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.

and

$$C(\tau) \triangleq \begin{cases} \sum_{j=0}^{n-\tau} a_j a_{j+\tau}^*, & 0 \le \tau \le n \\ \sum_{j=0}^{n+\tau} a_j^* a_{j-\tau}, & -n \le \tau \le 0 \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

where a^* denotes the complex conjugate of a. In particular

$$C(0) = \sum_{j=0}^{n} |a_j|^2$$

is known as the *total energy* of the sequence A.

The sequence polynomial is related to the aperiodic autocorrelation function of the sequence by the equation

$$f_A^*(z) f_A(z^{-1}) = \sum_{\tau=-n}^{n} C(\tau) z^\tau \tag{3}$$

where

$$f_A^*(z) = \sum_{j=0}^{n} a_j^* z^n.$$

For later convenience, the *correlation polynomial* is defined to be

$$g_A(z) \triangleq z^n f_A^*(z) f_A(z^{-1}) = \sum_{\tau=0}^{2n} C(\tau - n) z^\tau. \tag{4}$$

A *polyphase sequence* is a finite sequence of complex numbers such that each term of the sequence takes on values on the unit circle, i.e., $|a_j| = 1$ for $0 \le j \le n$. If the further constraint on the aperiodic autocorrelation function of such a sequence is imposed that $|C(\tau)| \le 1$ for $1 \le |\tau| \le n$, then the sequence A is called a *generalized Barker sequence* (GBS) [1]. The "original" (or *binary*) *Barker sequences* have terms limited to the values $a_j = \pm 1$ [2], [3]. This means that every GBS is a polyphase sequence but polyphase sequences do not necessarily satisfy the GBS condition. Polyphase sequences with weaker aperiodic autocorrelation constraints have also been studied [4]–[6].

II. On the Relationships Between Roots and Sequences

Four operations on the sequence A, which generate a group G of transformations on A, were observed in [1]. The sequence A and any new sequence B obtained from A by any operation in the group G, have the same values of $|C(\tau)|$ for all τ with $-n \le \tau \le n$. These operations are

- $A \to \hat{A}$: A Reversal Transformation (RT) operator maps $A \to \hat{A}$ such that $\hat{A} = \{a_{n-j}\}_{j=0}^n$, the *reverse* sequence of $A = \{a_j\}_{j=0}^n$.
- $A \to A^*$: A Conjugate Transformation (CT) operator maps $A \to A^*$ such that $A^* = \{a_j^*\}_{j=0}^n$, the *conjugate* sequence of A.
- $A \to A_\eta$: A Constant Multiplication Transformation (CMT) operator maps $A \to A_\eta$ such that $A_\eta = \{\eta a_j\}_{j=0}^n$, for any complex number η with $|\eta| = 1$.
- $A \to A^\rho$: A Progressive Multiplication Transformation (PMT) operator maps $A \to A^\rho$ such that $A^\rho = \{\rho^j a_j\}_{j=0}^n$, for any complex number ρ with $|\rho| = 1$.

Two sequences A and B related by any combination of these transformations are called *equivalent*. It is easy to show that every polyphase sequence is equivalent to one which begins $\{1, 1, e^{i\theta}, \cdots\}$ with $0 \le \theta \le \pi$, which is known as the *normalized form*.[1]

[1]The symbol i is reserved in this correspondence to denote $\sqrt{-1}$.

Let Λ be the set of the n complex roots of $f_A(z)$. The effect of each of the four generators of the group G, when applied to the sequence A, on the set of roots of the associated sequence polynomial, is determined as follows:

$A \to \hat{A}$:

$$f_{\hat{A}}(z) = \sum_{j=0}^{n} a_{n-j} z^j = \sum_{j=0}^{n} a_j z^{n-j} = z^n \sum_{j=0}^{n} a_j z^{-j} = z^n f(z^{-1}).$$

Thus the roots of $f_{\hat{A}}$ are the *reciprocals* of the roots of $f(z)$. Hence, for each

$$\alpha \in \Lambda, \qquad 1/\alpha \in \hat{\Lambda}.$$

If $\alpha = re^{i\theta}$, then $1/\alpha = \frac{1}{r} e^{-i\theta}$.

$A \to A^*$:

$$f_{A^*}(z) = \sum_{j=0}^{n} a_j^* z^j = f_A^*(z).$$

Thus the roots of $f_{A^*}(z)$ are the *conjugates* of the roots of $f_A(z)$. Hence, for each $\alpha \in \Lambda$, $\alpha^* \in \Lambda^*$. If $\alpha = re^{i\theta}$, then $\alpha^* = re^{-i\theta}$.

$A \to A_\eta$:

$$f_{A_\eta}(z) = \sum_{j=0}^{n} \eta a_j z^j = \eta f_A(z).$$

Thus the roots of $f_{A_\eta}(z)$ are *the same* as the roots of $f_A(z)$, and $\Lambda_\eta = \Lambda$ for all η.

$A \to A^\rho$:

$$f_{A^\rho}(z) = \sum_{j=0}^{n} a_j \rho^j z^j = f_A(\rho z).$$

Hence, for every root α of $f_A(z)$, $\rho^{-1}\alpha$ is a root of $f_{A^\rho}(z)$. If $\alpha = re^{i\theta}$ and $\rho = e^{i\phi}$, then $\rho^{-1}\alpha = re^{i(\theta-\phi)}$.

The restrictions $|\eta| = 1$ and $|\rho| = 1$ are required in all cases to preserve the values $|C(\tau)|$ for all τ and to satisfy the $|a_j| = 1$ condition for all j.

The four generators of the group G, and their effect on the set of roots of the associated sequence polynomial, when applied to the sequence A, are summarized in Table I. The subgroup U of G generated by the operators CT, CMT, and PMT has the effect of performing all *unitary transformations* on the complex plane (i.e., pure rotations around the origin, and reflections in any line through the origin). This is also the effect of the subgroup U on the set Λ of complex roots of $f_A(z)$. Taking into account the geometric effect of the operator RT, the full group G performs inversions in the unit circle of the complex plane, as well as rigid rotations and reflections. This also describes the actions of the operators in G on the set Λ of the roots of $f_A(z)$.

Note that the roots of $f_A(z^{-1})$ are the inversions, with respect to the unit circle, of the roots of $f_A^*(z)$. That is, if $\alpha = re^{i\theta}$ is a root of $f_A(z)$, then $\alpha^* = re^{-i\theta}$ is a root of $f_A^*(z)$ and $1/\alpha = \frac{1}{r} e^{-i\theta}$ is a root of $f_A(z^{-1})$. Hence, the set of roots of the correlation polynomial

$$z^n f_A^*(z) f_A(z^{-1}) = \sum_{\tau=0}^{2n} C(\tau - n) z^\tau$$

is *closed* with respect to inversion in the unit circle.

TABLE I
THE FOUR GENERATORS OF THE GROUP G, AND THEIR EFFECT ON THE SET Λ

Generator	Operation and Their Effect on the set of roots Λ
RT	$A \to \hat{A}$: $\hat{A} = \{a_{n-j}\}_{j=0}^{n}$, the *reverse* sequence of $A = \{a_j\}_{j=0}^{n}$
	$f_{\hat{A}}(z) = \sum_{j=0}^{n} a_{n-j} z^j = \sum_{j=0}^{n} a_j z^{n-j} = z^n \sum_{j=0}^{n} a_j z^{-j} = z^n f(z^{-1})$.
	The roots of $f_{\hat{A}}$ are the *reciprocals* of the roots of $f(z)$.
	For each $\alpha \in \Lambda$, $1/\alpha \in \hat{\Lambda}$. If $\alpha = re^{i\theta}$, then $1/\alpha = \frac{1}{r}e^{-i\theta}$.
CT	$A \to A^*$: $A^* = \{a_j^*\}_{j=0}^{n}$, the *conjugate* sequence of A.
	$f_{A^*}(z) = \sum_{j=0}^{n} a_j^* z^j = f_A^*(z)$.
	The roots of $f_{A^*}(z)$ are the *conjugates* of the roots of $f_A(z)$.
	For each $\alpha \in \Lambda$, $\alpha^* \in \Lambda^*$. If $\alpha = re^{i\theta}$, then $\alpha^* = re^{-i\theta}$.
CMT	$A \to A_\eta$: $A_\eta = \{\eta a_j\}_{j=0}^{n}$, for any complex number η with $\lvert\eta\rvert = 1$.
	$f_{A_\eta}(z) = \sum_{j=0}^{n} \eta a_j z^j = \eta f_A(z)$.
	The roots of $f_{A_\eta}(z)$ are *the same* as the roots of $f_A(z)$, and $\Lambda_\eta = \Lambda$ for all η
PMT	$A \to A^\rho$: $A^\rho = \{\rho^j a_j\}_{j=0}^{n}$, for any complex number ρ with $\lvert\rho\rvert = 1$.
	$f_{A^\rho}(z) = \sum_{j=0}^{n} a_j \rho^j z^j = f_A(\rho z)$.
	For every root α of $f_A(z)$, $\rho^{-1}\alpha$ is a root of $f_{A^\rho}(z)$.
	If $\alpha = re^{i\theta}$ and $\rho = e^{i\phi}$, then $\rho^{-1}\alpha = re^{i(\theta-\phi)}$.

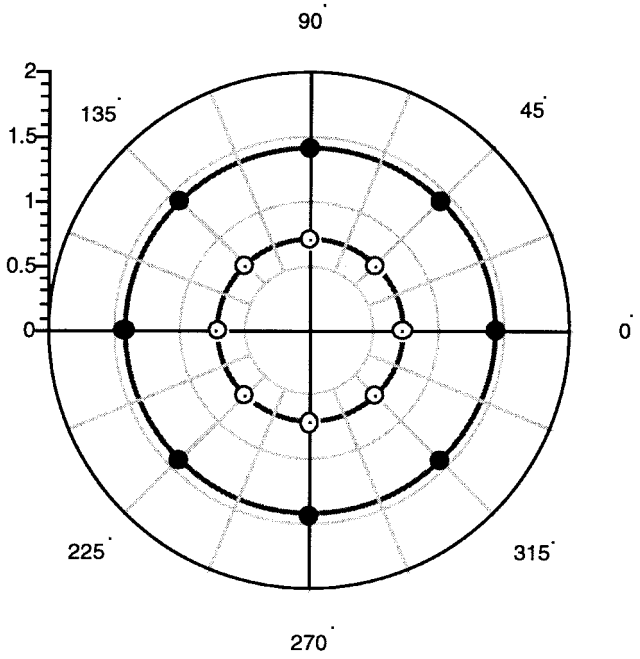

Fig. 1. Roots of the correlation polynomial corresponding to a sequence of length 9, satisfying Huffman's condition. The $2n = 2(9-1) = 16$ roots lie on two concentric circles around the origin with inner radius equal to $1/\sqrt{2}$, and outer radius equal to $\sqrt{2}$.

For a given sequence $A = \{a_j\}_{j=0}^{n}$, let

$$\Lambda = \{\alpha_1, \cdots, \alpha_n\} = \{r_1 e^{i\theta_1}, \cdots, r_n e^{i\theta_n}\}$$

be the set of the n complex roots of the associated polynomial $f_A(z)$. The *angle differences* set $\Delta\Lambda$ associated with the sequence A is defined to be $\Delta\Lambda = \{|\theta_k - \theta_l| : 1 \le k < l \le n\}$. Here, the angle difference $|\theta_k - \theta_l|$ is whichever one of $\theta_k - \theta_l$ and $\theta_l - \theta_k$ that is on the interval $[0, \pi]$. The cardinality of $\Delta\Lambda$ is

$$\binom{n}{2} = n(n-1)/2.$$

The angle differences set $\Delta\Lambda$ is invariant under all operators in the group G. If the elements of $\Delta\Lambda$ are not all distinct, these elements are preserved, *with their multiplicities*, by each operator in G. That is, $\Delta\Lambda$ is preserved as a *multiset* by every element of G. The effects noted above for these four types of transformations are valid in general for *any* sequences of complex numbers of length n (not necessarily polyphase sequences) and their corresponding sequence polynomials.

III. "IMPULSE EQUIVALENT PULSE TRAINS"

A related problem considered by Huffman can be stated as follows [7]. Let $A = \{a_0, a_1, \cdots, a_n\}$ be a sequence of *real* numbers of length $L = n + 1$, for which[2]

$$C(\tau) = \begin{cases} \sum_{j=0}^{n} a_j^2, & \tau = 0 \\ 0, & \tau = \pm 1, \pm 2, \cdots, \pm(n-1) \\ a_0 a_n, & \tau = \pm n. \end{cases} \tag{5}$$

Then the correlation polynomial

$$\begin{aligned} g_A(z) &= \sum_{\tau=0}^{2n} C(\tau - n) z^\tau \\ &= C(-n) + C(0) z^n + C(n) z^{2n} \end{aligned} \tag{6}$$

where $C(-n) = C(n) = a_0 a_n$. Normalizing to $C(n) = \pm 1$, (6) becomes

$$g_A(z) = \pm 1 + C(0) z^n \pm z^{2n}. \tag{7}$$

Finding the sequence satisfying the condition (5) is equivalent to finding the polynomial $f_A(z)$ (or its roots). To find the roots of $f_A(z)$,

[2]This is the strongest possible aperiodic autocorrelation constraint since $C(n) \neq 0$ for any sequence truly of length $L = n + 1$.

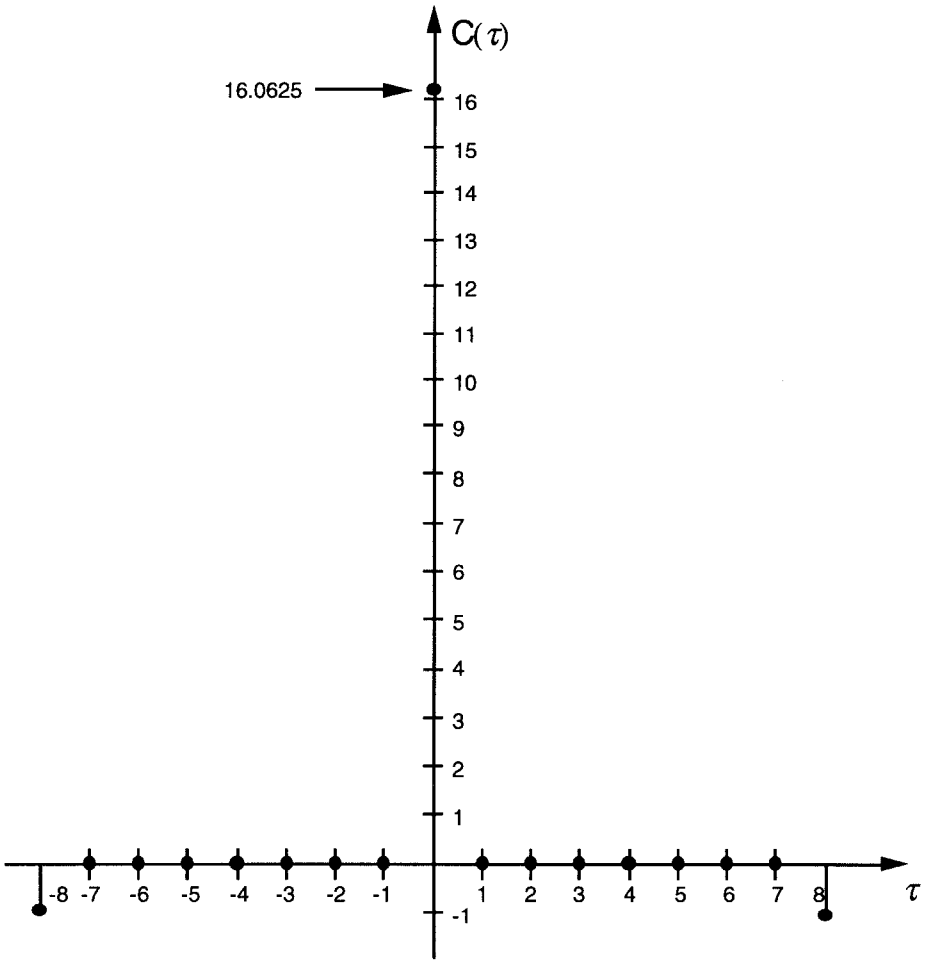

Fig. 2. Aperiodic autocorrelation function of the Huffman sequence of length 9.

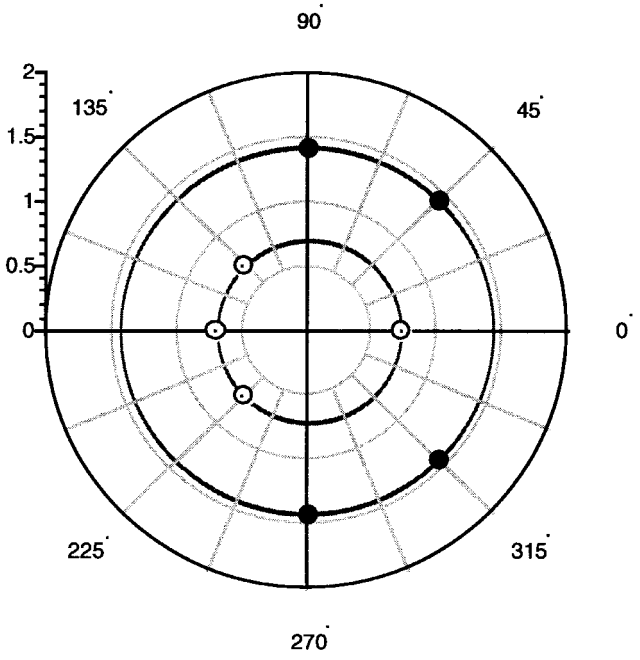

Fig. 3. Roots of the sequence polynomial corresponding to the Huffman sequence of length 9. The $n = (9-1) = 8$ roots lie on two concentric circles around the origin with inner radius equal to $1/\sqrt{2}$, and outer radius equal to $\sqrt{2}$.

set

$$0 = g_A(z) = \pm 1 + C(0)z^n \pm z^{2n}$$

so that $0 = 1 \pm C(0)Z + Z^2$, where $Z = z^n$. Then

$$Z = (\mp C(0) \pm \sqrt{C^2(0) - 4})/2$$

where the two values of Z are reciprocals of each other, say R and $r = 1/R$. Then $z^n f_A(z) f_A(z^{-1}) = 0$ has the n roots of $z^n = R$ and the n roots of $z^n = \frac{1}{R} = r$. Thus the $2n$ roots of $f_A(z) f_A(z^{-1}) = 0$ lie on two concentric circles around the origin. Of these $2n$ roots, n of them correspond to the roots of $f_A(z) = 0$ and the other n correspond to the roots of $f_A(z^{-1}) = 0$. Note that to every root α corresponding to $f_A(z) = 0$, there must be a corresponding root $1/\alpha$ corresponding to $f_A(z^{-1}) = 0$. Furthermore, the complex roots in Λ must occur in complex conjugate pairs, so that $f_A(z)$ will have real coefficients. Therefore, it is necessary and sufficient to pick one and *only one* root from each ray emanating from the origin, such that the set of roots Λ consists of complex conjugate pairs as well as possible real roots.

An example, with $n = 8$, is shown in Fig. 1, where $f_A(z) f_A(z^{-1}) = 0$ has $2n = 16$ roots on the two concentric circles around the origin. The correlation polynomial corresponding to this figure is $g_A(z) = -1 + 16.0625z^n - z^{2n}$ with $n = 8$. The associated aperiodic autocorrelation function is plotted in Fig. 2. The sequence polynomial of degree 8 with eight complex roots which

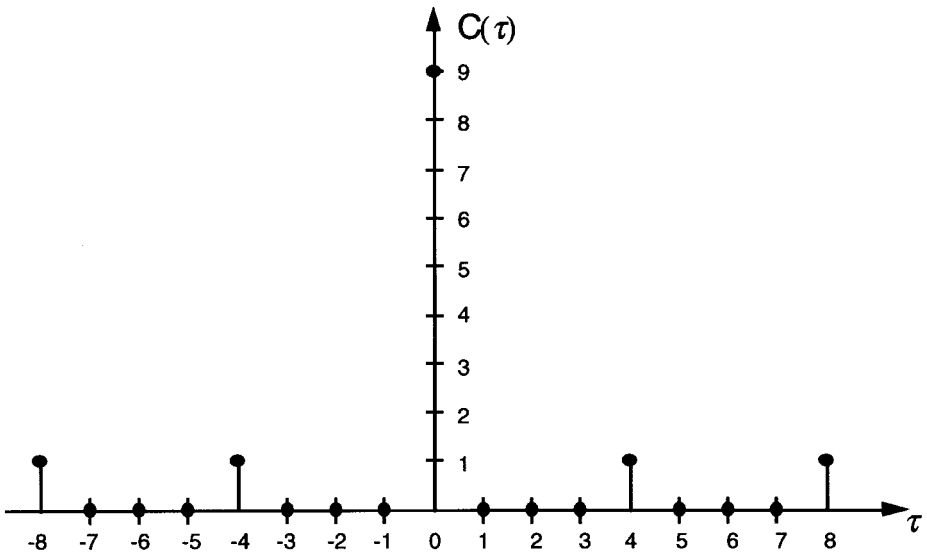

Fig. 4. Aperiodic autocorrelation function of a special sextic Barker sequence of length 9.

satisfy Huffman's conditions is

$$\begin{aligned} f_A(z) &= \left(z-\frac{1}{\sqrt{2}}\right)\left(z+\frac{1}{\sqrt{2}}\right)\left(z-\frac{-1+i}{2}\right)\left(z-\frac{-1-i}{2}\right) \\ &\quad \times \left(z-\sqrt{2}i\right)\left(z+\sqrt{2}i\right)(z-(1+i))(z-(1-i)) \\ &= \left(z^2-\frac{1}{2}\right)\left(z^2+z+\frac{1}{2}\right)(z^2+2)(z^2-2z+2) \\ &= \left(z^4+\frac{3}{2}z^2-1\right)\left(z^4-z^3+\frac{1}{2}z^2+z+1\right) \\ &= z^8-z^7+2z^6-\frac{1}{2}z^5+\frac{3}{4}z^4+\frac{5}{2}z^3+z^2-z-1. \end{aligned} \tag{8}$$

The roots of the sequence polynomial are plotted in Fig. 3. The corresponding Huffman sequence is

$$\{a_j\}_{j=0}^{8} = \left\{-1,-1,1,\frac{5}{2},\frac{3}{4},-\frac{1}{2},2,-1,1\right\}.$$

The total energy E of this sequence is given by

$$E = C(0) = \sum_{j=0}^{8}|a_j|^2 = \left(\sqrt{2}\right)^8 + \left(\frac{1}{\sqrt{2}}\right)^8 = 16.0625. \tag{9}$$

The energy in the largest term of the sequence is $(\frac{5}{2})^2 = 6.25$ which is 38.91% of the total energy, and the energy in the smallest term is $(\frac{1}{2})^2 = 0.25$ which is 1.6% of the total energy.

These "impulse equivalent pulse trains" exist for all lengths. This can be attributed to the fact that each term of the sequence is chosen from the continuum of real numbers, i.e. $a_i \in \mathbb{R}$, rather than being restricted to the values plus one and minus one as in the case of Barker [2]. However, there are at least two practical drawbacks associated with Huffman sequences. A device to transmit pulses with different amplitude values taken from the entire set of real numbers is not feasible. Secondly, the energy distribution across the sequences is not uniform. A small number of terms contain nearly all of the energy. This defeats the main purpose of using a sequence, which is to spread the total energy over a large number of terms, with each term being peak-power limited.

IV. Polynomials for Generalized Barker Sequences

A. Existence Results

Examples of GBS given in [1]–[3] and [8]–[12] are restricted to values which are kth roots of unity. If such restrictions are made on the values of the GBS, there seems to be a limit on the maximum length L, depending on k, for such sequences. Searches for GBS with no restriction on the values to kth roots of unity have been carried out using numerical optimization techniques. Examples of such sequences are now known for all $L \leq 36$ [13]–[15]. If there is no such restriction, some researchers believe that arbitrarily long sequences may exist. Every unrestricted sequence can be approximated by a sequence of kth roots of unity in such a way that the GBS condition is maintained, for a sufficiently large value of k.

B. Parallel with Huffman Sequences

The sixth roots of unity (with zero adjoined) have the property that they are closed under multiplication and partially closed under addition. GBS using sixth roots of unity as terms are called sextic Barker sequences (SBS), and are known up to length 15 [9]. One of the SBS of length 9 has a remarkable aperiodic autocorrelation function. The sequence is $\{1,1,\epsilon,\epsilon,\epsilon^5,\epsilon^4,\epsilon,-1,1\}$, where $\epsilon = e^{2\pi i/6}$. The aperiodic autocorrelation function $C(\tau)$ satisfies

$$C(\tau) = \begin{cases} 9, & \tau = 0 \\ 1, & \tau = \pm\frac{n}{2}, \pm n \\ 0, & \text{otherwise} \end{cases} \tag{10}$$

where $n+1 = 9$. The aperiodic autocorrelation function of this special SBS is plotted in Fig. 4.

Setting

$$f_A(z) = \sum_{j=0}^{8} a_j z^j$$

for this sequence, we have

$$\begin{aligned} g_A(z) &= z^8 f_A^*(z) f_A(z^{-1}) \\ &= 1 + z^4 + 9z^8 + z^{12} + z^{16} \\ &= 1 + Z + 9Z^2 + Z^3 + Z^4 \end{aligned} \tag{11}$$

where $Z = z^4$.

The parallel with Huffman sequences suggested the investigation of the roots of $f_A(z)$. The roots of the sequence polynomials have

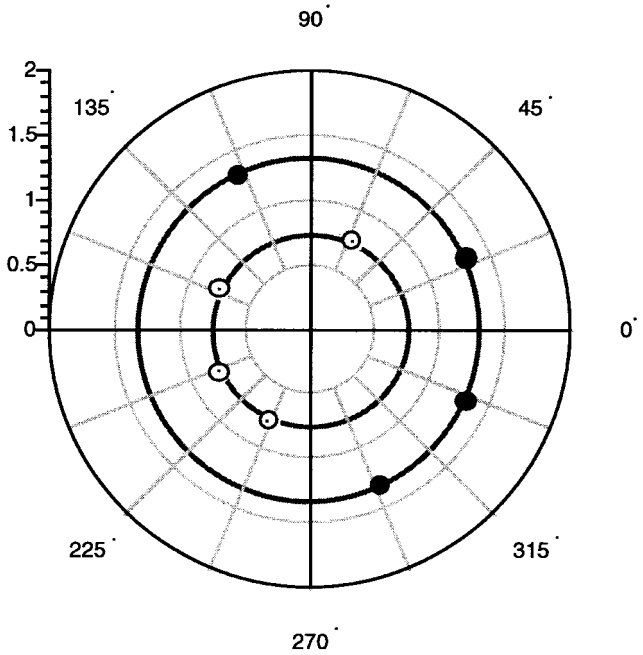

Fig. 5. Roots of the sequence polynomial corresponding to the special sextic Barker sequence of length 9. The $n = (9-1) = 8$ roots lie on two concentric circles around the origin with the inner radius equal to 0.762031, and the outer radius equal to 1.31228.

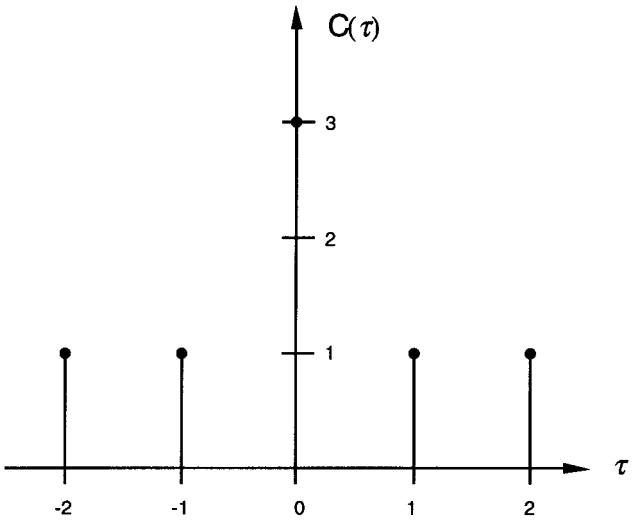

Fig. 6. Aperiodic autocorrelation function of a special sextic Barker sequence of length 3.

been computed for a large number of the known SBS. In particular, the roots of the special SBS of length 9 are plotted in Fig. 5. Note that for this sequence, the roots lie on two concentric circles around the origin with the inner radius equal to 0.762031, and the outer radius equal to 1.31228. The eight angles are of the form:

$$\left\{\theta, \theta+\frac{\pi}{2}, \theta+\pi, \theta+\frac{3\pi}{2}; -\theta, -\theta-\frac{\pi}{2}, -\theta-\pi, -\theta-\frac{3\pi}{2}\right\}.$$

One choice of θ is $\theta = 65.3232\cdots^{\circ}$.

C. Finding Other Examples

The obvious generalization of this special example involves $z^n f_A^*(z) f_A(z^{-1}) = g_A(z)$, with

$$g_A(Z) = 1 + Z + nZ^2 + Z^3 + Z^4 = 0$$

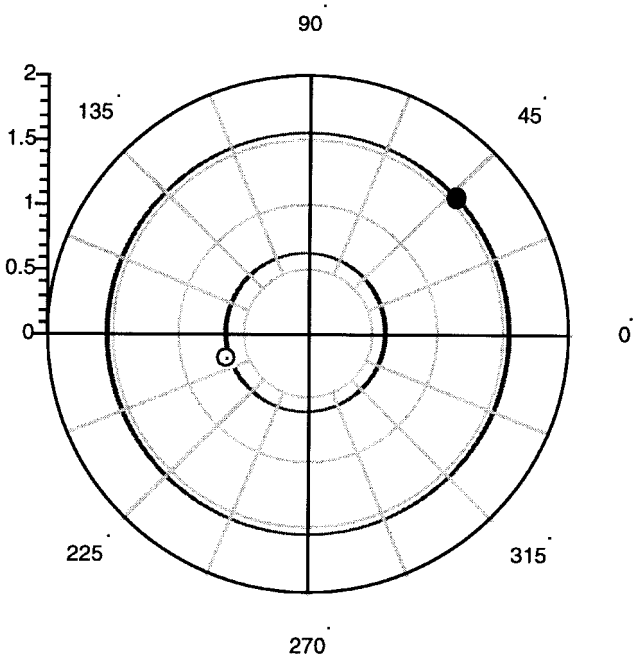

Fig. 7. Roots of the sequence polynomial corresponding to the special sextic Barker sequence of length 3. The $n = (3-1) = 2$ roots lie on two concentric circles around the origin with inner radius equal to 0.649679, and outer radius equal to 1.53922.

where $Z = z^{n/2}$. If α is one root of $g_A(Z)$, the set of roots must be $\{\alpha, \alpha^*, 1/\alpha, 1/\alpha^*\}$, since

$$g_A^*(Z) = g_A(Z) = Z^4 g_A(Z^{-1}).$$

Note that the lengths of the sequences which satisfy condition (10) must be odd. The natural question to ask is, are there odd lengths $n+1 > 2$ other than $n+1 = 9$, such that $f_A(z)$ can be found with all its coefficients on the unit circle?

Two examples were found, with $n+1 = 3$ and $n+1 = 5$. The sequence for $n+1 = 3$ is $\{1, \epsilon, 1\}$ where $\epsilon = e^{2\pi i/6}$. Here

$$\begin{aligned} g_A(z) &= z^2 f_A^*(z) f_A(z^{-1}) \\ &= z^2(1+\epsilon z + z^2)(1+\epsilon^* z^{-1} + z^{-2}) \\ &= 1 + Z + 3Z^2 + Z^3 + Z^4 \end{aligned} \tag{12}$$

with $Z = z^{(3-1)/2} = z$. The aperiodic autocorrelation function and the roots of the sequence polynomial of this length 3 special SBS are plotted in Figs. 6 and 7, respectively. Note that the roots of the sequence polynomial lie on two concentric circles around the origin with inner radius equal to 0.649679, and outer radius equal to 1.53922.

The sequence for $n+1 = 5$ is $\{1, 1, 1, -1, 1\}$ since

$$\begin{aligned} g_A(z) &= z^4 f_A^*(z) f_A(z^{-1}) \\ &= z^4(1+z+z^2-z^3+z^4)(1+z^{-1}+z^{-2}-z^{-3}+z^{-4}) \\ &= 1 + Z + 5Z^2 + Z^3 + Z^4 \end{aligned} \tag{13}$$

with $Z = z^{(5-1)/2} = z^2$. The aperiodic autocorrelation function and the roots of the sequence polynomial of this length 5 special SBS are plotted in Figs. 8 and 9, respectively. The roots of the sequence polynomial lie on two concentric circles around the origin with inner radius equal to 0.681405, and outer radius equal to 1.46756. (Note that this is one of the original *binary* Barker sequences.)

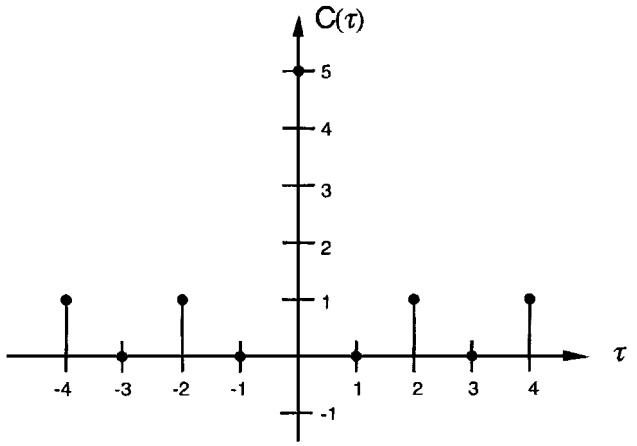

Fig. 8. Aperiodic autocorrelation function of a special sextic Barker sequence of length 5.

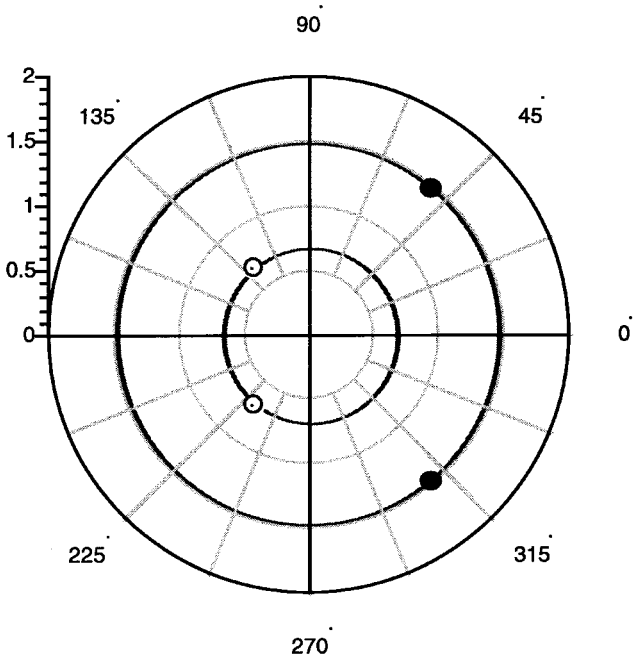

Fig. 9. Roots of the sequence polynomial corresponding to the special sextic Barker sequence of length 5. The $n = (5-1) = 4$ roots lie on two concentric circles around the origin with inner radius equal to 0.681405, and outer radius equal to 1.46756.

D. A Simplest Example

The shortest sequences $A = \{a_j\}_{j=0}^{n}$ for which the aperiodic autocorrelation function $C(\tau)$ has any "intermediate" values, with $0 < \tau < n$, are sequences of length 3. One such sequence, $\{1, 1, -1\}$, is *simultaneously* a (binary) Barker sequence *and* a Huffman sequence.[3] The corresponding sequence polynomial $f_A(z) = z^2 + z - 1$ has

$$g_A(z) = z^2 f_A^*(z) f_A(z^{-1}) = -1 + 3z^2 - z^4$$

so that $C(0) = 3, C(\pm 1) = 0, C(\pm 2) = -1$. The aperiodic autocorrelation function of this sequence is plotted in Fig. 10. The roots of $f_A(z)$ are the "golden ratios" $\phi = (\sqrt{5}-1)/2 = 0.618034$ and $-\phi' = -(\sqrt{5}+1)/2 = -1.618034$, where ϕ and ϕ' are reciprocals. That is, the roots ϕ and $-\phi'$ lie 180° apart on two concentric circles having reciprocal radii, as shown in Fig. 11. This is, however, the longest sequence which is *simultaneously* Barker

[3]The complex numbers $+1$ and -1 are *simultaneously* on the unit circle in the complex plane *and* real numbers.

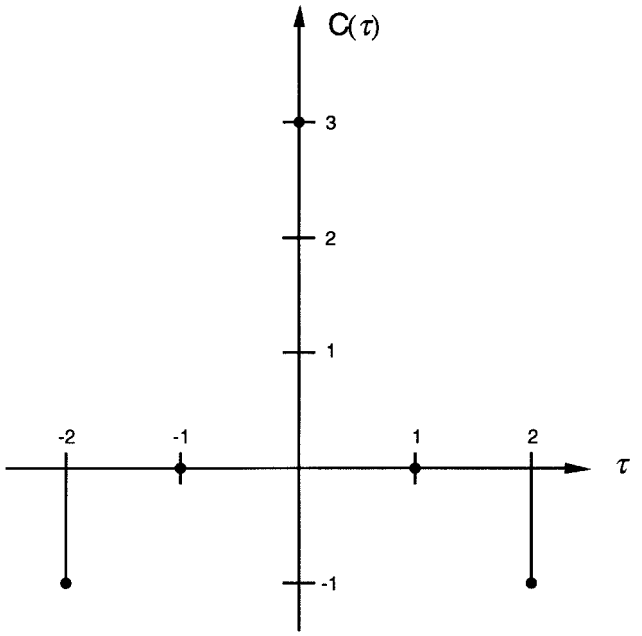

Fig. 10. Aperiodic autocorrelation function of a sequence which is *simultaneously* a (binary) Barker sequence *and* a Huffman sequence.

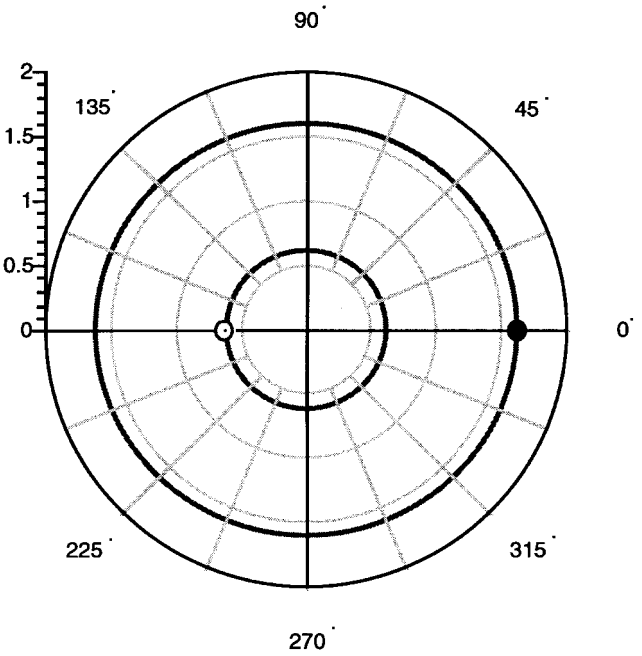

Fig. 11. Roots of the sequence polynomial corresponding to the sequence which is *simultaneously* a (binary) Barker sequence *and* a Huffman sequence. The roots lie 180° apart on two concentric circles having reciprocal radii 0.618034 and 1.618034, which are the "golden ratios."

and Huffman, since $|C(2)| = 1$ for all odd-length (binary) Barker sequences of length $n + 1 \geq 3$, while for even-length Barker sequences ($n + 1 = 2, n + 1 = 4$, and any possible others) $|C(1)| = 1$, violating the Huffman condition $C(\tau) = 0$ for all $\tau, 1 \leq \tau \leq n - 1$, whenever $n + 1 > 3$.

V. Conclusion

Generalized Barker sequences correspond to phase-modulation patterns for CW radar with finite-duration signals. Most of the examples of such sequences have been found by systematic searches, or by "hill-climbing" programs aimed at minimizing the maximum

value of $|C(\tau)|$ for $1 \leq \tau \leq n-1$ [13]–[15]. Our current efforts are directed toward discovering systematic methods of constructing such sequences.

ACKNOWLEDGMENT

The authors wish to thank P. Gaal, a graduate student at the University of Southern California, for helpful discussions and a careful review of the manuscript.

REFERENCES

[1] S. W. Golomb and R. A. Scholtz, "Generalized Barker sequences," *IEEE Trans. Inform. Theory*, vol. IT-11, pp. 533–537, Oct. 1965.
[2] R. H. Barker, "Group synchronization of binary digital systems," in *Communication Theory*, W. Jackson, Ed. London, U.K.: Butterworths, 1953, pp. 273–287. (Papers read at a Symposium on "Applications of Communication Theory" held at the Institution of Electrical Engineers, London, Sept. 22–26, 1952.)
[3] R. Turyn and J. Storer, "On binary sequences," *Proc. Amer. Math. Soc.*, vol. 12, pp. 394–399, June 1961.
[4] R. L. Frank, "Polyphase codes with good nonperiodic correlation properties," *IEEE Trans. Inform. Theory*, vol. IT-9, pp. 43–45, Jan. 1963.
[5] R. Turyn, "The correlation function of a sequence of roots of 1," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 524–525, July 1967.
[6] U. Somaini and M. H. Ackroyd, "Uniform complex codes with low autocorrelation sidelobes," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 381–382, Sept. 1974.
[7] D. A. Huffman, "The generation of impulse-equivalent pulse trains," *IRE Trans. Inform. Theory*, vol. IT-8, pp. s10–s16, Sept. 1962.
[8] N. Zhang and S. W. Golomb, "Uniqueness of the generalized Barker sequence of length 6," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1167–1170, Sept. 1990.
[9] N. Zhang, "Generalized Barker sequences," Ph.D. dissertation, Univ. Southern Calif., Los Angeles, May 1988.
[10] N. Zhang and S. W. Golomb, "Sixty-phase generalized Barker sequences," *IEEE Trans. Inform. Theory*, vol. 35, pp. 911–912, July 1989.
[11] N. Chang and S. W. Golomb, "On n-phase Barker sequences," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1251–1253, July 1994.
[12] ____, "7200-phase generalized Barker sequences," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1236–1238, July 1996.
[13] L. Bömer and M. Antweiler, "Polyphase Barker sequences," *Electron. Lett.*, vol. 25, pp. 1577–1579, Nov. 1989.
[14] M. Friese and H. Zottmann, "Polyphase Barker sequences up to length 31," *Electron. Lett.*, vol. 30, pp. 1930–1931, Sept. 1994.
[15] M. Friese, "Polyphase Barker sequences up to length 36," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1248–1250, July 1996.

Achievable Rates for Tomlinson–Harashima Precoding

Richard D. Wesel, *Member, IEEE*, and John M. Cioffi, *Fellow, IEEE*

***Abstract*— This correspondence examines Tomlinson–Harashima precoding (THP) on discrete-time channels having intersymbol interference and additive white Gaussian noise. An exact expression for the maximum achievable information rate of zero-forcing (ZF) THP is derived as a function of the channel impulse response, the input power constraint, and the additive white Gaussian noise variance. Information rate bounds are provided for the minimum mean-square error (MMSE) THP. The performance of ZF-THP and MMSE-THP relative to each other and to channel capacity is explored in general and for some example channels. The importance of symbol rate to ZF-THP performance is demonstrated.**

***Index Terms*— Additive white Gaussian noise, capacity, intersymbol interference, peak constraint, Tomlinson–Harashima precoding.**

I. INTRODUCTION

Tomlinson [1] and Harashima [2], [3] independently introduced precoding as a technique for intersymbol interference mitigation. The structure that they presented is referred to as the Tomlinson–Harashima Precoder (THP). There are other precoding structures [4]–[6], but this correspondence is concerned primarily with THP.

Price [7] and Harashima *et al*. [3] showed that zero-forcing THP (ZF-THP) achieves the maximum possible mutual information at high SNR for pulse amplitude modulation (PAM) inputs. Miyakawa et al. [2] computed the rates achievable with ZF-THP for a specific coaxial cable channel using high SNR approximations. Mazo and Salz [8] characterized the power difference between the inputs and outputs of a THP transmitter and extended the ZF-THP from real valued signals and filters to complex valued signals and filters. Cioffi and Dudevoir [9] introduced the MMSE-THP and compared its output SNR with that of the ZF-THP.

This correspondence quantifies loss from capacity of ZF-THP and MMSE-THP for any given intersymbol interference (ISI) channel and additive white Gaussian noise (AWGN) variance. An exact formula is derived for the ZF-THP information rate. Upper and lower bounds are provided for the MMSE-THP information rate. These information rate characterizations do not rely on high signal-to-noise ratio (SNR) approximations; they are valid for any SNR.

The loss from capacity at a particular SNR depends on the specific channel impulse response. Several impulse responses are studied as examples. For channels with severe ISI, the MMSE-THP can provide a significant performance improvement over the ZF-THP at low- to mid-range SNR. However, when the SNR becomes sufficiently large, the two techniques become identical. At high SNR the only loss from capacity incurred by THP is the shaping loss described by Forney [10].

Manuscript received March 1, 1996; revised July 15, 1997. This work was supported by an AT&T Foundation Fellowship, by JSEP under Contract DAAH04-94-G-0058-P01, by NSF under Contract NCR-9203131, and by CASIS under Contract NAG2-842. The material in this correspondence was presented in part at the IEEE International Symposium on Information Theory, Whistler, BC, Canada, September 1995, and the 28th Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, September 1994.

R. D. Wesel is with the Electrical Engineering Department, University of California, Los Angeles, CA 90024-1594 USA.

J. M. Cioffi is with the Information Systems Laboratory, Stanford University, Stanford, CA 94305-9510 USA.

Publisher Item Identifier S 0018-9448(98)00829-3.