4-Phase Sequences with Near-Optimum Correlation Properties

Serdar Boztaş, Roger Hammons, and P. Vijay Kumar

Abstract—**Two families of 4-phase sequences are constructed using irreducible polynomials over $\mathbb{Z}_4$. Family $\mathcal{A}$ has period $L = 2^r - 1$, size $L+2$, and maximum nontrivial correlation magnitude $C_{\max} \le 1 + \sqrt{L+1}$, where r is a positive integer. Family $\mathcal{B}$ has period $L = 2(2^r - 1)$, size $(L+2)/4$, and $C_{\max} \le 2 + \sqrt{L+2}$. Both families are asymptotically optimal with respect to the Welch lower bound on $C_{\max}$ for complex-valued sequences. Of particular interest, Family $\mathcal{A}$ has the same size and period as the family of binary Gold sequences, but its maximum nontrivial correlation is smaller by a factor of $\sqrt{2}$. Since the Gold family for r odd is optimal with respect to the Welch bound restricted to binary sequences, Family $\mathcal{A}$ is thus superior to the best possible binary design of the same family size. Unlike the Gold design, Families $\mathcal{A}$ and $\mathcal{B}$ are asymptotically optimal whether r is odd or even. Both families are suitable for achieving code-division multiple-access and are easily implemented using shift registers. The exact distribution of correlation values is given for both families.**

Index Terms—**Sequence design, pseudorandom sequences, nonbinary sequences, quadriphase sequences, periodic correlation, code-division multiple-access.**

I. Introduction

THE CODE-DIVISION multiple-access (CDMA) communication system with phase-shift keying (PSK) modulation [17] provides multiple users with simultaneous access to the full communication channel bandwidth by assigning unique phase code sequences to each transmitter-receiver pair. CDMA, therefore, requires a large family of reliably distinguishable code sequences. Family size and maximum nontrivial correlation parameter $C_{\max}$ are commonly used to evaluate sequence designs. Large family size is required in order to support a large number of simultaneous users. Small values of $C_{\max}$ are required to permit unambiguous message synchronization and to minimize interference due to competing, simultaneous traffic across the channel.

In the PSK modulation format, the code symbols are the complex qth roots of unity. Binary PSK ($q = 2$) and quadrature PSK ($q = 4$) are the cases most often used in practice. Welch [21] and Sidelnikov [16] have established well-known lower bounds regarding the smallest possible $C_{\max}$ for a given family size M and sequence length L. In general, (see [9, introduction] for details),

$$C_{\max} = \begin{cases} 0(\sqrt{2L}), & \text{when } q = 2, \\ 0(\sqrt{L}), & \text{when } q > 2. \end{cases}$$

Thus, the bounds suggest that non-binary designs may exist whose $C_{\max}$ performance exceeds that of the best binary designs by a factor of $\sqrt{2}$. In the CDMA context, this corresponds to a 3-dB improvement in signal-to-interference ratio.

In the binary case, the Gold code family with parameters $L = 2^r - 1$ and $M = L + 2$, for r an odd integer, has long been known [14] to be asymptotically optimal, with respect to the Welch and Sidelnikov bounds when restricted to binary sequences. Until recently, no asymptotically optimal 4-phase family has ever been found. The comprehensive 1984 survey of 4-phase sequence designs conducted by Krone and Sarwate [8] showed none to have performance comparable to that of the binary Gold family. In this paper, two different 4-phase families are presented that are asymptotically optimal with respect to the Welch and Sidelnikov bounds. These families achieve the potential $\sqrt{2}$ performance improvement for optimal nonbinary versus binary designs.

In the binary case, primitive irreducible polynomials in $\mathbb{Z}_2[x]$ yield maximal-length binary sequences with ideal autocorrelation functions. Our idea was to investigate the sequences over $\mathbb{Z}_4$ generated by irreducible polynomials belonging to $\mathbb{Z}_4[x]$. It turns out that the maximum period of a sequence generated by a degree r feedback polynomial in $\mathbb{Z}_4[x]$ is $2(2^r - 1)$. Hence, a single shift register can generate an entire family of cyclically distinct 4-phase sequences. Computer results indicated the existence of irreducible polynomials for which the correlation values of such a family are very close to the Welch lower bound. Analysis of these results led to the development of Families $\mathcal{A}$ and $\mathcal{B}$ presented in this paper. Analogous to the role played by the finite fields GF(2^r) in the study of binary m-sequences, the Galois rings GR(4, r) provide a natural framework for the investigation of these maximal-length 4-phase sequences.

Family $\mathcal{A}$ was originally discovered by P. Solé [18], who provided all possible correlation values (but not their distribution) when r is odd and, based on computer results, correctly conjectured on the possible correlation values when r is

Manuscript received April 20, 1990. This work was supported in part by the National Science Foundation under Grants NCR-8719626 and NCR-9016077, and by Hughes Aircraft Company under it Ph.D. fellowship program. This work was presented in part at the IEEE International Symposium on Information Theory, San Diego, CA January 14-19, 1990, and in part at the IEEE International Symposium on Information Theory, Budapest, Hungary, June 24-29, 1991.

S. Boztaş is with the Department of Electrical and Computer Systems Engineering, Monash University, Clayton, Victoria 3168, Australia.

R. Hammons is with the Hughes Aircraft Company, 8433 Fallbrook Avenue, Canoga Park, CA 91304-0445.

P. V. Kumar is with the Communication Sciences Institute, Electrical Engineering-Systems, University of Southern California, Los Angeles, CA 90089-2565.

IEEE Log Number 9106948.

0018-9448/92$03.00

even. Solé develops the theory of these sequences in terms of matrix algebras rather than Galois rings. To prove the correlation values, Solé first sets up an association scheme [13] whose elements are all the sequences of Family $\mathscr{A}$ together with their cyclic shifts. A theorem by Delsarte [6] is then invoked to show that the correlation values of the sequence family are precisely the eigenvalues of the adjacency matrices of this scheme. The proof is then completed by noting that these particular eigenvalues are computed in the paper by Liebler and Mena [11] on distance-regular digraphs. We became aware of the prior work by Solé only after the initial preparation of this paper.[1] P. Udaya and M. U. Siddiqi [19], who were aware of Solé's work, have also independently determined the correlation distribution of Family $\mathscr{A}$ in the case of r even. Family $\mathscr{B}$ is new.

In the Section II of this paper, the construction and correlation properties of the two families are summarized. In Section III, the properties of Galois rings that are important to our derivation are surveyed. In the subsequent sections, Families $\mathscr{A}$ and $\mathscr{B}$ are discussed in detail, leading up to the determination of their distribution of correlation values.

II. Major Results

In the construction of Families $\mathscr{A}$ and $\mathscr{B}$, we consider a certain class of polynomials in $\mathbb{Z}_4[x]$, referred to as *primitive basic irreducible* polynomials, whose modulo 2 projections are primitive, irreducible polynomials in $\mathbb{Z}_2[x]$. Specifically, let $f(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_1 x + a_0$ be a primitive basic irreducible of degree r in $\mathbb{Z}_4[x]$. Consider the rth-order linear recurrence [10, p. 404] [20] over $\mathbb{Z}_4$ having *characteristic polynomial*[2] $f(x)$:

$$s(t) + a_{r-1}s(t-1) + a_{r-2}s(t-2) + \cdots + a_0 s(t-r) = 0. \quad (2.1)$$

Let $S(f)$ denote the set of all sequences over $\mathbb{Z}_4$ satisfying (2-1); $S^+(f) \subset S(f)$, the set of all nonzero solutions; and $S^*(f) \subset S(f)$, the set of solutions whose entries are not all zero-divisors. Family $\mathscr{A}$ is then defined to be the family $S^+(f)$ provided $f(x)$ divides $x^{2^r-1} - 1$ in $\mathbb{Z}_4[x]$. Family $\mathscr{B}$ is defined to be the family $S^*(f)$ provided that 1) $f(x)$ has order $2(2^r - 1)$ and 2) its roots satisfy certain special restrictions (see conditions imposed on root α in Theorem 2).

Let $\zeta_{i,j}(\tau) = \sum_{t=0}^{L-1} \omega^{s_i(t+\tau) - s_j(t)}$ denote the complex periodic correlation between the 4-phase sequences $s_i(t+\tau)$ and $s_j(t)$ of common period L where $\omega \triangleq \sqrt{-1}$. By the *correlation distribution* of a family consisting of M cyclically distinct sequences of common period L, we shall mean the number of triples (i, j, τ) giving rise to each complex correlation ζ. Here, the integers i and j denote indexes between 1 and M inclusive, representing all cyclically distinct members of the family; and the integer τ represents all possible cyclic shifts of the sequence and lies between 0 and $L-1$ inclusive. The *maximum nontrivial correlation parameter* $C_{\max}$ is defined by

$$C_{\max} = \max\{|\zeta_{i,j}(\tau)| : \text{either } i \neq j \text{ or } \tau \neq 0\}. \quad (2.2)$$

In the following theorems, R will denote the Galois ring GR(4, r), T will denote the trace mapping from R onto $\mathbb{Z}_4$, and μ will denote the (modulo 2) projection mapping from R onto the Galois field GF(2^r).

Theorem 1: Family $\mathscr{A}$ has the following description and properties.

1) Every sequence in Family $\mathscr{A}$ has a unique representation as $s_\gamma(t) = T(\gamma\beta^t)$ for some element $\gamma \neq 0$ in R, where β is a fixed unit of R of multiplicative order $2^r - 1$. Conversely, every sequence of this form is a member of Family $\mathscr{A}$.
2) The sequences of Family $\mathscr{A}$ are periodic with common least period $L = 2^r - 1$. There are $M = L + 2$ cyclically distinct sequences in the family.
3) The maximum nontrivial correlation parameter of Family $\mathscr{A}$ is bounded above by $C_{\max} \leq 1 + \sqrt{L+1}$. The family is asymptotically optimal with respect to the Welch and Sidelnikov bounds.
4) The correlation distribution of Family $\mathscr{A}$ is as follows: If $r = 2s + 1$, then

$$\zeta_{i,j}(\tau) = \begin{cases} 2^r - 1, & 2^r + 1 \text{ times}, \\ -1, & 2^{2r} - 2 \text{ times}, \\ -1 + 2^s + \omega 2^s, & (2^{r-2} + 2^{s-1}) \cdot (2^{2r} - 2) \text{ times}, \\ -1 + 2^s - \omega 2^s, & (2^{r-2} + 2^{s-1}) \cdot (2^{2r} - 2) \text{ times}, \\ -1 - 2^s + \omega 2^s, & (2^{r-2} - 2^{s-1}) \cdot (2^{2r} - 2) \text{ times}, \\ -1 - 2^s - \omega 2^s, & (2^{r-2} - 2^{s-1}) \cdot (2^{2r} - 2) \text{ times}. \end{cases}$$

If $r = 2s$, then

$$\zeta_{i,j}(\tau) = \begin{cases} 2^r - 1, & 2^r + 1 \text{ times}, \\ -1, & 2^{2r} - 2 \text{ times}, \\ -1 + 2^s, & (2^{r-2} + 2^{s-1}) \cdot (2^{2r} - 2) \text{ times}, \\ -1 - 2^s, & (2^{r-2} - 2^{s-1}) \cdot (2^{2r} - 2) \text{ times}, \\ -1 + \omega 2^s, & 2^{r-2}(2^{2r} - 2) \text{ times}, \\ -1 - \omega 2^s, & 2^{r-2}(2^{2r} - 2) \text{ times}. \end{cases}$$

[1] Boztaş and Kumar [1], [2], [4] rediscovered Family $\mathscr{A}$ for odd integers r using the fact that the Galois ring GR(4, r) is the splitting ring of certain maximal order polynomials over $\mathbb{Z}_4$. Hammons and Kumar [7] subsequently developed the Galois ring theoretic trace description and analysis of Family $\mathscr{A}$ (r odd and even) which then led to the discovery of Family $\mathscr{B}$.

[2] The *feedback polynomial* commonly associated with the recurrence [22] is the reciprocal $x^r f(1/x)$ of the characteristic polynomial $f(x)$. Note that, if $f(x)$ is a primitive basic irreducible, so is its reciprocal. For our analysis, the characteristic polynomial is more convenient.

Theorem 2: Family $\mathscr{B}$ has the following description and properties.

1) Every sequence in Family $\mathscr{B}$ has a unique representation as $s_\gamma(t) = T(\gamma\alpha^t)$ for some unit γ in R, where $\alpha = (1 + 2\delta)\sqrt{\beta}$ is a fixed unit of R satisfying $\mu\{T(\delta)\} = 1$, $\mu\delta \neq 1$, and β is a unit of R of multiplicative order $2^r - 1$ with $\sqrt{\beta} \triangleq \beta^{2^{r-1}}$. Conversely, every sequence of this form is a member of the family.
2) The sequences of Family $\mathscr{B}$ are periodic with common least period $L = 2(2^r - 1)$. There are $M = (L + 2)/4$ cyclically distinct sequences in the family.
3) The maximum nontrivial correlation parameter of Family $\mathscr{B}$ is bounded above by $C_{\max} \leq 2 + \sqrt{L + 2}$. The family is asymptotically optimal with respect to the Welch and Sidelnikov bounds.
4) The correlation distribution of Family $\mathscr{B}$ is as follows. If $r = 2s$, then

$$\zeta_{i,j}(\tau) = \begin{cases} 2(2^r - 1), & 2^{r-1} \text{ times}, \\ -2, & 2^{2r-1} - 2^{r-1} \text{ times}, \\ -2 + 2^s + \omega 2^s, & (2^{r-2} + 2^{s-1}) \cdot (2^{2r-1} - 2^r) \text{ times}, \\ -2 + 2^s - \omega 2^s, & (2^{r-2} + 2^{s-1}) \cdot (2^{2r-1} - 2^r) \text{ times}, \\ -2 - 2^s + \omega 2^s, & (2^{r-2} - 2^{s-1}) \cdot (2^{2r-1} - 2^r) \text{ times}, \\ -2 - 2^s - \omega 2^s, & (2^{r-2} - 2^{s-1}) \cdot (2^{2r-1} - 2^r) \text{ times}. \end{cases}$$

If $r = 2s + 1$, then

$$\zeta_{i,j}(\tau) = \begin{cases} 2(2^r - 1), & 2^{r-1} \text{ times}, \\ -2, & 2^{2r-1} - 2^{r-1} \text{ times}, \\ -2 + 2^{s+1}, & (2^{r-2} + 2^s) \cdot (2^{2r-1} - 2^r) \text{ times}, \\ -2 - 2^{s+1}, & (2^{r-2} - 2^s) \cdot (2^{2r-1} - 2^r) \text{ times}, \\ -2 + \omega 2^{s+1}, & 2^{r-2}(2^{2r-1} - 2r) \text{ times}, \\ -2 - \omega 2^{s+1}, & 2^{r-2}(2^{2r-1} - 2^r) \text{ times}. \end{cases}$$

III. Galois Ring Preliminaries

Ring Structure: The Galois ring GR(4, r) denotes a Galois extension of dimension r over the integer ring $\mathbb{Z}_4$. It turns out [12] that as in the case of finite fields, Galois rings may be constructed as quotients of the associated polynomial ring—in this case, $\mathbb{Z}_4[x]$. The following notation will be used. For an integer $a \in \mathbb{Z}_4$, let $\bar{a} \in \mathbb{Z}_2$ denote its customary reduction modulo 2. Define the polynomial reduction mapping $\mu: \mathbb{Z}_4[x] \to \mathbb{Z}_2[x]$ in the obvious way:

$$f(x) = \sum_{i=0}^{k} a_i x^i \xrightarrow{\mu} \bar{f}(x) = \sum_{i=0}^{k} \bar{a}_i x^i.$$

A monic polynomial $f \in \mathbb{Z}_4[x]$ is said to be a *basic irreducible* if its projection μf is irreducible over $\mathbb{Z}_2[x]$. It can be shown [12] that every Galois ring GR(4, r) is isomorphic to a quotient ring $\mathbb{Z}_4[x]/(f(x))$, where $f(x)$ is a basic irreducible in $\mathbb{Z}_4[x]$. Consequently, as a $\mathbb{Z}_4$-module, GR(4, r) = $\langle 1, \beta, \beta^2, \cdots, \beta^{r-1} \rangle$, where β is a root of $f(x)$ in the Galois ring. Since μf is irreducible in $\mathbb{Z}_2[x]$, GF(2^r) $\cong \mathbb{Z}_2[x]/(\mu f(x))$. Thus, the mapping μ induces an obvious ring homomorphism of GR(4, r) onto GF(2^r). For convenience, this homomorphism will also be denoted μ and its action will be referred to as *reduction modulo 2* in the Galois ring.

For the remainder of this paper, let R = GR(4, r), and let R^* denote the multiplicative group of units of R. Similarly, let K = GF(2^r), with its group of units K^*. It is not hard to show that the Galois ring R is a local ring whose zero divisors form the unique maximal ideal $2R$. The units of R may be expressed [12] as a direct product of groups $R^* = G_1 \times G_2$, where G_1 is a cyclic group of order $2^r - 1$ and G_2 is a direct product of r cyclic groups of order 2.

Obviously, the maximal ideal $2R$ is the kernel of μ in R, so that $R/(2R) \cong K$. In addition, there is a natural identification of elements in K with elements in R that simplifies computations within the ideal $2R$. First, note that a polynomial with only 0 and 1 as coefficients can be regarded as either an element of $\mathbb{Z}_4[x]$ or and element of $\mathbb{Z}_2[x]$. For any polynomial $g(x) \in \mathbb{Z}_2[x]$, let $\underline{g}(x)$ denote the same polynomial viewed as an element of $\mathbb{Z}_4[x]$. Then, consider the embedding $\iota: K \to R$ given by

$$g(x) + (\bar{f}(x)) \in \mathbb{Z}_2[x]/(\bar{f}(x)) \xrightarrow{\iota} \underline{g}(x) + (f(x)) \in \mathbb{Z}_4[x]/(f(x)),$$

where $\bar{f} = \mu f$. Of course, ι is not a ring homomorphism, but the following relations hold for arbitrary γ and ν in R and their projections $\bar{\gamma} = \mu(\gamma)$ and $\bar{\nu} = \mu(\nu)$ in K:

$$\begin{aligned} 2\gamma &= 2\iota(\bar{\gamma}), \\ 2(\gamma + \nu) &= 2\iota(\bar{\gamma} + \bar{\nu}), \\ 2(\gamma\nu) &= 2\iota(\bar{\gamma}\bar{\nu}). \end{aligned} \tag{3.1}$$

Note that the computations in parentheses on the left side of (3.1) occur in R, while those in parentheses on the right occur in K. Thus, arithmetic problems involving only the zero divisors of R can often be solved more conveniently in the finite field. When the context is clear, the embedding ι will not be explicitly noted, and the element $\iota(\bar{\gamma})$ will be written as simply $\bar{\gamma}$.

Automorphism Group: A basic irreducible polynomial in $\mathbb{Z}_4[x]$ of degree r will be called a *primitive basic irreducible* if its projection by μ in $\mathbb{Z}_2[x]$ is primitive. Let

$f(x) \in \mathbb{Z}_4[x]$ be such a polynomial. Since $\mu f(x)$ is primitive, it factors in $K[x]$ as

$$\mu f(x) = \prod_{i=0}^{r-1} (x - \theta^{2^i}), \tag{3.2}$$

where θ is a primitive element of K. By [12], Lemma XV.1, $f(x)$ has exactly r distinct roots $\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{r-1}$ in R, where $\mu\alpha_i = \theta^{2^i}$.

Now consider the special case in which $f(x)$ divides $x^{2^r-1} - 1$ in $\mathbb{Z}_4[x]$, and let $\beta = \alpha_0$. Since $f(x)$ divides $x^{2^r-1} - 1$ and $\mu\beta = \theta$ is primitive in K, it follow that β has multiplicative order $2^r - 1$ in R and thus generates the multiplicative subgroup G_1 of R^*. Throughout the paper, β will denote a generator of G_1 whose projection $\mu\beta = \theta$ is a primitive element in GF(2^r). Since all roots of $x^{2^r-1} - 1$ in R belong to $G_1 = \{\beta, \beta^2, \beta^3, \cdots, \beta^{2^r-1}\}$, it follows that the roots of $f(x)$ are $\alpha_i = \beta^{2^i}$. Now $\beta^t - \beta^s$ is a unit whenever $t \neq s \pmod{2^r - 1}$. Hence (see also [15]), $f(x)$ factors in $R[x]$ as

$$f(x) = \prod_{i=0}^{r-1} (x - \beta^{2^i}). \tag{3.3}$$

From the previous section, $R = \langle 1, \beta, \beta^2, \cdots, \beta^{r-1}\rangle$ as a $\mathbb{Z}_4$-module, so that every Galois automorphism is uniquely determined by its action on β. Since the polynomial $f(x)$ is fixed by every Galois automorphism, it follows that the Galois group of R consists of exactly r different permutations of the roots in (3.3). Thus, the Galois group of R is isomorphic to that of K and is generated by an automorphism σ_R mapping β to β^2.

Let σ_K denote the corresponding Galois automorphism of K that maps θ to θ^2, and let tr: $K \to \mathbb{Z}_2$ denote the finite filed trace mapping. Similarly, let T: $R \to \mathbb{Z}_4$ denote the Galois ring trace mapping defined by $T(\gamma) = \sum_{i=1}^{r} \sigma_R^i(\gamma)$. The following commutativity relationships between the Galois ring and the corresponding Galois field are easily verified:

$$\mu \circ \sigma_R = \sigma_K \circ \mu,$$
$$\mu \circ T = \mathrm{tr} \circ \mu. \tag{3.4}$$

In particular, since tr is not identically zero, it follows that the Galois ring trace is *nontrivial* in the sense that $T(\gamma)$ is a unit for at least one element $\gamma \in R$ (i.e., T is onto).

Trace Distribution and Related Exponential Sums: In order to study the distribution of trace values, let each element $x \in R$ be associated with the r-tuple $\underline{V}_x \triangleq (T(x\beta^0), T(x\beta^1), \cdots, T(x\beta^{r-1}))$. Since $R = \langle 1, \beta, \beta^2, \cdots, \beta^{r-1}\rangle$ as a $\mathbb{Z}_4$-module and T is nontrivial, this association sets up a $1 - 1$ correspondence between the elements of R and the set of all r-tuples over $\mathbb{Z}_4$. As a result, as x ranges over R, each of the vector components $\underline{V}_x(i) = T(x\beta^i)$ must assume each of the values 0, 1, 2, and 3 equally often. Furthermore, every r-tuple having only 0 and 2 as entries appears precisely once as $\underline{V}_x$ for some $x \in R \setminus R^*$. Therefore, as x ranges over $R \setminus R^*$, each vector component assumes the values 0 and 2 equally often. Based on these results, the following exponential sums are easily computed:

$$\sum_{x\in R} \omega^{T(x)} = \sum_{x\in R\setminus R^*} \omega^{T(x)} = \sum_{x\in R^*} \omega^{T(x)} = 0, \tag{3.5}$$

$$\sum_{x\in R} (-1)^{T(x)} = 0,$$

$$\sum_{x\in R\setminus R^*} (-1)^{T(x)} = -\sum_{x\in R^*} (-1)^{T(x)} = 2^r. \tag{3.6}$$

IV. Family $\mathscr{A}$

Trace Description: Let $f(x)$ be a primitive basic irreducible dividing $x^{2^r-1} - 1$ in $\mathbb{Z}_4[x]$. Family $\mathscr{A}$ is defined to be the set $S^+(f)$ of nonzero sequences satisfying the linear recurrence over $\mathbb{Z}_4$ with characteristic polynomial $f(x)$. As discussed in the previous section, $R \cong \mathbb{Z}_4/(f)$ and $R = \langle 1, \beta, \beta^2, \cdots, \beta^{r-1}\rangle$ as a $\mathbb{Z}_4$-module, where β is a root of $f(x)$ in R. Furthermore, β is a generator of the cyclic group G_1 of R^*, and $f(x)$ factors over $R[x]$ as shown in (3.3).

Theorem 3: For every $\gamma \in R \setminus \{0\}$, the sequence $\{s_\gamma(t)\}_{t=0}^{\infty}$ defined by $s\gamma(t) \triangleq T(\gamma\beta^t)$ is a member of Family $\mathscr{A}$. Conversely, every sequence on Family $\mathscr{A}$ is of this form for a unique $\gamma \in R \setminus \{0\}$.

Proof: Direct substitution shows that all sequences of this form satisfy the linear recurrence defining Family $\mathscr{A}$. A simple counting argument than shows that these sequences in fact exhaust $\mathscr{A}$. □

From the trace description, it follows that the sequences of Family $\mathscr{A}$ are periodic with period $L = 2^r - 1$ equal to the multiplicative order of β in R. When γ is a unit, the corresponding sequences $s_\gamma \in \mathscr{A}$ are partitioned into cyclically distinct equivalence classes according to the cosets γG_1 of G_1 in R^*. When $\gamma \neq 0$ is a nonunit, there is a unit $\nu \in R^*$ such that $\gamma = 2\nu$. In this case, using (3.1) and (3.4),

$$s_\gamma(t) = T(\gamma\beta^t) = 2T(\nu\beta^t) = 2\mu\{T(\nu\beta^t)\} = 2\,\mathrm{tr}(\bar{\nu}\theta^t), \tag{4.1}$$

where $\bar{\nu} = \mu\nu$. Therefore, the nonunits $\gamma \neq 0$ give rise to 4-phase sequences that are cyclically equivalent, corresponding to all cyclic shifts of twice a binary m-sequence. Since there are 2^r cosets of G_1 in R^*, Family $\mathscr{A}$ thus consists of $2^r + 1$ cyclically distinct sequences. From (4.1), it is clear that the number of distinct versions of Family $\mathscr{A}$ is equal to the number of distinct binary m-sequences.

Since $\beta^t - \beta^s$ is a unit whenever $t \neq s \pmod{2^r - 1}$, the set $2G_1$ consists precisely of the zero divisors $\gamma \neq 0$. Hence, the cyclic equivalence classes of Family $\mathscr{A}$ are in $1 - 1$ correspondence with the partitioning of $R \setminus \{0\}$ into subsets $\gamma_0 G_1, \gamma_1 G_1, \gamma_2 G_1, \cdots, \gamma_{2^r} G_1$, where $\gamma_0 \neq 0$ is a nonunit and the remaining γ_i are units. In the following, $\Gamma \triangleq \{\gamma_0, \gamma_1, \cdots, \gamma_{2^r}\}$ will denote a standard set of *cyclic equivalence class representatives* in R. The corresponding sequences $s_i(t) = T(\gamma_i\beta^t)$ then provide a *standard enu-*

meration of the cyclically distinct sequences of Family $\mathscr{A}$. Similarly, $\Gamma^* = \{\gamma_1, \cdots, \gamma_{2^r}\} \subset \Gamma$ provides a standard set of coset representatives of G_1 in R^*.

Correlation Properties: Let $s(t) = T(\gamma\beta^t)$ and $s'(t) = T(\gamma'\beta^t)$ be distinct sequences in Family $\mathscr{A}$. The complex cross-correlation of the two sequences is given by

$$\zeta = \sum_{t=0}^{2^r-2} \omega^{s(t)-s'(t)} = \sum_{t=0}^{2^r-2} \omega^{T((\gamma-\gamma')\beta^t)} = \sum_{x\in G_1} \omega^{T(\gamma x)},$$

where $\gamma \triangleq \gamma - \gamma'$. Its squared magnitude is

$$|\zeta|^2 = \sum_{t=0}^{2^r-2}\sum_{t'=0}^{2^r-2} \omega^{T(\gamma(\beta^t-\beta^{t'}))} = \sum_{t=0}^{2^r-2}\sum_{x\in G_1} \omega^{T(\gamma(1-\beta^t)x)}. \tag{4.2}$$

The right side of (4.2) will now be related to the exponential sum $\sum_{x\in R^*}\omega^{T(x)}$ whose value is known from (3.5). When $t \neq 0, 1-\beta^t$ is a unit and thus may be represented as

$$1 - \beta^t = \beta^{t'}(1 + 2z), \tag{4.3}$$

for some integer $t'(0 \le t' \le 2^r - 2)$ and some $z \in R$. In the finite field K, the Zech logarithm [5] $\pi(t)$ is implicitly defined by the relationship $\theta^{\pi(t)} = 1 - \theta^t$. Reducing (4.3) modulo 2 shows that $t' = \pi(t)$. Note that the coset of G_1 containing $1 - \beta^t$ is entirely determined by the factor $1 + 2z$. Of course, while the element $2z$ is uniquely determined by (4.3), the element z itself is not unique.

Lemma 1: In R, the element $1 - \beta^t$, for $0 < t \le 2^r - 2$, may be expressed as

$$1 - \beta^t = \beta^{\pi(t)}\left(1 + 2\frac{\beta^{t/2}}{1+\beta^{t/2}}\right).$$

Consequently, the cosets of G_1 in R^* of the form $(1-\beta^t)G_1$ are all distinct and cover all cosets of G_1 with the exception of the two cosets $\pm G_1$.

Proof: Squaring both sides of (4.3) gives $1 - 2\beta + \beta^{2t} = \beta^{2\pi(t)}$. Applying the automorphism σ_R to both sides gives $1 - \beta^{2t} = \beta^{2\pi(t)}(1 + 2z^2)$, since $\sigma_R(2z) = 2z^2$ by repeated application of (3.1) and (3.4). Combining these results yields the equation $2(\beta^{2t} - \beta^t) = 2z^2\beta^{2\pi(t)}$ to be solved within the ideal $2R$. By (3.1), it suffices to solve $\theta^{2t} + \theta^t = \bar{z}^2\theta^{2\pi(t)}$ in K. Since one can show $\bar{z} = \theta^{t/2}/[1 + \theta^{t/2}]$ in K, it follows that $z = \beta^{t/2}/[1 + \beta^{t/2}]$ satisfies (4.3) as required.

Note that, as t varies from 1 to $2^r - 2$, $\bar{z} = \theta^{t/2}/[1 + \theta^{t/2}]$ assumes each value in K precisely once, except for 0 and 1 which are never assumed. Since $1 + 2z$ and $1 + 2z'$ are in the same coset of G_1 in R^* iff $\mu z = \mu z'$, all cosets of G_1 in R^* except $\pm G_1$ are of the form $(1-\beta^t)G_1$. □

Consequently, for arbitrary $\nu \in R^*$, one may take

$$\Gamma_\nu = \{2\nu, -\nu, +\nu, (1-\beta)\nu, (1-\beta^2)\nu, \cdots, (1-\beta^{2^r-2})\nu\} \tag{4.4}$$

as the standard set of cyclic equivalence class representatives in R.

Theorem 4: Let $\zeta = \sum_{x\in G_1}\omega^{T(\gamma x)}$. The following relationships hold:

1) if $\gamma \in R^*$ then ζ lies on the circle $|1 + \zeta|^2 = 2^r$;
2) if $\gamma \in R \setminus R^*$ and $\gamma \neq 0$, then $\zeta = -1$.

Proof: In the case of 1), let γ be a unit of R and consider

$$|\zeta|^2 = \sum_{t=0}^{2^r-2}\sum_{x\in G_1}\omega^{T(\gamma(1-\beta^t)x)} = \sum_{x\in G_1}\omega^{T(0)} + \sum_{t=1}^{2^r-2}\sum_{x\in G_1}\omega^{T(\gamma(1-\beta^t)x)}.$$

By (4.4), this can be rewritten as

$$|\zeta|^2 = (2^r - 1) + \sum_{x\in R^*}\omega^{T(x)} - \zeta - \zeta^*;$$

so that $|1 + \zeta|^2 = 2^r$ as claimed.

In the case of 2), let $\gamma \neq 0$ be a nonunit of R. As in (4.1),

$$\sum_{x\in G_1}\omega^{T(\gamma x)} = \sum_{t=0}^{2^r-2}\omega^{2T(\nu\beta^t)} = \sum_{t=0}^{2^r-2}(-1)^{tr(\bar{\nu}\theta^t)} = -1,$$

from properties of the binary trace function. □

Since the correlations have integral real and imaginary parts, all possible values of ζ can be found by solving an elementary Diophantine equation. The conjugate symmetry of the correlation values together with known moments turn out to be sufficient to completely determine the weight distribution of Family $\mathscr{A}$.

Proposition 1: For $\gamma \in R^*$, the only possible values of $\zeta = \sum_{x\in G_1}\omega^{T(\gamma x)}$ are as follows:

1) if $r = 2s + 1$, then $\zeta = -1 \pm 2^s \pm \omega 2^s$;
2) if $r = 2s$, then $\zeta = -1 \pm 2^s$ or $\zeta = -1 \pm \omega 2^s$.

Proof: From the previous theorem, $(1 + \mathrm{Re}\{\zeta\})^2 + (\mathrm{Im}\{\zeta\})^2 = 2^r$. Since $\mathrm{Re}\{\zeta\}$ and $\mathrm{Im}\{\zeta\}$ are integers, the desired results follow by a simple induction argument. □

Theorem 5 (Weight Distribution): The correlation sum $\zeta(\gamma) = \sum_{x\in G_1}\omega^{T(\gamma x)}$ assumes the following distribution of values as γ varies over R:

1) If $r = 2s + 1$, then

$$\zeta(\gamma) = \begin{cases} 2^r - 1, & \text{for } \gamma = 0, \\ -1, & \text{for } 2^r - 1 \text{ nonunits } \gamma \neq 0, \\ -1 + 2^s + \omega 2^s, & \text{for } (2^{r-2} + 2^{s-1}) \cdot (2^r - 1) \text{ units } \gamma, \\ -1 + 2^s - \omega 2^s, & \text{for } (2^{r-2} + 2^{s-1}) \cdot (2^r - 1) \text{ units } \gamma, \\ -1 - 2^s + \omega 2^s, & \text{for } (2^{r-2} - 2^{s-1}) \cdot (2^r - 1) \text{ units } \gamma, \\ -1 - 2^s - \omega 2^s, & \text{for } (2^{r-2} - 2^{s-1}) \cdot (2^r - 1) \text{ units } \gamma. \end{cases}$$

2) If $r = 2s$, then

$$\zeta(\gamma) = \begin{cases} 2^r - 1, & \text{for } \gamma = 0, \\ -1, & \text{for } 2^r - 1 \text{ nonunits } \gamma \neq 0, \\ -1 + 2^s, & \text{for } (2^{r-2} + 2^{s-1}) \cdot (2^r - 1) \text{ units } \gamma, \\ -1 - 2^s, & \text{for } (2^{r-2} - 2^{s-1}) \cdot (2^r - 1) \text{ units } \gamma, \\ -1 + \omega 2^s, & \text{for } 2^{r-2}(2^r - 1) \text{ units } \gamma, \\ -1 - \omega 2^s, & \text{for } 2^{r-2}(2^r - 1) \text{ units } \gamma. \end{cases}$$

Proof: In either case, when γ is a nonunit, the distribution is clear. Hence, assume $\gamma \in R^*$ throughout the following. First consider case 1) in which r is odd. Let the standard set Γ^* of coset representatives of G_1 in R^* be partitioned according to the possible values of ζ:

$$\Gamma_{+,+} = \{\gamma \in \Gamma^* \mid \zeta(\gamma) = -1 + 2^s + \omega 2^s\},$$
$$\Gamma_{+,-} = \{\gamma \in \Gamma^* \mid \zeta(\gamma) = -1 + 2^s - \omega 2^s\},$$
$$\Gamma_{-,+} = \{\gamma \in \Gamma^* \mid \zeta(\gamma) = -1 - 2^s + \omega 2^s\},$$
$$\Gamma_{-,-} = \{\gamma \in \Gamma^* \mid \zeta(\gamma) = -1 - 2^s - \omega 2^s\}.$$

Note that the cosets γG_1 and $-\gamma G_1$ are distinct for $\gamma \in R^*$ and that the corresponding values of the correlation sums are complex conjugates ζ and ζ^*. As a result, one may let $M = |\Gamma_{+,+}| = |\Gamma_{+,-}|$ and $N = |\Gamma_{-,+}| = |\Gamma_{-,-}|$ denote the number of cosets of each type. Since there are 2^r cosets of G_1 in R^*,

$$2(M + N) = 2^r. \tag{4.5}$$

Now, expand the first moment sum $\sum_{x \in R^*} \omega^{T(x)} = 0$ over the cosets of G_1 in R^* as follows:

$$\sum_{i=1}^{2^r} \sum_{x \in \gamma_i G_1} \omega^{T(x)} = \sum_{\gamma \in \Gamma_{+,+}} \zeta(\gamma) + \sum_{\gamma \in \Gamma_{+,-}} \zeta(\gamma) + \sum_{\gamma \in \Gamma_{-,+}} \zeta(\gamma) + \sum_{\gamma \in \Gamma_{-,-}} \zeta(\gamma) = 0.$$

Since $\zeta(\gamma)$ is constant in each of these sums, the result is

$$2(M + N) = 2^{s+1}(M - N). \tag{4.6}$$

Solving (4.5) and (4.6) gives $M = 2^{r-2} + 2^{s-1}$ and $N = 2^{r-2} - 2^{s-1}$. Since each coset of G_1 has $2^r - 1$ elements, the weight distribution for the case r odd is established.

Now consider case 2) in which r is even. The analysis now involves three unknowns:

$$M = |\{\gamma \in \Gamma^* : \zeta(\gamma) = -1 + 2^s\}|,$$
$$N = |\{\gamma \in \Gamma^* : \zeta(\gamma) = -1 - 2^s\}|,$$
$$P = |\{\gamma \in \Gamma^* : \zeta(\gamma) = -1 + \omega 2^s\}| = |\{\gamma \in \Gamma^* : \zeta(\gamma) = -1 - \omega 2^s\}|.$$

Proceeding as before, it is easy to show that (4.5) and (4.6) are now replaced by

$$M + N + 2P = 2^r,$$
$$M + N + 2P = 2^s(M - N). \tag{4.7}$$

A third equation sufficient to solve for M, N, and P can be derived by considering the following second moment:

$$\begin{aligned} \sum_{i=1}^{2^r} \left[\sum_{x \in \gamma_i G_1} \omega^{T(x)} \right]^2 &= \sum_{i=1}^{2^r} \left[\sum_{t=0}^{2^{r-2}} \sum_{t'=0}^{2^{r-2}} \omega^{T(\gamma_i(\beta^t + \beta^{t'}))} \right] \\ &= \sum_{i=1}^{2^r} \left[\sum_{t=0}^{2^{r-2}} \sum_{\tau=0}^{2^{r-2}} \omega^{T(\gamma_i \beta^t (1 + \beta^\tau))} \right] \\ &= \sum_{i=1}^{2^r} \left[\sum_{t=0}^{2^{r-2}} \omega^{T(2\gamma_i \beta^t)} \right] \\ &\quad + \sum_{i=1}^{2^r} \left[\sum_{t=0}^{2^{r-2}} \sum_{\tau=1}^{2^{r-2}} \omega^{T(\gamma_i \beta^t (1 + \beta^\tau))} \right] \\ &= \sum_{x \in R^*} (-1)^{T(x)} + \sum_{\tau=1}^{2^{r-2}} \sum_{x \in R^*} \omega^{T(x)} \\ &= -2^r. \end{aligned} \tag{4.8}$$

When the left side of (4.8) is rewritten in terms of M, N, and P and simplified using (4.7), one obtains

$$M + N - 2P = 0. \tag{4.9}$$

The solution is then $M = 2^{r-2} + 2^{s-1}$, $N = 2^{r-2} - 2^{s-1}$, and $P = 2^{r-2}$. This establishes the weight distribution for r even. □

For the correlation distribution analysis, attention is restricted to the cyclically distinct, standard enumeration $\{s_0(t), s_1(t), \cdots, s_{2^r}(t)\}$ of Family $\mathscr{A}$. Note that $\zeta_{i,j}(\gamma) = \sum_{t=0}^{2^r-2} \omega^{s_i(t+\tau) - s_j(t)} = \zeta(\gamma)$, where

$$\gamma = \gamma_i \beta^\tau - \gamma_j, \quad \gamma_i, \gamma_j \in \Gamma. \tag{4.10}$$

Thus, the crux of the problem lies in determining for each $\gamma \in R$ the number of triples (i, j, τ) satisfying (4.10).

Theorem 6 (Correlation Distribution): For Family $\mathscr{A}$, the correlation distribution is as follows

1) If $r = 2s + 1$, then

$$\zeta_{i,j}(\tau) = \begin{cases} 2^r - 1, & 2^r + 1 \text{ times}, \\ -1, & 2^{2r} - 2 \text{ times}, \\ -1 + 2^s + \omega 2^s, & (2^{r-2} + 2^{s-1}) \cdot (2^{2r} - 2) \text{ times}, \\ -1 + 2^s - \omega 2^s, & (2^{r-2} + 2^{s-1}) \cdot (2^{2r} - 2) \text{ times}, \\ -1 - 2^s + \omega 2^s, & (2^{r-2} - 2^{s-1}) \cdot (2^{2r} - 2) \text{ times}, \\ -1 - 2^s - \omega 2^s, & (2^{r-2} - 2^{s-1}) \cdot (2^{2r} - 2) \text{ times}. \end{cases}$$

2) If $r = 2s$, then

$$\zeta_{i,j}(\tau) = \begin{cases} 2^r - 1, & 2^r + 1 \text{ times}, \\ -1, & 2^{2r} - 2 \text{ times}, \\ -1 + 2^s, & (2^{r-2} + 2^{s-1}) \cdot (2^{2r} - 2) \text{ times}, \\ -1 - 2^s, & (2^{r-2} - 2^{s-1}) \cdot (2^{2r} - 2) \text{ times}, \\ -1 + \omega 2^s, & 2^{r-2}(2^{2r} - 2) \text{ times}, \\ -1 - \omega 2^s, & 2^{r-2}(2^{2r} - 2) \text{ times}. \end{cases}$$

Proof: Consider (4.10) with $\gamma \in R$ fixed. In any solution, the parameters i and τ are uniquely determined by the choice of γ_j. Hence the number of triples (i, j, τ) satisfying (4.10) is equal to the number of possible choices for γ_j from Γ. The special case $\gamma = 0$ permits a solution for each choice of γ_j, so there is a total of $2^r + 1$ triples in this case. When $\gamma \neq 0$, (4.10) has a solution iff $\gamma \neq -\gamma_j$. In this case, note that by (4.4) the set $\{-\gamma_0, -\gamma_1, \cdots, -\gamma_{2^r}\}$ is also a valid set of distinct cyclic equivalence class representatives in R. Thus, if γ is not one of the equivalence class representatives $\{-\gamma_i\}_{i=0}^{2^r}$, all $2^r + 1$ choices of γ_j in Γ yield solutions. If γ is such a representative, only 2^r of the $\gamma_j \in \Gamma$ are possible. Hence, within each cyclic equivalence class in R, there are $2^r - 2$ members having $2^r + 1$ solutions each and one member having 2^r solutions. Thus, each cyclic equivalence class in R provides a total of $(2^r + 1)(2^r - 2) + 2^r = 4^r - 2$ triples (i, j, τ) satisfying (4.10). The correlation distribution then follows directly from the weight distribution results (dividing by $2^r - 1$ and multiplying by $4^r - 2$ as appropriate). □

In-phase and Quadrature Sequences: In the engineering literature, it is customary to regard a 4-phase sequence $s(t)$ as the composition of two binary sequences $u(t)$ and $v(t)$ referred to as the in-phase and quadrature components, respectively. From [8, (4)],

$$\omega^{s(t)} = \frac{1}{2}(1 + \omega)(-1)^{u(t)} + \frac{1}{2}(1 - \omega)(-1)^{v(t)}.$$

On the other hand, every 4-phase sequence in Family $\mathscr{A}$ may be uniquely written as

$$s(t) = 2a(t) + b(t),$$

where $a(t)$ and $b(t)$ are binary sequences with symbols $\{0, 1\}$. Note that $b(t) = s^2(t)$ and $2a(t) = s(t) - s^2(t)$. Using these relationships, one can show after some work (see [1]) that, for Family $\mathscr{A}$ with $r = 2s + 1$, the binary components $a(t)$ and $b(t)$ are of the form

$$a(t) = \operatorname{tr}(x\theta^t) + \sum_{i=1}^{s} \operatorname{tr}\left((w\theta^t)^{1+2^i}\right),$$

$$b(t) = \operatorname{tr}(w\theta^t),$$

where $w, x \in \mathrm{GF}(2^r)$ and either w or x is nonzero.

It is then straightforward to show that the in-phase and quadrature components, $u(t)$ and $v(t)$, of $s(t)$ are given by

$$u(t) = a(t),$$

$$v(t) = a(t) + b(t).$$

Thus, by adding these components, one obtains a binary m-sequence, which could prove important in practice.

Example: Family $\mathscr{A}$ is defined as the set of all nonzero solutions of a linear recurrence over $\mathbb{Z}_4$ whose characteristic polynomial is a primitive basic irreducible dividing $x^{2^r-1} - 1$ in $\mathbb{Z}_4[x]$. Table I lists the primitive basic irreducible polynomials over $\mathbb{Z}_4$ up to degree 10 that are suitable for generating Family $\mathscr{A}$. Any of the polynomials of degree r from the table may be used to generate Family $\mathscr{A}$ with parameters $L = 2^r - 1$ and $M = 2^r + 1$. Note that the polynomials of Table I are in 1-1 correspondence with the binary primitive irreducible polynomials.

For example, the polynomial $f(x) = x^3 + 2x^2 + x + 3$ is the characteristic polynomial of the linear recurrence

$$s(t) = 2s(t-1) + 3s(t-2) + s(t-3), \quad (4.11)$$

over $\mathbb{Z}_4$ and generates Family $\mathscr{A}$ with period 7 and size 9. The shift register implementation of (4.11) is diagrammed in Fig. 1. Different sequences in Family $\mathscr{A}$ may be generated by loading the shift register with any set of initial conditions not identically zero and cycling the shift register through a full period L. Cyclically distinct members of the family may be found by loading the shift register with triples not previously seen during the generation of prior sequences.

Table II provides a standard enumeration of the cyclically distinct sequences of Family $\mathscr{A}$ as generated by the polynomial $f(x) = x^3 + 2x^2 + x + 3$. Family members are identified by their trace representations. Corresponding correlation sums are also given in the table. From these, the weight distribution of the family is readily verified: $M = 2^{r-2} + 2^{s-1} = 3$ and $N = 2^{r-2} - 2^{s-1} = 1$. In the correlation distribution, the peak correlation value 7 occurs $2^r + 1 = 9$ times, -1 occurs $2^{2r} - 2 = 62$ times, $-1 + 2^s \pm \omega 2^s$ occurs $(2^{r-2} + 2^{s-1})(2^{2r} - 2) = 186$ times each, and $-1 - 2^s \pm \omega 2^s$ occurs $(2^{r-2} - 2^{s-1})(2^{2r} - 2) = 62$ times each.

V. Family $\mathscr{B}$

Trace Description: Family $\mathscr{B}$ is defined as the family $S^*(f)$ of linearly recurring sequences over $\mathbb{Z}_4$ whose characteristic polynomial $f(x)$ is a primitive basic irreducible of degree r and order $2(2^r - 1)$ with roots of a special kind in GR(4, r). Before restricting attention to Family $\mathscr{B}$, we first consider the general case of primitive basic irreducibles and their associated families. Let $f(x)$ be an arbitrary primitive basic irreducible in $\mathbb{Z}_4[x]$. As noted in Section III during the discussion of the Galois automorphism group, $f(x)$ has precisely r distinct roots $\alpha_0, \alpha_1, \cdots, \alpha_{r-1}$ satisfying $\mu\alpha_i = \theta^{2^i}$. Since α_0 is a unit, it may be written as $(1 + 2\delta_0)\beta$, where β is a multiplicative generator of the subgroup G_1 of

TABLE I
CHARACTERISTIC POLYNOMIALS FOR LINEAR RECURRENCE DEFINING FAMILY $\mathscr{A}$

Degree 3	1213	1323			
Degree 4	10231	13201			
Degree 5	100323	113013	113123	121003	123133
	130133				
Degree 6	1002031	1110231	1211031	1301121	1302001
	1320111				
Degree 7	10020013	10030203	10201003	10221133	10233123
	11122323	11131123	11321133	11332133	11332203
	12122333	12303213	12311203	12331333	13002003
	13210123	13212213	13223213		
Degree 8	100103121	100301231	102231321	111002031	111021311
	111310321	113120111	121102121	121201121	121301001
	121320031	123013111	123132201	130023121	130200111
	132103001				
Degree 9	1000030203	1001011333	1001233203	1002231013	1020100003
	1020332213	1021123003	1021301133	1021331123	1022121323
	1023112133	1110220323	1111300013	1111311013	1112201133
	1113303003	1130312123	1131003213	1131003323	1131030123
	1132331203	1133013203	1133022333	1210032123	1210220333
	1211003133	1211213013	1213232203	1230103133	1230313123
	1231310123	1232100323	1232310133	1232322013	1233113203
	1300013333	1301110213	1301301213	1301323323	1302210213
	1302212123	1303122003	1303313333	1320322013	1320333013
	1321003133	1322110203	1323013013		
Degree 10	10000203001	10002102111	10002123121	10020213031	10030023231
	10030200001	10203103311	10203122121	10211131111	10213010311
	10213330231	10231100111	10233222121	11100113201	11111110231
	11113111201	11120120001	11120232311	11122031321	11131011031
	11301031201	11301210321	11301320031	11312010231	11321001121
	11323133321	11323202111	11330130201	11330223121	12100122031
	12102023121	12110012311	12120311321	12122130201	12122233201
	12132020121	12132120001	12132203311	12301210311	12311302121
	12313022111	12321103231	12321222031	12331133031	12333132311
	13002310311	13011013111	13011232231	13020010231	13022100121
	13022212321	13031202001	13033113321	13201002031	13201021311
	13201111111	13203331201	13223211031	13230112321	13232003001

Note: For degree 3, the entry 1213 represents the polynomial $x^3 + 2x^2 + x + 3$. For definition of the characteristic polynomial, refer to (2.1).

R^* and $\delta_0 \in G_1 \cup \{0\}$. Applying the Galois automorphism σ_R shows that

$$\alpha_i = \left(1 + 2\delta_0^{2^i}\right)\beta^{2^i},$$

for $i = 0, 1, \cdots, r-1$. It is easy to show that $\alpha_i - \alpha_j$ is a unit whenever $i \neq j$. Hence, $f(x)$ factors in $R[x]$ as

$$f(x) = \prod_{i=0}^{r-1} (x - \alpha_i).$$

As a notational convenience, let $\alpha = (1 + 2\delta)\sqrt{\beta}$, where $\delta = \delta_0^{2^{r-1}}$ and $\sqrt{\beta} = \beta^{2^{r-1}}$. Note that, unless $\delta = 0$, α has multiplicative order $2(2^r - 1)$ in R^* and that

$$f(x) = \prod_{i=1}^{r} \left[x - \sigma_R^i(\alpha)\right].$$

In order to emphasize dependence on the root α, the linear recurrence family $S(f)$ will also be denoted by $\mathscr{S}_\alpha$. When $\delta = 0$, $\mathscr{S}_\alpha^+$ is Family $\mathscr{A}$. When $\delta \neq 0$, $f(x)$ has order $2(2^r - 1)$. The families are new but do not necessarily have correlation properties that are nearly optimal. However, if in addition $\mu\{T(\delta)\} = 1$ and $\mu\delta \neq 1$, then $\mathscr{S}_\alpha^*$ is Family $\mathscr{B}$ and does have nearly optimal correlation properties. As in the case of Family $\mathscr{A}$, the following trace characterization is easily proven.

Theorem 7: For every $\gamma \in R$, the sequence $\{s_\gamma(t)\}_{t=0}^{\infty}$ defined by $s_\gamma(t) \triangleq T(\gamma\alpha^t)$ is a member of the family $\mathscr{S}_\alpha$. Conversely, every sequence in $\mathscr{S}_\alpha$ is of this form for a unique $\gamma \in R$.

In order to identify family membership, the following notation will be used:

$$s_\gamma(t; \beta) = T(\gamma\beta^t),$$

$$s_\gamma(t; \alpha) = T(\gamma\alpha^t).$$

If γ is a unit, then $s_\gamma(t; \alpha)$ has period equal to the multiplicative order of α in R^*. For nonunits $\gamma = 2\nu$, with $\nu \in R^*$, $s_\gamma(t; \alpha) = 2\mathrm{tr}(\bar{\nu}\theta^t)$ is twice a binary m-sequence and has period $2^r - 1$ regardless of the multiplicative order of α. Thus, when $\delta \neq 0$, the family $\mathscr{S}_\alpha^*$ (from which the zero-divisor sequences are excluded) consists entirely of sequences of period $2(2^r - 1)$. The number of cyclically distinct sequences in $\mathscr{S}_\alpha^*$, for $\delta \neq 0$, is

$$\frac{4^r - 2^r}{2(2^r - 1)} = 2^{r-1}.$$

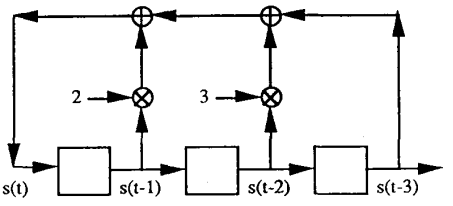

Fig. 1. Shift register implementation of family $\mathscr{A}$ as generated by characteristic polynomial $f(x) = x^3 + 2x^2 + x + 3$.

TABLE II
ENUMERATION OF FAMILY $\mathscr{A}$ AS GENERATED BY $x^3 + 2x^2 + x + 3$

γ	$S_\gamma(t)$	$\zeta(\gamma)$
2	2002022	-1
1	3221211	$-3 + 2\omega$
-1	1223233	$-3 - 2\omega$
$1 - \beta$	1013102	$1 + 2\omega$
$1 - \beta^2$	1100123	$1 + 2\omega$
$1 - \beta^3$	2010333	$1 - 2\omega$
$1 - \beta^4$	1112030	$1 + 2\omega$
$1 - \beta^5$	2133003	$1 - 2\omega$
$1 - \beta^6$	2303130	$1 - 2\omega$

Note: $\omega = \exp(j\pi/2)$.

For two sequences $s(t)$ and $s'(t)$ of common period L, their interleaving is a sequence of period $2L$ denoted here by

$$s(t)\Lambda s'(t) \triangleq \{s(0), s'(0), s(1), s'(1), \cdots, s(t), s'(t), \cdots\}.$$

The next proposition shows that the families $\mathscr{S}_\alpha^*$, for $\delta \neq 0$, consist of special interleavings of sequences from Family $\mathscr{A}$. As a result, the correlations of these families are the sum of two Family $\mathscr{A}$ correlation values. Not all families of this type will have near optimum correlation properties. For example, if the two interleaved sequences have the same Family $\mathscr{A}$ correlation value, the interleaved sequence will have a correlation sum too large for the family to be nearly optimal. For Family $\mathscr{B}$, the interleaved sequences retain nearly optimal correlation properties.

Proposition 2: Let $\alpha = (1 + 2\delta)\sqrt{\beta}$ with $\mu\delta \neq 0$. Then, every sequence in $\mathscr{S}_\alpha^*$ is an interleaving of two cyclically distinct sequences of Family $\mathscr{A}$. Furthermore, the cyclic equivalence classes of $\mathscr{S}_\alpha^*$ correspond to a partitioning of the cosets of G_1 in R^* into distinct pairs $(\gamma G_1, \alpha\gamma G_1)$.

Proof: Let $s_\gamma(t; \alpha)$ with $\gamma \in R^*$ be a sequence in $\mathscr{S}_\alpha^*$. Since $\alpha^2 = \beta$, it is easy to see that

$$s_\gamma(t; \alpha) = s_\gamma(t; \beta)\Lambda s_{\alpha\gamma}(t; \beta). \tag{5.1}$$

All cyclic shifts of $s_\gamma(t; \alpha)$ are interleavings of either a cyclic shift of s_γ with a cyclic shift of $s_{\alpha\gamma}$ or, in the opposite order, a cyclic shift of $s_{\alpha\gamma}$ with a cyclic shift of s_γ. Hence, the cyclic equivalence class of s_γ in $\mathscr{S}_\alpha^*$ corresponds to the pair $(\gamma G_1, \alpha\gamma G_1)$ of cosets of G_1 in R^*. Since $\alpha^2\gamma G_1 = \gamma G_1$, the pairing is unique and partitions the cosets of G_1 in R^*. Since α is not a power of β, the cosets γG_1 and $\alpha\gamma G_1$ in R^* are distinct. □

Correlation Properties: The remainder of the paper will now focus upon the correlation properties of Family $\mathscr{B}$. The correlation sums associated with Families $\mathscr{A}$ and $\mathscr{B}$ will be written as

$$\zeta(\gamma; \beta) = \sum_{t=1}^{2^r-1} \omega^{T(\gamma\beta^t)},$$

$$\zeta(\gamma; \alpha) = \sum_{t=1}^{2(2^r-1)} \omega^{T(\gamma\alpha^t)}. \tag{5.2}$$

By (5.1), the correlation sum $\zeta(\gamma; \alpha)$ has value

$$\zeta(\gamma; \alpha) = \zeta(\gamma; \beta) + \zeta(\alpha\gamma; \beta), \tag{5.3}$$

which is the sum of correlation values associated with cyclically distinct sequences from Family $\mathscr{A}$. Since the period of sequences from Family $\mathscr{B}$ is twice that of Family $\mathscr{A}$, the maximum nontrivial correlation parameter of Family $\mathscr{B}$ can only be larger by a factor of $\sqrt{2}$ in order for the family to be asymptotically optimal with respect to the Welch bound. Thus, when viewed as vectors, the complex numbers $\zeta(\gamma; \beta)$ and $\zeta(\alpha\gamma; \beta)$ must be nearly orthogonal. This is proven in the next two lemmas.

Lemma 2: For $\alpha = (1 + 2\delta)\sqrt{\beta}$ with $\mu\{T(\delta)\} = 1$ and $\mu\delta \neq 1$, the element $1 - \alpha\beta^t$ in R may be expressed as

$$1 - \alpha\beta^t = \beta^{\pi(t+1/2)}(1 + 2z),$$

where $z \in R$ has projection $\bar{z} = \mu z$ satisfying

$$x^2(\bar{z}^2 + \bar{\delta}^2 + 1) + x + \bar{z}^2 = 0,$$

in K with $x = \theta^{t+1/2}$ and $\bar{\delta} = \mu\delta$. Consequently, among the cosets $(1 - \alpha\beta^t)G_1$ for $0 \leq t \leq 2^r - 2$, $t \neq 2^{r-1} - 1$, the cosets $+G_1$ and $-\alpha G_1$ each appear once. The remaining cosets appear either twice or not at all depending on whether $\mathrm{tr}(\bar{z}\bar{\delta}) = 0$ or $\mathrm{tr}(\bar{z}\bar{\delta}) = 1$, respectively. Furthermore, the coset γG_1 appears as some $(1 - \alpha\beta^t)G_1$ iff the coset $-\gamma G_1$ does not.

Proof: It is easy to show that $1 - \alpha\beta^\tau$ is a unit except when $\tau = 2^{r-1} - 1$. If $\tau = 2^{r-1} - 1$, then $\beta^\tau = 1/\sqrt{\beta}$ and $1 - \alpha\beta^\tau = -2\delta \neq 0$ is a zero-divisor. When $1 - \alpha\beta^\tau$ is a unit, it may be written as

$$1 - \alpha\beta^\tau = \beta^{\pi(\tau+1/2)}(1 + 2z), \tag{5.4}$$

for some $z \in R$. Recall that the cosets of G_1 in R^* are determined by the term $1 + 2z$ and that $1 + 2z$ and $1 + 2z'$ are in the same coset iff $\mu z = \mu z'$. Squaring both sides of (5.4) yields $1 - 2\alpha\beta^\tau + \beta^{2\tau+1} = \beta^{2\pi(\tau+1/2)}$, while applying the automorphism σ_R yields $1 - (1 + 2\delta^2)\beta^{2\tau+1} = \beta^{2\pi(\tau+1/2)}(1 + 2z^2)$. Combining these two results gives the equation $2[\beta^{\tau+1/2} - (1 + \delta^2)\beta^{2\tau+1}] = 2z^2(1 + \beta^{2\tau+1})$. By (3.1), it suffices to solve the corresponding equation in K:

$$x^2(\bar{z}^2 + \bar{\delta}^2 + 1) + x + \bar{z}^2 = 0,$$
$$x = \theta^{\tau+1/2} \qquad (\tau \neq 2^{r-1} - 1). \tag{5.5}$$

Note that the side conditions $x = \theta^{\tau+1/2}$ and $\tau \neq 2^{r-1} - 1$ exclude both $x = 0$ and $x = 1$ as legitimate solutions.

The cosets not appearing among the $(1 - \alpha\beta^t)G_1$ correspond to elements $1 + 2z$ for which (5.5) has no solution $x \in K \setminus \{0, 1\}$. The remaining cosets appear once or twice depending on whether there are one or two distinct solutions of (5.5) in $K \setminus \{0, 1\}$. Since $\bar{\delta} \neq 1$, the exceptional case $x = 1$ is never a possible solution. The exceptional case $x = 0$, however, must be specifically excluded when $\bar{z} = 0$. Thus, when $\bar{z} = 0$, the only solution to (5.5) is $x = 1/(1 + \bar{\delta}^2)$. Hence, the corresponding coset $+G_1$ appears as $(1 - \alpha\beta^\tau)G_1$ for precisely one choice of τ. When $\bar{z} = 1 + \bar{\delta}$, the quadratic term of (5.5) vanishes. The only solution in this case is $x = 1 + \bar{\delta}^2$. Hence, the corresponding coset $-\alpha G_1$ appears only once.

For other values of $\bar{z}$, (5.5) has either two distinct solutions in $K \setminus \{0, 1\}$(when $\mathrm{tr}(\bar{z}\bar{\delta}) = 0$) or it has none (when $\mathrm{tr}(\bar{z}\bar{\delta}) = 1$). Note that $\gamma G_1 = (1 + 2z)G_1$ implies $-\gamma G_1 = (1 + 2(z + 1))G_1$. Hence, when $\bar{z} \notin \{0, 1, 1 + \bar{\delta}, \bar{\delta}\}$, the coset γG_1 appears as $(1 - \alpha\beta^\tau)G_1$ for precisely two different choices of τ iff the coset $-\gamma G_1$ never appears for any choice of τ. This follows since $\mathrm{tr}(\bar{\delta}) = 1$. Note that $\mathrm{tr}(\bar{z}\bar{\delta}) = 1$ when $\bar{z} = 1$ or $\bar{z} = \bar{\delta}$, so that, in general, even allowing $\bar{z} \in \{0, 1, 1 + \bar{\delta}, \bar{\delta}\}$, the coset γG_1 appears at least once among the $(1 - \alpha\beta^t)G_1$ iff the coset $-\gamma G_1$ never appears. □

Lemma 3: Let $\gamma \in R^*$ and $\alpha = (1 + 2\delta)\sqrt{\beta}$, with $\mu\{T(\delta)\} = 1$ and $\mu\delta \neq 1$. Interpreted as vectors, the complex numbers $1 + \zeta(\gamma; \beta)$ and $1 + \zeta(\alpha\gamma; \beta)$ are orthogonal.

Proof: Let $\zeta(\gamma) = \zeta(\gamma; \beta)$ and $\zeta(\alpha\gamma) = \zeta(\alpha\gamma; \beta)$. Note that $1 + \zeta(\gamma)$ and $1 + \zeta(\alpha\gamma)$ are orthogonal iff

$$\zeta(\gamma)\zeta^*(\alpha\gamma) + \zeta^*(\gamma)\zeta(\alpha\gamma) + \zeta(\gamma) + \zeta^*(\gamma) + \zeta(\alpha\gamma) + \zeta^*(\alpha\gamma) + 2 = 0. \quad (5.6)$$

Consider the product

$$\begin{aligned}\zeta(\gamma)\zeta^*(\alpha\gamma) &= \sum_{t=0}^{2^r-2}\sum_{t'=0}^{2^r-2}\omega^{T(\gamma(\beta^t-\alpha\beta^{t'}))}\\ &= \sum_{\tau=0}^{2^r-2}\sum_{t=0}^{2^r-2}\omega^{T(\gamma(1-\alpha\beta^\tau)\beta^t)}\\ &= \sum_{t=0}^{2^r-2}\omega^{T(-2\delta\gamma\beta^t)}\\ &\quad + \sum_{\substack{\tau=0\\ \tau\neq 2^{r-1}-1}}^{2^r-2}\sum_{t=0}^{2^r-2}\omega^{T(\gamma(1-\alpha\beta^\tau)\beta^t)}\\ &= -1 + \sum_{\substack{\tau=0\\ \tau\neq 2^{r-1}-1}}^{2^r-2}\sum_{t=0}^{2^r-2}\omega^{T(\gamma(1-\alpha\beta^\tau)\beta^t)}. \quad (5.7)\end{aligned}$$

From Lemma 2,

$$\begin{aligned}&\sum_{\substack{\tau=0\\ \tau\neq 2^{r-1}-1}}^{2^r-2}\sum_{t=0}^{2^r-2}\omega^{T(\gamma(1-\alpha\beta^\tau)\beta^t)}\\ &\quad = 2\sum_{\substack{\gamma_i\in\Gamma^*\\ \gamma_i=1+2z_i\\ tr(\bar{z}_i\bar{\delta})=0}}\sum_{x\in\gamma_iG_1}\omega^{T(x)} - \sum_{x\in\gamma G_1}\omega^{T(x)} - \sum_{x\in-\alpha\gamma G_1}\omega^{T(x)}\\ &\quad = 2\sum_{\substack{\gamma_i\in\Gamma^*\\ \gamma_i=1+2z_i\\ tr(\bar{z}_i\bar{\delta})=0}}\sum_{x\in\gamma_iG_1}\omega^{T(x)} - \zeta(\gamma) - \zeta^*(\alpha\gamma). \quad (5.8)\end{aligned}$$

Hence, from (5.7), (5.8), and Lemma 2,

$$\zeta(\gamma)\zeta^*(\alpha\gamma) + \zeta^*(\gamma)\zeta(\alpha\gamma) = -2 + 2\left(\sum_{\gamma_i\in\Gamma^*}\sum_{x\in\gamma_iG_1}\omega^{T(x)}\right) - \zeta(\gamma) - \zeta^*(\gamma) - \zeta(\alpha\gamma) - \zeta^*(\alpha\gamma),$$

thereby proving (5.6) and establishing the lemma. □

Proposition 4: Let $\zeta = \sum_{t=1}^{2(2^r-1)}\omega^{T(\gamma\alpha^t)}$ with $\gamma \in R^*$. Then, ζ lies on the circle $|2 + \zeta|^2 = 2^{r+1}$. Consequently, the only possible values of ζ are as follows:

1) if $r = 2s$, then $\zeta = -2 \pm 2^s \pm \omega 2^s$;
2) if $r = 2s + 1$, then $\zeta = -2 \pm 2^{s+1}$ or $\zeta = -2 \pm \omega 2^{s+1}$.

Proof: By (5.3) and Lemma 3,

$$\begin{aligned}|2 + \zeta|^2 &= |(1 + \zeta(\gamma; \beta)) + (1 + \zeta(\alpha\gamma; \beta))|^2\\ &= |1 + \zeta(\gamma; \beta)|^2 + |1 + \zeta(\alpha\gamma; \beta)|^2.\end{aligned}$$

Then $|2 + \zeta|^2 = 2(2^r)$ by Theorem 4. All possible correlation values follow by solving a simple Diophantine equation as in Proposition 1. □

Paralleling the development of the weight distribution of Family $\mathscr{A}$, we now consider the first and second moments associated with Family $\mathscr{B}$. The first moment sum is

$$\sum_{\gamma_i\in\Gamma^*}\zeta(\gamma_i; \alpha) = \sum_{\gamma_i\in\Gamma^*}\zeta(\gamma_i; \beta) + \sum_{\gamma_i\in\Gamma^*}\zeta(\alpha\gamma_i; \beta) = \sum_{x\in R^*}\omega^{T(x)} + \sum_{x\in R^*}\omega^{T(x)} = 0. \quad (5.9)$$

Using (4.8), the second moment sum may be written

$$\begin{aligned}\sum_{\gamma_i\in\Gamma^*}\left[\zeta(\gamma_i; \alpha)\right]^2 &= \sum_{i=1}^{2^r}\left[\zeta^2(\gamma_i; \beta) + 2\zeta(\gamma_i; \beta)\zeta(\alpha\gamma_i; \beta) + \zeta^2(\alpha\gamma_i; \beta)\right]\\ &= 2(-2^r) + 2\sum_{i=1}^{2^r}\zeta(\gamma_i; \beta)\zeta(\alpha\gamma_i; \beta).\end{aligned}$$

The product $\zeta(\gamma_i; \beta)\zeta(\alpha\gamma_i; \beta)$ may be expanded as

$$\begin{aligned}\zeta(\gamma_i;\beta)\zeta(\alpha\gamma_i;\beta) &= \sum_{\tau=0}^{2^r-2}\sum_{t=0}^{2^r-2}\omega^{T(\gamma_i(1+\alpha\beta^\tau)\beta^t)} \\ &= \sum_{x\in G_1}\omega^{T(\gamma_i(1+\alpha\beta^{2^{r-1}-1})x)} \\ &\quad + \sum_{\substack{\tau=0\\ \tau\neq 2^{r-1}-1}}^{2^r-2}\left[\sum_{x\in G_1}\omega^{T(\gamma_i(1+\alpha\beta^\tau)x)}\right].\end{aligned}$$

As in Lemma 2, one can show that $1 + \alpha\beta^\tau$ is a unit except when $\tau = 2^{r-1} - 1$. Hence, for fixed $\tau \neq 2^{r-1} - 1$, summing the bracketed term on the right over all coset representatives $\gamma_i \in \Gamma$ gives zero by (3.5). For the first term on the right, note that $1 + \alpha\beta^{2^{r-1}-1} = 2(1 + \delta) \neq 0$ since $\mu\delta \neq 1$. Then, by (3.5), the first term is

$$\sum_{x\in G_1}\omega^{T(\gamma_i(1+\alpha\beta^{2^{r-1}-1})x)} = \sum_{\substack{x\in R\setminus R^*\\ x\neq 0}}\omega^{T(x)} = -1.$$

Hence, the second moment sum has value

$$\sum_{i=1}^{2^r}\left[\zeta(\gamma_i;\alpha)\right]^2 = -2^{r+2}. \tag{5.10}$$

Theorem 8 (Weight Distribution): As γ varies over R^*, the correlation sum $\zeta(\gamma; \alpha)$ assumes the following distribution of values.

1) If $r = 2s$, then

$$\zeta(\gamma;\alpha) = \begin{cases} 2(2^r-1), & \text{for } \gamma = 0,\\ -2, & \text{for } 2^r-1 \text{ nonunits } \gamma\neq 0,\\ -2+2^s+\omega 2^s, & \text{for } (2^{r-2}+2^{s-1})\cdot(2^r-1) \text{ units } \gamma,\\ -2+2^s-\omega 2^s, & \text{for } (2^{r-2}+2^{s-1})\cdot(2^r-1) \text{ units } \gamma,\\ -2-2^s+\omega 2^s, & \text{for } (2^{r-2}-2^{s-1})\cdot(2^r-1) \text{ units } \gamma,\\ -2-2^s-\omega 2^s, & \text{for } (2^{r-2}-2^{s-1})\cdot(2^r-1) \text{ units } \gamma. \end{cases}$$

2) If $r = 2s + 1$, then

$$\zeta(\gamma;\alpha) = \begin{cases} 2(2^r-1), & \text{for } \gamma = 0,\\ -2, & \text{for } 2^r-1 \text{ nonunits } \gamma\neq 0,\\ -2+2^{s+1}, & \text{for } (2^{r-2}+2^s)\cdot(2^r-1) \text{ units } \gamma,\\ -2-2^{s+1}, & \text{for } (2^{r-2}-2^s)\cdot(2^r-1) \text{ units } \gamma,\\ -2+\omega 2^{s+1}, & \text{for } 2^{r-2}(2^r-1) \text{ units } \gamma,\\ -2-\omega 2^{s+1}, & \text{for } 2^{r-2}(2^r-1) \text{ units } \gamma. \end{cases}$$

Proof: For case 1), one lets

$$\begin{aligned} M &= |\{\gamma\in\Gamma^*: \zeta(\gamma;\alpha) = -2+2^s+\omega 2^s\}| \\ &= |\{\gamma\in\Gamma^*: \zeta(\gamma;\alpha) = -2+2^s-\omega 2^s\}|, \\ N &= |\{\gamma\in\Gamma^*: \zeta(\gamma;\alpha) = -2-2^s+\omega 2^s\}| \\ &= |\{\gamma\in\Gamma^*: \zeta(\gamma;\alpha) = -2-2^s-\omega 2^s\}|. \end{aligned}$$

For case 2), one lets

$$\begin{aligned} M &= |\{\gamma\in\Gamma^*: \zeta(\gamma;\alpha) = -2+2^{s+1}\}|, \\ N &= |\{\gamma\in\Gamma^*: \zeta(\gamma;\alpha) = -2-2^{s+1}\}|, \\ P &= |\{\gamma\in\Gamma^*: \zeta(\gamma;\alpha) = -2+\omega 2^{s+1}\}| \\ &= |\{\gamma\in\Gamma^*: \zeta(\gamma;\alpha) = -2-\omega 2^{s+1}\}|. \end{aligned}$$

From the first moment sum (5.9), the second moment sum (5.10), and the fact that $|\Gamma^*| = 2^r$, the following sets of simultaneous equations may be derived as in the proof of Theorem 5. When $r = 2s$,

$$\begin{aligned} 2(M+N) &= 2^r, \\ 2(M+N) &= 2^s(M-N). \end{aligned}$$

When $r = 2s + 1$,

$$\begin{aligned} M+N+2P &= 2^r, \\ M+N+2P &= 2^s(M-N), \\ M+N-2P &= 0. \end{aligned}$$

Solving these equations gives the claimed weight distributions. □

Let $\{s_\lambda: \lambda\in\Lambda\}$ be a complete set of cyclically distinct sequences from Family $\mathscr{B}$ with $\Lambda = \{\lambda_1, \lambda_2, \lambda_3, \cdots, \lambda_{2^{r-1}}\} \subset R^*$. Then, by Proposition 2, $\Lambda \cup \alpha\Lambda$ is a complete set of distinct coset representatives for the cosets of G_1 in R^*. As in the proof of Theorem 6, the correlation distribution of Family $\mathscr{B}$ follows directly from the weight distribution once the number of solutions to the equation

$$\begin{aligned} &\lambda_i\alpha^\tau - \lambda_j = \gamma, \\ &\lambda_i, \lambda_j\in\Lambda, \\ &0\le\tau<2(2^r-1) \end{aligned} \tag{5.11}$$

is known for each $\gamma \in R$.

Theorem 9 (Correlation Distribution): For Family $\mathscr{B}$, the correlation distribution is as follows.

1) If $r = 2s$, then

$$\zeta(\gamma;\alpha) = \begin{cases} 2(2^r - 1), & 2^{r-1} \text{ times}, \\ -2, & 2^{2r-1} - 2^{r-1} \text{ times}, \\ -2 + 2^s + \omega 2^s, & (2^{r-2} + 2^{s-1}) \cdot (2^{2r-1} - 2^r) \text{ times}, \\ -2 + 2^s - \omega 2^s, & (2^{r-2} + 2^{s-1}) \cdot (2^{2r-1} - 2^r) \text{ times}, \\ -2 - 2^s + \omega 2^s, & (2^{r-2} - 2^{s-1}) \cdot (2^{2r-1} - 2^r) \text{ times}, \\ -2 - 2^s - \omega 2^s, & (2^{r-2} - 2^{s-1}) \cdot (2^{2r-1} - 2^r) \text{ times}. \end{cases}$$

2) If $r = 2s + 1$, then

$$\zeta(\gamma;\alpha) = \begin{cases} 2(2^r - 1), & 2^{r-1} \text{ times}, \\ -2, & 2^{2r-1} - 2^{r-1} \text{ times}, \\ -2 + 2^{s+1}, & (2^{r-2} + 2^s) \cdot (2^{2r-1} - 2^r) \text{ times}, \\ -2 - 2^{s+1}, & (2^{r-2} - 2^s) \cdot (2^{2r-1} - 2^r) \text{ times}, \\ -2 + \omega 2^{s+1}, & 2^{r-2}(2^{2r-1} - 2^r) \text{ times}, \\ -2 - \omega 2^{s+1}, & 2^{r-2}(2^{2r-1} - 2^r) \text{ times}. \end{cases}$$

Proof: Fix $\lambda_j \in \Lambda$. Then, for each $\gamma \in R$, if there is a solution to (5.11), it is unique. Thus, the number of triples (i, j, τ) satisfying (5.11) for fixed λ_j is equal to the number of $\gamma \in R$ for which solutions exists. Note that (5.11) has a solution iff $\gamma \neq -\lambda_j + 2\nu$ for any $\nu \in R$. Since the $-\lambda_j + 2\nu$ are all units, every nonunit γ admits a unique solution. Hence, for each $\lambda_j \in \Lambda$, the correlation value $2(2^r - 1)$ corresponding to $\gamma = 0$ appears once in the correlation distribution. The correlation sum -2 appears $2^r - 1$ times, once for each nonzero $\gamma \in R \setminus R^*$. Then, as λ_j varies over Λ, there are a total of 2^{r-1} triples having correlation value $2(2^r - 1)$ and $2^{r-1}(2^r - 1)$ triples having correlation value -2.

For the units in R, note that $-\lambda_j + 2\nu$ and $-\lambda_j + 2\nu'$ are in different cosets of G_1 in R^* whenever $\mu\nu \neq \mu\nu'$. Thus, for fixed $\lambda_j \in \Lambda$, each coset of G_1 in R^* has $2^r - 2$ choices of γ that yield valid solutions to (5.11). Therefore, as λ_j varies over Λ, each coset of G_1 gives rise to $2^{r-1}(2^r - 2)$ triples with its associated correlation value. The correlation distribution then follows in this case by multiplying M, N, and P of Theorem 8 by $2^{2r-1} - 2^r$. □

Example: Family $\mathscr{B}$ is defined as the family $\mathscr{S}^*(f)$ of linearly recurring sequences over $\mathbb{Z}_4$ whose characteristic polynomial $f(x)$ is a primitive basic irreducible having root $\alpha = (1 + 2\delta)\sqrt{\beta}$ with $\mu\{T(\delta)\} = 1$ and $\mu\delta \neq 1$. Table III provides representative polynomials of this type for degrees 3 to 10. (Of course, the list is by no means exhaustive. Neither have we tried to identify the characteristic polynomial of fewest nonzero coefficients.) The polynomial of degree r in the table may be used to generate Family $\mathscr{B}$ with parameters $L = 2(2^r - 1)$ and $M = 2^{r-1}$.

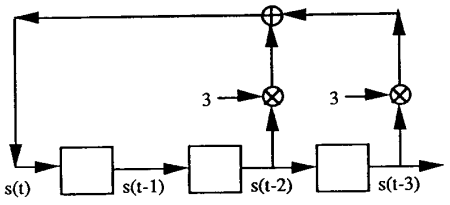

Fig. 2. Shift register implementation of family $\mathscr{B}$ as generated by characteristic polynomial $f(x) = x^3 + x + 1$.

TABLE III
SELECTED CHARACTERISTIC POLYNOMIALS FOR FAMILY $\mathscr{B}$

Degree 3	1011
Degree 4	12213
Degree 5	100101
Degree 6	1202013
Degree 7	12201001
Degree 8	122231103
Degree 9	1000010221
Degree 10	10020201003

Note: Entry 1011 represents the polynomial $x^3 + x + 1$. For definition of the characteristic polynomial, refer to (2.1).

TABLE IV
ENUMERATION OF FAMILY $\mathscr{B}$ AS GENERATED BY $x^3 + x + 1$

γ	$s_\gamma(t;\alpha)$	$\zeta(\gamma;\alpha)$
1	30212111221013	$-2 + 4\omega$
-1	10232333223031	$-2 - 4\omega$
$1 - \beta$	13001033120123	2
$1 - \beta^2$	13100301132032	2

Note: $\omega = \exp(j\pi/2)$ and $\beta^3 + 2\beta^2 + \beta + 3 = 0$.

For example, the polynomial $f(x) = x^3 + x + 1$ is the characteristic polynomial of the linear recurrence

$$s(t) = 3s(t-2) + 3s(t-3), \qquad (5.12)$$

over $\mathbb{Z}_4$ and generates Family $\mathscr{B}$ with period 14 and size 4. The shift register implementation of (5.12) is diagrammed in Fig. 2. Different sequences in Family $\mathscr{B}$ may be generated by loading the shift register with different initial conditions and cycling through a full period L. Initial conditions consisting only of zero-divisors in $\mathbb{Z}_4$, however, are prohibited.

Table IV provides an enumeration of the cyclically distinct sequences of Family $\mathscr{B}$ as generated by the polynomial $f(x) = x^3 + x + 1$. Family members are identified by their trace representations. Corresponding correlation sums are also given in the table. Recalling that each equivalence class of Family $\mathscr{B}$ corresponds to a unique pair of cosets of G_1 in R^*, the weight distribution of the family is readily verified from the table: $M = 2^{r-2} + 2^s = 4$, $N = 2^{r-2} - 2^s = 0$, and $P = 2^{r-2} = 2$. In the correlation distribution, the peak correlation value 14 occurs $2^{r-1} = 4$ times, -2 occurs $2^{2r-1} - 2^{r-1} = 28$ times, $-2 + 2^{s+1}$ occurs $(2^{r-2} +$

$2^s)(2^{2r-1} - 2^r) = 96$ times, and $-2 \pm \omega 2^{s+1}$ occurs $(2^{r-2})(2^{2r-1} - 2^r) = 48$ times each.

ACKNOWLEDGMENT

The authors would like to thank A. Tietäväinen for drawing attention to the paper by P. Solé.

REFERENCES

[1] S. Boztaş, "Near-optimal 4ϕ (four-phase) sequences and optimal binary sequences for CDMA," Ph.D. dissert. Univ. of Southern California, Los Angeles, CA, 1990.

[2] S. Boztaş and P. V. Kumar, "Near-optimal 4ϕ (four-phase) sequences for CDMA," presented at the "*Recent Results*" *session of the IEEE Int. Symp. Inform. Theory*, San Diego, CA, Jan. 1990.

[3] ——, "Near-optimal 4ϕ (four-phase) sequences for CDMA," tech. rep. CSI-90-03-01, Communication Sciences Inst., Univ. of Southern California, Los Angeles, CA, Mar. 1990

[4] ——, "Near-optimal 4ϕ sequences for CDMA," presented at *IEEE Int. Symp. Inform. Theory*, Budapest, Hungary, June 1991.

[5] G. C. Clark and J. B. Cain, *Error-Correction Coding for Digital Communications*, Plenum Press, New York, 1981.

[6] P. Delsarte, "An algebraic approach to the association schemes of coding theory," Phillips Res. Rep., Suppl. no. 10, 1973.

[7] A. R. Hammons and P. V. Kumar, "Applications of Galois ring theory to sequence design and related topics," Tech. Rep. CSI-91-05-04, Communication Sciences Inst., Univ. of Southern California, Los Angeles, CA, May 1991.

[8] S. M. Krone and D. V. Sarwate, "Quadriphase sequences for spread-spectrum multiple-access communication," *IEEE Trans. Inform. Theory*, vol. IT-30, no. 3, pp. 520–529, May 1984.

[9] P. V. Kumar and O. Moreno, "Polyphase sequences with periodic correlation properties better than binary sequences," *IEEE Trans. Inform. Theory*, vol. 37, no. 3, pp. 603–616, May 1991.

[10] R. Lidl and H. Niederreiter, *Finite Fields*, *Encyclopedia of Mathematics and Its Applications*, vol. 20. Reading, MA: Addison-Wesley Publishing Company, 1983.

[11] R. A. Liebler and R. A. Mena, "Certain distance-regular digraphs and related rings of characteristic 4," *J. Combinat. Theory*, ser. A, vol. 47, pp. 111–123, 1988.

[12] B. R. MacDonald, *Finite Rings with Identity*. New York: Marcel Dekker, Inc., 1974.

[13] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.

[14] D. V. Sarwate and M. B. Pursley, "Cross-correlation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, pp. 593–618, May 1980.

[15] P. Shankar, "On BCH codes over arbitrary integer rings," *IEEE Trans. Inform. Theory*, vol. IT-25, no. 4, pp. 480–483, July 1979.

[16] V. M. Sidelnikov, "On mutual correlation of sequences," *Soviet Math Doklady*, vol. 12, pp. 197–201, 1971.

[17] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*, vol. I. Rockville, MD: Computer Science Press, 1985.

[18] P. Solé, "A quarternary cyclic code and a family of quadriphase sequences with low correlation properties," in *Coding Theory and Applications,* Lecture Notes in Computer Science. New York: Springer-Verlag, vol. 388, 1989.

[19] P. Udaya and M. U. Siddiqi, "Large linear complexity sequences over $\mathbb{Z}_4$ for quadriphase modulated communication systems having good correlation properties," presented at *IEEE Int. Symp. Inform. Theory*, Budapest, Hungary, June 24–28, 1991.

[20] M. Ward, "The arithmetical theory of linear recurring series," *Trans. Amer. Math. Soc.*, vol. 35, pp. 600–628, 1931.

[21] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 397–399, May 1974.

[22] N. Zierler, "Linear recurring sequences," *J. Soc. Indust. Appl. Math.*, vol. 7, no. 1, pp. 31–48, Mar. 1959.