Discrete Mathematics 309 (2009) 2559–2563

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Note

On the symmetry of Welch- and Golomb-constructed Costas arrays

Konstantinos Drakakis [a,*,1], Rod Gow [a,1], Liam O'Carroll [b]

[a] UCD CASL, University College Dublin, Belfield, Dublin 4, Ireland

[b] School of Mathematics, University of Edinburgh, JCMB, KB, Mayfield Road, Edinburgh EH9 3JZ, UK

ARTICLE INFO

Article history:
Received 17 January 2007
Received in revised form 26 April 2008
Accepted 28 April 2008
Available online 5 June 2008

Keywords:
Costas arrays
Golomb rulers
Golomb and Welch constructions
Finite fields

ABSTRACT

We prove that Welch Costas arrays are in general not symmetric and that there exist two special families of symmetric Golomb Costas arrays: one is the well-known Lempel family, while the other, although less well known, leads actually to the construction of dense Golomb rulers.

1. Introduction

Costas arrays appeared for the first time in the engineering literature [5,6] 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 [9,12,16,8,11,14]. This work, firmly set within the realm of mathematics, is concerned with the conditions under which algebraically constructed (namely Golomb and Welch) Costas arrays are symmetric, as well as with some of the properties of these symmetric arrays.

2. Definitions

Definition 1 (*Costas Permutation/Array*). Let $[n] := \{1, \ldots, n\}$, $n \in \mathbb{N}$ and consider a bijection $f : [n] \to [n]$; f is a Costas permutation iff

$$\forall i, j, k \quad \text{such that } 1 \le i, j, i+k, j+k \le n : f(i+k) - f(i) = f(j+k) - f(j) \Rightarrow i = j \text{ or } k = 0.$$

A Costas array A^f is the permutation array corresponding to a Costas permutation f, so that the jth element of the permutation is the position of the (unique) 1 in the jth column of the array, $j \in [n]$, counting from top to bottom in the usual array convention: $f(i) = j \Leftrightarrow a^f_{j,i} = 1$. It is customary to refer to (and denote) the 1's of a permutation array as "dots" and to 0's as "blanks".

The terms "Costas array" and "Costas permutation" will be used interchangeably; the superscript f in A^f is omitted when there is no danger of confusion.

* Corresponding author.
E-mail addresses: Konstantinos.Drakakis@ucd.ie (K. Drakakis), Rod.Gow@ucd.ie (R. Gow), L.O'Carroll@ed.ac.uk (L. O'Carroll).
[1] The author is also affiliated with the School of Mathematics, University College Dublin, Ireland.

0012-365X/$ – see front matter
doi:10.1016/j.disc.2008.04.058

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

An 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.

The Costas property is invariant under the symmetry group of the square: flipping a Costas array horizontally, vertically, or around the main diagonal (that is, transposing it) leads to an array that still has the Costas property; also, if a permutation array is the transpose of another, their corresponding permutations are the inverse of each other.

Definition 2 (*Golomb Ruler*). An increasing sequence of integers $f(i), i \in [n]$, with the property that

$$\forall i, j, k \quad \text{such that } 1 \le i, j, i+k, j+k \le n : f(i+k) - f(i) = f(j+k) - f(j) \Rightarrow i = j \text{ or } k = 0$$

is a *Golomb ruler*. Without loss of generality $f(1) = 1$, in which case $f(n)$ is the *length* of the ruler.

It is easy to see that the positions of the dots 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 [9,12]. Both are defined within the framework of finite fields [2,3,1] and make use of the *primitive roots* of a finite field [14,15,17,13].

We assume the reader is familiar with the definition of a field; we now collect some useful properties of finite fields in a theorem (their proofs can be found in [2,3,1]):

Theorem 1. *Let $m, n \in \mathbb{N}$, $m < n$, and let p be a prime.*

- *The size q of a finite field can only be a power of a prime: $q = p^n$; all finite fields of the same size are isomorphic to each other, so we can talk about the field of size $q = p^n$, denoted by $\mathbb{F}(q)$.*
- *$\mathbb{F}(q)$ contains $\phi(q-1)$ primitive roots, where ϕ denotes Euler's function, namely the number of positive integers less than and relatively prime to the function's argument.*
- *$\mathbb{F}(p^m) \subset \mathbb{F}(p^n)$ (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.*
- *$\binom{r}{i} \equiv 0 \bmod p, i = 1, \ldots, r-1 \Leftrightarrow \exists m \in \mathbb{N} : r = p^m$.*
- *Suppose a polynomial $P(x)$ with coefficients in $\mathbb{F}(p^n)$ of degree m is* irreducible [10] *over $\mathbb{F}(p^n)$, i.e. it cannot be factored into two polynomials of degrees at least 1 with coefficients in $\mathbb{F}(p^n)$; then, the new field generated by $\mathbb{F}(p^n)$ and the symbol a such that $P(a) = 0$ is isomorphic to $\mathbb{F}(p^{nm})$.*

Theorem 2 (*Welch Construction $W_1(p, g, c)$*). *Let p be a prime, $c \in \{0, \ldots, p-2\}$, and consider the sequence $f(i) = g^{i-1+c} \bmod p, i = 1, \ldots, p-1$, where g is a primitive root of the Galois field $\mathbb{F}(p)$; then f corresponds to a Costas array.*

Theorem 3 (*Golomb Construction $G_2(p, n, a, b)$*). *Let p be a prime, and consider the sequence f defined by the equation $a^i + b^{f(i)} = 1, i = 1, \ldots, q-2$, 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 [9,12]. Golomb constructions with $a = b$ are commonly known as *Lempel Costas arrays*.

3. Symmetry of Welch constructions

Theorem 4. *Let $f = W_1(p, g, c)$ and $f' = W_1(p, g', c')$ be two Welch-constructed permutations, for p prime and $p > 5$; then it cannot be that $f' = f^{-1}$, i.e. that $f'(f(i)) = i,\ i \in [p-1]$.*

Proof. Assume otherwise; as, for the given range of i, $p-i$ has the same range, it is also true that $f'(f(p-i)) = p-i, i \in [p-1]$. Summing together, and taking mod p of both sides, we get

$$f'(f(i)) + f'(f(p-i)) \equiv p \equiv 0 \bmod p \Leftrightarrow (g')^{c'-1}(g')^{g^{i-1+c} \bmod p} + (g')^{c-1}(g')^{g^{p-i-1+c} \bmod p} \equiv p \equiv 0 \bmod p,$$
$$i \in [p-1]$$

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

$$(g')^{g^{i-1+c} \bmod p} + (g')^{g^{p-i-1+c} \bmod p} \equiv 0 \bmod p \Rightarrow (g')^{g^{i-1+c} \bmod p} \equiv -(g')^{g^{p-i-1+c} \bmod p} \bmod p$$
$$\Leftrightarrow (g')^{g^{i-1+c} \bmod p - g^{p-i-1+c} \bmod p} \equiv -1 \bmod p.$$

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

$$(g')^{g^{i-1+c} \bmod p - g^{p-i-1+c} \bmod p} \equiv (g')^{\frac{p-1}{2}} \bmod p \Rightarrow g^{i-1+c} \bmod p - g^{p-i-1+c} \bmod p \equiv \frac{p-1}{2} \bmod (p-1) \quad (1)$$

because, according to Fermat's Little Theorem, $g^{p-1} \equiv 1 \bmod p$, hence exponents are unique modulo $p-1$. 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 (1) becomes:

$$g^{i-1+c} \bmod p - g^{p-i-1+c} \bmod p = \pm\frac{p-1}{2} \Rightarrow g^{i-1+c} - g^{p-i-1+c} \equiv \frac{p-1}{2} \text{ or } p - \frac{p-1}{2} \bmod p \equiv \frac{p \pm 1}{2} \bmod p. \quad (2)$$

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

$$x^2 - g \equiv x g^{1-c} \frac{p \pm 1}{2} \bmod p, \quad x \in [p-1], \quad (3)$$

since $g^p \equiv g \bmod p$. But a quadratic equation over a field can have at most 2 roots, so the pair of quadratics in (3) can have at most 4 roots. Hence, if $f' = f^{-1}$, it is necessary that $p - 1 \leq 4 \Leftrightarrow p \leq 5$. □

Remark 1. An older result in the literature can be used to offer an alternative proof of Theorem 4, although we believe our proof to be simpler and more direct: let us call a Costas array *doubly periodic* iff an arbitrary cyclic shift of either its rows or its columns results in a Costas array; Theorem 2 in [7] states that $W_1(p, g, c)$ for $p > 5$ is never doubly periodic. But $W_1(p, g, c)$ is *singly periodic*, in the sense that an arbitrary cyclic shift of its columns leads to a Costas array; then, the additional assumption of symmetry would imply that the corresponding cyclic shift of its rows would lead to the same (Costas) array (its rotation by 90^o to be exact), whence double periodicity would follow, contradicting the aforementioned theorem.

Corollary 1. 1. *$W_1(p, g, c)$ is never symmetric if $p > 5$;*
2. *There are exactly $2(p-1)\phi(p-1)$ Costas arrays of degree $p-1$ generated by Welch constructions through the symmetries of the square.*

Proof. 1. Use Theorem 4 with $c = c', g = g'$, in which case $f' = f$, hence $f = f^{-1}$.
2. To begin with, there are exactly $\phi(p-1)$ ways to choose g, and $p-1$ ways to choose c, hence there are $(p-1)\phi(p-1)$ constructions in total; furthermore, they are all distinct, as the pair of consecutive integers 1g, along with its position, identifies them uniquely (consider the integers ordered on a ring, so that 1 and g are still consecutive when $c = 1$). According to Theorem 4, no $W_1(p, g, c)$ permutation is the inverse of another such if $p > 5$, so inversion leads to a disjoint set of another $(p-1)\phi(p-1)$ permutations distinct between them as well. □

Symmetric Welch constructions exist for $p \leq 5$: for example, $W_1(5, 2, 0)$ is 1243, which is symmetric: $x = 1$ and $x = 3$ satisfy (3) with "−", whereas $x = 2$ and $x = 4$ satisfy (3) with "+".

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:*

- *$a = b$ (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 Theorem 3 and Definition 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 $a^i + a^{rf(i)} = 1 = a^{f(i)} + a^{ri}$, $i \in [q-2]$. Then $a^{f(i)} = 1 - a^{ri}$ and $a^i + (1 - a^{ir})^r = 1$, $i \in [q-2]$. Setting $x = a^i$ and observing that the resulting equation remains true for $x = 0$ and $x = 1$, we obtain:

$$x + (1 - x^r)^r = 1, \quad \forall x \in \mathbb{F}(q). \quad (4)$$

But since $b = a^r$ is itself a primitive root, r must be relatively prime to $q-1$; expanding the binomial term in (4), we obtain $r+1$ powers of x, namely $(lr) \bmod (q-1)$, $l = 0, \ldots, r$, and, since $r \leq q-2$ and relatively prime to $q-1$, these powers modulo $q-1$ are all distinct:

$$x + \sum_{l=0}^{r} \binom{r}{l} (-1)^l x^{rl} = 1, \quad \forall x \in \mathbb{F}(q). \quad (5)$$

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 (5):

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

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:

$$(-1)^r x^{r^2} + x \equiv 0 \Leftrightarrow x = (-1)^{r+1} x^{r^2}. \tag{6}$$

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, (6) becomes:

$$x^{r^2} \equiv x, \quad \text{with } 1 \leq r \leq q-2. \tag{7}$$

But the remaining coefficients in (4) must also be 0, so the relations $\binom{r}{l} \equiv 0 \bmod p$, $l = 1, \ldots, r-1$ must hold; this implies that $r = p^s$ for some $s \in \mathbb{N}$, according to Theorem 1.

Since (7) 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 Theorem 1; 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 (4) 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 $a^i + a^{ri} = 1$, or, equivalently, $x^r + x - 1 = 0$, where $i = \log_a(x)$. 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 $P(x) = 0 \Leftrightarrow T(x) = 1$.

- *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 Theorem 1; 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 $x^r \equiv x^{p^m \bmod (p-1)} \equiv x^{(p \bmod (p-1))^m} \equiv x^{1^m} \equiv x$, whence $P(x) = 0$ is really $x + x - 1 = 0 \bmod p \Leftrightarrow 2x = 1 \bmod p$ if $p > 2$ and $0 = 1 \bmod 2$ 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 $\phi : \mathbb{F}(q) \to \mathbb{F}(q)$, 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 of Theorem 1 was made).
- $\dim(\mathrm{Ker}[T]) = 1 \Leftrightarrow |\mathrm{Ker}[T]| = r$:
  - 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 Theorem 1). Hence, $\mathrm{Ker}[T] = \mathbb{F}(r) \Rightarrow \dim(\mathrm{Ker}[T]) = 1$.
  - If $p > 2$, we find $\dim(\mathrm{Im}[T])$ instead, and then use the Rank-Nullity Theorem: $\dim(\mathrm{Im}[T]) + \dim(\mathrm{Ker}[T]) = \dim(\mathbb{F}(r^2)) = 2$. First we show that $\mathrm{Im}[T] = \mathbb{F}(r)$:
    - Let $w \in \mathrm{Im}[T]$; $\exists x \in \mathbb{F}(r^2) : \phi^m(x) + x = w \Rightarrow \phi^m(w) = \phi^m(\phi^m(x) + x) = \phi^{2m}(x) + \phi^m(x) = \phi^m(x) + x = w$, so that $w \in \mathbb{F}(r)$ (by Theorem 1).
    - 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 $w \in \mathrm{Im}[T]$.

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

  We have now shown that in all cases $\dim(\mathrm{Im}[T]) = 1 = \dim(\mathrm{Ker}[T])$, so that $|\mathrm{Ker}[T]| = r$. Set $K = \mathrm{Ker}[T]$ 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 Theorem 1. 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 $h \in \mathbb{F}(r^2)/\mathbb{F}(r)$. □

Corollary 2. *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.*

Remark 2. This construction of Golomb rulers is related to the Bose–Chowla construction for Sidon sets [4].

Remark 3. The sufficiency of the two conditions for the symmetry of the $G_2(p, n, a, b)$ construction is a result already known in the literature (see [12], Section III.F); the structure of our proof, however, permitted us to show additionally the necessity of these two conditions.

5. 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 experts 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.

Acknowledgement

The authors wish to thank the anonymous reviewer, whose comments resulted in a better, more coherent paper.

References

[1] E. Artin, Galois Theory, Dover, 1998.
[2] M. Artin, Algebra, Prentice Hall, 1991.
[3] G. Birkhoff, S. MacLane, A Survey of Modern Algebra, 2nd edition, Macmillan, 1965.
[4] R.C. Bose, An affine analogue of Singer's theorem, Journal of the Indian Mathematical Society (N.S.) 6 (1942) 1–15.
[5] J.P. Costas, Medium constraints on sonar design and performance, Technical Report Class 1 Rep. R65EMH33, GE Co.
[6] J.P. Costas, A study of detection waveforms having nearly ideal range-doppler ambiguity properties, Proceedings of the IEEE 72 (8) (1984) 996–1009.
[7] T. Etzion, Combinatorial Designs Derived from Costas Arrays, in: R.M. Capocelli (Ed.), Workshop on Sequences, Positano, Italy, June 1988, in Sequences, Springer-Verlag, 1990, pp. 208–227.
[8] T. Etzion, S.W. Golomb, H. Taylor, Tuscan-k squares, Advances in Applied Mathematics 10 (1989) 164–174.
[9] S.W. Golomb, Algebraic Constructions for Costas Arrays, Journal of Combinatorial Theory, Series A 37 (1984) 13–21.
[10] S. Golomb, Obtaining specified irreducible polynomials over finite fields, SIAM Journal of Algebra and Discrete Mathematics 1 (4) (1980) 411–418.
[11] S.W. Golomb, T. Etzion, H. Taylor, Polygonal path constructions for Tuscan-k squares, Ars Combinatoria 30 (1990) 97–140.
[12] S.W. Golomb, H. Taylor, Constructions and Properties of Costas Arrays, Proceedings of the IEEE 72 (9) (1984) 1143–1163.
[13] J. Johnson, On the distribution of powers in finite fields, Journal für die reine und angewandte Mathematik (Crelles Journal) 251 (1971) 10–19.
[14] O. Moreno, On primitive elements of trace equal to 1 in GF(2^m), Discrete Mathematics 41 (1) (1982) 53–56.
[15] M. Szalay, On the distribution of primitive roots of a prime, Journal of Number Theory 7 (2) (1975) 184–188.
[16] H. Taylor, Non-attacking Rooks with distinct differences, EE Systems, University of Southern California, Technical Report CSI-84-03-2.
[17] E. Vegh, A note on the distribution of the primitive roots of a prime, Journal of Number Theory 3 (1) (1971) 13–18.