

- [14] B. Ya. Ryabko, "Data compression by means of a book stack, *Probl. Inform. Transm.*, vol. 16, no. 4, pp. 16–21, 1980 (in Russian). (In English: vol. 16, no. 4, pp. 265–269, 1981).
- [15] —, "Letter in *Commun. ACM*, vol. 30, no. 9, pp. 792, 1987.
- [16] —, "A fast sequential code," *Soviet Math. Doklady*, vol. 39, no. 3, pp. 533–537, 1989.
- [17] —, "The fast on-line adaptive code," *Probl. Inform. Transm.* (to be published, in Russian).
- [18] Yu. M. Starkov, "Shannon codes," *Probl. Inform. Transm.*, vol. 20, no. 9, pp. 3–16, 1984 (in Russian).
- [19] J. A. Storer, *Data Compression. Method and Theory*. New York: Computer Science Press, 1988.
- [20] J. S. Vitter, "Two papers on dynamic Huffman codes," Techn. Rep. CS95-13. Brown Univ., Dept. Comput. Sci., Providence, RI. Revised Dec. 1986.
- [21] F. M. J. Willems, "Universal data compression and repetition times," *IEEE Trans. Inform. Theory*, vol. 35, pp. 54–58, Jan. 1989.
- [22] J. H. Witten, R. M. Neal, and J. G. Cleary, "Arithmetic coding for data compression," *Commun. ACM*, vol. 30, no. 6, pp. 520–540, 1987.
- [23] J. Ziv and A. Lempel, "Compression of individual sequences via variable rate coding," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 530–536, Sept. 1978.

The T_4 and G_4 Constructions for Costas Arrays

Solomon W. Golomb

Abstract—Two of the algebraic constructions for Costas arrays, designated as T_4 and G_4 , are described in detail, and necessary and sufficient conditions are given for the sizes of Costas arrays for which these constructions occur. These constructions depend on the existence of primitive roots satisfying certain equations in finite fields.

Index Terms—Costas arrays, primitive roots, Lempel's construction.

In [1], a number of systematic algebraic constructions for Costas Arrays are described. The validity of several of these constructions is proved in [2]. However, two of the algebraic constructions, designated T_4 and G_4 in [1], are not discussed in [2]. The present note proves the assertions made in [1] concerning these two constructions, and furnishes some additional algebraic information.

We briefly review a few of the definitions from [1] and [2].

Definition 1: A Costas array of order n is an $n \times n$ permutation matrix with the property that the $\binom{n}{2}$ vectors connecting two 1's of the matrix are all distinct as vectors. (That is, no two vectors are equal in both magnitude and slope).

Specifically, if we have four distinct entries $a_{i_1 j_1} = a_{i_2 j_2} = a_{i_3 j_3} = a_{i_4 j_4} = 1$ in the matrix, we must not have $(i_2 - i_1, j_2 - j_1) = (i_4 - i_3, j_4 - j_3)$, nor may we have $(i_2 - i_1, j_2 - j_1) = (i_3 - i_2, j_3 - j_2)$.

Definition 2: If $n = q - 2$, where $q = p^k$ is the size of a finite field, then the Lempel construction L_2 for a Costas array of order n sets $a_{ij} = 1$ iff $\alpha^i + \alpha^j = 1$, $1 \leq i, j \leq q - 2$, where α is any fixed primitive root in $\text{GF}(q)$. (Note that the Lempel construction gives a symmetric permutation matrix with the Costas property.)

Definition 3: The T_4 construction occurs for $\text{GF}(q)$ iff there is a primitive element α in $\text{GF}(q)$ with $\alpha + \alpha^2 = 1$.

Manuscript received August 29, 1991. This work was supported in part by the United States Office of Naval Research, under Grant No. N00014-90-J-1341.

The author is with the Department of Electrical Engineering-Systems, University of Southern California, University Park, EEB-504a, Los Angeles, CA 90089-2565.

IEEE Log Number 9107518.

H. Taylor's T_4 construction leads to a Costas Array of order $n = q - 4$. Specifically, from the Lempel construction L_2 , using the primitive root α which satisfies $\alpha + \alpha^2 = 1$ in $\text{GF}(q)$, we have both $\alpha^1 + \alpha^2 = 1$ and $\alpha^2 + \alpha^1 = 1$. Thus both $a_{12} = 1$ and $a_{21} = 1$ in the L_2 construction of order $q - 2$. Removing the two topmost rows and the two leftmost columns from the L_2 array leaves a Costas array of order $q - 4$, which is the T_4 array.

Theorem 1: A necessary condition for the T_4 construction is that q is 4, or 5, or 9, or a prime p with $p \equiv \pm 1 \pmod{10}$.

Proof: We are asking for a field $\text{GF}(q)$ in which the equation $x^2 + x - 1$ has roots, and in which at least one of these roots is primitive in $\text{GF}(q)$.

Over $\text{GF}(2)$, $x^2 + x - 1$ is irreducible, but generates $\text{GF}(4)$. In no other field of characteristic 2 will a root of $x^2 + x - 1$ be primitive, since these roots have only primitivity 3.

Over $\text{GF}(3)$, $x^2 + x - 1$ is irreducible, but generates $\text{GF}(9)$. In no other field of characteristic 3 will a root of $x^2 + x - 1$ be primitive, since these roots have only primitivity 8.

For $p > 5$, the roots of $x^2 + x - 1 = 0$ are given by the quadratic formula as $(-1 \pm \sqrt{5})/2 \equiv (-1 \pm \sqrt{5})((p+1)/2)$ (mod p), which lie in $\text{GF}(p)$ iff 5 is a quadratic residue modulo p , and in $\text{GF}(p^2)$ otherwise. Now, 5 is a quadratic residue modulo $p > 5$ iff $p \equiv \pm 1 \pmod{10}$, from the law of quadratic reciprocity:

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) (-1)^{(p-1)/2 \cdot (5-1)/2} = \left(\frac{p}{5}\right), \quad \text{and} \quad \left(\frac{a}{5}\right) = +1$$

iff $a \equiv \pm 1 \pmod{5}$;

and since p is odd, this becomes $p \equiv \pm 1 \pmod{10}$. Thus, only primes with unit digit 1 or 9 are candidates for the T_4 construction, and the construction occurs iff at least one root of $x^2 + x - 1$ is primitive in $\text{GF}(p)$. (It is possible for neither root, exactly one root, or both roots, to be primitive, depending on p .)

If 5 is a quadratic nonresidue modulo $p > 5$, then the roots of $x^2 + x - 1$ lie in $\text{GF}(p^2)$ but not in $\text{GF}(p)$. However, they cannot be primitive in $\text{GF}(p^2)$, because a necessary condition for $x^2 + x + g$ to have primitive roots in $\text{GF}(p^2)$ is that g be primitive in $\text{GF}(p)$, and the only prime fields in which $g = -1$ is primitive are $\text{GF}(2)$ and $\text{GF}(3)$.

Finally, for $p = 5$, $\alpha = 2$ is a root of $x^2 + x - 1 \pmod{5}$, and the T_4 construction occurs in this case. (Here, in effect, $\sqrt{5} = 0$, and $x^2 + x - 1 = (x - 2)(x - 2)$ has a repeated root.) \square

The following generalization G_2 of Lempel's construction is due to Golomb [2].

Definition 4: Let α and β be any two primitive roots in $\text{GF}(q)$. Then G_2 is the Costas array of order $n = q - 2$ for which $a_{ij} = 1$ iff $\alpha^i + \beta^j = 1$.

Moreno *et al.* [3] have proved Golomb's Conjecture A in [2], which asserts: Every finite field $\text{GF}(q)$ with $q > 2$ contains two primitive roots α and β (not necessarily distinct) with $\alpha + \beta = 1$. This leads to the following definition.

Definition 5: For every $q = p^k > 3$, the G_3 construction for a Costas array of order $n = q - 3$ is obtained from the G_2 construction using α and β with $\alpha + \beta = 1$ (which has $a_{11} = 1$, since $\alpha^1 + \beta^1 = 1$), by removing the topmost row and the leftmost column.

Definition 6: The G_4 construction occurs for $\text{GF}(q)$ iff there are two primitive elements, α and β , in $\text{GF}(q)$ with $\alpha + \beta = 1$ and $\alpha^2 + \beta^{-1} = 1$.

If both $\alpha + \beta = 1$ and $\alpha^2 + \beta^{-1} = 1$, the G_2 construction for a Costas array of order $n = q - 2$ has $a_{11} = 1$ (from $\alpha^1 + \beta^1 = 1$)

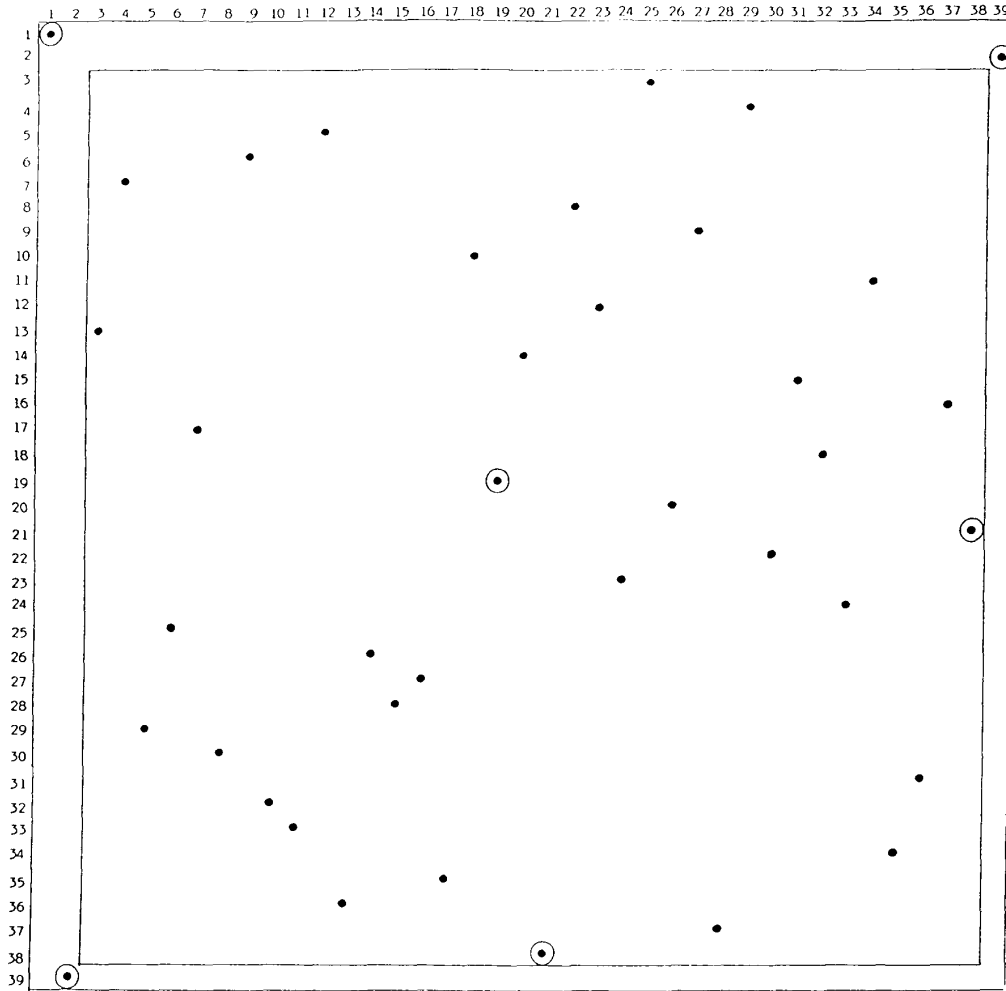


Fig. 1. $p = 41$, α and β the roots of $x^2 - x - 1 = 0 \pmod{41}$, namely $\alpha = 7$, $\beta = 35$.

and $a_{2, q-2} = 1$ (since $\beta^{-1} = \beta^{q-2}$, and thus $\alpha^2 + \beta^{-1} = \alpha^2 + \beta^{q-2} = 1$). Hence, after removing row 1 and column 1 to obtain the G_3 array, $a_{2, q-2} = 1$ is at the upper right corner of this new array. Thus the top row and the rightmost column of the G_3 array are removed to obtain the G_4 Costas Array of order $n = q - 4$.

Here are the further consequences of the G_4 construction.

Theorem 2: If the G_4 construction occurs for $\text{GF}(q)$, then α and β are the two roots of $x^2 - x - 1 = 0$ in $\text{GF}(q)$.

Proof: From $\alpha + \beta = 1$ and $\alpha^2 + \beta^{-1} = 1$, we have

$$\beta = 1 - \alpha,$$

$$\beta^{-1} = 1 - \alpha^2.$$

Multiplying, $\beta\beta^{-1} = (1 - \alpha)(1 - \alpha^2)$,

$$1 = 1 - \alpha - \alpha^2 + \alpha^3$$

$$\alpha^3 - \alpha^2 - \alpha = 0$$

$$\alpha^2 - \alpha - 1 = 0$$

and α is a root of $x^2 - x - 1 = 0$. However, dividing $\alpha^2 - \alpha -$

$1 = 0$ by α , we have

$$\alpha - 1 - \frac{1}{\alpha} = 0, \alpha - \frac{1}{\alpha} = 1, \text{ and since}$$

$$\alpha + \beta = 1, \beta = -\frac{1}{\alpha}, \alpha\beta = -1.$$

Thus, $(x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta = x^2 - x - 1$, and α and β are the two roots of $x^2 - x - 1 = 0$. \square

Theorem 3: The values of q such that the G_4 construction occurs in $\text{GF}(q)$ are precisely the following subset of the values of q for which the T_4 construction occurs: $q = 4, 5, 9$, and those primes p for which the T_4 construction occurs which satisfy either $p \equiv 1 \pmod{20}$ or $p \equiv 9 \pmod{20}$.

Proof: From Theorem 2, the values of q for which the G_4 construction occurs are those for which $x^2 - x - 1 = 0$ has its roots in $\text{GF}(q)$ where these roots are primitive in $\text{GF}(q)$. Analogous to the proof of Theorem 1, the only possible fields of characteristic 2, 3, or 5 which qualify are $\text{GF}(4)$, $\text{GF}(9)$, and $\text{GF}(5)$, and it is easily verified that for each of these three fields the G_4 construction

occurs. Also, if $q = p^k$ and $p > 5$, it is necessary to have $k = 1$, as in the proof of Theorem 1.

For primes $p > 5$, the roots of $x^2 - x - 1 = 0$ are $(1 \pm \sqrt{5})/2 \equiv (1 \pm \sqrt{5})(p+1)/2 \pmod{p}$. As in the proof of Theorem 1, this restricts us to primes for which 5 is a quadratic residue. There is, however, the further restriction that both α and $\beta = -1/\alpha$ must be primitive in $\text{GF}(p)$. Since $1/\alpha$ is primitive iff α is primitive, the extra condition is that the factor of -1 must not destroy primitivity. Now, multiplication by -1 preserves primitivity iff -1 is a quadratic residue mod p , which occurs iff $p \equiv 1 \pmod{4}$. Combined with the requirement that 5 be a quadratic residue, namely $p \equiv \pm 1 \pmod{10}$, this restricts G_4 to primes $p \equiv 1 \pmod{20}$ or $p \equiv 9 \pmod{20}$.

It remains only to show that all primes in these two residue classes modulo 20 for which the T_4 construction occurs also have the G_4 construction, and that no other such primes have the G_4 construction.

If $f(x) = x^2 + x - 1$ then $f(-x) = x^2 - x - 1$, so the roots of $x^2 - x - 1$ are the negatives of the roots of $x^2 + x - 1$. Also, we are considering only primes for which a factor of -1 has no effect on primitivity. We have already seen that the roots of $x^2 - x - 1$ are primitive or imprimitive together in the fields under consideration, so this also must hold for the roots of $x^2 + x - 1$. By Theorem 1, the T_4 construction occurs iff at least one of the roots of $x^2 + x - 1$ is primitive in $\text{GF}(p)$; but for $p \equiv 1, 9 \pmod{20}$ this will mean that both roots are primitive, and also that both roots of $x^2 - x - 1$ will be primitive. Conversely, if a root of $x^2 - x - 1$ is not primitive, then both its roots are imprimitive, and the roots of $x^2 + x - 1$ are also imprimitive. \square

In the G_4 construction for Costas arrays, since $\alpha + \beta = 1$ and $\alpha\beta = -1$, certain symmetries can be expected relative to the main diagonal.

Theorem 4: Every Costas array given by the G_4 construction modulo a prime $p > 5$ has the points $(1, 1)$ and $((p-3)/2, (p-3)/2)$ on the main diagonal, and the pairs of points $(2, p-2)$, $(p-2, 2)$ and $((p+1)/2, p-3)$, $(p-3, (p+1)/2)$ situated symmetrically with respect to the main diagonal.

Proof: Since $\alpha + \beta = \alpha^1 + \beta^1 = 1$, $(1, 1)$ is a point of the array. From $\alpha = -\beta^{-1}$ and $\beta = -\alpha^{-1}$, and using $\alpha^{(p-1)/2} = \beta^{(p-1)/2} = -1$, it follows that $\alpha = (-1)(\beta^{-1}) = \beta^{(p-1)/2}\beta^{-1} = \beta^{(p-3)/2}$, and similarly $\beta = (-1)(\alpha^{-1}) = \alpha^{(p-1)/2}\alpha^{-1} = \alpha^{(p-3)/2}$. Thus, $1 = \alpha + \beta = \beta^{(p-3)/2} + \alpha^{(p-3)/2}$, whence $((p-3)/2, (p-3)/2)$ is a point of the array.

From Definition 2, $\alpha^2 + \beta^{-1} = 1$; that is, $\alpha^2 + \beta^{p-2} = 1$, and $(2, p-2)$ is a point of the array. From $\alpha\beta = -1$, $\beta^2 + \alpha^{-1} = \beta^2 - \beta = 1$, because (as shown in the proof of Theorem 2), β is a root of $x^2 - x - 1 = 0$. Hence, $(-1, 2) = (p-2, 2)$ is also a point of the array. Next, $\alpha^{p-3} + \beta^{(p+1)/2} = \alpha^{-2} + \beta \cdot \beta^{(p-1)/2} = \beta^2 - \beta = 1$, and similarly $\beta^{p-3} + \alpha^{(p+1)/2} = \beta^{-2} + \alpha \cdot \alpha^{(p-1)/2} = \alpha^2 - \alpha = 1$, from which both $(p-3, (p+1)/2)$ and $((p+1)/2, p-3)$ are points of the array. \square

Note: Fig. 1 shows that, except for the six points identified in Theorem 4, none of the other points of the G_4 construction need be symmetrically situated relative to the main diagonal.

REFERENCES

- [1] S. W. Golomb and H. Taylor, "Constructions and properties of Costas arrays," *Proc. IEEE*, vol. 72, pp. 1143-1163, Sept. 1984.
- [2] S. W. Golomb, "Algebraic constructions for Costas arrays," *J. Combin. Theory (A)*, vol. 37, no. 1, pp. 13-21, July 1984.

- [3] O. Moreno and J. Sotero, "Computational approach to conjecture A of Golomb," *Congressus Numerantium*, vol. 70, pp. 7-16, 1990.

Generalized Chirp-Like Polyphase Sequences with Optimum Correlation Properties

Branislav M. Popović

Abstract—A new general class of polyphase sequences with ideal periodic autocorrelation function is presented. The new class of sequences is based on the application of Zadoff-Chu polyphase sequences of length $N = sm^2$, where s and m are any positive integers. It is shown that the generalized chirp-like sequences of odd length have the optimum crosscorrelation function under certain conditions. Finally, recently proposed generalized P4 codes are derived as a special case of the generalized chirp-like sequences.

Index Terms—Sequences, codes, spread-spectrum, radar, pulse compression.

I. INTRODUCTION

Sequences with ideal periodic autocorrelation function [1]–[5] are finding their applications in the field of spread spectrum communications [1], construction of (super) complementary sets [6], [7], etc. These sequences usually have small aperiodic autocorrelation and ambiguity function sidelobes, so they are very useful in the pulse compression radars [7]–[10].

On the other hand, spread spectrum multiple access systems demand minimum possible crosscorrelation between the sequences within selected set of sequences having good periodic autocorrelation function properties. Sarwate [5] has shown that the maximum magnitude of the periodic crosscorrelation function and the maximum magnitude of the periodic autocorrelation function are related through an inequality, which provides a lower bound on one of the maxima if the value of the other is specified. By using this inequality the optimum correlation properties of the set of sequences can be defined. So, when the maximum magnitude of the periodic autocorrelation function equals zero, from the Sarwate's inequality it follows that the lower bound for the maximum magnitude of the periodic crosscorrelation is equal to \sqrt{N} , where N is the length of sequences.

In this correspondence, we shall present a new general class of polyphase sequences with ideal periodic autocorrelation function, having at the same time the optimum crosscorrelation function. The new sequences can be classified as the *modulatable orthogonal sequences*, according to the terminology from [1]. The generalized Frank sequences, of length $N = m^2$, where m is any positive integer, are presented in [1] as the only known example of the modulatable orthogonal sequences. It is noticed that these sequences also have interesting aperiodic autocorrelation function properties [10].

In Section II, the basic definitions are given. In Section III, we present the generalized chirp-like sequences. In Section III-A, we show that the generalized chirp-like sequences have the ideal periodic autocorrelation function. Section III-B concerns the periodic crosscorrelation function of the generalized chirp-like sequences. Finally, in Section IV, we show that the recently proposed general-

Manuscript received June 11, 1991; revised November 19, 1991.

The author is with IMTEL Institute of Microwave Techniques and Electronics, B. Lenjina 165b., 11071 Novi Beograd, Yugoslavia.
IEEE Log Number 9107517.