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 $(1 \pm \sqrt{5})/2 \equiv (1 \pm \sqrt{5})((p+1)/2)$ $(mod\ p)$. 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 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 $p \equiv 1$ (mod 4). Combined with the requirement that 5 be a quadratic residue, namely $p \equiv \pm 1$ (mod 10), this restricts G_4 to primes $p \equiv 1$ (mod 20) or $p \equiv 9$ (mod 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 GF(p); but for $p \equiv 1, 9$ (mod 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. □

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. □

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.

0018-9448/92$03.00 © 1992 IEEE

ized P4 codes are only a special case of the generalized chirp-like sequences.

II. Basic Definitions

The following definitions will be useful.

A primitive nth root of unity W_n is defined as

$$W_n = \exp(-j2\pi r/n), \qquad j = \sqrt{-1}, \tag{1}$$

where r is any integer relatively prime to n.

It can be easily shown that for any integer u, $0 < u \leq n - 1$, the following relation is valid [11]

$$\sum_{k=0}^{n-1} W_n^{\pm uk} = 0, \qquad W_n \neq 1. \tag{2}$$

The sequence $\{s_k\}$ of length L is said to have the ideal periodic autocorrelation function $\theta(p)$ if it satisfies the following relation

$$\theta(p) = \sum_{k=0}^{L-1} s_k s^*_{(k+p) \bmod L} = \begin{cases} E, & p = 0 (\bmod L), \\ 0, & p \neq 0 (\bmod L), \end{cases} \tag{3}$$

where the asterisk denotes complex conjugation, the index $(k + p)$ is computed modulo L, time shift p is assumed to be positive because $\theta(-p) = \theta^*(p)$, $E = \theta(0)$ is energy of the sequence $\{s_k\}$.

Besides the well-known Frank sequences, and recently proposed generalized Frank sequences [1], there is another large class of polyphase sequences with ideal periodic autocorrelation function. The so-called Zadoff–Chu sequences [2], [3] are defined as

$$a_k = \begin{cases} W_N^{k^2/2+qk}, & k = 0, 1, 2, \cdots, N - 1, \quad \text{for } N \text{ even}, \\ W_N^{k(k+1)/2+qk}, & k = 0, 1, 2, \cdots, N - 1, \quad \text{for } N \text{ odd}, \\ & q \text{ is any integer}. \end{cases} \tag{4}$$

The similar construction is proposed by Ipatov [4] and is defined by

$$a_k = W_N^{k^2+qk}, \qquad k = 0, 1, 2, \cdots, N - 1; \quad N \text{ is odd}; \ q \text{ is any integer}. \tag{5}$$

However, one of the referees pointed out that the class of Ipatov sequences is equal to the class of Zadoff–Chu sequences of odd length N. Namely, starting from the definition of Zadoff–Chu sequences of odd length $N = 2t - 1$, it follows

$$W_N^{k(k+1)/2+qk} = \left(W_N^t\right)^{k^2+(1+2q)k}, \tag{6}$$

where $t = 2^{-1} \bmod N$. Since t is relatively prime to N, W_N^t is a primitive Nth root of unity. Hence, the right-hand side of (6) corresponds to the definition of Ipatov sequences.

Based on the Zadoff–Chu sequences, the new, more general, class of polyphase sequences with optimum periodic autocorrelation and crosscorrelation function properties will be presented in the next section.

III. Generalized Chirp-Like Polyphase Sequences

Let $\{a_k\}$, $k = 0, 1, \cdots, N - 1$, be a Zadoff–Chu sequence of length $N = sm^2$, where m and s are any positive integers. Let $\{b_i\}$, $i = 0, \cdots, m - 1$, be any sequence of m complex numbers having the absolute values equal to 1. The generalized chirp-like (GCL) sequence $\{s_k\}$ is defined as

$$s_k = a_k b_{(k) \bmod m}, \qquad k = 0, \cdots, N - 1, \tag{7}$$

where $(k) \bmod m$ means that index k is reduced modulo m.

Example: For $N = 8$, we have that $s = 2$ and $m = 2$, so the generalized chirp-like sequence $\{s_k\}$ is given by

$$\{s_k\} = \{b_0, b_1 W^{0.5}, b_0 W^2, b_1 W^{4.5}, b_0, b_1 W^{4.5}, b_0 W^2, b_1 W^{0.5}\}, \tag{8}$$

where $W = \exp(-j2\pi r/8)$, $j = \sqrt{-1}$, r is any integer relatively prime to $N = 8$, $q = 0$, while b_0 and b_1 are arbitrary complex numbers with magnitude equal to 1.

A. Periodic Autocorrelation Function of the Generalized Chirp-Like Sequences

Theorem 1: The generalized chirp-like polyphase sequences have the ideal periodic autocorrelation function.

Proof: It can be seen in [2] that Zadoff–Chu sequences are defined separately for N even and N odd, in order to satisfy the following condition

$$a_{k+d-N} = a_{k+d}, \tag{9}$$

where d is an arbitrary delay.

It can be easily proved that generalized chirp-like polyphase sequence $\{s_k\}$, defined by (7), also satisfy the condition (9). In that case, the periodic autocorrelation function $\theta(p)$ of the sequence $\{s_k\}$ can be written as

$$\theta(p) = \sum_{k=0}^{N-p-1} s_k s^*_{k+p} + \sum_{k=N-p}^{N-1} s_k s^*_{k+p} = \sum_{k=0}^{N-1} s_k s^*_{k+p}. \tag{10}$$

For N even, from (4), (7), and (10), it follows

$$\theta(p) = W_N^{-p^2/2-qp} \sum_{k=0}^{N-1} W_N^{-pk} b_{(k) \bmod m} b^*_{(k+p) \bmod m}. \tag{11}$$

We shall introduce here the following change of variables:

$$k = ism + d, \qquad i = 0, 1, \cdots, m - 1, \quad d = 0, 1, \cdots, sm - 1. \tag{12}$$

From (11) and (12) we obtain

$$\theta(p) = W_N^{-p^2/2\text{-}qp} \sum_{d=0}^{sm-1} W_N^{-pd} b_{(d) \bmod m} \cdot b^*_{(d+p) \bmod m} \sum_{i=0}^{m-1} W_m^{-ip}. \tag{13}$$

If $p \neq xm$, $x = 0, 1, \cdots, sm - 1$, the second summation in (13) is obviously zero, according to (2).

For $p = xm$, $x = 0, 1, \cdots, sm - 1$, from (13) we obtain

$$\theta(xm) = m W_N^{-(xm)^2/2-qxm} \sum_{d=0}^{sm-1} W_{sm}^{-xd}. \tag{14}$$

If $x \neq 0$, the summation in (14) equals zero according to (2). In that way, we have proved Theorem 1 when N is even. The proof for N odd is the same. □

B. Periodic Crosscorrelation Function of the Generalized Chirp-Like Sequences

Let $\{x_k\}$ and $\{y_k\}$, $k = 0, 1, \cdots, N - 1$, be the two generalized chirp-like sequences of odd length, obtained from any two complex vectors $\{b1_i\}$ and $\{b2_i\}$, $i = 0, 1, \cdots, m-1$, and from the two different primitive Nth roots of unity $\exp(j2\pi v/N)$ and $\exp(j2\pi u/N)$, i.e.,

$$x_k = W_N^{v[k(k+1)/2+qk]} b1_{(k) \bmod m}, \tag{15}$$

$$y_k = W_N^{u[k(k+1)/2+qk]} b2_{(k) \bmod m},$$

$$W_N = \exp(j2\pi/N),$$

$$(v, N) = 1; (u, N) = 1; v \neq u. \ N \text{ is odd}.$$

Theorem 2: The absolute value of the periodic crosscorrelation function between any two generalized chirp-like sequences of odd length N, obtained from the two different primitive Nth roots of unity $\exp(j2\pi v/N)$ and $\exp(j2\pi u/N)$, is constant and equal to $\sqrt{N}$, if $(v-u)$ is relatively prime to N.

Proof: The squared absolute value of the periodic crosscorrelation function $R_{xy}(p)$ of sequences $\{x_k\}$ and $\{y_k\}$ is defined as

$$|R_{xy}(p)|^2 = \sum_{k=0}^{N-1} x_k y_{k+p}^* \sum_{l=0}^{N-1} x_l^* y_{l+p}. \tag{16}$$

Substituting (15) into (16), we obtain

$$\begin{aligned} |R_{xy}(p)|^2 &= \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} W_N^{(v-u)(k-l)[(k+l+1)/2+q]-up(k-l)} \\ &\quad \cdot b1_{(k) \bmod m} b1_{(l) \bmod m}^* \\ &\quad \cdot b2_{(k+p) \bmod m}^* b2_{(l+p) \bmod m} \end{aligned} \tag{17}$$

We can introduce the following change of variables:

$$l = k + e, e = 0, 1, \cdots, N-1. \tag{18}$$

From (17) and (18), we obtain

$$\begin{aligned} |R_{xy}(p)|^2 &= \sum_{k=0}^{N-1} \sum_{e=0}^{N-1} W_N^{-(v-u)e[(2k+e+1)/2+q]+upe} \\ &\quad \cdot b1_{(k) \bmod m} b1_{(k+e) \bmod m}^* \\ &\quad \cdot b2_{(k+p) \bmod m}^* b2_{(k+e+p) \bmod m}. \end{aligned} \tag{19}$$

This expression can be rewritten as

$$|R_{xy}(p)|^2 = \sum_{e=0}^{N-1} W_N^{-(v-u)e[(e+1)/2+q]+pue} S_e, \tag{20}$$

where S_e is defined as

$$\begin{aligned} S_e = \sum_{k=0}^{N-1} & W_N^{-(v-u)ek} \\ & \cdot b1_{(k) \bmod m} b1_{(k+e) \bmod m}^* \\ & \cdot b2_{(k+p) \bmod m}^* b2_{(k+p+e) \bmod m}. \end{aligned} \tag{21}$$

From (20) and (21), it is obvious that

$$|R_{xy}(p)|^2 = N, \qquad \text{if } e = 0. \tag{22}$$

We shall prove now that

$$|R_{xy}(p)|^2 = 0, \qquad \text{if } e \neq 0. \tag{23}$$

We shall introduce the following change of variables

$$k = ism + d, \quad \begin{matrix} i = 0, 1, \cdots, m-1, \\ d = 0, 1, \cdots, sm-1 \end{matrix}. \tag{24}$$

From (21) and (24), we obtain

$$\begin{aligned} S_e = \sum_{d=0}^{sm-1} & W_N^{-(v-u)ed} b1_{(d) \bmod m} b1_{(d+e) \bmod m}^* \\ & \cdot b2_{(d+p) \bmod m}^* b2_{(d+p+e) \bmod m} \cdot \sum_{i=0}^{m-1} W_m^{-(v-u)ei}. \end{aligned} \tag{25}$$

As $(v-u)$ is relatively prime to N, it is also relatively prime to m, so according to (2) the inner summation in (25) is equal to zero if $e \neq xm$, $x = 0, 1, \cdots, sm-1$.

For $e = xm$, $x = 0, 1, \cdots, sm-1$, S_e also becomes equal to zero, i.e..

$$S_e = m \sum_{d=0}^{sm-1} W_{sm}^{-(v-u)xd} = 0, \qquad \text{if } x \neq 0. \tag{26}$$

On that way we have proved the Theorem 2. □

Although the GCL sequences are defined either for odd and even lengths, we have seen that Theorem 2. is valid only for the odd lengths. We shall briefly discuss why it cannot be valid for even lengths.

If the length of sequences N is even, and v and u are integers relatively prime to N, then v and u must be odd. Consequently, $(v-u)$ must be an even integer, because the difference between any two odd integers is always an even integer. In that way, $(v-u)$ can never be relatively prime to N, and that is the reason why the Theorem 2 is defined only for the odd lengths.

It is interesting to note that the same fact is true for the generalized Frank sequences [1]. Namely, the generalized Frank sequences are defined for lengths $N = m^2$, where m is any positive integer. It is shown in [1] that when $(v-u)$ and m are relatively prime, the two generalized Frank sequences, corresponding to v and u, have optimum crosscorrelation function. However, from the previous discussion it follows that the pairs or sets of such sequences, having the optimum crosscorrelation function, can exist only if *m is an odd number*. This important property of the generalized Frank sequences is not explicitly mentioned in [1].

If N is a second power of a prime number m, the set of $m-1$ GCL polyphase sequences can be constructed using $m-1$ different primitive Nth roots of unity. Any pair of sequences in such a set has the optimum crosscorrelation function, having the constant magnitude equal to $\sqrt{N}$.

IV. Generalized P4 Codes

In [9], the authors claimed that it has been found by computer simulation that a P4 code of length $N = m^2$ can be written in terms of an $m \times m$ matrix with mutually orthogonal rows, and with additional property that all rotations of any two columns are mutually orthogonal. By postmultiplying such a matrix with the diagonal matrix B, and concatenating the rows of the resultant matrix, the so-called generalized P4 codes with ideal periodic autocorrelation function can be obtained.

It can be easily seen that the generalized P4 codes can also be obtained from the definition of generalized chirp-like sequences, by taking the sequence $\{a_k\}$ in (7) to be the P4 code.

We shall show below that the P4 codes are only a special case of the Zadoff–Chu sequences, what means that the generalized P4 codes are only a special case of the generalized chirp-like sequences of length $N = m^2$.

The P4 code elements $\{a_k\}$ are given by [8], [9]

$$a_k = \exp\left[j\left(\frac{\pi}{N}k^2 + \pi k\right)\right], \qquad k = 0, 1, \cdots, N-1. \quad (27)$$

where N is any positive integer.

This expression can be rewritten as

$$a_k = W_N^{k^2/2 + (N/2)k}, \qquad W_N = \exp\left(j\frac{2\pi}{N}\right). \quad (28)$$

For N even, the P4 code can be obtained by substituting $q = N/2$ in (4). For N odd, the P4 code can be obtained by substituting $q = (N-1)/2$ in (4).

As the P4 codes are only a special case of the Zadoff–Chu sequences, it is not surprising that the P4 codes have ideal periodic autocorrelation [9].

In [2], it was shown that all the cyclic time shifted versions of the Zadoff–Chu sequences have the same absolute value of the aperiodic autocorrelation function. Consequently, the same is true for the P4 codes [9].

V. Conclusion

In this correspondence, we have presented the new general class of polyphase sequences with ideal periodic autocorrelation function, having at the same time the optimum periodic crosscorrelation function. If the length of sequences N is a second power of a prime number m, the set of $m-1$ generalized chirp-like polyphase sequences can be constructed using $m-1$ different primitive Nth roots of unity. Any pair of sequences in such a set has the optimum crosscorrelation function, with the constant magnitude equal to $\sqrt{N}$.

Compared with the generalized Frank sequences, the generalized chirp-like sequences offer the higher degree of freedom for the choice of sequence length.

Acknowledgment

The author is grateful to the referees for their valuable comments.

References

[1] N. Suehiro and M. Hatori, "Modulatable orthogonal sequences and their application to SSMA systems," *IEEE Trans. Inform. Theory,* vol. 34, pp. 93–100, Jan. 1988.

[2] D. C. Chu, "Polyphase codes with good periodic correlation properties," *IEEE Trans. Inform. Theory,* vol. IT-18, pp. 531–532, July 1972.

[3] R. L. Frank, "Comments on Polyphase codes with good correlation properties," *IEEE Trans. Inform. Theory,* vol. IT-19, p. 244, Mar. 1973.

[4] V. P. Ipatov, "Multiphase sequences spectrums," *Izvestiya VUZ. Radioelektronika (Radioelectronics and Communications Systems),* vol. 22, no. 9, pp. 80–82, 1979.

[5] D. V. Sarwate, "Bounds on crosscorrelation and autocorrelation of sequences," *IEEE Trans. Inform. Theory,* vol. IT-25, pp. 720–724, Nov. 1979.

[6] B. M. Popović, "Complementary sets based on sequences with ideal periodic autocorrelation," *Electron. Lett.,* vol. 26, no. 18, pp. 1428–1430, Aug. 30, 1990.

[7] ——, "Complementary sets of chirp-like polyphase sequences," *Electron. Lett.,* vol. 27, no. 3, pp. 254–255, Jan. 31, 1991.

[8] B. L. Lewis and F. F. Kretschmer, "Linear frequency modulation derived polyphase pulse compression codes," *IEEE Trans. Aerospace Electron. Syst.,* vol. AES-18, no. 5, pp. 637–641, Sept. 1982.

[9] F. F. Kretschmer, Jr. and K. Gerlach, "Low sidelobe radar waveforms derived from orthogonal matrices," *IEEE Trans. on AES,* vol. 27, no. 1, pp. 92–101, Jan. 1991.

[10] B. M. Popović, "Comment on Merit factor of Frank and Chu sequences," *Electron. Lett.,* vol. 27, no. 9, pp. 776–777, April 25, 1991.

[11] R. C. Heimiller, "Author's comment," *IRE Trans.,* vol. IT-8, p. 382, Oct. 1962.

Nonbinary Kasami Sequences over GF(p)

Shyh-Chang Liu and John J. Komo, *Senior Member, IEEE*

***Abstract*—The correlation values and the distribution of these correlation values are presented for the small set of nonbinary Kasami sequences over GF(p) (p prime). The correlation results are an extension of the binary results and have $p+2$ correlation levels. This nonbinary Kasami set is asymptotically optimum with respect to its correlation properties. These sequences are obtained, as in the binary case, from a large primitive polynomial of degree $n = 2m$ and a small primitive polynomial of degree m that yields a sequence length of $p^n - 1$ and maximum nontrivial correlation value of $1 + p^m$. Nonbinary Kasami sequences are directly implemented using shift registers and are applicable for code division multiple access systems.**

***Index Terms*—Kasami sequence, nonbinary, correlation levels and distribution, code division multiple access.**

I. Introduction

The set of binary Kasami sequences over GF(2) can be expressed as [1], [2]

$$S = \{s_i(t) \mid 0 \le t \le N-1, 1 \le i \le 2^m\}, \quad (1)$$

where

$$s_i(t) = \mathrm{tr}_1^m\{\mathrm{tr}_m^n(\alpha^t) + \gamma_i \alpha^{Tt}\}, \quad (2)$$

$n = 2m$, $N = 2^n - 1$, $T = (2^n - 1)/(2^m - 1) = 2^m + 1$, α is a primitive element of GF(2^n), and γ_i takes on each value of GF(2^m) for $1 \le i \le 2^m$. Since α^T is a primitive element of GF(2^m), one $s_i(t)$ is an m-sequence with period N and each other $s_i(t)$ is the sum of an m-sequence with period N and a different phase of an m-sequence with shorter period $2^m - 1$. The shorter m-sequence is a decimation by T of the longer m-sequence and the period of the shorter m-sequence divides the period of the longer m-sequence.

The correlation function, $R_{ij}(\tau)$, $1 \le i, j \le 2^m$, of the ith and jth sequences of S is given by

$$R_{ij}(\tau) = \sum_{t=0}^{N-1} (-1)^{s_i(t+\tau) + s_j(t)}, \qquad 0 \le \tau \le N-1, \quad (3)$$

where $t + \tau$ is modulo N addition. If i and j are not cyclically distinct, $R_{ij}(\tau)$ reduces to the autocorrelation function. The correla-

Manuscript received January 15, 1991; revised November 21, 1991. This work was presented in part at the IEEE International Symposium on Information Theory, Budapest, Hungary, June 24–28, 1991.

The authors are with the Department of Electrical and Computer Engineering, Clemson University, Clemson, SC 29634-0915.

IEEE Log Number 9108026.

0018-9448/92$03.00 © 1992 IEEE