International Journal of Mathematics and
Computer Science, **10**(2015), no. 2, 239–249

Golomb-Lempel Construction of Costas Arrays Revisited

Ishani Barua

University of Engineering & Management
Jaipur, India

email: ishani.barua@gmail.com

(Received August 4, 2015, Accepted September 2, 2015)

Abstract

Costas arrays are a special type of permutation matrices with interesting combinatorial properties and are useful in radar engineering. Using properties of finite fields, Golomb gave a construction of obtaining Costas arrays of dimension $q-2$, where q is a power of a prime. A special case of Golomb construction, also due to Lempel, yields symmetric Costas arrays. The Golomb-Lempel method only gives a general thumb rule. To explicitly contruct the array one may have to resort to table look-up which is not practical for large q. In this article, we give a simple algorithm which considerably reduces the time complexity.

1 Introduction

Costas arrays is a fascinating topic as they are useful to engineers [1] and fascinating to mathematicians due to their interesting properties. Until now Costas arrays have been generated using one of the following methods.

1. Exhaustive search of $\mathcal{P}_n$ the set of $n \times n$ permutation matrices. This method yields Costas arrays of size $n \leq 26$.

2. Construction algorithms. This method yields Costas arrays of dimension slightly smaller than powers of primes.

Key words and phrases: Costas arrays, finite fields, Golomb-Lempel construction.
AMS (MOS) Subject Classifications: 05B20, 68R05, 68W01.
ISSN 1814-0432, 2015, http://ijmcs.future-in-tech.net

3. Trial and error approach (See [2] and [4] for details).

We shall be interested in the second approach and, more precisely, in Golomb's construction. In the symmetric case, we provide an efficient algorithm for constructing Costas arrays of dimension $q-2$, where q , a power of a prime, is the order of a finite field.

1.1 Our Contribution

Golomb's construction [3] yields Costas arrays of dimension $q-2$, where q is the order of a finite field, by using simple properties of finite fields. A particular case of this construction yields symmetric Costas arrays and is also due to Lempel. This construction, however, throws no light on how to solve equations of the form

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

for every $i, 1 \leq i \leq j$, where α is a primitive element of the finite field. Using elementary properties of finite fields, we shall show that most, if not all, such equations can be solved very easily using little computations. We also show that, given a Costas array of order $q-2$, one can obtain all symmetric Costas arrays of order $q-2$ that can be formed using the Golomb-Lempel construction.

2 Preliminaries

Notation The following notation will be used:

1. $\mathcal{M}_n$: the set of all $0-1$ square matrices of order n.

2. $\mathcal{P}_n$: the set of permutation matrices of order n; i.e., all those square matrices of order n, where each row and each column contains exactly one element equal to 1 with the remaining elements being 0.

3. $\mathcal{C}_n$: the set of Costas arrays of order n (to be defined below).

4. Let $A = (a_{i,j}) \in \mathcal{P}_n$. If $a_{i,j} = 1$ then set $f(j) = i, 1 \leq i, j \leq n$. In other words, $f(j) = i$ means that the jth column contains 1 at the ith position of the column. Clearly, f is well-defined and is a bijection. Note that f completely defines A; hence there is a one to one correspondence between permutation matrices and permutations of $\{1, 2, \ldots, n\}$.

Clearly $\mathcal{C}_n \subseteq \mathcal{P}_n \subseteq \mathcal{M}_n$.

Definition 2.1. (Costas Property) Let $A \in \mathcal{P}_n$ and let f denote the associated permutation of $\{1, 2, \ldots, n\}$. Then A is a Costas array of dimension or order n (or f has the Costas property) if the following condition is satisfied: For all $1 \leq i_1, i_2, i_3, i_4 \leq n, i_1 \leq i_2, i_3 \leq i_4$

$$(i_1 - i_2, f(i_1) - f(i_2)) = (i_3 - i_4, f(i_3) - f(i_4)) \Rightarrow i_1 = i_2, i_3 = i_4.$$

In other words, all tuples of the form $(i_1 - i_2, f(i_1) - f(i_2)), 1 \leq i_1 < i_2 \leq n$ are distinct.

3 Golomb's Construction

Let $\mathbf{F} = F_q$ denote a finite field of order q where $q = p^m$, p a prime. Let α, β be two generators of the multiplication group $\mathbf{F}^* = \mathbf{F} - \{0\}$. In other words, α, β are primitive elements of $\mathbf{F}$. Since $1 - \alpha^i \neq 0$, for each $i, 1 \leq i \leq q - 2$, there is a unique $j, 1 \leq j \leq q - 2$ such that $\beta^j = 1 - \alpha^i$ or,

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

Set $f(i) = j$. The following is due to Golomb [3]. We give a proof for the sake of completeness.

Theorem 3.1. *The function f, defined above, is a permutation of $\{1, 2, \ldots, q-2\}$ and this permutation yields a Costas array of order $q - 2$*

Proof. We first show that f is a bijection. For if $f(i_1) = f(i_2) = j$, say, then by definition, we have

$$\alpha^{i_1} + \beta^j = 1 = \alpha^{i_2} + \beta^j.$$

Thus $\alpha^{i_1} = \alpha^{i_2}$ which implies $i_1 \equiv i_2 \bmod (q-1)$; i.e., $i_1 = i_2$.

Next we show that f satisfies the Costas property. Suppose for $1 \leq i_1, i_2, i_3, i_4 \leq q-2, i_1 \leq i_2, i_3 \leq i_4$ and $(i_1, i_2) \neq (i_3, i_4)$,

$$(i_1 - i_2, f(i_1) - f(i_2)) = (i_3 - i_4, f(i_3) - f(i_4))$$

Thus $i_1 - i_2 = i_3 - i_4; f(i_1) - f(i_2) = f(i_3) - f(i_4)$. Hence,

$$\begin{aligned} i_1 + i_4 &= i_2 + i_4 \qquad (3.1) \\ f(i_1) + f(i_4) &= f(i_2) + f(i_4) \qquad (3.2) \end{aligned}$$

Now, by definition, we have

$$\alpha^{i_1} + \beta^{f(i_1)} = \alpha^{i_2} + \beta^{f(i_2)} = \alpha^{i_3} + \beta^{f(i_3)} = \alpha^{i_4} + \beta^{f(i_4)} = 1$$

Hence

$$\beta^{f(i_1)+f(i_4)} = \beta^{f(i_1)}.\beta^{f(i_4)} = (1 - \alpha^{i_1})(1 - \alpha^{i_4}) = 1 - \alpha^{i_1} - \alpha^{i_4} + \alpha^{i_1+i_4}$$

Similarly,

$$\beta^{f(i_2)+f(i_3)} = (1 - \alpha^{i_2})(1 - \alpha^{i_3}) = 1 - \alpha^{i_2} - \alpha^{i_3} + \alpha^{i_2+i_3}$$

Using equations (3.1) and (3.2), we obtain

$$\alpha^{i_1} + \alpha^{i_4} = \alpha^{i_2} + \alpha^{i_3} = a, \text{ say}$$

Also, from equation (3.1), we have

$$\alpha^{i_1}.\alpha^{i_4} = \alpha^{i_2}.\alpha^{i_3} = b, \text{ say}$$

Thus, $\alpha^{i_1}, \alpha^{i_4}$ are the roots of the quadratic equation $X^2 - aX + b = 0$. Similarly, $\alpha^{i_2}, \alpha^{i_3}$ are also the roots of the same quadratic equation. Since a quadratic equation over $\mathbf{F}$ has at most two roots, we conclude that $i_1 = i_2$ and $i_3 = i_4$. Thus the Costas property holds for f. □

3.1 Symmetric Costas arrays

If in the above construction we take $\alpha = \beta$, then we obtain a symmetric Costas array $A = (a_{ij})$ of dimension $q-2$. This construction, also due to Lempel, yields a symmetric array. For, if $\alpha^i + \alpha^j = 1$, then $f(i) = j$ and also $f(j) = i$. Thus

$$a_{ij} = 1 \leftrightarrow a_{ji} = 1.$$

We now obtain some properties of the permutation f associated with the symmetric Costas array of dimension $q = p^m$. The following is well-known:

Lemma 3.2. *Let α be a primitive element of the finite field $\mathbf{F}_q, q = p^m$ and p an odd prime. Then*

$$\alpha^{(q-1)/2} = -1.$$

Proof. Since α is a primitive element, we have

$$\alpha^{q-1} = 1.$$

Hence

$$(\alpha^{(q-1)/2} - 1)(\alpha^{(q-1)/2} + 1) = 0.$$

Since $\alpha^{(q-1)/2} - 1 \neq 0$, we must have $\alpha^{(q-1)/2} + 1 = 0$, or $\alpha^{(q-1)/2} = -1$. □

Theorem 3.3. *Let α be a primitive element of the finite field $\mathbf{F}_q, q = p^m$ and p a prime. Let f be the permutation associated with the Golomb-Lempel construction of the symmetric Costas array of order $q-2$. Then*

1. *$f(i) = j$ iff $f(j) = i$.*
2. *For $k \geq 1$ and $1 \leq i \leq q-2$,*

$$f(p^k i) = p^k f(i) \bmod (q-1).$$

3. *For $p = 2$; i.e., for fields of characteristic 2, we have*

$$f(q - \overline{i+1}) = f(i) - i \bmod (q-1).$$

For fields of characteristic $p \neq 2$ we have

$$f(q - \overline{i+1}) = (q-1)/2 + f(i) - i \bmod (q-1).$$

Proof. (1) This follows from the definition of f.
(2) We have $\alpha^i + \alpha^{f(i)} = 1$. Since the characteristic of $\mathbf{F}$ is p, for any $k \geq 1$

$$(\alpha^i + \alpha^{f(i)})^{p^k} = \alpha^{p^k i} + \alpha^{p^k f(i)} = 1.$$

This shows that $f(p^k i) = p^k f(i) \bmod (q-1)$.
(3)**Case 1,** $p = 2$. Suppose $f(i) = j$. Then we have

$$\alpha^i + \alpha^j = 1 = \alpha^{q-1}$$

$$\Rightarrow 1 + \alpha^{j-i} = \alpha^{q-\overline{i+1}}$$

$$\Rightarrow \alpha^{q-\overline{i+1}} - \alpha^{j-i} = 1$$

$$\Rightarrow \alpha^{q-\overline{i+1}} + \alpha^{j-i} = 1,$$

since for a field of characteristic 2, $-a = +a$ in $\mathbf{F}$. Hence, by definition of f,

$$f(q - \overline{i+1}) = j - i = f(i) - i \bmod (q-1).$$

Case 2, $p \neq 2$. As in Case 1, we have

$$\alpha^{q-\overline{i+1}} - \alpha^{j-i} = 1.$$

Using Lemma 2.2, this yields

$$\alpha^{q-\overline{i+1}} + \alpha^{(q-1)/2+j-i} = 1$$

Hence, $f(q - \overline{i+1}) = (q-1)/2 + j - i = (q-1)/2 + f(i) - i \bmod (q-1)$. This completes the proof.

□

Remarks: Theorem 3.3 enables us to obtain a simple algorithm for constructing the array using the properties of f. First observe that by Theorem 3.3 (3), it is enough to obtain the values of $f(i)$ for $1 \leq i \leq \frac{q-1}{2}$. For, if $\frac{q-1}{2} \leq j \leq q-2$, then $j = \frac{q-1}{2} - \overline{k+1}$, where $1 \leq k \leq \frac{q-1}{2}$. Hence, $f(j)$ can be expressed in terms of $f(k)$, by Theorem 3.3 (3)

Next, if $f(i) = j$, then $f(j) = i$ and both $f(i)$ and $f(j)$ are evaluated and we mark both in our algorithm. Also by Theorem 3.3, if $f(i) = j$, then

$f(p^k i) = p^k j \bmod (q-1)$ and hence we mark all pairs $\{p^k i, p^k j\}$, modulo $(q-1)$. Finally, if $f(i) = j$, then $f(q-\overline{i+1}) = \frac{q-1}{2} + f(i) - i \bmod (q-1)$ and so the pair $\{q-\overline{i+1}, \frac{q-1}{2} + j - i\}$, modulo $q-1$, is marked. If any unmarked element remains in the list $1, 2, 3, \ldots, q-2$ the first i is considered and the procedure is repeated.

We now present our algorithm:

Algorithm(Golomb-Lempel)

Input: A list $L = \{1, 2, \ldots, q-2\}$ where $q = p^m$, the order of the field and α, a primitive element.

Output: A list L^* of pairs (i, j) such that $f(i) = j$.

1. Set $i = 1$

2. Find j such that $\alpha^i + \alpha^j = 1$. Mark i, j and add the pair $\{i, j\}$ to L^*. Also mark and add to L^* all pairs $\{p^k i, p^k j\}$, modulo $(q-1)$ for $k \geq 1$.

3. **If** i is the least marked i such that $q - \overline{i+1}$ is unmarked
   then add the pair $\{q - \overline{i+1}, \frac{q-1}{2} + f(i) - i\}$ to L^*.
   Set $i = min\{q - \overline{i+1}, \frac{q-1}{2} + f(i) - i\}$ modulo $q-1$
   Go to Step 2
   Else find the first unmarked i.

4. **If** i is the only unmarked element of L, **then** add the pair $\{i, i\}$ to L^*.
   Go to Step 5
   Else go to Step 2.

5. Output list L^*.

Remarks. In the case of fields of characteristic 2, steps 3 and 4 are replaced by

- 3^* **If** i is the least marked i such that $q - \overline{i+1}$ is unmarked
  then add the pair $\{q - \overline{i+1}, f(i) - i\}$ to L^*.
  Set $i = min\{q - \overline{i+1}, f(i) - i\}$ modulo $q-1$
  Go to Step 2
  Else find the first unmarked i.

- 4^* **If** i, j are the only unmarked elements in L, set $f(i) = j$ and add the pair $\{i, j\}$ to L^*.
  Go to Step 5.
  Else go to Step 2.

3.2 Examples

We illustrate our method with some examples. The following example is from Drakakis [2]

Example 1

Take $q = 2^4 = 16$ and consider the irreducible polynomial $x^4 + x + 1$ over $\mathbf{F}_2$ to construct the field $\mathbf{F}_{2^4}$. Note that here $\alpha = x$ is a primitive element of $\mathbf{F}_{2^4}$. To construct a Costas array of order 14, one needs to find (from a table look-up) or calculate for each $i, 1 \leq i \leq 14$ an integer $j, 1 \leq j \leq 14$ such that $\alpha^i + \alpha^j = 1$. In [2], it was shown that one needs to find $f(i)$ for seven values of i viz for $i = 1, 2, 3, 5, 6, 7, 11$ and the corresponding values of $f(i)$ are $4, 8, 14, 10, 13, 9, 12$. We shall show that by our method, we need to find j for only *one* value of i viz for $i = 1$.

1. Set $i = 1$. It is easy to see that $\alpha + \alpha^4 = 1$ and hence $f(1) = 4$. So mark $\{1, 4\}$

2. Since the characteristic of the field is 2 we mark the pair $\{2, 8\}$ so that $f(2) = 8$. (No other new pairs are generated)

3. For $i = 1, q - \overline{i + 1} = 14$ and hence $f(14) = f(i) - i = 4 - 1 = 3$. So the pair $\{3, 14\}$ is marked.

4. Now mark $\{6, 28 \bmod 15\} = \{6, 13\}$. Then $\{12, 26 \bmod 15\} = \{12, 11\}$, $\{24 \bmod 15, 22 \bmod 15\} = \{9, 7\}$.(No more new pairs are obtained)

Since only the unmarked elements $5, 10$ remain, we set $f(5) = 10$ and add the pair $\{5, 10\}$ to L^*. Hence our algorithm yields the following list
$L^* = \{1, 4\}, \{2, 8\}, \{3, 14\}, \{6, 13\}, \{11, 12\}, \{7, 9\}, \{5, 10\}$. Thus we are able to evaluate all values of $f(i)$ by just solving one equation viz

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

Note: In general, if the irreducible polynomial used in constructing the finite field of characteristic 2 is $x^n + x^m + 1$ and x is a primitive element, then we

have

$$x^m + x^n = 1$$

and so $f(m) = n$. Hence, $\{m, n\}$ could be our starting pair. We shall illustrate this with the next example.

Example 2

Take $q = 2^5 = 32$ and consider the irreducible polynomial $x^5 + x^3 + 1$ over $\mathbf{F}_2$ to construct the field $\mathbf{F}_{2^5}$. Clearly $\alpha = x$ is a primitive root, since $\mathbf{F}^*_{2^5}$=$\mathbf{F}_{2^5} - \{0\}$ is a multiplicative group of prime order. To construct a Costas Array of order 30, one needs to find for each $i, 1 \leq i \leq 30$ a j such that $\alpha^i + \alpha^j = 1$. To do so, one needs to calculate $f(i)$ for 15 values of i viz $i = 1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 1517, 21, 26$. The corresponding values of $f(i)$ are $14, 28, 5, 25, 10, 16, 19, 24, 23, 20, 30, 22, 18, 27, 29$. We now show that by our algorithm, no such calculation will be involved.

1. Since $\alpha^3 + \alpha^5 = 1$, $f(3) = 5$ and so we mark $\{3, 5\}$.
2. Since the characteristic of the field is 2, we mark the pairs $\{6, 10\}, \{12, 20\}, \{24, 40 \bmod 31\}$; i.e., we mark $\{9, 24\}$. Then we mark $\{18, 48 \bmod 31\}$; i.e., $\{17, 18\}$ (no new pairs are generated).
3. For $i = 3, q - \overline{i+1} = 28$ and so $f(28) = f(i) - i = 5 - 3 = 2$. Hence we mark $\{2, 28\}$.
4. Now mark $\{4, 56 \bmod 31\} = \{4, 25\}$. Then $\{8, 50 \bmod 31\} = \{8, 19\}$ and so $\{16, 38 \bmod 31\} = \{7, 16\}$ and finally mark $\{14, 32 \bmod 31\}$; i.e., $\{1, 14\}$. (No new pairs will be generated)
5. For $i = 1, q - \overline{i+1} = 30$. So $f(30) = f(1) - 1 = 14 - 1 = 13$. Therefore, we mark the pair $\{13, 30\}$.
6. Now mark $\{26, 60 \bmod 31\} = \{26, 29\}$. Then $\{52 \bmod 31, 58 \bmod 31\} = \{21, 27\}$; and so $\{42 \bmod 31, 54 \bmod 31\} = \{11, 23\}$ and finally $\{22, 46 \bmod 31\}$; i.e., $\{15, 22\}$.

Thus our list $L^* =$
$\{1, 14\}, \{2, 28\}, \{3, 5\}, \{4, 25\}, \{6, 10\}, \{7, 16\}, \{8, 19\}, \{9, 24\}, \{11, 23\}, \{12, 20\}, \{13, 30\}, \{15, 22\}, \{17, 18\}, \{21, 27\}, \{26, 29\}$.

Note that we do not need to solve any equation of the form $\alpha^i + \alpha^j = 1$. □

It is not hard to see that one can obtain *all* Costas arrays that can be constructed using the Golomb-Lempel method as we shall show below.

Theorem 3.4. *Let α be a primitive element of the finite field $\mathbf{F}_q, q = p^m$*

and p a prime. Let f be the permutation associated with the Golomb-Lempel construction of the symmetric Costas array of order $q-2$. Let β be another primitive element of $\mathbf{F}_q$ and suppose g is the associated permutation obtained from the Golomb-Lempel construction. Then, for some integer k coprime to $q-1$,

$$g(i) = \frac{1}{k} f(ki) \bmod (q-1).$$

Proof. Suppose $g(i) = j$. Then, by definition, $\beta^i + \beta^j = 1$. Since α is a primitive element of $\mathbf{F}_q$ for some integer coprime to $q-1, \beta = \alpha^k$. Hence we have

$$\alpha^{ki} + \alpha^{kj} = 1.$$

. Thus $f(ki) = kj \bmod (q-1)$. Hence, $g(i) = j = \frac{1}{k} f(ki)$. This completes the proof. □

Remark: Since α^k is a primitive element of $\mathbf{F}_q$ iff $gcd(k, q-1) = 1$, the number of primitive elements is $\phi(q-1)$ and hence the number of Costas arrays obtained by this construction is also $\phi(q-1)$

Conclusion: In this article we have obtained a simple algorithm for constructing Costas arrays using the Golomb-Lempel method. The efficiency of our algorithm was illustrated by means of some examples, showing that our algorithm involves very little calculations. The exact complexity of the algorithm depends on the primitive or irreducible polynomial over $\mathbf{F}_p$ used for constructing the finite field $\mathbf{F}_{p^m}$. Obtaining the complexity of the algorithm would be an interesting topic to study.

Acknowledgement: This work was done when the author was visiting IIT, Kharagpur as a Summer Intern under Dr. Ratna Dutta. The author thanks her for her help in the study of Costas Arrays.

References

[1] J. Costas, A Study of Detection Waveforms Having Nearly Ideal Range-Doppler Ambiguity Properties, *Proc. IEEE,* **72,** no. 8, 1984, 996–1009.

[2] K. Drakakis, A Review of Costas Arrays, *Journal of Appl. Math.,* 2006.

[3] S. W. Golomb, Algebraic Constructions for Costas arrays, *J. Combin. Theory, Series A,* **37,** no. 1, 1984, 13–21.

[4] K. Taylor, S. Rickard, K. Drakakis, Costas Arrays: Survey, Standardization, and MATLAB Toolbox, *Journal of ACM Transactions on Mathematical Software,* **37,** no. 4, February 2011.