

# On the parity populations of Welch-constructed Costas arrays

Konstantinos Drakakis  
School of Mathematics  
University of Edinburgh

Rod Gow  
Department of Mathematics  
University College Dublin

Scott Rickard  
Department of Electrical  
and Electronic Engineering  
University College Dublin

February 08, 2005

## Abstract

We prove that, in the case of Welch-constructed Costas arrays, the number of dots whose coordinates are both even (*ee*), both odd (*oo*), even and odd (*eo*), and odd and even (*oe*) are all equal if the prime  $p$  used has the property that  $p \bmod 4 = 1$ ; and that, if  $p \bmod 4 = 3$ , the relation between these 4 quantities can again be determined, and that it involves an unexpected appearance of class numbers.

**Keywords:** Costas arrays, Welch construction, class numbers, finite fields, parity

## 1 Introduction

Costas arrays appeared for the first time in the engineering literature [3, 4] in connection with optimal transmission patterns in SONARs and RADARs; shortly afterwards, though, they came to start a new, independent life in the mathematical literature [1, 2].

This work is firmly set within the realm of mathematics and presents some previously unknown parity properties of Welch-constructed Costas arrays. Due to space considerations we will have to assume that the reader is familiar with the algebraic definition of a field and the basic facts about finite (or Galois) fields, but all remaining relevant definitions and properties will be given below.

### 1.1 Basic definitions on Costas arrays

We start by defining what a Costas array is.

**Definition 1 (Costas array).** Let  $A$  be a permutation array of order  $n$ : that is,

$$A = [a_{ij}], \quad a_{ij} = \begin{cases} 1 & \text{iff } i = f(j) \\ 0 & \text{otherwise} \end{cases}, \quad i, j = 1, \dots, n$$

where  $f: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$  is a bijection.  $A$  will be a *Costas array* iff all vectors between 1s are distinct. It is as easy to think of the array as having dots instead of 1s and empty spaces instead of 0s.

The set of Costas arrays of a given order  $n$  is closed under the group of symmetries of the square: if a Costas array is flipped vertically or horizontally, or transposed, or undergoes any combination of these operations in any order, it remains a Costas array.

A mathematical method to construct Costas arrays is the *Welch construction* [1]:

**Theorem 1 (Welch construction  $W_1(p, g, c)$ ).** Let  $p$  be a prime and  $g$  a primitive root of the field  $\mathbb{F}(p)$ ; for  $c \in \{0, \dots, p-2\}$  constant, the permutation

$$f(i) = g^{i-1+c} \pmod{p}, \quad i = 1, \dots, p-1$$

corresponds to a Costas array of order  $p-1$ .

The horizontal and vertical flips of  $W_1(p, g, c)$  constructions are themselves  $W_1(p, g, c)$  constructions; their transpositions, however, are not. It is sometimes customary to refer to the former as *exponential* Welch arrays and to the latter as *logarithmic* Welch arrays.

### 1.2 Definition of parity populations

**Definition 2 (Parity populations).** For  $n \in \mathbb{N}$ , set  $R(n) = \{1, \dots, n\}$ ; for  $p$  prime, let  $A$  be the Costas array constructed by  $W_1(p, g, c)$ , and let  $S[W_1(p, g, c)] = \{(i, j) \in R(p-1) \times R(p-1) : a_{ij} = 1\}$ . The *parity populations* are defined as follows:

- $EE[A] = \{(i, j) \in S[A] : i \bmod 2 = j \bmod 2 = 0\}$ ,  
 $ee[A] = \#(EE[A])$ ;
- $OO[A] = \{(i, j) \in S[A] : i \bmod 2 = j \bmod 2 = 1\}$ ,  
 $oo[A] = \#(OO[A])$ ;
- $EO[A] = \{(i, j) \in S[A] : i \bmod 2 = 0, j \bmod 2 = 1\}$ ,  
 $eo[A] = \#(EO[A])$ ;
- $OE[A] = \{(i, j) \in S[A] : i \bmod 2 = 1, j \bmod 2 = 0\}$ ,  
 $oe[A] = \#(OE[A])$ .

All of these 4 parameters can be combined in the *parity vector* of  $A$ :  $\mathcal{P}[A] = (ee[A], oo[A], eo[A], oe[A])$ . We will be dropping the argument  $[A]$  when there is no danger of confusion.

### 1.3 Definitions on finite fields [6]

**Definition 3 (Quadratic residues and the Jacobi symbol).**

- $a \in \mathbb{F}(p)$  is a *quadratic residue* of  $p$  ( $QR(p)$ ) iff  $\exists x \in \mathbb{F}(p) : x^2 = a \pmod{p}$ ;
- the Jacobi symbol  $\left(\frac{i}{p}\right), i = 1, \dots, p-1$  equals 1 if  $i$  is a  $QR(p)$  and  $-1$  otherwise.

There are exactly  $\frac{p-1}{2}$   $QRs$  in  $\mathbb{F}(p)$  (they constitute half of its nonzero elements) and they form a subgroup of its multiplicative group.

**Definition 4 (Class number).** The *class number* of the ring of algebraic integers in the imaginary quadratic field  $\mathbb{Q}(\sqrt{-p})$  is the number of ideal classes in the ring; when  $p$  is prime,  $p \pmod{4} = 3$ , and  $p > 3$ , it is equal to

$$h(-p) = -\frac{1}{p} \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) i$$

In other words, it is the sum of all non- $QRs$  minus the sum of all  $QRs$  divided by  $p$ .

The reason for the mysterious negative sign in the argument of  $h$  is simply compatibility with the literature (the class number of some positive integers can be defined analogously, but we shall have no use of it).

### 1.4 A basic result on parity populations

In any permutation the values of the parity populations are constrained pairwise.

**Theorem 2.** For any permutation matrix  $A$  of order  $n$ ,  $oe = eo$  and  $oo = ee + n \pmod{2}$ .

*Proof.* Let  $E_1[A] = \{(i, j) \in S[A] : i \pmod{2} = 0\}$ ; then  $E_1 = EE \cup EO \Rightarrow |E_1| = ee + eo$ . Let also  $E_2[A] = \{(i, j) \in S[A] : j \pmod{2} = 0\}$ ; then  $E_2 = EE \cup OE \Rightarrow |E_2| = ee + oe$ . But  $|E_1| = |E_2| = \lfloor \frac{n}{2} \rfloor$ , hence  $oe = eo$ . Let now similarly  $O_1[A] = \{(i, j) \in S[A] : i \pmod{2} = 1\}$ ; it follows that  $O_1 = OE \cup OO \Rightarrow |O_1| = oe + oo$ . But  $|O_1| = |E_1| + n \pmod{2} \Rightarrow oo + oe = eo + ee + n \pmod{2} \Rightarrow oo = ee + n \pmod{2}$ .  $\square$

To sum up, the quantities  $ee, oo, oe, eo$  satisfy 3 linear equations:

- $ee + oo + eo + oe = n$ ;
- $eo = oe$ ;
- $oo = ee + n \pmod{2}$ ;

If we can find a fourth one, we can determine them uniquely. We will now proceed to show that in the special case of  $W_1(p, g, c)$  this can indeed be done; in this case, and for  $p > 2, n = p - 1$  even, so that  $oo = ee$ .

## 2 Results

### 2.1 The effect of $g$ and $c$ on the parity populations of $W_1(p, g, c)$

We will show first that  $g$  and  $c$  have no effect on the values of the pairs  $ee = oo$  and  $oe = eo$ , except perhaps swapping their roles.

**Theorem 3.**

- If  $A$  and  $A'$  are constructed by  $W_1(p, g, c)$  and  $W_1(p, g', c)$ , respectively, then  $\mathcal{P}[A] = \mathcal{P}[A']$ .
- If  $A_c$  and  $A_{c+1}$  are constructed by  $W_1(p, g, c)$  and  $W_1(p, g, c+1)$ , respectively, then  $ee[A_{c+1}] = oe[A_c]$ ,  $oe[A_{c+1}] = ee[A_c]$ ,  $eo[A_{c+1}] = oo[A_c]$ , and  $oo[A_{c+1}] = eo[A_c]$ ; hence, the equal pairs swap roles.
- If  $A$  is constructed by  $W_1(p, g, c)$ , then  $\mathcal{P}[A] = \mathcal{P}[A^T]$ ; hence, flipping around the diagonal does not affect the parity vector.

*Proof.*

- There exists  $1 \leq r \leq p-2$  relatively prime to  $p-1$  so that  $g' = g^r$ , since  $g$  is a primitive root; in particular,  $r$  is odd. Then,  $f'(i) = (g')^{i-1+c} \pmod{p} = g^{r(i-1+c)} \pmod{p} = g^{(ri-r+1+(r-1)c)-1+c} \pmod{p} = f((ri + (r-1)(c-1)) \pmod{(p-1)})$ ,  $i = 1, \dots, p-1$ . Now, since  $r-1$  and  $p-1$  are even,  $((ri + (r-1)(c-1)) \pmod{(p-1)}) \pmod{2} = (ri + (r-1)(c-1)) \pmod{2} = ri \pmod{2} = i \pmod{2}$ .
- Imagine that  $f_c$  is represented by two bands of values, the top band being  $1, \dots, p-1$  and the bottom band being  $f_c(1), \dots, f_c(p-1)$ , so that  $i$  is immediately above  $f_c(i)$ ,  $i = 1, \dots, p-1$ . Increasing  $c$  by 1 results to a cyclic shift of the top band to the right by one position, so that the values of  $f_c$  that were under even indices are now found under odd indices and vice versa.
- In terms of the same two bands representation as above, transposition implies swapping the bands; the result is that  $EE[A] = EE[A^T]$ ,  $OO[A] = OO[A^T]$ ,  $EO[A] = OE[A^T]$ , and  $OE[A] = EO[A^T]$ . But  $eo[A] = oe[A]$ , so that  $\mathcal{P}[A] = \mathcal{P}[A^T]$ .  $\square$

To sum up, the set  $\{ee[A], eo[A]\}$ , when  $A$  is constructed by  $W_1(p, g, c)$ , is uniquely determined by  $p$ . We will carry out the computation below; the case  $p \bmod 4 = 1$  is quite simple, as it involves exclusively elementary number theory; the case  $p \bmod 4 = 3$  is not as simple, though, and here we will need the quite advanced concept of class numbers.

## 2.2 The case $p \bmod 4 = 1$

**Theorem 4.** *If  $A$  is constructed by  $W_1(p, g, 0)$  where  $p \bmod 4 = 1$ , then  $ee = oo = oe = eo$ .*

*Proof.* Assume that  $m$  is the biggest exponent for which  $2^m | p - 1$ ; necessarily  $m \geq 2$ . Divide  $\{1, \dots, p - 1\}$  into  $\frac{p-1}{2^m}$  groups of  $2^m$  (consecutive) numbers each: the  $k$ th group,  $k = 1, \dots, \frac{p-1}{2^m}$ , contains the numbers  $i_{l,k} = l + (k-1)\frac{p-1}{2^m}$ ,  $l = 1, \dots, \frac{p-1}{2^m}$ . Set now  $x_{l,k} = g^{i_{l,k}-1+c} \bmod p$ ,  $y = g^{\frac{p-1}{2^m}} \bmod p$ , and note that  $y^{2^{m-1}} = g^{\frac{p-1}{2}} \bmod p = -1 \bmod p$ ; in other words, in this type of finite field  $-1$  is a square.

Notice further that  $x_{l,k} + x_{l+2^{m-1},k} = g^{l-1+(k-1)\frac{p-1}{2^m}} (y^{2^{m-1}} + 1) \bmod p = 0 \bmod p$ , so that  $x_{l,k} + x_{l+2^{m-1},k} = p$ , for  $l = 1, \dots, 2^{m-1}$ . In other words,  $i_{l,k}$  and  $i_{l+2^{m-1},k}$  have the same parity, as  $2^{m-1}$  is even, but  $x_{l,k}$  and  $x_{l+2^{m-1},k}$  have opposite parities, as they sum to an odd number.

Since every group contains  $2^m$  numbers, which is a multiple of 4, there will be as many instances of  $i_{l,k}$  odd as even in each group; hence, every possible combination of parities of  $i$  and  $x$  will appear the same number of times in each group, and consequently overall.  $\square$

## 2.3 The case $p \bmod 4 = 3$ and the general approach

Suppose that we want to determine the set  $EO[A]$ , where  $A$  has been constructed by  $W_1(p, g, 0)$ ; the members of  $EO[A]$  will be the pairs  $(f(i), i)$ ,  $i = 1, \dots, p - 1$  for which  $i \bmod 2 = 1$  and  $f(i) \bmod 2 = 0$ , or equivalently those pairs for which  $\exists 0 \leq u, v \leq \frac{p-1}{2} : i = 2u + 1$  and  $f(2u + 1) = g^{2u} \bmod p = 2v$ . In other words, what we are looking for is the set of “even QRs” of  $\mathbb{F}(p)$ .

It may not be immediately apparent how unnatural the question we ask is: however, the elements of  $\mathbb{F}(p)$  are not integers but equivalence classes of integers under the modulo  $p$  operation, and the parity of the equivalence class is not well defined. For example,  $7^2 = 3 \bmod 11$ , so that the equivalence class of 3 is a QR(11); 3 itself is odd, whereas  $3 + 11 = 14$ , which is another member of the equivalence class of 3, is even. What we really mean then is that we

want to examine the parity of a specific representative of the equivalence class, and more precisely of the smallest positive representative.

As a result, we have mixed two different worlds in our question: field multiplication (the square) along with ordinary integer multiplication (by 2). Most textbooks on Algebra and Number Theory do not discuss such issues, and for a good reason: answers to such questions are rare, and, when they exist, more often than not extremely esoteric. Our question falls in this category.

A first step towards the answer is to distinguish between the cases when 2 is a QR( $p$ ):

**Theorem 5.** *Let  $p$  be a prime:*

- If  $p \equiv 3 \pmod{8}$ , 2 is not a QR( $p$ );
- If  $p \equiv 7 \pmod{8}$ , 2 is a QR( $p$ ).

*Proof.* See [6], p. 337.  $\square$

Let us now set:

$$\Omega_1 = \{z \in \mathbb{Z} : 0 < z < \frac{p}{2} \text{ and } z \text{ is a QR}(p)\}$$

$$\Omega_2 = \{z \in \mathbb{Z} : 0 < z < \frac{p}{2} \text{ and } z \text{ is not a QR}(p)\}$$

and also  $V = |\Omega_1|$  and  $N = |\Omega_2|$ .

- Suppose that  $p \equiv 7 \pmod{8}$ ; then 2 is a QR( $p$ ), so that, if  $z \in \Omega_1$ ,  $2z$  is an even QR satisfying  $0 < 2z < p$ . Conversely, any even QR  $w$  satisfying  $0 < w < p$  is expressible as  $w = 2w'$ , where  $w' \in \Omega_1$ . Thus the number of even QRs in  $R(p - 1)$  is  $V$ . Similarly, if  $z \in \Omega_2$ ,  $2z$  is an even non-QR and we deduce similarly that the number of even non-QRs in  $R(p - 1)$  is  $N$ . Thus:

$$eo[A] - ee[A] = V - N$$

- Suppose that  $p \equiv 3 \pmod{8}$ ; following a similar reasoning, we obtain:

$$eo[A] - ee[A] = N - V$$

These differences can be further evaluated by means of  $h$  (see Dfn. 4):

**Theorem 6.** *Let  $A$  be constructed by  $W_1(p, g, 0)$ .*

- If  $p \bmod 8 = 3$ , then  $eo[A] - ee[A] = -3h(-p)$ .
- If  $p \bmod 8 = 7$ , then  $eo[A] - ee[A] = h(-p)$ .

*Proof.* It is an immediate consequence of one of Dirichlet’s classic 1839 formulas for the class number; see [6], Thm. 4, p. 346, as well as [5] and references therein for more details.  $\square$

This theorem provides, along with the 3 equations of section 1.4 the last equation we need for the determination of the parity populations.

**Corollary 1.** *Let  $A$  be constructed by  $W_1(p, g, 0)$ .*

- If  $p \bmod 8 = 3$ , then

$$\begin{aligned} eo[A] = oe[A] &= \frac{1}{2} \left( \frac{p-1}{2} - 3h(-p) \right) \\ oo[A] = ee[A] &= \frac{1}{2} \left( \frac{p-1}{2} + 3h(-p) \right) \end{aligned}$$

- If  $p \bmod 8 = 7$ , then

$$\begin{aligned} eo[A] = oe[A] &= \frac{1}{2} \left( \frac{p-1}{2} + h(-p) \right) \\ oo[A] = ee[A] &= \frac{1}{2} \left( \frac{p-1}{2} - h(-p) \right) \end{aligned}$$

It can be shown that  $h(-p) = 1$  whenever  $p \bmod 4 = 1$  and that, in this case,  $oe[A] - ee[A] = h(-p) - 1 = 0$ ; in other words, class numbers can be used for that case as well, but we saw that a direct much simpler computation is possible.

### 3 Discussion and motivation

We computed the parity populations of the  $W(p, g, 0)$  construction for all primes  $p > 3$ ; the cases  $p = 2$  and  $p = 3$  are trivial. The computation for primes such that  $p \bmod 4 = 1$  was simple, whereas for primes such that  $p \bmod 4 = 3$  it involved the advanced notion of the class number and it had to be further broken into 2 subcases.

Why were we interested in such a computation in the first place? It is certainly legitimate from the point of view of pure mathematics, of course, but does it have any practical implications on the quest for new Costas arrays? It is our hope that it does, by helping us eliminate permutations that could not possibly have the Costas property.

A search through the database of known Costas arrays shows that the parity vector takes very few values for a given order; if it is also true that some of the values are exclusively due to the mathematical (Golomb and Welch) constructions (the corresponding computation for the Golomb construction can be found in [7]), we can reduce the range of the vector's values for non-mathematically constructed Costas arrays even further, speeding up considerably the (brute-force) search for such Costas arrays, by seeking them exclusively among permutations having the admissible parity vectors.

### References

- [1] S. W. Golomb. *Algebraic Constructions for Costas Arrays* Journal of Combinatorial Theory, Series A 37, 13-21 (1984)
- [2] S. W. Golomb, H. Taylor. *Constructions and Properties of Costas Arrays* Proceedings of the IEEE, 72(9), September 1984
- [3] J. P. Costas. *Medium constrains on sonar design and performance* Technical Report Class 1 Rep. R65EMH33, GE Co.
- [4] J. P. Costas. *A study of detection waveforms having nearly ideal range-doppler ambiguity properties* Proceedings of the IEEE, 72(8):996-1009, August 1984
- [5] T. W. Cuisick. *Properties of the  $x^2 \bmod N$  Pseudo-random Number Generator* IEEE Transactions on Information Theory, Vol. 41, No. 4, July 1995
- [6] Z. I. Borevich, I. R. Shafarevich. *Number Theory* New York: Academic Press, 1966
- [7] R. Gow. *A regularity property of Golomb-Costas arrays* (To appear in CISS 2006)