

# A REGULARITY PROPERTY OF GOLOMB-COSTAS ARRAYS

ROD GOW

ABSTRACT. A Golomb-Costas array is an arrangement of dots and blanks, defined for each positive integer power of a prime and satisfying certain unusual conditions. A dot occurring in such an array is an even/even position if it occurs in the  $i$ -th row and  $j$ -th column, where  $i$  and  $j$  are both even integers, and there are similar definitions of odd/odd, even/odd and odd/even positions for dots. When  $q$  is a power of an odd prime, we enumerate the number of even/even, odd/odd, even/odd and odd/even positions for dots in a Golomb-Costas array of order  $q - 2$ . We show that three of these numbers are equal and they differ by  $\pm 1$  from the fourth. More general Costas arrays do not exhibit this regularity. We also show that if  $q = r^t$ , where  $r$  is a power of a prime and  $t$  is an integer greater than 1, any Golomb-Costas array of order  $q - 2$  contains in a natural way a Golomb-Costas array of order  $r - 2$  which can easily be identified.

## 1. INTRODUCTION

A *Costas array* of order  $n$  is an  $n \times n$  array of dots and blanks satisfying the two conditions:

- there are  $n$  dots in the array, one in each row and in each column;
- no two of the  $\binom{n}{2}$  line segments joining two dots in the array have the same length and slope.

We shall call an  $n \times n$  array of dots and blanks satisfying the first condition a *permutation array* of order  $n$ , since it corresponds to the well known concept of a permutation matrix.

For an arbitrary positive integer  $n$ , there do not seem to be any systematic ways of constructing Costas arrays, and it is an open question whether Costas arrays actually exist for all integers  $n \geq 1$ . For certain values of  $n$ , finite fields provide a framework to produce Costas arrays, as we shall now explain.

Let  $p$  be a prime integer and let  $q = p^m$ , where  $m$  is a positive integer. Let  $\mathbb{F}_q$  denote the finite field of size  $q$  and let  $\mathbb{F}_q^*$  denote the multiplicative group of non-zero elements in  $\mathbb{F}_q$ . It is well known that  $\mathbb{F}_q^*$  is a cyclic group, of order  $q - 1$ . Let  $\alpha$  and  $\beta$  be generators of  $\mathbb{F}_q^*$  (we allow the possibility that  $\alpha = \beta$ ). We construct a corresponding permutation array of order  $q - 2$  by putting a dot in the  $(i, j)$ -position, where  $1 \leq i, j \leq q - 2$ , whenever

$$\alpha^i + \beta^j = 1.$$

It is well known that such an array has the Costas property, [1]. We shall call an array constructed by this procedure a *Golomb-Costas array*.

We might expect Costas arrays derived from the special properties of finite fields to have regularities not shared by all Costas arrays of the same order, and it is the purpose of this paper to point out one such regularity when  $q$  is odd. We will say that a dot occurring in a permutation array is an even/even position if it occurs in the  $i$ -th row and  $j$ -th column, where  $i$  and  $j$  are both even integers. We may likewise define odd/odd, even/odd and odd/even positions for dots.

We first show that all permutation arrays possess some regularity in the distribution of their dots throughout the array.

**Lemma 1.** *Let  $P$  be a permutation array of order  $n$ . Suppose that the number of dots of  $P$  in even/even, odd/odd, even/odd and odd/even positions are  $a$ ,  $b$ ,  $c$  and  $d$ , respectively, where  $a + b + c + d = n$ . Then we have*

$$c = d$$

and

$$\begin{cases} b = a + 1, & \text{if } n \text{ is odd;} \\ b = a, & \text{if } n \text{ is even.} \end{cases}$$

*Proof.* Let  $\Delta$  be the subset of ordered pairs  $(i, j)$ , where there is a dot in the  $(i, j)$ -position of  $P$ . Let  $E$  denote the subset of even integers lying between 1 and  $n$ , and  $O$  the subset of odd integers in the same interval. There are  $|E|$  elements  $(i, j)$  in  $\Delta$  with  $i \in E$  and, by considering whether the second component  $j$  is even or odd, we see that

$$|E| = a + c.$$

Equally, there are  $|E|$  elements  $(k, l)$  in  $\Delta$  with  $l \in E$  and the same argument shows that

$$|E| = a + d.$$

It follows that  $c = d$ . It is also clear that

$$a + c = |E|, \quad b + d = |O|.$$

Since  $|E| = |O| - 1$  if  $n$  is odd, and  $|E| = |O|$  if  $n$  is even, the equations relating  $a$  and  $b$  in the two cases are immediate from the equality  $c = d$ .  $\square$

We are grateful to John Murray (NUI, Maynooth) for supplying this self-contained argument.

Suppose for the present that  $q$  is a power of an *odd* prime. We recall that an element  $c$  of  $\mathbb{F}_q^*$  is a *square* if  $c = d^2$  for some  $d \in \mathbb{F}_q^*$ . Given a generator  $\alpha$  of  $\mathbb{F}_q^*$ , the squares in  $\mathbb{F}_q^*$  are the elements expressible in the form  $\alpha^{2i}$ , for some integer  $i$ . We use this simple observation to begin enumerating the even/even positions in a Golomb-Costas array.

**Lemma 2.** *Let  $P$  be a Golomb-Costas array of order  $q - 2$ , where  $q$  is odd. Then the number of even/even positions in  $P$  equals the number of non-identity elements  $z$  in  $\mathbb{F}_q^*$  such that  $z$  and  $1 - z$  are squares.*

*Proof.* We may suppose that  $P$  is defined using generators  $\alpha$  and  $\beta$  of  $\mathbb{F}_q^*$ . Suppose that  $P$  has a dot at an even/even position  $(i, j)$ . Then we may write  $i = 2u$ ,  $j = 2v$  for unique positive integers  $u$  and  $v$ , and by definition of  $P$ ,

$$\alpha^{2u} + \beta^{2v} = 1.$$

It follows that if we set  $z = \alpha^{2u}$ ,  $z$  is a square and  $1 - z = \beta^{2v}$  is also a square. Thus a dot in an even/even position in  $P$  determines an element  $z$  with the stated property.

Conversely, suppose that  $w$  is a non-identity element in  $\mathbb{F}_q^*$  such that  $w$  and  $1 - w$  are both squares. Then we may write  $w = \alpha^{2s}$  and  $1 - w = \beta^{2t}$  for suitable positive integers  $s$  and  $t$ , with  $1 < 2s, 2t < q - 2$ . Clearly,

$$\alpha^{2s} + \beta^{2t} = 1,$$

and thus  $P$  has a dot in the even/even position  $(2s, 2t)$ .  $\square$

To determine the number of elements  $z$  with the property described in Lemma 2, we consider the polynomial

$$f(x, y) = x^2 + y^2 - 1$$

in  $\mathbb{F}_q[x, y]$ .

**Lemma 3.** *Suppose that  $q$  is odd and there are  $S$  elements  $(\lambda, \mu)$  in  $\mathbb{F}_q^2$  satisfying  $f(\lambda, \mu) = 0$ . Then the number of even/even positions in a Golomb-Costas of order  $q - 2$  equals*

$$\frac{S - 4}{4}.$$

*Proof.* Let  $R$  denote the set of roots  $(\lambda, \mu)$  of  $f$  in  $\mathbb{F}_q^* \times \mathbb{F}_q^*$  and let  $T$  denote the set of non-identity elements  $z$  in  $\mathbb{F}^*$  such that  $z$  and  $1 - z$  are squares. The elements  $(\pm 1, 0)$  and  $(0, \pm 1)$  are all the roots of  $f$  in  $\mathbb{F}_q^2$  in which one component is 0. Thus  $|R| = S - 4$ . We define a mapping  $\pi : R \rightarrow T$  by

$$\pi(\lambda, \mu) = \lambda^2.$$

It is clear that  $\pi$  is surjective. We also have

$$\pi(\lambda, \mu) = \pi(\lambda_1, \mu_1)$$

if and only if

$$\lambda^2 = \lambda_1^2, \quad \mu^2 = \mu_1^2.$$

The equality of the two squares above occurs if and only if  $\lambda_1 = \pm\lambda$ ,  $\mu_1 = \pm\mu$ . Thus  $\pi$  is 4-to-1, and it follows that

$$|R| = 4|T|.$$

Finally, Lemma 2 shows that the number of even/even positions in a Golomb-Costas array of order  $q - 2$  equals  $|T|$  and the result follows.  $\square$

The value of  $S$  above is well known and can be calculated in various ways. Our next lemma gives the details.

**Lemma 4.** *We have*

$$\begin{cases} S = q - 1, & \text{if } q \equiv 1 \pmod{4}; \\ S = q + 1, & \text{if } q \equiv 3 \pmod{4}. \end{cases}$$

*Proof.* The statements above are results in the elementary theory of quadratic forms. Proofs are also given in [2], Chapter 8, §3 in the case that  $q$  is a prime. We can give self-contained proofs, as follows. Suppose that  $q \equiv 1 \pmod{4}$ . Then there is an element  $\epsilon$ , say, in  $\mathbb{F}_q$  satisfying  $\epsilon^2 = -1$ . Let  $\lambda$  and  $\mu$  be elements of  $\mathbb{F}_q$  satisfying

$$\lambda^2 + \mu^2 = 1.$$

We can write

$$\lambda = \epsilon a + b, \quad \mu = a + \epsilon b$$

for unique elements  $a$  and  $b$  in  $\mathbb{F}_q$ , and then the equation for  $\lambda$  and  $\mu$  above transforms into

$$4\epsilon ab = 1,$$

which clearly has  $q - 1$  different solutions for  $a$  and  $b$ . This implies that  $S = q - 1$  in this case.

Suppose now that  $q \equiv 3 \pmod{4}$ . The field  $\mathbb{F}_{q^2}$  contains an element  $\iota$  with  $\iota^2 = -1$ , and the elements of field  $\mathbb{F}_{q^2}$  may be written in the form  $\lambda + \mu\iota$ , for unique  $\lambda$  and  $\mu$  in  $\mathbb{F}_q$ . The norm mapping  $N : \mathbb{F}_{q^2}^* \rightarrow \mathbb{F}_q^*$  is a surjective homomorphism given by

$$N(\lambda + \mu\iota) = \lambda^2 + \mu^2$$

and its kernel has order  $q + 1$ . Thus there are  $q + 1$  ordered pairs  $(\lambda, \mu)$  satisfying  $\lambda^2 + \mu^2 = 1$  and we see that  $S = q + 1$  in this case.  $\square$

**Corollary 1.** *Suppose that  $q$  is odd. Then the number of non-identity squares  $z$  in  $\mathbb{F}_q^*$  with the property that  $1 - z$  is also a square equals  $(q - 5)/4$  when  $q \equiv 1 \pmod{4}$  and  $(q - 3)/4$  when  $q \equiv 3 \pmod{4}$ .*

*Proof.* This follows from Lemmas 3 and 4.  $\square$

Using Lemma 1, we immediately deduce the following information concerning the distribution of dots in a Golomb-Costas array defined with respect to a power of an odd prime.

**Theorem 1.** *Let  $P$  be a Golomb-Costas array of order  $q - 2$ , where  $q$  is a power of an odd prime. Suppose that the number of dots of  $P$  in even/even, odd/odd, even/odd and odd/even positions are  $a, b, c$  and  $d$ , respectively, where  $a + b + c + d = q - 2$ . Then we have*

$$a = (q - 5)/4, \quad b = c = d = (q - 1)/4$$

when  $q \equiv 1 \pmod{4}$ , and

$$a = c = d = (q - 3)/4, \quad b = (q + 1)/4$$

when  $q \equiv 3 \pmod{4}$ .

Finally, we report on a regularity displayed by Golomb-Costas arrays which are defined using prime powers, rather than simply primes. Suppose then that  $q$  is not a prime (we allow  $q$  to be a power of 2 here). Then we may write  $q = r^t$ , where  $r$  is a power of a prime and  $t$  is an integer greater than 1. In this case  $\mathbb{F}_r$  is a subfield of index  $t$  in  $\mathbb{F}_q$ . We set

$$s = \frac{r^t - 1}{r - 1}$$

and we let  $\alpha$  be a generator of  $\mathbb{F}_q^*$ . It is straightforward to prove that  $\alpha^i \in \mathbb{F}_r$  if and only if  $s$  divides  $i$ , and furthermore that  $\alpha^s$  is a generator of  $\mathbb{F}_r$ .

**Lemma 5.** *Let  $q = r^t$ , where  $r$  is a power of a prime and  $t$  is an integer greater than 1, and let  $s = (r^t - 1)/(r - 1)$ . Let  $\alpha$  and  $\beta$  be generators of  $\mathbb{F}_q^*$ . Suppose that for some integers  $i$  and  $j$  we have*

$$\alpha^i + \beta^j = 1.$$

*Then  $s$  divides  $i$  if and only if  $s$  divides  $j$ .*

*Proof.* This follows from our observation above describing when  $\alpha^i$  is in  $\mathbb{F}_r$  and the obvious fact that, under our given hypothesis on  $\alpha$  and  $\beta$ ,  $\alpha^i \in \mathbb{F}_r$  if and only if  $\beta^j \in \mathbb{F}_r$ .  $\square$

Suppose as before that  $q = r^t$ ,  $s = (r^t - 1)/(r - 1)$ , and  $P$  is a Golomb-Costas array of order  $q - 2$  defined using generators  $\alpha$  and  $\beta$  of  $\mathbb{F}_q^*$ . Let  $\Omega$  be the set of coordinates  $(i, j)$  such that  $s$  divides  $i$  and  $P$  has a dot at the position  $(i, j)$ . Then as shown in Lemma 5,  $s$  also divides  $j$ . It follows that  $|\Omega| = r - 2$  and if  $(i, j) \in \Omega$ , we can write

$$(i, j) = (si', sj'),$$

where  $1 \leq i', j' \leq r - 2$ . Furthermore, if we set

$$\Omega' = \{(i', j') : (si', sj') \in \Omega\}$$

and take  $P'$  to be the Golomb-Costas array of order  $r - 2$  defined with respect to the generators  $\alpha^s$  and  $\beta^s$  of  $\mathbb{F}_r^*$ , it is straightforward to see that the elements of  $\Omega'$  are precisely the positions where  $P'$  has dots.

Thus within the Golomb-Costas array  $P$  of order  $q - 2$ , we can easily locate the array  $P'$  of order  $r - 2$  by identifying those positions in  $P$  belonging to  $\Omega$ . We may consider  $P'$  to be a substructure of  $P$ .

As we have remarked, a Costas array of order  $n$  defines a permutation of  $n$  objects. A natural question to ask is: when does the permutation defined by a Golomb-Costas array of order  $q - 2$  consist of a single cycle of length  $q - 2$ ? The experimental evidence suggests that this occurs very infrequently. Using the idea explained above, we can show that if the permutation of order  $q - 2$  defined by the Golomb process is a single cycle, then either  $q$  is a prime or  $q = 2^t$ , where  $t$  is a prime. We note that there exist examples of single cycles when  $q = 5$  and  $q = 8$  but there are none when  $q$  is a power of 3 or of 7.

#### REFERENCES

- [1] S. W. Golomb, *Algebraic constructions for Costas arrays*, J. Combinatorial Theory, Series A, **37** (1984), 13-21.
- [2] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, second edition. Springer-Verlag, Berlin-Heidelberg-New York, 1990.

MATHEMATICS DEPARTMENT, UNIVERSITY COLLEGE, BELFIELD, DUBLIN 4, IRELAND  
*E-mail address:* rod.gow@ucd.ie