Costas arrays and a new transformation

MathCoRe Research Project of Ali Ardalani

Funded Fellow since January 2019 Advisors: Alexander Pott Mentor: Eliana Duarte

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

DFG-Graduiertenkolleg MATHEMATISCHE KOMPLEXITÄTSREDUKTION

MAX-PLANCK-INSTITUT FÜR DYNAMIK KOMPLEXER TECHNISCHER SYSTEME MAGDEBURG

Summary

In 1965 in the context of sonar detection, J. P. Costas studied a particular class of permutations of n elements to improve the poor performance of Radar and Sonar systems [1]. These classes are now known as Costas Arrays. A Costas array of size n is an $n \times n$ binary matrix such that there is exactly a single 1 per each row and each column (i.e., it is a permutation matrix) and such that the line segments formed by joining pairs of 1s are all distinct [2]. There are two basic approaches currently being adopted in research into Costas arrays. One is the finite field-based construction approach, and the other is computer search. Although extensive research has been carried out on Costas arrays, many fundamental questions are not yet answered, especially, do Costas arrays exist in all sizes?. Since 1984, the smallest sizes for which no Costas array is currently known are 32 and 33.

A new transformation

Definition 1. Let $X = (x_{ij})$ be a permutation matrix of size n, where $n \in \mathbb{N}$, $1 \leq i, j \leq n$. Then X is a Costas array if for any pairs of integers $(r, s) \neq (0, 0)$, $|r| \leq n$, $|s| \leq n$, the aperiodic autocorrelation function of A satisfies

$$C_X^a(r,s) = \sum_{i,j} x_{i,j} x_{i+s,j+r} \leq 1,$$

where X is extended with zeros when required.

Definition 2. Let $X = [f(1), f(2), ..., f(n)]$ represent a permutation array of size n, where $n \in \mathbb{N}$, and $f(i)$ is the position of the nonzero entry in the ith column of X, counting from top to bottom. Suppose that k is a positive integer such that n is divisible by k. Let us define $\mathcal{A}_k(X) = [g(1), g(2), ..., g(n)]$, where

$$g(i) = f\left(\frac{i + ((k-i) \text{ mod } k)n + [(k-i) \text{ mod } k]}{k}\right).$$

Relation to Complexity Reduction

Until today, the enumeration of Costas arrays has been completed via computational methods for all $n \leq 29$. However, the total run-time of the search for $n = 29$ on a single CPU required the equivalent of 366.55 years, but, the real time required was approximately 230 days as a result of high parallelization of the tasks [3]. One way of tackling the Costas arrays problem would be to recognize any pattern in sporadic Costas arrays, which is an arduous task to do [4]. Our primary purpose was to introduce a new transformation under which the Costas property is invariant. Interestingly, this transformation leaves the Costas property invariant for algebraically constructed Costas arrays and some sporadic Costas arrays. In our next step, we will search for the possible existence of common property of sporadic Costas arrays and algebraically constructed ones for which the Costas property is invariant after applying our newly introduced transformation. By doing so, we expect to reduce the search space for such arrays.

Main Results

Theorem 1 (Welch Construction [2]). *Let α be a primitive root of $GF(p)$, with p a prime. Then the $(p-1) \times (p-1)$ permutation matrix with $x_{ij} = 1$ if and only if $i \equiv \alpha^j$ (**mod** p), $1 \leq i \leq p-1$, $0 \leq j \leq p-2$, is a Costas array.*

Theorem 2 (Lempel-Golomb Construction [2]). *Let α and β be two primitive roots of $GF(q)$ with $q > 2$. Then the $(q-2) \times (q-2)$ permutation matrix with $x_{ij} = 1$ if and only if $\alpha^i + \beta^j = 1$, $1 \leq i, j \leq q-2$, is a Costas array.*

Theorem 3 ([5]). *Let $X = [f(1), f(2), ..., f(n)]$ represent a Costas array of size n, where $n \in \mathbb{N}$, and k is a positive integer such that n is divisible by k. Then the aperiodic Auto-Correlation function values of $\mathcal{A}_k(X)$ for all possible non-zero shifts are at most two, where $\mathcal{A}_k(X)$ is the transformation introduced in Definition 2.*

Theorem 4 ([5]). *Let $X = [f(1), f(2), ..., f(n)]$ represent a Costas array constructed by the Welch Construction from theorem 1. Then $\mathcal{A}_k(X)$ is a Costas array, where $\mathcal{A}_k(X)$ is the transformation introduced in Definition 2.*

Theorem 5 ([5]). *Let X be a Costas array obtained via the Lempel or Golomb construction, as in theorem 2 of size $q-2$. Then $\mathcal{A}_k(X)$ is a Costas array, where $\mathcal{A}_k(X)$ is the transformation introduced in Definition 2.*

1	0	0	0	0	0
0	0	1	0	0	0
0	1	0	0	0	0
0	0	0	0	0	1
0	0	0	1	0	0
0	0	0	0	1	0

$X = [1, 3, 2, 5, 6, 4]$

0	1	0	0	0	0
0	0	0	0	0	1
0	0	0	1	0	0
0	0	0	0	1	0
1	0	0	0	0	0
0	0	1	0	0	0

$\mathcal{A}_2(X) = [5, 1, 6, 3, 4, 2]$

Figure 1: The array X is Welch Costas array generated over $GF(7)$ with $\alpha = 3$. By taking $k = 2$ we can construct $\mathcal{A}_2(X)$ as in Definition 2.

Publications and References

[1] John P Costas. Medium constraints on sonar design and performance. Technical Report Class 1 Rep. R65EMH33, GE Co., November 1965, a synopsis of this report appeared in the Eascon. Conv. Rec., 1975, pp. 68A–68L, 1965.

[2] Solomon W Golomb. Algebraic constructions for costas arrays. *Journal of Combinatorial Theory, Series A*, 37(1):13–21, 1984.

[3] Konstantinos Drakakis, Francesco Iorio, Scott Rickard, and John Walsh. Results of the enumeration of costas arrays of order 29. *Advances in Mathematics of Communications*, 5(3):547, 2011.

[4] Oscar Moreno. Survey on costas arrays and their generalizations. In *Mathematical Properties of Sequences and Other Combinatorial Structures*, pages 55–64. Springer, 2003.

[5] Alexander Pott and Ali Ardalani. A new transformation to preserve costas property. 2020. Unpublished manuscript.

Acknowledgement We would like to show our gratitude to MathCoRe for all the support.