A SHIFTING PROPERTY OF SOME COSTAS SEQUENCES

Oscar Moreno[1]

Department of Mathematics
University of Puerto Rico
Río Piedras
PUERTO RICO 00931

Abstract. There is a conjecture of Golomb and Taylor that asserts that the Welch construction for Costas sequences with length $p-1$, p prime, is the only one with the property of single periodicity.

In the present paper we present and prove a weaker conjecture: the Welch construction is the only one with the property that its differences are a shift of the original sequence.

Introduction.

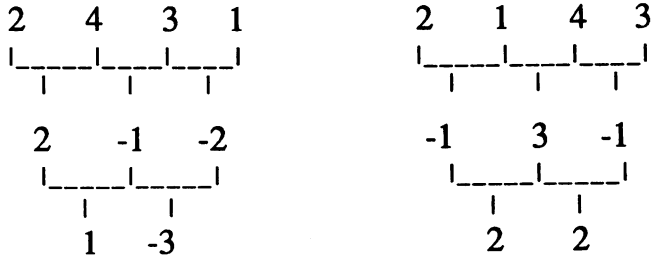
We would like to give a short introduction and define our terms. For more details see [2, 3, 4].

Costas Arrays or Costas Sequences. *A* Costas sequence $a_0, \ldots, a_{n-1}$ *is a sequence which is a permutation of the integers* $1, \ldots, n$ *satisfying the property*

$$a_{s+k} - a_s \neq a_{t+k} - a_t$$

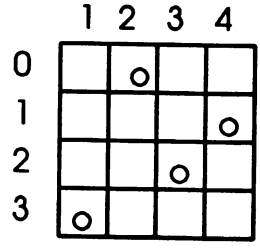
for every s, t *and* k, *such that* $0 \leq s < t < t+k \leq n-1$.

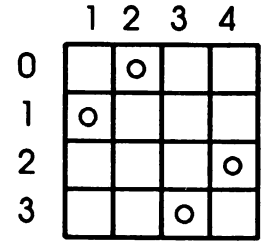
Example: a) Costas sequence: b) not a Costas sequence:



[1] Oscar Moreno was supported in part by the Office of on Naval Research under grant number N00014-90-J-1301, the NSF-EPSCOR of Puerto Rico Project, and the NSF grant number DCI-8601555.

We can put these sequences in an array form as follows:





and the property of the differences can be put as follows: if we form all the vectors joining any two dots, no two vectors have the same length and magnitude. An array which results from Costas sequence in this way is called a Costas array.

The problem of finding a Costas array or sequence is equivalent to a problem of Costas [1], who encountered it in constructing sonar signal patterns.

Welch Exponential Construction. *Let p prime and α a primitive element in $GF(p)$. Then Welch, [3, 4] showed that $\alpha^1, \alpha^2, \ldots, \alpha^{p-1} = 1$ is a Costas sequence.*

We refer to this construction as the *Welch construction*, and call such a sequence a *Welch sequence*.

The Welch construction is singly periodical. This is to say $\alpha^i, \alpha^{i+1}, \ldots, \alpha^{i+p-2}$ is also a Costas sequence, that is, any circular shift of the sequence is also a Costas sequence.

Example: If $p = 7$ and $n = 6$, $\alpha = 3$ is primitive in $GF(7)$. The sequences $\{3,2,6,4,5,1\}, \{2,6,4,5,1,3\}, \{6,4,5,1,3,2\}, \{4,5,1,3,2,6\}, \{5,1,3,2,6,4\}$, and $\{1,3,2,6,4,5\}$ are all Costas sequences.

Conjecture (Golomb and Taylor). *Single periodicity characterizes the Welch Construction.*

The above conjecture was given in [3]. We will now prove our main result.

Section 1. A shifting property of some Costas sequences.

Let us consider the circular differences $a_{0+h}-a_0, a_{1+h}-a_1, a_{2+h}-a_2, \ldots, a_{n-1+h}-a_{n-1}$ ($i + h$ is considered modulo n). We do this for $h = 1,2,\ldots,n-1$. We say that the circular differences have the *shifting property*, if these differences considered modulo $n+1$ are always a circular shift of the original sequence, and circular shifts are considered as in the above example where all the circular shifts of $\{3,2,6,4,5,1\}$ are given.

Example: Notice that in the Welch sequence $2,4,3,1$: the circular (index sums modulo 4) differences modulo 5 are $\{2,4,3,1\}$, $\{1,2,4,3\}$, and $\{4,3,1,2\}$, for $h = 1,2,3$ respectively. Therefore, they have the shifting property.

Our main result is as follows:

Theorem. *The Shifting property characterizes the Welch construction.*

Proof: We assume first that the sequence $a_0,\ldots,a_{n-1}$ has the shifting property, and we prove it is a Welch sequence. To do this we will prove first that $n+1$ is a prime.

We know $a_1 - a_0, a_2 - a_0, \ldots, a_{n-1} - a_0$ gives all the elements of $\boldsymbol{Z}_{n+1}$ excluding only 0 and $-a_0$. Also, $a_i - a_0, a_{i+1} - a_1, \ldots, a_{i+n-1} - a_{n-1}$ $(i = 1,2,\ldots,n-1)$ is a shift of $a_0,\ldots,a_{n-1}$ and, therefore, it gives all the possible shifts of $a_0,\ldots,a_{n-1}$ except the one beginning with $-a_0$.

Since a shift of a sequence with the shifting property also has the shifting property, we can assume that $a_0 = 1$. Since in the differences we can get all the possible shifts of $a_0,\ldots,a_{n-1}$ excluding the one beginning with $-a_0$ or in other words n, we can get the one beginning with a_0 unless $a_0 = -a_0$, that is, $2a_0 = 0$ in $\boldsymbol{Z}_{n+1}$, but $a_0 = 1$ implies $n = 1$ and $n+1 = 2$, a prime. Therefore, there exist k such that $a_k - a_0 = a_0, a_{k+1} - a_1 = a_1, \ldots, a_{k+n-1} - a_{n-1} = a_{n-1}$. This implies $a_k = 2a_0, a_{k+1} = 2a_1, \ldots, a_{k+n-1} = 2a_{n-1}$. Notice that we can continue doing this exactly $n-1$ times as follows: now there is one beginning with $a_k = 2$, unless $2 = -1$, that is, $n = 2$. That is, there exist a_m such that:

$$a_m - a_0 = a_k = 2a_0 \qquad a_m = 3a_0$$

then

$$a_{m+1} - a_1 = a_{k+1} = 2a_1 \qquad a_{m+1} = 3a_1$$

$$\vdots \qquad\qquad \vdots$$

it is the original 3 times and $a_m = 3$. It is clear we can continue multiplying the original by $2,3,4,\ldots$, up to $n-1$ (excluding only $n = -1$) and get a shift of the original sequence containing all the nonzero elements of $\boldsymbol{Z}_{n+1}$.

This implies that for every nonzero element a of $\boldsymbol{Z}_{n+1}$ if we multiply the set $\{1,2,\ldots,n\}$ by any a we get again the same set. In particular 1 is always in $\{1,2,\ldots,n\}$ and for $a = 2,3,\ldots,n$ we have that a is, therefore, invertible in $\boldsymbol{Z}_{n+1}$ and we have, therefore, a field and $n+1$ must be a prime.

In order to finish our proof consider now M the circulant $n \times n$ matrix over $\boldsymbol{Z}_{n+1}$ ($n+1$ a prime):

$$M = \begin{bmatrix} -1 & 1 & \ldots & 0 & 0 \\ 0 & -1 & \ldots & 0 & 0 \\ & & \vdots & & \\ 0 & 0 & \ldots & -1 & 1 \\ 1 & 0 & \ldots & 0 & -1 \end{bmatrix}$$

But we just proved that:

$$M\begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} a_1 - a_0 \\ a_2 - a_1 \\ \vdots \\ a_0 - a_{n-1} \end{bmatrix} = c\begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix} \text{ for some } c$$

Therefore, c is an eigenvalue and $x = (a_0, \ldots, a_{n-1})^t$ is an eigenvector of M. We will finish our proof if we obtain that any eigenvector of M must be as in the Welch construction. Let τ be a primitive root in $GF(p)$. For any $f \in GF(p)$ $f \neq 0$ then $f = \tau^i$. Then the characteristic equation of M is $(x+1)^n - 1 = 0$. So the eigenvalues are $1 + \tau^i$ $(i = 0, 1, \ldots, n-1)$ and are simple. Thus, each eigenvalue has a unique eigenvector up to scalar multiples.

$$\text{Since } y_i = \begin{bmatrix} 1 \\ \tau^i \\ (\tau^i)^2 \\ \vdots \\ (\tau^i)^{p-2} \end{bmatrix} \text{ is an eigenvector for } -1 + \tau^i,$$

we can conclude that $x = ay_i$, for some i, and $a \in GF(p)$. Since the coordinates of x are distinct, it follows that τ^i must be primitive. Since $a_0 = 1$, $x = y_i$ and x is as in the Welch construction. The converse, that a Welch sequence, has the shifting property is easily checked. ∎

References

1. J.P. Costas, *Medium constraints on solar design and performance*, EASCON Conv. Rec. (1975), 68A–68L.
2. S.W. Golomb and H. Taylor, *Two dimensional synchronization patterns for minimum ambiguity*, IEEE Trans. on. Inf. Th. **II-28, No. 4** (July 1982).
3. S.W. Golomb and H. Taylor, *Construction and properties of Costas arrays*, Proceedings of the IEEE, no. 9 **72** (September 1984).
4. S.W. Golomb, *Algebraic constructions for Costas arrays*, Journal of Combinatorial Theory, Series A **37, No. 1** (July 1984).