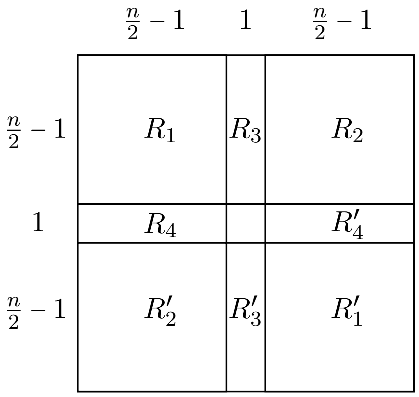


FIGURE 2. Regions of T for the proof of Theorem 1.7

Therefore $D(A) = 2(z_1 + z_2 + z_3 + z_4) + z \geq n - 3$, as required. □

Definition 1.6 was introduced in the paper [12], which describes how the smallness of the deficiency of a permutation array corresponding to $\alpha \in S_n$ measures how close the $n-1$ "difference" mappings $j \mapsto \alpha(j+w) - \alpha(j)$ with $w \neq 0$ are to being surjective. The authors of [12] sought permutation arrays whose deficiency attains the lower bound of Theorem 1.7. They used permutation polynomials over finite fields to construct permutation arrays of order $q-1$, where q is a prime power, having small deficiency. A related paper [11], correcting some oversights in [12], showed that the deficiency of these constructed permutation arrays attains the lower bound of Theorem 1.7 when q is a power of a prime other than 3. Otherwise, when q is a power of 3, the deficiency is one greater than the lower bound (and in this case it is not yet known whether the lower bound of Theorem 1.7 can be attained by some permutation array). The authors of [11] stated (p. 7651): "Functions that meet these bounds [of Theorem 1.7, or those for the related property of *ambiguity*] are of particular interest".

This paper studies the deficiency of Costas arrays. In Section 2 we show that all Welch Costas arrays of a given order $n > 1$ have the same deficiency, but that the same is not in general true of Golomb Costas arrays. We also examine the deficiency of all Costas arrays of order $n \leq 29$ numerically. In Section 3 we note that the minimum deficiency of Costas arrays of order n is anomalously small for certain values of $n \leq 29$ of the form $q-1$ (where q is a prime power), and that these anomalous minimum deficiencies are at most one greater than the minimum value among all permutation arrays of order n. We explain how all these anomalous minimum deficiencies arise from Golomb-Rickard Costas arrays, and describe exactly when the deficiency of a Golomb-Rickard Costas array attains the lower bound of Theorem 1.7 and when it is one greater than this bound. In this way we provide new examples of functions that were described in [11] as being of particular interest; furthermore, these new examples have the additional property of corresponding to Costas arrays. Some of these functions are related to the construction of [11, Theorem 14], although the connection with Golomb-Rickard Costas arrays was not recognised in [11]. In Section 4 we consider in more detail the deficiency distribution of Costas arrays for each order $n \le 29$. We show that these distributions act as a filter that highlights the Welch Costas arrays, isolates the Golomb-Rickard Costas arrays, and gives further insights into the structure of other Costas arrays. In particular, we recognise four Costas arrays with exceptionally small deficiency, that are not explained by any known construction, and ask whether they could be used to identify a new algebraic construction for Costas arrays. In Section 5 we demonstrate connections with the work of several other authors.

2. Deficiency of Costas arrays

In this section, we consider the deficiency of Welch Costas arrays theoretically. We also consider the deficiency of Golomb Costas arrays, and of all Costas arrays of order at most 29, numerically.

In Corollary 2.4, we prove that any two Welch Costas arrays of order $n > 1$ have the same deficiency. To do so, we consider the decimation of Welch Costas arrays.

Definition 2.1. *Let $A = (A_{i,j})$ be an $n \times n$ array and let $k \in \mathbb{N}$ satisfy* $\gcd(k,n) = 1$*. The k*-decimation *of A with respect to columns is the $n \times n$ array $(A_{i,((jk-1) \bmod n)+1})$.*

The index $((jk-1) \bmod n) + 1$ in Definition 2.1 is the unique integer in $\{1, \dots, n\}$ congruent to jk modulo n. This expression is used instead of the simpler expression $(jk) \bmod n$ in order to account for the case when $(jk) \bmod n = 0$, because columns of A are numbered from 1 to n rather than from 0 to $n-1$. We can regard the k-decimation of A with respect to columns as the array whose columns (in order) are column k of A followed by every k^{th} column of A, wrapping around as necessary. This leads to the following remark.

Remark 2.2. *The toroidal vector (w,h) is contained in the k-decimation of A with respect to columns exactly when the toroidal vector $((wk) \bmod n, h)$ is contained in A. (We can use the simple expression $(wk) \bmod n$ here, since $0 < w < n$ and $\gcd(k,n) = 1$, so $(wk) \bmod n \ne 0$.)*

Proposition 2.3. *Let p be prime, let ϕ be primitive in $\mathbb{F}_p$ and let $k \in \mathbb{N}$ satisfy $\gcd(k, p-1) = 1$. Then the $W_1(p, \phi^k, 1)$ Welch Costas array is the k-decimation with respect to columns of the $W_1(p, \phi, 1)$ Welch Costas array.*

Proof. By the Welch construction, for $1 \le i, j \le p-1$, there is a '1' entry at position (i,j) in $W_1(p, \phi^k, 1)$ exactly when $i \equiv \phi^{jk} \pmod{p}$. This occurs exactly when there is a '1' entry at position (i, ℓ) in $W_1(p, \phi, 1)$, where ℓ is the unique integer in $\{1,\dots,p-1\}$ congruent to jk modulo $(p-1)$. This gives the value of ℓ as $((jk-1) \bmod (p-1))+1$, and the result follows from Definition 2.1. □

Corollary 2.4. *Let p be prime, let ϕ be primitive in $\mathbb{F}_p$, and let W be a Welch Costas array of order $p-1$. Then there is a one-to-one multiplicity-preserving correspondence between the multiset of toroidal vectors in W and the multiset of toroidal vectors in the $W_1(p,\phi,1)$ Welch Costas array.*

Proof. Let W be the $W_1(p,\rho,c)$ Costas array, where ρ is primitive in $\mathbb{F}_p$ and $0 \le c \le p-2$. Since cyclic column permutation does not affect toroidal vectors, we may take $c = 1$. Since ϕ and ρ are both primitive in $\mathbb{F}_p$, we have $\rho = \phi^k$ for some $k \in \mathbb{N}$ satisfying $\gcd(k,p-1) = 1$. Therefore by Proposition 2.3, W is the k-decimation with respect to columns of $W_1(p,\phi,1)$. Then by Remark 2.2, the toroidal vector (w,h) is contained in W exactly when the toroidal vector $((wk) \bmod (p-1), h)$ is contained in $W_1(p,\phi,1)$. □

In particular, Corollary 2.4 implies that all Welch Costas arrays of order $p-1$ have the same deficiency. Table 3 gives the deficiency of Welch Costas arrays of order $n \le 40$, obtained numerically.

Order	1	2	4	6	10	12	16	18	22	28	30	36	40
Deficiency	0	0	1	4	12	21	37	48	72	121	140	209	253

Table 3. Deficiency of Welch Costas arrays

In contrast to the situation for Welch Costas arrays, the deficiency $D(G)$ is not necessarily the same for all Golomb Costas arrays G of a given order. Figure 4 displays the minimum, mean and maximum deficiency of Golomb Costas arrays of order $n \le 39$. These data suggest that, roughly speaking, $D(G)$ grows faster than linearly with n.

Figure 5 shows the minimum, mean and maximum deficiency of all Costas arrays of order n for $2 \le n \le 29$, calculated using the database [13] of Costas arrays up to order 29.

3. Outlying minimum deficiency values for Costas arrays of order n

A striking feature of Figure 5 is the outlying minimum deficiency values for several orders $n \ge 8$. These outlying values, together with values for some orders $n < 8$, are listed in Table 6. For $n > 2$, each of these outlying deficiency values attains the lower bound of Theorem 1.7 (which is the minimum value over all order-n permutation arrays), except that the value for order 8 and 26 is one greater than the lower bound. In this section we explain how the values in Table 6 arise.

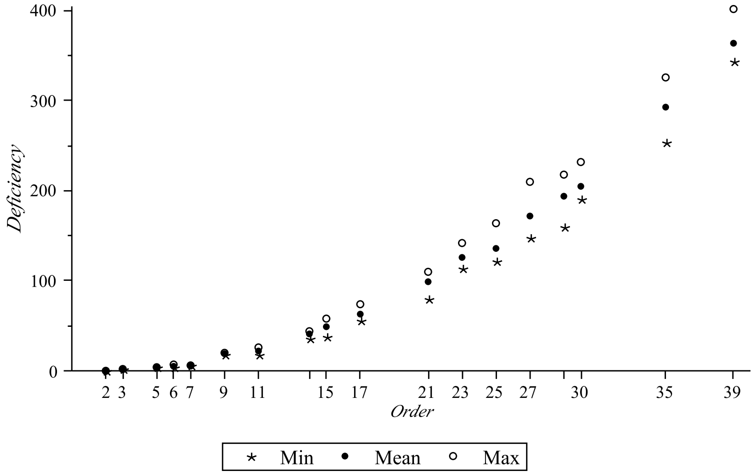


Figure 4. Deficiency of Golomb Costas arrays

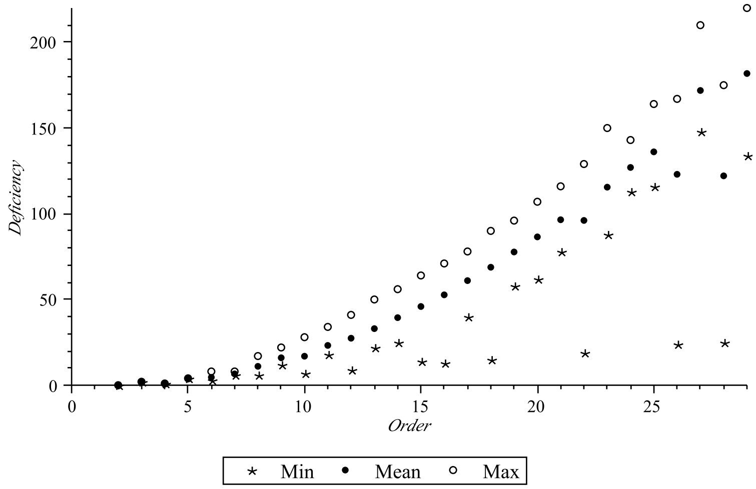


Figure 5. Deficiency of Costas arrays up to order 29

Order	2	3	4	6	7	8	10	12	15	16	18	22	26	28
Minimum deficiency	0	2	1	3	6	6	7	9	14	13	15	19	24	25

Table 6. Outlying minimum deficiency values

Definition 3.1. *Let G be a Golomb Costas array of order $q-2$. The* augmented Golomb Costas array G_+^+ *associated with G is the* $(q-1) \times (q-1)$

array formed by adding a row of 0*s on the bottom of G and a column of* 0*s on the right of G.*

For example, let G be the $G_2(8, x+1, x)$ Costas array, with $\mathbb{F}_8$ constructed using the primitive polynomial x^3+x+1. The augmented array G_+^+ is shown in Figure 7.

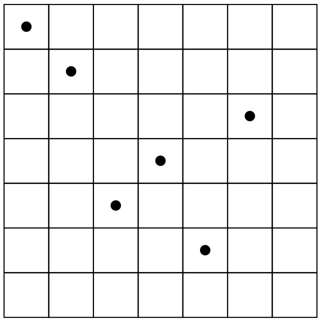


Figure 7. An augmented Golomb Costas array

Proposition 3.2 shows that an augmented Golomb Costas array G_+^+ has no repeated toroidal vectors (which can be inferred from part of the discussion of Section II.C of Beard et al. [2]), and specifies exactly which toroidal vectors are missing. The derivation of Proposition 3.2 is as in the proof of Lemma 1 of [5], except that we replace G with G_+^+ since the rows and columns of a Golomb Costas array both have period $q-1$.

Proposition 3.2. *Let q be a prime power, let ϕ and ρ be primitive in $\mathbb{F}_q$ and let G be the $G_2(q, \phi, \rho)$ Costas array. Then G_+^+ contains the toroidal vector $(w, h) \in \{1, 2, \dots, q-2\}^2$ exactly once if $\phi^h \neq \rho^w$ and otherwise never. Furthermore, if the toroidal vector (w, h) is contained in G_+^+ starting from position (i, j), then*

$$\rho^j = 1 - \phi^i = (\phi^h - \rho^w)^{-1}(\phi^h - 1). \tag{3.1}$$

Proof. Let $(w, h) \in \{1, 2, \dots, q-2\}^2$. By the Golomb construction, the toroidal vector (w, h) occurs in G_+^+ starting from position (i, j) if and only if there exist $i, j \in \{1, \dots, q-2\}$ such that

$$\phi^i + \rho^j = 1 \quad \text{and} \tag{3.2}$$

$$\phi^{i+h} + \rho^{j+w} = 1. \tag{3.3}$$

(For the "if" part of the statement, we must ensure that (3.3) does not introduce solutions involving a '1' entry in the additional row or column of G_+^+. Such solutions would have $i+h = q-1$ or $j+w = q-1$, and are excluded because ϕ and ρ are primitive in $\mathbb{F}_q$.)

Multiply (3.2) by ϕ^h and subtract (3.3) to give $\rho^j(\phi^h - \rho^w) = \phi^h - 1$. If $\phi^h = \rho^w$ then this has no solution. Otherwise,

$$\rho^j = (\phi^h - \rho^w)^{-1}(\phi^h - 1),$$

which has a unique solution for $j \in \{1,\dots,q-2\}$ since $\phi^h \neq 1$ and $\rho^w \neq 1$. Then (3.2) has a unique solution for $i \in \{1,\dots,q-2\}$, since $\rho^j \notin \{0,1\}$. □

Viewing an augmented Golomb Costas array G_+^+ as being written on the surface of a torus provides an alternative interpretation of the Golomb-Rickard construction, which involves adding a row and column to a Golomb Costas array, with a '1' at their intersection, and then testing all cyclic row/column permutations of the resulting $(q-1)\times(q-1)$ array for the Costas property [14]. Indeed, we may view the Golomb-Rickard construction as starting with the toroidal G_+^+ array, adding a '1' at the intersection of its additional row and column, and then trying to "cut" the torus along a vertical and a horizontal boundary so that the resulting $(q-1)\times(q-1)$ array in the plane has the Costas property. The list of toroidal vectors present in G_+^+ is known by Proposition 3.2; we wish to cut the torus so that at least one of each pair of repeated toroidal vectors, arising from the introduction of the extra '1', is eliminated. Theorem 3.3 determines the deficiency of a Golomb-Rickard Costas array.

Theorem 3.3. *Let $q > 2$ be a power of a prime p, let ϕ and ρ be primitive in $\mathbb{F}_q$ and let R be a Golomb-Rickard Costas array of order $q-1$ obtained from the $G_2(q,\phi,\rho)$ Golomb Costas array. Then $D(R) = q - \min(p,4)$.*

Proof. Define the set

$$S = \{(w,h) \in \{1,\dots,q-2\}^2 : \rho^w = \phi^h\},$$

and, for $p > 2$, let (w^*,h^*) be the element of this set for which $\rho^w = \phi^h = \frac{p+1}{2}$.

We shall show that the set M of toroidal vectors missing from R is

$$M = \begin{cases} S & \text{for } p = 2 \\ S \setminus \{(w^*,h^*),(q-1-w^*,q-1-h^*)\} & \text{for } p > 2, \end{cases} \tag{3.4}$$

so that

$$D(R) = |M| = \begin{cases} q-2 & \text{for } p = 2 \\ q-2-|\{(w^*,h^*),(q-1-w^*,q-1-h^*)\}| & \text{for } p > 2. \end{cases}$$

The vectors (w^*,h^*) and $(q-1-w^*,q-1-h^*)$ are distinct exactly when $p > 3$ because

$$\begin{aligned} (w^*,h^*) = (q-1-w^*,q-1-h^*) &\Leftrightarrow w^* = h^* = \frac{q-1}{2} \\ &\Leftrightarrow \rho^{w^*} = \phi^{h^*} = -1 \\ &\Leftrightarrow \frac{p+1}{2} = -1 \\ &\Leftrightarrow p = 3. \end{aligned}$$

We therefore conclude that

$$D(R) = \begin{cases} q-2 & \text{for } p = 2 \\ q-3 & \text{for } p = 3 \\ q-4 & \text{for } p > 3, \end{cases}$$

as required.

We now prove (3.4). By Proposition 3.2, the set of toroidal vectors missing from G_+^+ is S. The Golomb-Rickard Costas array R contains the same multiset of toroidal vectors as the array obtained by adding a '1' at position $(q-1, q-1)$ of G_+^+. The two toroidal vectors formed between this new '1' and the '1' at position (i, j), where i and j satisfy

$$\phi^i + \rho^j = 1 \tag{3.5}$$

by the Golomb construction, are (j, i) and $(q-1-j, q-1-i)$.

The introduction of the new '1' reduces the size of the set of missing toroidal vectors when one or both of (j, i) and $(q-1-j, q-1-i)$ belongs to S. This occurs exactly when

$$\rho^j = \phi^i. \tag{3.6}$$

Equations (3.5) and (3.6) have no solution for $p = 2$ (in which case $M = S$), and the unique solution $\rho^j = \phi^i = \frac{p+1}{2}$ for $p > 2$ (in which case $(j, i) = (w^*, h^*)$). This establishes (3.4). □

Theorem 3.3 explains the outlying minimum deficiency values in Table 6, which occur exactly at orders $q-1 \le 28$ for which there is a Golomb-Rickard Costas array. (There is no such outlying minimum deficiency value for order 24 because there is no Golomb-Rickard Costas array of this order.) In fact, analysis of the database [13] of Costas arrays up to order 29 shows that Golomb-Rickard Costas arrays are the only Costas arrays attaining the minimum values in Table 6.

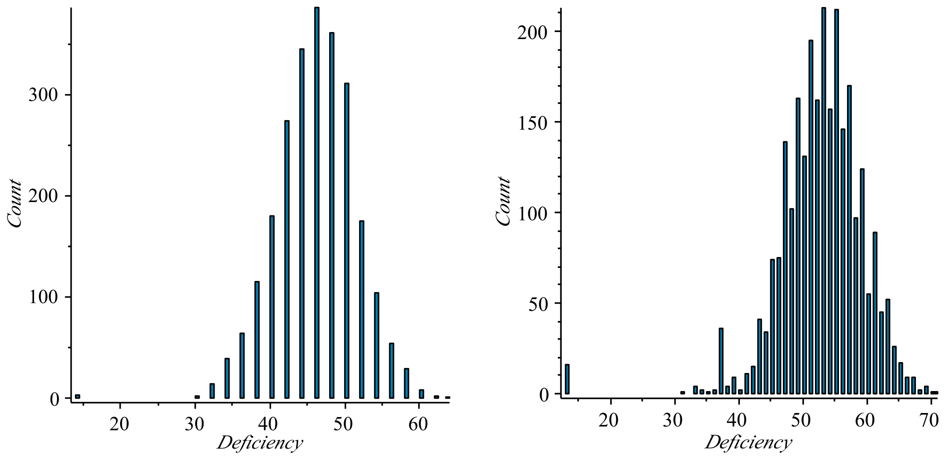
Corollary 3.4. *Let $q > 3$ be a power of a prime p, let ϕ and ρ be primitive in $\mathbb{F}_q$ and let R be a Golomb-Rickard Costas array of order $q-1$ obtained from the $G_2(q, \phi, \rho)$ Golomb Costas array. Then the deficiency of R attains the minimum value over all permutation arrays of order $q-1$ when $p \ne 3$, and is at most one greater than the minimum value when $p = 3$.*

Proof. By Theorem 1.7, the deficiency of a permutation array of order $q-1 > 2$ is at least

$$\begin{cases} q-2 & \text{for } p = 2 \\ q-4 & \text{for } p \text{ odd}, \end{cases}$$

and this bound can be attained when $p \ne 3$ [11]. The result follows from Theorem 3.3. □

The special case $\phi = \rho$ of Proposition 3.2, Theorem 3.3 and Corollary 3.4 is related to the construction of [11, Theorem 14], although the connection with Golomb and Golomb-Rickard Costas arrays was not recognised in [11].



(a) Order 15

(b) Order 16

FIGURE 8. Deficiency distribution for inequivalent Costas arrays of order 15 and 16

4. DEFICIENCY DISTRIBUTION FOR COSTAS ARRAYS OF ORDER $n \leq 29$

Figure 5 shows the minimum, mean and maximum deficiency (number of missing toroidal vectors) of Costas arrays of order n for each $n \leq 29$. In this section we consider in more detail the deficiency distribution for each of these orders. We shall see that these distributions act as a filter that highlights the Welch Costas arrays, isolates the Golomb-Rickard Costas arrays, and gives further insights into the structure of other Costas arrays.

Figures 8(a) and 8(b) show the deficiency distribution over all equivalence classes of Costas arrays of order 15 and 16, respectively. (All elements of an equivalence class of Costas arrays have the same deficiency.) These orders were chosen to represent the general trends observed by considering all orders, while also providing examples of several anomalous features. We begin by describing two features of the distributions that can be explained by the results of Sections 2 and 3.

Firstly, Figure 8(b) has a spike representing 40 Costas arrays having $D = 37$, of which 36 are Welch Costas arrays. We know from Corollary 2.4 that all Welch Costas arrays of order $p - 1$ have the same deficiency, and the location of the "Welch spike" for $p - 1 \leq 40$ is given in Table 3. For all orders $n \leq 29$, the location of the Welch spike is consistently smaller than the median deficiency.

Secondly, Figure 8(b) has a smaller spike representing 16 Costas arrays with $D = 13$, all of which are Golomb-Rickard Costas arrays; likewise, Figure 8(a) has a spike representing three Costas arrays with $D = 14$, all of which are also Golomb-Rickard Costas arrays. Provided there is at least one

Golomb-Rickard Costas array of order $q-1$, the location of the "Golomb-Rickard spike" is given by Theorem 3.3. For all prime powers $q \le 29$ except 25, there is a Golomb-Rickard Costas array of order $q-1$, the location of the Golomb-Rickard spike is at the extreme left of the deficiency distribution, and Golomb-Rickard Costas arrays are the only arrays contributing to the spike.

When the Welch spike and the Golomb-Rickard spike (if present) are disregarded, Figures 8(a) and 8(b) represent a typical background deficiency distribution for Costas arrays of odd order and even order, respectively. Unlike the Welch and Golomb-Rickard Costas arrays, the Golomb Costas arrays form part of the background distribution (for orders $q-2$ where q is a prime power).

We observe that the Costas arrays represented in Figure 8(a) have only even deficiencies. We now show that this is a general property of permutation arrays of odd order.

Proposition 4.1. *Let A be a permutation array of odd order. Then $D(A)$ is even.*

Proof. The toroidal vector (w,h) is missing from A if and only if the toroidal vector $(n-w,n-h)$ is missing. Since n is odd, we have $(w,h) \ne (n-w,n-h)$ and so the toroidal vectors missing from A can be partitioned into distinct pairs. □

We further observe that the Costas arrays represented in Figure 8(b) have odd deficiency more often than they have even deficiency. This appears to be a general property of inequivalent Costas arrays of even order.

Observation 4.2. *For each even $n \le 28$, Costas arrays of order n have odd deficiency more often than they have even deficiency.*

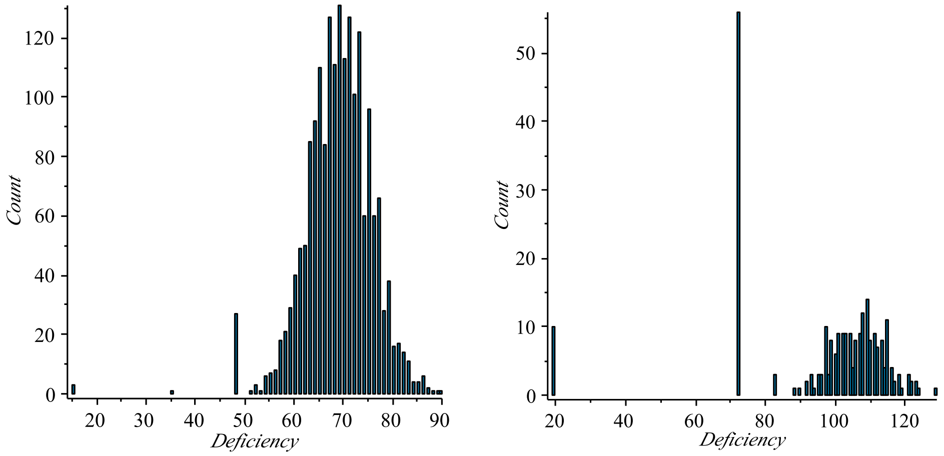
A similar argument to that used in the proof of Proposition 4.1 shows that the toroidal vectors missing from a Costas array of even order n can be partitioned into distinct pairs, except for $(\frac{n}{2},\frac{n}{2})$. Observation 4.2 therefore implies that, for each even $n \le 28$, the toroidal vector $(\frac{n}{2},\frac{n}{2})$ is missing from a Costas array of order n more often than not.

We have now accounted for all apparent features of the deficiency distribution for Costas arrays of order at most 29, with two exceptions: order 18 and order 22.

The order-18 distribution, shown in Figure 9(a), contains a Golomb-Rickard spike at $D = 15$ and a Welch spike at $D = 48$. After disregarding these, there remains one outlying bar representing a single Costas array with $D = 35$, corresponding to the permutation

$$[7,17,15,16,2,11,8,13,5,1,12,18,3,10,4,6,14,9]$$

and displayed in Figure 10. This Costas array is symmetric about a diagonal. It is not explained by any known construction [1].



(a) Order 18

(b) Order 22

Figure 9. Deficiency distribution for inequivalent Costas arrays of order 18 and 22

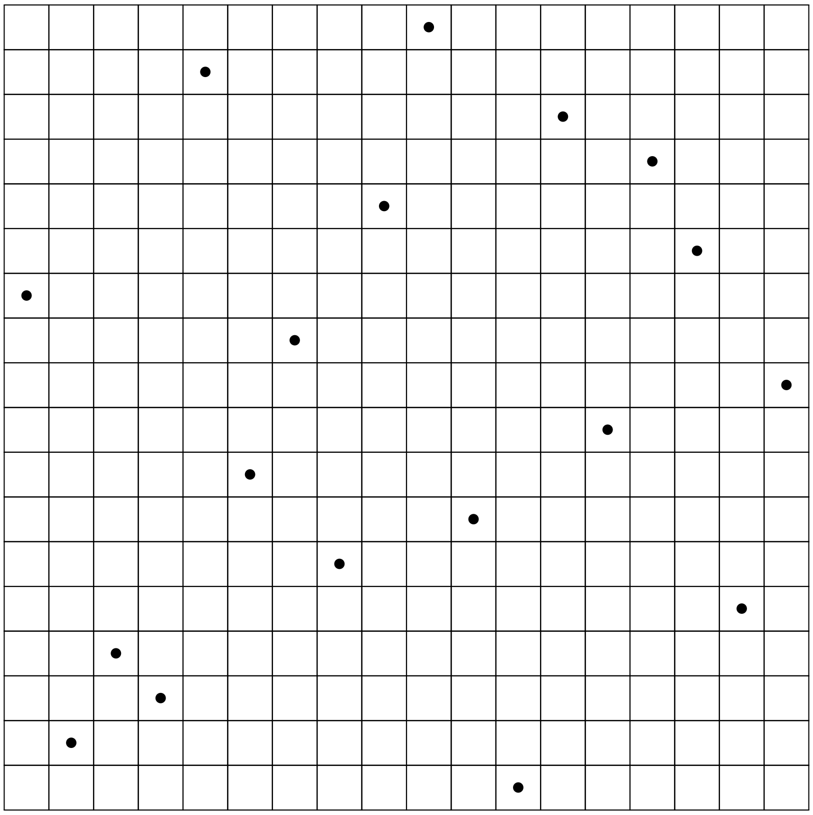


Figure 10. Order-18 Costas array with $D = 35$

The order-22 distribution, shown in Figure 9(b), contains a Golomb-Rickard spike at $D = 19$ and a Welch spike at $D = 72$ (which includes one non-Welch Costas array that is toroidally equivalent to a Welch Costas array under cyclic permutation of its rows). After disregarding these, there remains one outlying bar representing three Costas arrays with $D = 83$, corresponding to the permutations

$$[1,13,7,10,20,15,6,22,14,18,16,17,5,11,8,21,3,12,19,4,9,2],$$
$$[2,1,13,7,10,20,15,6,22,14,18,16,17,5,11,8,21,3,12,19,4,9],$$
$$[5,15,4,7,21,3,19,14,1,16,9,22,2,10,6,11,13,20,18,17,8,12].$$

These arrays are not explained by any known construction [1]; the first two are toroidally equivalent under cyclic permutation of their columns.

We conclude that the deficiency distributions act as a filter, allowing us to recognise one order 18 and three order 22 Costas arrays as exceptional. Could these examples be used to identify a new algebraic construction for Costas arrays?

5. Toroidal vectors in augmented Welch Costas arrays

In Section 3 we used the augmented Golomb Costas array G_+^+ to explain the outlying minimum deficiency values in Table 6. In Definition 5.1 below, we define the augmented array A^+ of a permutation array A. We then show in Theorem 5.2 that the augmented array W^+ of a Welch Costas array W contains every possible toroidal vector exactly once.

Definition 5.1. *Let A be a permutation array of order n. The* augmented array *A^+ associated with A is the $(n+1)\times n$ array formed by adding a row of 0s on the bottom of A.*

Theorem 5.2. *Let W be a $W_1(p,\phi,c)$ Costas array. Then the $p\times(p-1)$ augmented array W^+ contains every toroidal vector $(w,h)\in\{1,\dots,p-2\}\times\{1,\dots,p-1\}$ exactly once.*

Proof. Let $(w,h)\in\{1,\dots,p-2\}\times\{1,\dots,p-1\}$. By the Welch construction, the toroidal vector (w,h) occurs in W^+ starting from position (i,j) if and only if there exist $i,j\in\{1,\dots,p-1\}$ such that

$$i \equiv \phi^{j+c-1} \pmod p \quad \text{and} \tag{5.1}$$
$$i+h \equiv \phi^{j+w+c-1} \pmod p. \tag{5.2}$$

(Equation (5.2) does not introduce solutions involving a '1' entry in the additional row of W^+, because solutions with $i+h=p$ cannot occur.) Multiply the first congruence by ϕ^w and subtract the second congruence to give $i(\phi^w-1)\equiv h \pmod p$. This has a unique solution for $i\in\{1,\dots,p-1\}$, since $\phi^w\neq 1$. Then (5.1) has a unique solution for $j\in\{1,\dots,p-1\}$. □

Theorem 5.2 is not new, but we have included it in order to demonstrate connections with earlier sections of this paper and with the work of several other authors. Golomb and Moreno [9] defined an order-n Costas array A to correspond to a *circular Costas sequence* if A^+ contains every toroidal vector $(w, h) \in \{1, \dots, n-1\} \times \{1, \dots, n\}$ exactly once. Rephrased in this language, Theorem 5.2 states that every Welch Costas array corresponds to a circular Costas sequence. In 1996, Golomb and Moreno [9] conjectured that the reverse implication also holds, and proved the partial result that an order-n circular Costas sequence exists only when $n+1$ is prime. Q. Wang reported (personal communication, Sep. 2014) that this conjecture was proved in [10]. Drakakis, Gow and McGuire [4] explored the relationship between almost perfect nonlinear permutations and Costas arrays; their Theorem 3 can be seen to be equivalent to Theorem 5.2 of this paper. Part of the discussion of Section II.C of Beard et al. [2] can also be interpreted in terms of the toroidal vectors of W^+. Theorem 5 of Drakakis, Gow and Rickard [5] states: "All possible distance vectors are contained within a Welch Costas array (assuming the array wraps around at the boundaries)." This should not be understood to mean that a Welch Costas array of order $p-1$ has zero deficiency (which is not the case); instead, the array wrapping should be interpreted as occurring with period $p-1$ for the columns but with period p for the rows, and the statement then coincides with Theorem 5.2.

Acknowledgements

We are grateful to Matt DeVos for many helpful and stimulating discussions. We appreciate the generosity of James K. Beard and Scott Rickard in each making his database of Costas arrays publically available. We are grateful to Brett Stevens for pointing out prior research on the deficiency of permutation arrays [12], [11], to David Thomson for pointing out an early result on augmented Welch Costas arrays [9], and to Lucia Moura and Daniel Panario for organising the 2013 *International Workshop on Finite Fields Constructions of Combinatorial Arrays* in Florianópolis, Brazil at which these connections with our work became apparent. We thank Qiang Wang for his personal communication regarding [10].

References

[1] J. K. Beard, *Database of Costas arrays, orders three through 100*, http://jameskbeard.com/jameskbeard/Files.html#CostasArrays.

[2] 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 **43** (2007), 522–538.

[3] K. Drakakis, *Open problems in Costas arrays*, arXiv 1102.5727v1 [math.CO] (2011).

[4] K. Drakakis, R. Gow, and G. McGuire, *APN permutations on $\mathbb{Z}_n$ and Costas arrays*, Discrete Appl. Math. **157** (2009), 3320–3326.

[5] K. Drakakis, R. Gow, and S. Rickard, *Common distance vectors between Costas arrays*, Advances in Mathematics of Communications **3** (2009), 35–52.

[6] K. Drakakis, F. Iorio, S. Rickard, and J. Walsh, *Results of the enumeration of Costas arrays of order 29*, Advances in Mathematics of Communications **5** (2011), 547–553.

[7] E. N. Gilbert, *Latin squares which contain no repeated digrams*, SIAM Review **7** (1965), 189–198.

[8] S. Golomb, *Algebraic constructions for Costas arrays*, Journal of Combinatorial Theory Series A **37** (1984), 13–21.

[9] S. Golomb and O. Moreno, *On periodicity properties of Costas arrays and a conjecture on permutation polynomials*, IEEE Trans. Inform. Theory **42** (1996), 2252–2253.

[10] A. Muratović-Ribić, A. Pott, D. Thomson, and Q. Wang, *On the characterization of a semi-multiplicative analogue of planar functions over finite fields*, Proc. 11th International Conference on Finite Fields and their Applications (G.M. Kyureghyan, G. Mullen, A. Pott, eds.), Contemporary Math., to appear.

[11] D. Panario, A. Sakzad, B. Stevens, and Q. Wang, *Two new measures for permutations: ambiguity and deficiency*, IEEE Trans. Inform. Theory **57** (2011), 7648–7657.

[12] D. Panario, B. Stevens, and Q. Wang, *Ambiguity and deficiency in Costas arrays and APN permutations*, LATIN 2010: Theoretical Informatics (A. López-Ortiz, ed.), Lecture Notes in Comput. Sci., vol. 6034, Springer, Berlin, 2010, pp. 397–406.

[13] S. Rickard, *Database of Costas arrays*, `http://osl-vps-4.ucd.ie/downloader`.

[14] ______, *Searching for Costas arrays using periodicity properties*, Proceedings of the 2004 IMA International Conference on Mathematics in Signal Processing (Cirencester, UK).

[15] A. Sterling, *An independent discovery of Costas arrays*, `http://nanoexplanations.wordpress.com/2011/10/09/an-independent-discovery-of-costas-arrays/`.

[16] K. Taylor, K. Drakakis, and S. Rickard, *Generated, emergent, and sporadic Costas arrays*, Proceedings of the 2008 IMA International Conference on Mathematics in Signal Processing (Cirencester).