

# On some properties of Costas arrays generated via finite fields

Konstantinos Drakakis  
School of Mathematics  
University of Edinburgh

Rod Gow  
Department of Mathematics  
University College Dublin

Liam O'Carroll  
School of Mathematics  
University of Edinburgh

February 08, 2005

## Abstract

We prove that Welch-constructed Costas arrays are in general not symmetric and that the Golomb-constructed ones are symmetric in two cases only, namely the Lempel one and a (rare) second one leading to the construction of dense Golomb rulers. Finally, we look into the (hard) problem of the number of fixed points of a Welch-constructed Costas array and formulate a conjecture.

**Keywords:** Costas arrays, Golomb rulers, Golomb and Welch constructions, finite fields

## 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, it was realized that some fundamental questions about their properties (and even about their very existence) should be formulated within the framework of Algebra and Combinatorics, and thus they came to start a new, independent life in the mathematical literature [1, 2, 5, 6, 7, 8].

This work is firmly set within the realm of mathematics and presents some previously unknown properties of Costas arrays generated via finite fields. 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.

## 2 Definitions

**Definition 1 (Costas array).** A *Costas array*  $A = [a_{ij}]$  of order  $n \in \mathbb{N}$  is a square  $n \times n$  array whose elements are equal to either 0 or 1 so that:

- Exactly one 1 appears per row and column (the remaining elements being 0); and

- Assuming that the elements that are equal to 1 are  $a_{f(i),i}$ ,  $i = 1, \dots, n$ , the vectors  $(i_1 - i_2, f(i_1) - f(i_2))$ ,  $i_1, i_2 = 1, \dots, n$ ,  $i_1 > i_2$ , are all distinct.

Thus  $f : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$  is actually a permutation, i.e. a bijection; in what follows, we will make no distinction between a Costas array and its corresponding permutation.

Equivalently, consider the (multi)sets  $S_k = \{f(i+k) - f(i) \mid i = 1, \dots, n-k\}$ ,  $k = 1, \dots, n-1$ ;  $A$  is Costas iff all the  $S_k$  are sets, i.e. none contains a duplicate entry.

A Costas array is *symmetric* iff  $A^T = A$ ; in terms of its permutation, this is equivalent to  $f(f(i)) = i$ ,  $i = 1, \dots, n$ .

A element equal to 1 lies on the main diagonal of  $A$  iff  $f(i) = i$  for some  $i$ , that is iff  $i$  is a fixed point of the corresponding permutation.

**Definition 2 (Golomb ruler).** An increasing sequence of integers  $f(i)$ ,  $i = 1, \dots, n$ , such that the (multi)set  $\{f(i) - f(j) \mid i > j, i, j = 1, \dots, n\}$  is actually a set (it does not contain duplicate entries) is a *Golomb ruler*. Without loss of generality  $f(1) = 0$ , in which case  $f(n)$  is the *length* of the ruler.

It is easy to see that the positions of the elements equal to 1 on the diagonal of a Costas array (or, equivalently, the sequence of fixed elements of its corresponding permutation) define a Golomb ruler. An important problem is the determination of the minimal  $f(n)$  for a given  $n$  for which Golomb rulers exist.

There are two known algorithms to construct a Costas array: the Golomb construction and the Welch construction [1, 2]. Both are defined within the framework of finite fields [13, 14, 15] and make use of the *primitive roots* of a finite field [8, 9, 10, 11].

**Definition 3.** The nonzero elements of a finite field  $\mathbb{F}$  form a multiplicative cyclic group, i.e. they can be written as  $g^i$ ,  $i = 0, \dots, q-2$ , where  $g \in \mathbb{F}$ ; the elements  $g$  of  $\mathbb{F}$  with this property are called the *primitive roots* of  $\mathbb{F}$ .

**Theorem 1 (Welch construction  $W_1(p, g, c)$ ).** Let  $p$  be a prime,  $c \in \{0, \dots, p-2\}$ , and consider the sequence

$f(i) = g^{i-1+c} \pmod p$ ,  $i = 1, \dots, p-1$ , where  $g$  is a primitive root of the Galois field  $\mathbb{F}(p)$ ; then  $f$  corresponds to a Costas array.

**Theorem 2 (Golomb construction  $G_2(p, n, a, b)$ ).** Let  $p$  be a prime, and consider the sequence  $f$  defined by the equation  $a^i + b^{f(i)} = 1$ ,  $i = 1, \dots, q-2$ , where  $q = p^n$  for some  $n \in \mathbb{N}$  and  $a, b$  are primitive roots of  $\mathbb{F}(q)$ , not necessarily distinct; then  $f$  corresponds to a Costas array.

The proofs are omitted [1, 2].

**Theorem 3.** Let  $m, n \in \mathbb{N}$ ,  $m < n$ , and let  $p$  be a prime.

- $\mathbb{F}(p^m) \subset \mathbb{F}(p^n)$ , in the sense that the field  $\mathbb{F}(p^n)$  contains a unique subfield isomorphic to  $\mathbb{F}(p^m)$  iff  $m$  divides  $n$ .
- $\forall x \in \mathbb{F}(p^n)$ ,  $x^{p^n} = x$ .
- Let  $x \in \mathbb{F}(p^n)$  and suppose that  $m$  divides  $n$  so that  $\mathbb{F}(p^m) \subset \mathbb{F}(p^n)$ ; then  $x \in \mathbb{F}(p^m)$  iff  $x^{p^m} = x$ .
- A polynomial  $P(x)$  of degree  $d$  over  $\mathbb{F}(p^n)$  can have at most  $d$  roots in it.
- $\binom{r}{i} \equiv 0 \pmod p$ ,  $i = 1, \dots, r-1 \Leftrightarrow \exists m \in \mathbb{N} : r = p^m$ .

The proof is omitted [13, 14, 15].

### 3 Symmetry of Welch constructions

**Theorem 4.** A Costas array constructed by  $W_1(p, g, c)$  for  $p$  prime and  $p > 5$  cannot be symmetric.

*Proof.* If a  $W_1(p, g, c)$ -constructed array is symmetric, then, according to Def. 1 and Thm. 1:

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

Now  $i$  and  $p-i$  have the same range, so we can substitute to obtain

$$\begin{aligned} \forall i \in \{1, \dots, p-1\}, \\ p-i = g^{c-1} g^{g^{p-i-1+c}} \pmod p \pmod p. \end{aligned} \quad (2)$$

By adding the two formulas, we obtain further that

$$\begin{aligned} g^{c-1} g^{g^{i-1+c}} \pmod p + g^{c-1} g^{g^{p-i-1+c}} \pmod p &\equiv \\ &\equiv p \equiv 0 \pmod p \end{aligned} \quad (3)$$

and since the common factor  $g^{-1+c}$  is not equivalent to 0, we can cancel it, obtaining:

$$\begin{aligned} g^{g^{i-1+c}} \pmod p + g^{g^{p-i-1+c}} \pmod p &\equiv 0 \pmod p \Rightarrow \\ g^{g^{i-1+c}} \pmod p &\equiv -g^{g^{p-i-1+c}} \pmod p \pmod p \Leftrightarrow \\ g^{g^{i-1+c}} \pmod p - g^{g^{p-i-1+c}} \pmod p &\equiv -1 \pmod p. \end{aligned} \quad (4)$$

But  $-1 \equiv g^{\frac{p-1}{2}} \pmod p$  for any primitive root  $g$ , so finally

$$g^{g^{i-1+c}} \pmod p - g^{g^{p-i-1+c}} \pmod p \equiv g^{\frac{p-1}{2}} \pmod p. \quad (5)$$

It follows that

$$\begin{aligned} g^{i-1+c} \pmod p - g^{p-i-1+c} \pmod p &\equiv \\ &\equiv \frac{p-1}{2} \pmod{(p-1)} \end{aligned} \quad (6)$$

because, according to Fermat's Little Theorem,  $g^{p-1} \equiv 1 \pmod p$ , hence exponents are unique  $\pmod{(p-1)}$ . But if the difference of two positive integers less than  $p$  is equal to  $\frac{p-1}{2}$  modulo  $p-1$ , it will have to be equal to either  $\frac{p-1}{2}$  or  $\frac{p-1}{2} - (p-1) = -\frac{p-1}{2}$ , so (6) becomes:

$$g^{i-1+c} \pmod p - g^{p-i-1+c} \pmod p = \pm \frac{p-1}{2} \quad (7)$$

and taking  $\pmod p$  on both sides, we obtain:

$$\begin{aligned} g^{i-1+c} - g^{p-i-1+c} &\equiv \frac{p-1}{2} \text{ or } p - \frac{p-1}{2} \pmod p \equiv \\ &\equiv \frac{p \pm 1}{2} \pmod p. \end{aligned} \quad (8)$$

Multiplying both sides by  $g^{i+1-c} \pmod p$  and setting  $x = g^i$ , we finally obtain the equation:

$$x^2 - g \equiv x g^{1-c} \frac{p \pm 1}{2} \pmod p, \quad x = 1, \dots, p-1, \quad (9)$$

since  $g^p \equiv g \pmod p$ . But a quadratic equation over a field can have at most 2 roots, so the pair of quadratics in (9) can have at most 4 roots. Hence, if a  $W_1(p, g, c)$ -constructed array is to be symmetric, it is necessary that  $p-1 \leq 4 \Leftrightarrow p \leq 5$ . Indeed, for  $p = 5$ ,  $c = 0$ ,  $g = 2$ , we obtain the permutation 1243, which is symmetric:  $x = 1$  and  $x = 3$  satisfy (9) with “-”, whereas  $x = 2$  and  $x = 4$  satisfy (9) with “+”.  $\square$

### 4 Symmetry of Golomb constructions

**Theorem 5.** A Costas array constructed by  $G_2(p, n, a, b)$  is symmetric iff one of the following conditions holds for the relevant  $a$  and  $b$  used:

- $a = b$  (this special case is also known as the Lempel construction), in which case the corresponding permutation has exactly 1 fixed point, unless  $p = 2$  when no fixed point exists;
- $q = r^2$ ,  $b = a^r$ , in which case the corresponding permutation has exactly  $r$  fixed points.

*Proof.* We break the proof into steps, in order to make it clearer:

### Two possibilities for symmetric arrays

From Thm. 2 and Def. 1 we obtain the pair of equations  $a^i + b^{f(i)} = 1 = a^{f(i)} + b^i$ , which we can further simplify. As  $a$  is a primitive root, there exists an  $r$ ,  $1 \leq r \leq q-2$ , such that  $b = a^r$ , so that  $a^i + a^{rf(i)} = 1 = a^{f(i)} + a^{ri}$ ,  $i = 1, \dots, q-2$ . Then  $a^{f(i)} = 1 - a^{ri}$  and  $a^i + (1 - a^{ri})^r = 1$ ,  $i = 1, \dots, q-2$ . Setting  $x = a^i$  and observing that the resulting equation remains true for  $x = 0$  and  $x = 1$ , we obtain:

$$x + (1 - x^r)^r = 1, \quad \forall x \in \mathbb{F}(q). \quad (10)$$

But since  $b = a^r$  is itself a primitive root,  $r$  must be relatively prime to  $q-1$ ; expanding the binomial term in (10), we obtain  $r+1$  powers of  $x$ , namely  $(lr) \bmod (q-1)$ ,  $l = 0, \dots, r$ , and, since  $r \leq q-2$  and relatively prime to  $q-1$ , these powers modulo  $q-1$  are all distinct:

$$x + \sum_{l=0}^r \binom{r}{l} (-1)^l x^{rl} = 1, \quad \forall x \in \mathbb{F}(q). \quad (11)$$

In particular,  $l = 0$  yields a power equal to  $x^0 = 1$  with a coefficient of 1, which cancels the 1 of the RHS of (11):

$$x + \sum_{l=1}^r \binom{r}{l} (-1)^l x^{rl} = 0, \quad \forall x \in \mathbb{F}(q). \quad (12)$$

We end up with a polynomial of degree at most  $q-2$  and  $q$  roots, hence this polynomial needs to be identically equal to 0; in particular, the term corresponding to  $l = r$ , namely  $(-1)^r x^{r^2}$ , must be canceled by something: this something cannot be another term of the binomial expansion, for, as we saw above, all powers of the expansion are distinct modulo  $q-1$ . Therefore, it has to be canceled by  $x$ :

$$(-1)^r x^{r^2} + x \equiv 0 \Leftrightarrow x = (-1)^{r+1} x^{r^2}. \quad (13)$$

If  $p \neq 2$ ,  $r$  is necessarily odd, hence  $(-1)^{r+1} = 1$ ; if  $p = 2$ ,  $-1 = 1$  and we end up with the same result; hence, in all cases, (13) becomes:

$$x^{r^2} \equiv x, \quad \text{with } 1 \leq r \leq q-2. \quad (14)$$

But the remaining coefficients in (12) must also be 0, so the relations  $\binom{r}{l} \equiv 0 \pmod{p}$ ,  $l = 1, \dots, r-1$  must hold;

this implies that  $r = p^s$  for some  $s \in \mathbb{N}$ , according to Thm. 3.

Since (14) holds for all  $x \in \mathbb{F}(q)$ , it follows that  $\mathbb{F}(q = p^n) \subset \mathbb{F}(r^2 = p^{2s})$ , so that  $n$  divides  $2s$ , according to Thm. 3; but, as  $1 \leq r \leq q-2$ ,  $s < n$  must hold. Therefore, either  $2s = 0 \Leftrightarrow s = 0 \Leftrightarrow r = 1$ , or  $2s = n \Leftrightarrow r^2 = q$ . Direct substitution in (10) verifies that the polynomial indeed becomes identically 0 in both cases.

### Fixed points for $r = 1$

Now  $i$  will be a fixed point iff  $i = f(i)$ . If  $r = 1$  we get  $a = b$  and therefore  $i$  must satisfy  $a^i + a^i = 1$ ; if  $p = 2$  this yields the impossible  $0 = 1$  and no fixed points exist, but, otherwise, we get  $2a^i = 1 \Leftrightarrow i = \log_a(2^{-1})$ , so that  $i$  is unique.

### Fixed points for $q = r^2$

If  $q = r^2$ , things are rather different: now we need  $a^i + a^{ri} = 1$ , so that  $i = \log_a(x)$  where  $x^r + x - 1 = 0$ . Setting  $P(x) = x^r + x - 1$ , we find that  $P'(x) = rx^{r-1} + 1 = 1$ , and therefore all roots of  $P(x)$  are distinct in  $\mathbb{F}(q)$ . Set  $r = p^m$  so that  $q = p^{2m}$ , and  $T(x) = x^r + x$ , so that  $P(x) = 0$  becomes  $T(x) = 1$ .

- $T$  is a linear transformation from  $\mathbb{F}(q)$  to  $\mathbb{F}(q)$ , when  $\mathbb{F}(q)$  is viewed as a linear space over the field  $\mathbb{F}(r)$  (hence of dimension 2):  $T(x+y) = (x+y)^r + x+y = x^r + y^r + x+y = T(x) + T(y)$ , by Thm. 3; moreover  $T(cx) = cT(x)$  when  $c \in \mathbb{F}(r)$ ,  $x \in \mathbb{F}(q)$ :  $T(cx) = (cx)^r + cx = c^r x^r + cx = c(x^r + x) = T(cx)$ , as  $c \in \mathbb{F}(r)$  means that  $c^r = c$ .
- If  $p > 2$ ,  $x_0 = \frac{p+1}{2}$  is the only root of  $T(x) = 1$  lying in  $\mathbb{F}(p)$ ; if  $p = 2$ , no such root exists: if  $x \in \mathbb{F}(p)$ ,  $x^p = x$ , so that  $x^r \equiv x^{p^m} \pmod{p-1} \equiv x^{(p \bmod (p-1))^m} \equiv x^{1^m} \equiv x$ , whence  $P(x) = 0$  is really  $x + x - 1 = 0 \pmod{p} \Leftrightarrow 2x = 1 \pmod{p}$  if  $p > 2$  and  $0 = 1 \pmod{2}$  if  $p = 2$ . This proves that there is a unique root for  $p > 2$  and we can see that it is  $x_0$  by direct substitution. As  $\mathbb{F}(p) \subset \mathbb{F}(q)$ ,  $x_0$  is still a root of  $T(x) = 1$  in  $\mathbb{F}(q)$ .
- The transformation  $\phi : \mathbb{F}(q) \rightarrow \mathbb{F}(q)$ , where  $\phi(x) = x^p$  is a homomorphism;  $\phi^s(y) = y$  iff  $y \in \mathbb{F}(p^s)$ : for  $\phi^s(y) = y^{p^s} = y$  if  $y \in \mathbb{F}(p^s)$ , and since the equation has degree  $p^s$  and already  $p^s$  roots, it can have no other. As for the homomorphism property, it is immediate that  $(xy)^p = x^p y^p$ , and also  $(x+y)^p = x^p + y^p$ . (In this proof, repeated use was made of Thm. 3).
- $\dim(\text{Ker}[T]) = 1 \Leftrightarrow |\text{Ker}[T]| = r$ :
  - If  $p = 2$  and  $x \in \mathbb{F}(r)$ , it follows that  $T(x) = x^r + x = x + x = 0$ ; moreover, since  $T(x)$  is a polynomial of degree  $r$ , it can have at most  $r$

roots in  $\mathbb{F}(r^2)$  (by Thm. 3). Hence,  $\text{Ker}[T] = \mathbb{F}(r) \Rightarrow \dim(\text{Ker}[T]) = 1$ .

- If  $p > 2$ , we find  $\dim(\text{Im}[T])$  instead, and then use the Rank-Nullity Theorem:  $\dim(\text{Im}[T]) + \dim(\text{Ker}[T]) = \dim(\mathbb{F}(r^2)) = 2$ . First we show that  $\text{Im}[T] = \mathbb{F}(r)$ :

- \* Let  $w \in \text{Im}[T]$ ;  $\exists x \in \mathbb{F}(r^2) : \phi^m(x) + x = w \Rightarrow \phi^m(w) = \phi^m(\phi^m(x) + x) = \phi^{2m}(x) + \phi^m(x) = \phi^m(x) + x = w$ , so that  $w \in \mathbb{F}(r)$  (by Thm. 3).
- \* Let  $w \in \mathbb{F}(r)$ ; then  $T(2^{-1}w) = \phi^m(2^{-1}w) + 2^{-1}w = 2(2^{-1}w) = w$ , so that  $w \in \text{Im}[T]$ .

It follows that  $\dim(\text{Im}[T]) = \dim(\mathbb{F}(r)) = 1$ , hence  $\dim(\text{Ker}[T]) = 1$ .

We have now shown that in all cases  $\dim(\text{Im}[T]) = 1 = \dim(\text{Ker}[T])$ , so that  $|\text{Ker}[T]| = r$ . Set  $K = \text{Ker}[T]$  and consider the equivalence classes (blocks)  $X = x + K$ ,  $x \in \mathbb{F}(r^2)$ .

- $T(x_1) = T(x_2) \Leftrightarrow x_1 - x_2 \in K$ :  $T(x_1) = T(x_2) \Leftrightarrow T(x_1 - x_2) = 0 \Leftrightarrow x_1 - x_2 \in K$ . Hence it makes sense to define  $T(X) = T(x)$  for any  $x \in X$ , and the new map is still linear on the quotient space  $\mathbb{F}(r^2)/\mathbb{F}(r)$  and has the same image.
- $T(X) = 1$  has a unique solution: there are exactly  $r^2/r = r$   $X$ s and exactly  $r$  possible values of  $T(X)$ , and we saw that no two different  $X$ s can lead to the same value. Furthermore,  $(T(X))^r = (X^r + X)^r = X^{2r} + X^r = X^r + X = T(X)$  so that  $T(X) \in \mathbb{F}(r)$ , by Thm. 3. This means that  $T(X) = 1$  has a unique root, so that  $T(x) = 1$  has  $r$  roots.

The argument above shows that if  $p > 2$ , the roots of  $T(x)=1$  are  $x = \frac{p+1}{2} + y$ ,  $y \in \mathbb{F}(r^2)/\mathbb{F}(r)$ ; and if  $p = 2$ , that they are of the form  $x = h + y$ ,  $y \in \mathbb{F}(r)$ , for some  $h \in \mathbb{F}(r^2)/\mathbb{F}(r)$ .  $\square$

**Corollary 1.** *There exists a Golomb ruler of  $p^m$  integers whose length is at most  $p^{2m} - 2$ ; it corresponds to the main diagonal of a  $G_2(p, 2m, a, a^{p^m})$ -constructed Costas array.*

Note that the sufficiency of the two conditions for the symmetry of the  $G_2(p, n, a, b)$  construction has already been proved (see [2], Section III.F); the structure of our proof, however, permitted us to show additionally the necessity of these two conditions.

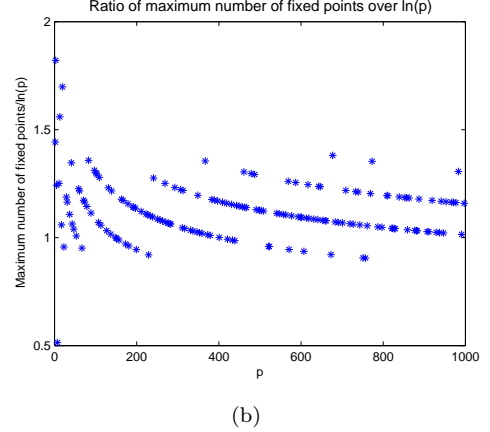
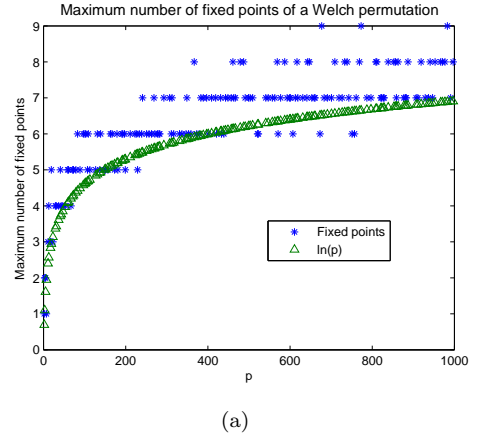


Figure 1: Maximum number of fixed points of a  $W_1(p, g, c)$ -constructed permutation versus  $\ln(p)$ ; the ratio of the two quantities is close to 1, and a linear fit actually gives for the ratio a constant of 1.15 and a first order term practically 0, but even simple inspection reveals that  $\ln(p)$  is a good match.

## 5 Fixed points of Welch constructions

The fixed points of a  $W_1(p, g, c)$ -constructed permutation are given as the solutions of the equation:

$$i \equiv g^{i-1+c} \pmod{p} \text{ for } i \in \{1, \dots, p-1\}. \quad (15)$$

We don't know of any algorithm to obtain its solution, except exhaustive search on the values of  $i$ ; such a search for all primes up to 1000 shows that the maximum number of fixed points as a function of  $p$  behaves asymptotically as  $O(\ln(p))$ .

## 6 Discussion

This work determines the conditions under which the Golomb and Welch constructions of Costas arrays lead to

symmetric arrays; it also shows that the Golomb construction is symmetric not only in the obvious (Lempel) special case of equal primitive roots, but also in another case, which is rarer but far more interesting, as it leads to the construction of reasonably “dense” Golomb rulers.

Incidentally, the proofs presented dispel the illusion held by many, even those expert on Costas arrays, that the Welch construction is a very tame and simple one, while the Golomb construction is exotic and complicated; the reality is just the opposite, as the Golomb construction is easy to manipulate algebraically, whereas the Welch construction is essentially transcendental.

As possible future work, we propose to investigate the number of fixed points of a Golomb or a Welch construction; for the latter, we offer evidence to support the conjecture that the maximum number of fixed points grows as  $O(\ln(p))$ .

## 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] H. Taylor. *Non-attacking Rooks with distinct differences* EE Systems, University of Southern California, Tech. Rep. CSI-84-03-2
- [6] T. Etzion, S. W. Golomb, H. Taylor. *Tuscan-k squares* Advances in Applied Mathematics, 10 (1989), pp. 164-174
- [7] S. W. Golomb, T. Etzion, H. Taylor. *Polygonal path constructions for Tuscan-k squares* Ars Combinatorica, 30, 1990, pp. 97-140
- [8] O. Moreno. *On primitive elements of trace equal to 1 in  $GF(2^m)$* , Discrete Mathematics 41, No. 1 (1982), pp.53-56
- [9] M. Szalay. *On the distribution of primitive roots of a prime* J. Number Theory, vol. 7, no. 2, pp. 184-188, May 1975
- [10] E. Vegh. *A note on the distribution of the primitive roots of a prime* J. Number Theory, vol. 3, pp. 13-18, 1971
- [11] J. Johnson. *On the distribution of powers in finite fields* J. Reine Angew. Math., vol. 251, pp. 10-19 (Crelles J.), 1971
- [12] S. Golomb. *Obtaining specified irreducible polynomials over finite fields* SIAM J. Algebra Discrete Math. 1, No. 4 (1980), pp. 411-418
- [13] M. Artin. *Algebra* Prentice Hall, 1991
- [14] G. Birkhoff, S. MacLane. *A Survey of Modern Algebra (Revised Edition)* Macmillan, 1953
- [15] E. Artin. *Galois Theory* Dover, 1998