III. New $[58, 29, 10]$ Codes

For $j = 0, 10$ and $1 \leq i < 30$, let $C_i^{(j)}$ denote the code generated by the 29×58 matrix obtained by deleting row i and columns i and 30 from $G^{(j)}$. The codes $C_i^{(j)}$ are extremal self-dual $[58, 29, 10]$ codes with weight enumerator (2). For $j = 0$ we get $\beta = 0$ and for $j = 10$ we get $\beta = 2$.

We get the following different weight distributions:

$C_{10}^{(0)}$	$\beta = 0$	$\gamma = 114$
$C_{13}^{(0)}$	$\beta = 0$	$\gamma = 116$
$C_{2}^{(0)}$	$\beta = 0$	$\gamma = 118$
$C_{28}^{(0)}$	$\beta = 0$	$\gamma = 120$
$C_{19}^{(0)}$	$\beta = 0$	$\gamma = 122$
$C_{29}^{(10)}$	$\beta = 2$	$\gamma = 62$
$C_{26}^{(10)}$	$\beta = 2$	$\gamma = 70$
$C_{16}^{(10)}$	$\beta = 2$	$\gamma = 74$
$C_{4}^{(10)}$	$\beta = 2$	$\gamma = 78$
$C_{8}^{(10)}$	$\beta = 2$	$\gamma = 82$
$C_{11}^{(10)}$	$\beta = 2$	$\gamma = 86$
$C_{7}^{(10)}$	$\beta = 2$	$\gamma = 88$

Acknowledgment

The authors wish to thank T. Kløve for helpful comments and suggestions for improving the presentation. The assistance of the National Center for High-Performance Computing is gratefully appreciated.

References

[1] S. Buyuklieva and I. Boukliev, "Extremal self-dual codes with an automorphism of order 2," *IEEE Trans. Inform. Theory*, vol. 44, pp. 323–328, Jan. 1998.

[2] I. Boukliev and S. Buyuklieva, "Some new extremal self-dual codes with lengths $44, 50, 54,$ and 58," this issue, pp. 809–812.

[3] J. H. Conway and N. J. A. Sloane, "A new upper bound on the minimal distance of self-dual codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1319–1333, Nov. 1990.

[4] M. Harada and H. Kimura, "On extremal self-dual codes," *Math. J. Okayama Univ. 37*, pp. 1–14, 1995.

[5] H. P. Tsai, "Existence of certain extremal self-dual codes," Ph.D. dissertation, University of Illinois at Chicago, 1992.

Binary Pseudorandom Sequences of Period $2^n - 1$ with Ideal Autocorrelation

Jong-Seon No, Solomon W. Golomb, *Fellow, IEEE*, Guang Gong, Hwan-Keun Lee, and Peter Gaal

***Abstract*—In this correspondence, we present five new classes of binary sequences of period $2^n - 1$ with ideal autocorrelation. These sequences, which correspond to new cyclic Hadamard difference sets, were found by extensive computer search. Conjectures on the general construction of these sequences are formulated.**

***Index Terms*—Binary sequences, cyclic Hadamard difference sets, ideal autocorrelation, pseudorandom sequences.**

I. Introduction

Binary sequences with ideal autocorrelation properties are widely used in spread-spectrum communication systems, ranging, stream cipher cryptosystems, code-division multiple access (CDMA) systems, etc. The sequence $\{b(t), t = 0, 1, \cdots, N-1\}$ is said to have the ideal autocorrelation property if its periodic autocorrelation function $R_b(\tau)$ is given by

$$R_b(\tau) = \begin{cases} N, & \text{for } \tau \equiv 0 \bmod N \\ -1, & \text{otherwise} \end{cases}$$

where $R_b(\tau)$ is defined as

$$R_b(\tau) = \sum_{t=0}^{N-1} (-1)^{b(t+\tau)+b(t)}.$$

In the literature, the well-known families of binary sequences of period $2^n - 1$ with ideal autocorrelation include m-sequences [9], GMW sequences [13], generalized GMW sequences [14], Legendre sequences [15], Hall's sextic residue sequences [2], [16], extended sequences [16], and miscellaneous sequences [4]–[6], [16] whose general constructions are not known so far. In general, these sequences can be easily described using the trace function. Let F_{2^n} be the finite field with 2^n elements. The trace function $\mathrm{tr}_m^n(\cdot)$ is a linear mapping from F_{2^n} to F_{2^m}, defined by

$$\mathrm{tr}_m^n(x) = \sum_{i=0}^{(n/m)-1} x^{2^{mi}}$$

where m divides n.

When formulating the miscellaneous sequences with ideal autocorrelation of period 127 [4], 255 [5], and 511 [6], by trace functions, No and Lee and then, independently, Golomb and Gong found three entirely new infinite families of binary PN sequences with the ideal autocorrelation property and they decided to write a joint paper. Two additional infinite families of new ideal correlation sequences, obtained by a transformation on two of the three families just mentioned, were found by Golomb, Gong, and Gaal, and are also described in this correspondence, along with their results on the number of cyclically distinct sequences in some of these families.

Manuscript received November 1, 1996; revised October 3, 1997. The work of J. S. No and H. K. Lee was supported in part by the Institute of Information Technology Assessment under Grant 96003-RT-I1 from the Korean Ministry of Information and Communications.

J. S. No and H. K. Lee are with the Department of Electronic Engineering, Konkuk University, Seoul 143-701, Korea.

S. W. Golomb, G. Gong, and P. Gaal are with the Communication Sciences Institute, University of Southern California, Los Angles, CA 90089-2565 USA.

Publisher Item Identifier S 0018-9448(98)00981-X.

II. Conjectures About Three New Families

Any binary sequence of period $2^n - 1$ with ideal autocorrelation can be used to construct extended binary sequences of longer period with ideal autocorrelation [16], as well as an optimal family of binary sequences of period $2^{2n} - 1$ [17]. This fact motivates studying new constructions of binary sequences with ideal autocorrelation. The basic previously known constructions for such sequences can be categorized as: i) m-sequences [9]; ii) residue sequences such as Legendre sequences (also called quadratic residue sequences) of Mersenne prime period [15] and Hall's sextic residue sequences for $n = 5, 7$, or 17 (and whenever the period is a prime of the form $4a^2 + 27$ [2]); and iii) extended sequences [16] of longer period from the shorter period sequences with ideal autocorrelation, including GMW sequences [13] and generalized GMW sequences [14].

Based on a computer search, we present three new constructions of binary sequences of period $2^n - 1$ with ideal autocorrelation in the following conjectures. (Each of these constructions is equivalent to taking the term-by-term sum of a small number of m-sequences.)

Conjecture 1: Let k be a positive integer and let $n = 2k + 1$. Let

$$b(t) = \mathrm{tr}_1^n(\alpha^t) + \mathrm{tr}_1^n(\alpha^{(2^k+1)t}) + \mathrm{tr}_1^n(\alpha^{(2^k+2^{2k-1}+1)t})$$

where α is a primitive element of F_{2^n}. Then the sequence $\{b(t)\}$ is a binary sequence of period $2^n - 1$ with ideal autocorrelation.

If $k = 1, \{b(t)\}$ reduces to an m-sequence of period 7. For $k = 2, \{b(t)\}$ becomes a Legendre sequence of period 31. It has been proved by computer verification that Conjecture 1 is true for $n \leq 23$.

Conjecture 2: Let k be a positive integer ≥ 2 and let $n = 3k - 1$. Let

$$b(t) = \mathrm{tr}_1^n(\alpha^t) + \mathrm{tr}_1^n(\alpha^{(2^k+1)t}) + \mathrm{tr}_1^n(\alpha^{(2^{2k-1}+2^{k-1}+1)t}) + \mathrm{tr}_1^n(\alpha^{(2^{2k-1}-2^{k-1}+1)t}) + \mathrm{tr}_1^n(\alpha^{(2^{2k-1}+2^k-1)t})$$

where α is a primitive element of F_{2^n}. Then the sequence $\{b(t)\}$ is a binary sequence of period $2^n - 1$ with ideal autocorrelation.

For $k = 2, \{b(t)\}$ becomes a Legendre sequence of period 31. It has been proved by computer verification that Conjecture 2 is true for $n \leq 23$.

Conjecture 3: Let k be a positive integer ≥ 2 and let $n = 3k - 2$. Let

$$b(t) = \mathrm{tr}_1^n(\alpha^t) + \mathrm{tr}_1^n(\alpha^{(2^{k-1}+1)t}) + \mathrm{tr}_1^n(\alpha^{(2^{2k-2}+2^{k-1}+1)t}) + \mathrm{tr}_1^n(\alpha^{(2^{2k-2}-2^{k-1}+1)t}) + \mathrm{tr}_1^n(\alpha^{(2^{2k-1}-2^{k-1}+1)t})$$

where α is a primitive element of F_{2^n}. Then the sequence $\{b(t)\}$ is a binary sequence of period $2^n - 1$ with ideal autocorrelation.

It has been proved by computer verification that Conjecture 3 is true for $n \leq 22$.

In the case of $n = 7$, Conjectures 1 and 3 result in sequences which are equivalent to Examples 127F and 127D, respectively, in the listing of difference sets given by Baumert [2]. For $n = 9$, the sequence given by Conjecture 1 is equivalent to one of the three miscellaneous families found by Dreier [6].

III. Conjectures About Two Further New Families

L. R. Welch observed a symmetry between the two "miscellaneous" examples of degree $n = 8$ and period $= 2^8 - 1 = 255$ found by U. Cheng [5], and generalized this symmetry to all even values of n. This was further generalized by G. Gong to odd as well as even values of n, as follows.

Let $\{b(t)\}$ be a binary sequence of period $2^n - 1$ with two-level autocorrelation and define $g(x)$ for $x \in F_{2^n}$ by $b(t) = \mathrm{tr}_1^n(g(\alpha^t))$. Then, let $b'(t) = \mathrm{tr}_1^n(g(\alpha^t + 1) + 1)$. In many interesting cases, $\{b'(t)\}$ is also a binary sequence of period $2^n - 1$ with two-level autocorrelation.

Conjecture 4: If $\{b(t)\}$ is a sequence of the form given in Conjecture 2, and $\{b'(t)\}$ is derived from it by the Welch–Gong method, then this is also an ideal correlation sequence of the same period.

Conjecture 5: If $\{b(t)\}$ is a sequence of the form given in Conjecture 3, and $\{b'(t)\}$ is derived from it by the Welch–Gong method, then this is also an ideal correlation sequence of the same period.

Conjectures 4 and 5 have been verified by computer for all $k \leq 7$, corresponding to $n \leq 20$ and $n \leq 19$, respectively.

All six of the families of cyclic Hadamard difference sets found by Baumert's exhaustive search for $n = 7$ and $p = 127$ [2] are now accounted for: one each of m-sequence, Legendre sequence, sextic residue sequence, Conjecture 1 sequence, Conjecture 3 sequence, and Conjecture 5 sequence.

Similarly, all four of the families of cyclic Hadamard difference sets found by Cheng's exhaustive search for $n = 8$ and $p = 255$ [5] are now accounted for: one each of m-sequence, GMW sequence, Conjecture 2 sequence, and Conjecture 4 sequence.

Only three of the five families of cyclic Hadamard defference sets found by Dreier's exhaustive search for $n = 9, p = 511$ [6] are now accounted for: one each of m-sequence, GMW sequence, and Conjecture 1 sequence.

For many families of ideal-correlation binary sequences, including the m-sequences, the GMW sequences, the quadratic residue (Legendre) sequences, the sextic residue (Hall) sequences, and the Conjecture 1 sequences, the Welch–Gong transformation merely generates a "new" sequence in the same family, or even the original sequence back again. However, when represented as sums of m-sequences and decimation sequences of m-sequences, the Conjectures 4 and 5 sequences look strikingly different from the Conjectures 2 and 3 sequences to which they correspond under Welch–Gong.

IV. Lemmas and Theorems About Family Members

Lemma 1: The numbers $p = 2^{2k+1} - 1, q_1 = 2^k + 1$, and $q_2 = 2^k + 2^{k-1} + 1$, are pairwise relatively prime, for all $k \geq 2$.

Proof: We note first that for $k \geq 2$, all three of p, q_1, and q_2 are odd.

a) $p - 2q_1(q_1 - 2) = 1$. Hence $(p, q_1) = 1$.
b) $3q_1 - 2q_2 = 1$. Hence $(q_1, q_2) = 1$.
c) $3p - (2^{k+2} - 3)q_2 = 2^{k-1}$, so $(p, q_2) = 1$. □

Note: At $k = 1$, with $p = 7, q_1 = 3, q_2 = 4$, the result still holds.

Lemma 2: *If* $q_1 = 2^k + 1, q_2 = 2^k + 2^{k-1} + 1, p = 2^{2k+1} - 1$, then $2^k q_1^2 \equiv q_2 \pmod{p}$.

Proof: $2^k q_1^2 - q_2 = (2^{k-1} + 1)p$. □

Lemma 3: For $k \geq 3$

$$(2^k + 1)^3 \equiv 2a_k \pmod{2^{2k+1} - 1}$$

where

$$a_k = 2^{2k-1} + 2^{k+1} - 2^{k-2} + 1.$$

(Note that a_k is an odd number greater than 1, with $1 < 2a_k < p$, for all $k \geq 3$. Thus, $q_1^3 = (2^k + 1)^3$ is not in the same cyclotomic coset as 1, modulo $p = 2^{2k+1} - 1$, for $k > 2$.)

Proof:

$$q_1^3 = (2^{k-1}+1)p + 2(2^{2k-1} + 7\cdot 2^{k-2} + 1)$$
$$\equiv 2^{2k} + 2^{k+1} + 2^k + 2^{k-1} + 2 \pmod p$$

whereas the cyclotomic coset of 1 consists of $C_1 = \{1, 2, 2^2, \cdots, 2^{2k}\}$, modulo $p = 2^{2k+1} - 1$. Hence $q_1^3 \notin C_1$, for $k \geq 3$. □

Theorem 1: In any case where

$$b(t) = \mathrm{tr}_1^n(\alpha^t) + \mathrm{tr}_1^n(\alpha^{q_1 t}) + \mathrm{tr}_1^n(\alpha^{q_2 t})$$

is a two-level autocorrelation sequence of odd degree $n \geq 7$ and period $p = 2^n - 1$, the number of cyclically distinct sequences which can be obtained from it by decimation (which will also be two-level autocorrelation sequences of period p) is equal to $\phi(2^n-1)/n$, which is the number of primitive polynomials of degree n over F_2, as well as the number of cyclically distinct m-sequences of period p.

Proof: We have seen that q_2 is in the cyclotomic coset of q_1^2, so that $1, q_1, q_2$ are in separate cyclotomic cosets for all odd $n \geq 5$. If $\mathrm{tr}_1^n(\alpha^i) = a_i, \mathrm{tr}_1^n(\alpha^{q_1 i}) = b_i$, and $\mathrm{tr}_1^n(\alpha^{q_2 i}) = c_i$, then $b_i = a_{q_1 i}$ and $c_i = b_{q_1 i} = a_{q_1^2 i}$. For each primitive polynomial of degree n over $F_2(2)$, letting α be one of its roots leads to a different sequence s_i, unless the *next* iteration of decimation by $q_1, \{a_{q_1^3 i}\}$ is $\{a_i\}$ again. (This actually happens at $n = 5$, where there are six m-sequences, but only two sequences (the quadratic residue sequence and its reverse) by the new construction, since $\{a_i\} + \{a_{q_1 i}\} + \{a_{q_1^2 i}\}$ is the same sequence as $\{a_{q_1 i}\} + \{a_{q_1^2 i}\} + \{a_{q_1^3 i}\}$, etc.) By Lemma 3, since q_1^3 is not in the same coset as 1, this degeneracy does not arise for $n \geq 7$. □

Theorem 2: For $g(x)$ as used in Conjectures 4 and 5,

$$\mathrm{tr}_1^n(g(x+1)+1) = \sum_{t\in I} \mathrm{tr}_1^n(x^t) \tag{1}$$

where $I = \{1\} \cup I_1 \cup I_2$ for $k = (n+2)/3$, where

$$I_1 = \{2^{k-1} + 2 + i | 0 \leq i \leq 2^{k-1} - 3\}, \tag{2}$$

and

$$I_2 = \{2^{2k-1} + 2^{k-1} + 2 + i | 0 \leq i \leq 2^{k-1} - 3\} \tag{3}$$

and where $I = I_3 \cup I_4$ for $k = (n+1)/3$, where

$$I_3 = \{2^{2k-1} + 2^{k-1} + 2 + i | 0 \leq i \leq 2^{k-1} - 3\} \tag{4}$$

and

$$I_4 = \{2^{2k} + 3 + 2i | 0 \leq i \leq 2^{k-1} - 2\}. \tag{5}$$

Moreover, in each case, all the elements in I belong to distinct cyclotomic cosets modulo $p = 2^n - 1$.

Proof:

Case 1. $k = (n+2)/3$: From Conjecture 3

$$(x+1)^{2^{2k-1}+1} = x^{2^{2k-1}+1} + x^{2^{k-1}} + x + 1 \tag{6}$$

$$\begin{aligned}(x+1)^{2^{2k-2}+2^{k-1}+1} &= x^{2^{2k-2}+2^{k-1}+1} \\ &\quad + x^{2^{2k-2}+2^{k-1}} \\ &\quad + x^{2^{2k-2}+1} + x^{2^{k-1}+1} \\ &\quad + x^{2^{2k-2}} + x^{2^{k-1}} + x + 1.\end{aligned} \tag{7}$$

$$\begin{aligned}(x+1)^{2^{2k-2}-2^{k-1}+1} &= (x+1)^{2^{k-1}(2^{k-1}-1)+1} \\ &= (x+1)(x^{2^{k-1}}+1)^{2^{k-1}-1} \\ &= (x+1)\left(\sum_{i=0}^{2^{k-1}-1} x^{i2^{k-1}}\right) \\ &= \sum_{i=0}^{2^{k-1}-1} x^{i2^{k-1}} + \sum_{i=0}^{2^{k-1}-1} x^{i2^{k-1}+1}\end{aligned} \tag{8}$$

$$\begin{aligned}(x+1)^{2^{2k-1}-2^{k-1}+1} &= (x+1)^{2^{k-1}(2^k-1)+1} \\ &= (x+1)(x^{2^{k-1}}+1)^{2^k-1} \\ &= (x+1)\left(\sum_{i=0}^{2^k-1} x^{i2^{k-1}}\right) \\ &= \sum_{i=0}^{2^k-1} x^{i2^{k-1}} + \sum_{i=0}^{2^k-1} x^{i2^{k-1}+1}.\end{aligned} \tag{9}$$

From (6)–(9), by combining like terms

$$\begin{aligned}&\mathrm{tr}_1^n(g(x+1)+1) \\ &\quad = \mathrm{tr}_1^n\left(x^{2^{2k-2}+2^{k-1}+1} + x^{2^{2k-2}+2^{k-1}} + x^{2^{2k-2}+1}\right. \\ &\qquad \left. + \sum_{i=2^{k-1}}^{2^k-1} x^i + \sum_{i=2^{k-1}}^{2^k-1} x^{i2^{k-1}+1}\right) \\ &\quad = \mathrm{tr}_1^n\left(x + x^{2^{2k-2}+2^{k-1}+1} + x^{2^{2k-2}+2^{k-1}}\right. \\ &\qquad \left. + \sum_{i=2^{k-1}+1}^{2^k-1} x^i + \sum_{i=2^{k-1}+1}^{2^k-1} x^{i2^{k-1}+1}\right).\end{aligned}$$

Notice that for $i = 2^{k-1}+1$ in the inner sums of the above identity, it can be combined with the second and third terms to yield

$$\begin{aligned}&\mathrm{tr}_1^n(g(x+1)+1) \\ &\quad = \mathrm{tr}_1^n\left(x + \sum_{i=2^{k-1}+2}^{2^k-1} x^i + \sum_{i=2^{k-1}+2}^{2^k-1} x^{i2^{k-1}+1}\right) \\ &\quad = \mathrm{tr}_1^n\left(x + \sum_{i=2}^{2^{k-1}-1} x^{2^{k-1}+i} + \sum_{i=2}^{2^{k-1}-1} x^{2^{2k-2}+i2^{k-1}+1}\right).\end{aligned}$$

Notice that $n = 3k-2$, whence

$$(2^{2k-2} + i2^{k-1} + 1)2^{2k-1} \equiv 2^{2k-1} + 2^{k-1} + i \pmod p.$$

Hence (1) is true. It can be easily seen that the elements in $\{1\} \cup I_1 \cup I_2$ belong to different cosets modulo p.

Case 2. $k = (n+1)/3$: Similarly, from Conjecture 2

$$\begin{aligned}\mathrm{tr}_1^n(g(x+1)+1) = \mathrm{tr}_1^n\Big(&x^{2^{2k-1}+2^{k-1}+1} \\ &+ \sum_{i=2}^{2^k-1} x^{2^{2k-1}+i} + \sum_{i=2}^{2^k-1} x^{i2^{k-1}+1}\Big).\end{aligned} \tag{10}$$

Let

$$N(i) = i + 2^{2k-1}, \qquad 2 \leq i \leq 2^k - 1. \tag{11}$$

$$M(i) = 1 + i2^{k-1}, \qquad 2 \leq i \leq 2^k - 1. \tag{12}$$

Note that $n = 3k-1$, so $M(i) \equiv i + 2^{2k} \pmod p$. Thus

$$2N(i) = 2(i + 2^{2k-1}) = 2i + 2^{2k} \equiv M(2i), \qquad 2 \leq i \leq 2^{k-1} \tag{13}$$

where

$$2^k M(2\cdot 2^{k-1}) = 2^k(2^k + 2^{2k}) \equiv 2 + 2^{2k} = M(2) \pmod p.$$

Therefore, (10) becomes

$$\begin{aligned}\mathrm{tr}_1^n(g(x+1)+1) = \mathrm{tr}_1^n\Big(&x^{2^{2k-1}+2^{k-1}+1} \\ &+ \sum_{i=2^{k-1}+1}^{2^k-1} x^{N(i)} + \sum_{i=1}^{2^{k-1}-1} x^{M(2i+1)}\Big).\end{aligned} \tag{14}$$

Since $N(2^{k-1}+1) = 2^{k-1}+1+2^{2k-1}$, from (14) we get

$$\mathrm{tr}_1^n(g(x+1)+1) = \mathrm{tr}_1^n\left(\sum_{i=0}^{2^{k-1}-3} x^{2^{2k-1}+2^{k-1}+2+i} + \sum_{i=1}^{2^{k-1}-1} x^{2^{2k}+1+2i}\right)$$

which is (1). From $n = 3k-1$ and the definition of coset leaders modulo p, we can derive that the elements in $I_3 \cup I_4$ belong to different cosets modulo p. □

Corollary: The sequences related by

$$b(t) = \mathrm{tr}_1^n(g(\alpha^t)) \quad \text{and} \quad b'(t) = tr_1^n(g(\alpha^t+1)+1)$$

in Conjectures 4 and 5 correspond to nonequivalent cyclic difference sets. Also, each of them can generate $\phi(2^n-1)/n$ cyclically distinct sequences obtained from it by decimation, which will also be two-level correlation sequences of period $p = 2^n - 1$.

Proof: For $k \geq 4$, Theorem 2 yields that $\{b(t)\}$ and $\{b'(t)\}$ correspond to nonequivalent cyclic difference sets. For $k = 3, 3k-1 = 8$, and $3k-2 = 7$, with these results illustrated in Section III. Hence, $\{b(t)\}$ and $\{b'(t)\}$ correspond to nonequivalent cyclic difference sets for $k > 2$. By a similar argument as in Corollary 1, we can obtain that $\{b(t)\}$ and its decimation sequences are shift-distinct. Hence $\{b(t)\}$ can generate $\phi(2^n-1)/n$ cyclically distinct sequences obtained from it by decimation. Considering the shift-distinct property of $\{b(t)\}$, letting $u(x) = \mathrm{tr}_1^n(g(x))$ and $v(x) = \mathrm{tr}_1^n(g(x+1)+1)$, then we have $v(x+1) = u(x)+n$. Thus there is a one-to-one correspondence between $u(x^r)$ and $v(x^r)$ as r runs through all numbers less than p and relatively prime to p. Since $\{b(t)\}$ and its r-decimation sequence are shift-distinct, we have $\{b'(t)\}$ and its r-decimation are shift-distinct.

ACKNOWLEDGMENT

The authors wish to thank M. Yun, H. Chung, K. Yang, and H. Song for many interesting discussions and their useful comments.

REFERENCES

[1] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of *Encyclopedia of Mathematics and Its Applications.* Reading, MA: Addison-Wesley, 1983.
[2] L. D. Baumert, *Cyclic Difference Sets* (Lecture Notes in Mathematics). Berlin, Germany: Springer-Verlag, 1971.
[3] D. Jungnickel, "Difference sets," in *Contemporary Design Theory*, J. H. Dinitz and D. R. Stinson, Eds. New York: Wiley, 1992, pp. 241–324.
[4] L. D. Baumert and H. M. Fredricksen, "The cyclotomic numbers of order 18 with applications to difference sets," *Math. Comp.*, vol. 21, pp. 204–219, 1967.
[5] U. Cheng, "Exhaustive construction of $(255, 127, 63)$ cyclic difference sets," *J. Comb. Theory*, vol. A-35, pp. 115–125, 1983.
[6] R. Dreier, "(511, 255, 127) cyclic difference sets," IDA talk, July 1992.
[7] S. W. Golomb, "On the classification of balanced binary sequences of period $2^n - 1$," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 730–732, Nov. 1980.
[8] U. Cheng and S. W. Golomb, "On the characterization of PN sequences," *IEEE Trans. Inform. Theory*, vol. IT-29, p. 600, July 1983.
[9] S. W. Golomb, *Shift-Register Sequences*. San Francisco, CA: Holden-Day, 1967; Laguna Hills, CA: Aegean Park, 1982.
[10] J.-S. No and P. V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," *IEEE Trans. Inform. Theory*, vol. 35, pp. 371–379, Mar. 1989.
[11] J.-S. No, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," Ph.D. dissertation, Univ. Southern California, Los Angeles, CA, May 1988.
[12] B. Gordon, W. H. Mills, and L. R. Welch, "Some new difference sets," *Canadian J. Math.*, vol. 14, no. 4, pp. 614–625, 1962.
[13] R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 548–553, May 1984.
[14] J.-S. No, "Generalization of GMW sequences and No sequences," *IEEE Trans. Inform Theory*, vol. 42, pp. 260–262, Jan. 1996.
[15] J.-S. No, H.-K. Lee, H. Chung, H.-Y. Song, and K. Yang, "Trace representation of Legendre sequences of Mersenne prime period," *IEEE Trans. Inform. Theory*, vol. 42, pp. 2254–2255, Nov. 1996.
[16] J.-S. No, K. Yang, H. Chung, and H.-Y. Song, "On the construction of binary sequences with ideal autocorrelation property," in *Proc. 1996 IEEE Int. Symp. Information Theory and Its Applications (ISITA '96)* (Victoria, B.C., Canada, Sept. 17–20, 1996), pp. 837–840.
[17] ——, "A new family of binary sequences with optimal correlation properties," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1596–1602, Sept. 1997.

Recent Results on Polyphase Sequences

Solomon W. Golomb, *Fellow, IEEE*, and Moe Z. Win, *Member, IEEE*

***Abstract*— A polyphase sequence of length $n+1$, $A = \{a_j\}_{j=0}^n$, is a sequence of complex numbers, each of unit magnitude. The (unnormalized) aperiodic autocorrelation function of a sequence is denoted by $C(\tau)$. Associated with the sequence A, the sequence polynomial $f_A(z)$ of degree n and the correlation polynomial $g_A(z)$ of degree $2n$ are defined. For each root α of $f_A(z)$, $1/\alpha^*$ is a corresponding root of $f_A^*(z^{-1})$. Transformations on the sequence A which leave $|C(\tau)|$ invariant are exhibited, and the effects of these transformations on the roots of $f_A(z)$ are described. An investigation of the set of roots Λ of the polynomial $f_A(z)$ has been undertaken, in an attempt to relate these roots to the behavior of $C(\tau)$. Generalized Barker sequences are considered as a special case of polyphase sequences, and examples are given to illustrate the relationship described above.**

***Index Terms*— Aperiodic autocorrelation, correlation magnitude preserving transformations, correlation polynomial, impulse equivalent pulse trains, polyphase sequences, roots of polynomial, sequence polynomial.**

I. PRELIMINARIES

Let $A = \{a_j\}_{j=0}^n$ be any sequence of complex numbers of length $L = n+1$. The *sequence polynomial* $f_A(z)$ and the unnormalized finite *aperiodic autocorrelation function* $C(\tau)$ of the sequence A are defined, respectively, to be

$$f_A(z) \triangleq \sum_{j=0}^{n} a_j z^j \tag{1}$$

Manuscript received August 15, 1996; revised August 1, 1997. The material in this correspondence was presented in part at the IEEE International Symposium on Information Theory, Whistler, BC, Canada, September 1995.

S. W. Golomb is with the Communication Sciences Institute, Department of Electrical Engineering–Systems, University of Southern California, Los Angeles, CA 90089-2565 USA.

M. Z. Win was with the Communication Sciences Institute, Department of Electrical Engineering–Systems, University of Southern California, Los Angeles, CA 90089-2565 USA. He is now with the Wireless Systems Research Department, Newman Springs Laboratory, AT&T Labs.–Research, Red Bank, NJ 07701-7033 USA.

Publisher Item Identifier S 0018-9448(98)00830-X.