Complex Sequences with Low Periodic Correlations

W. O. Alltop

Abstract—Three types of families of complex periodic sequences are shown to have nearly minimal correlation magnitudes. The sequences contain no zero entries. For certain pairs of sequences of period \( N = (p - 1)/2, p \) a prime, all nonpeak correlation coefficients have magnitude close to \( (2N)^{-1/2} \).

I. INTRODUCTION

Periodic sequences are useful in the design of signals for spread spectrum radar and communication systems. A major objective in the construction of such sequences is the minimization of the magnitudes of autocorrelation sidelobes and cross correlations. Here only periodic rather than aperiodic correlations will be discussed.

Welch [1] has shown that for a family of \( M \) distinct complex-valued sequences, each of period \( N \) and norm one, a lower bound for the maximum nonpeak correlation magnitude is

\[
B(M, N) = \left( \frac{M}{MN - 1} \right)^{1/2}.
\]

That is, at least one of the \( MN - M \) autocorrelation sidelobes or \( (M^2 - M)N \) cross correlation coefficients has magnitude as great as \( B(M, N) \). Thus \( (2N)^{1/2} \) serves as a lower bound for a pair of sequences, while the lower bound increases to about \( N^{-1/2} \) as \( M \), the number of sequences, increases to \( N \).

Employing characters on the group of units in \( Z_N \), the ring of integers modulo \( N \), Scholtz and Welch [2] have constructed families of sequences of period \( N \) which possess desirable correlation properties. Each of their sequences contains \( \phi(N) \) nonzero elements per period, where \( \phi(N) \) is the number of units in \( Z_N \); \( \phi(N) \) is better known as the Euler \( \phi \)-function [3]. For \( N \) a prime, their sequences have autocorrelation sidelobes of magnitude \( 1/(N - 1) \) and cross correlations of magnitude zero and \( N^{-1/2} \). For composite \( N \) the autocorrelation sidelobes may reach \( (\phi(N))^{-1} \) for certain divisors \( d \) of \( N \). (It should be noted that the sequences in [2] have norm \( \phi(N) \) rather than one, giving the correlation magnitudes a different appearance.) Gold [4] has constructed families of binary sequences of period \( N = 2^m - 1 \), which have maximum correlation magnitudes close to \( 2N^{-1/2} \) and \( 2^{m-1}N^{-1/2} \) for \( m = 2 \) (mod 4) and \( m \) odd, respectively.

In Sections III and IV three types of families are presented that nearly meet the bound (1). All elements of the sequences have magnitude \( N^{-1/2} \), while the nonpeak correlations all have magnitudes at most \( N^{-1/2} \). The families of Section III contain \( p - 1 \) or \( p \) distinct sequences, where \( p \) is the smallest prime divisor of \( N \). Those of Section IV contain \( M \) sequences, where \( MN + 1 \) is a prime. The pairs \( (M, N) \) giving rise to these families depend upon a particular type of cyclic difference set in the additive group of \( Z_p \), the ring of integers modulo \( p \), whose order \( p < MN + 1 \). The nonpeak correlations for these sequences are approximately \( cn^{-1/2} \), where \( c = -((M - 1)/M)^{-1/2} \), \( M = 2, 4, \) or \( 8 \). Chakrabarti and Tomlinson [5] use primes \( p \) of form \( MN + 1 \) to construct complex sequences of period \( p \) rather than \( N \). Certain shifts of these give sequences with small aperiodic correlations. Gaussian sums of the type evaluated in Lemma 1 are discussed in [6].

REFERENCES


II. BASIC DEFINITIONS

Let $X$ denote a family $\{h_\lambda : 1 \leq \lambda \leq M\}$ of complex sequences of period $N$. The $k$th element of $h_\lambda$ is $h_\lambda(k)$, and one period of $h_\lambda$ is $(h_\lambda(0), h_\lambda(1), \ldots, h_\lambda(N-1))$. $Z_N$ denotes the ring of integers modulo $N$, so that $Z_p$ is isomorphic to the finite field $GF(p)$ when $p$ is prime. The $r$th correlation coefficient between $h_\lambda$ and $h_\mu$ is given by

$$H_{h_\lambda}(r) = \sum_{k=0}^{N-1} h_\lambda(k+r)*h_\mu(k),$$

where $h_\lambda(k)*$ is the complex conjugate of $h_\lambda(k)$. The arguments $k+r$ and $k$ in $h_\lambda$ and $h_\mu$ can be reduced modulo $N$ to one of the integers $0, 1, \ldots, N-1$. If the sequences are considered to be doubly infinite with period $N$, the reduction modulo $N$ is unnecessary. All sequences are assumed to have norm one over one period. That is

$$||h_\lambda||^2 = \sum_{k=0}^{N-1} |h_\lambda(k)|^2 = 1.$$ 

From this it follows that all correlation peaks $H_{h_\lambda}(0)$ are one. The measure of correlation magnitude of primary interest is

$$\max(3C) = \max\{|H_{h_\lambda}(r)| : \lambda \neq \mu \neq r \neq 0\}.$$ 

Thus $\max(3C)$ is the maximum of the magnitudes of the $M^2N-M$ nonpeak correlation coefficients. Welch's bound (1) says that

$$\max(3C) > \left(\frac{M-1}{MN-1}\right)^{1/2}.$$ 

Every $h_\lambda$ will be a sequence of roots of unity scaled by $N^{-1/2}$, $h_\lambda(k) = N^{-1/2}\omega_{N^2}^{\lambda f(k)}$, where $\omega_N = \exp(2\pi i/N)$ and $f$ is a function from $Z_M \times Z_N$ into $Z_M$. 

For the sequences of Section III $N = n$, while for those of Section IV $n = MN + 1 = p$.

As an example, let $M = N = n = 2$, and let $f(\lambda, k) = \lambda k$. Here a period of $h_\lambda$ is

$$N^{-1/2}(\omega_N^0, \omega_N^1, \omega_N^{2\lambda}, \ldots, \omega_{N^{N-1}^k}),$$

the conjugate of the $\lambda$th row of the $N \times N$ discrete Fourier transform matrix. In this case

$$|H_{h_\lambda}(r)| = \begin{cases} 0, & \text{if } \lambda \neq \mu, \\ 1, & \text{if } \lambda = \mu. \end{cases}$$

All cross correlation coefficients are zero, while all autocorrelation coefficients have magnitude one; hence $\max(3C) = 1$.

III. QUADRIC AND CUBIC PHASE SEQUENCES

For $N$ an odd integer greater than two, the $\lambda$th quadric phase sequence $a_\lambda$ is defined by

$$a_\lambda(k) = N^{-1/2}\omega_N^{k \lambda}.$$ 

The $\lambda$th cubic phase sequence $b_\lambda$ is defined by

$$b_\lambda(k) = N^{-1/2}\omega_N^{k \lambda}.$$ 

The quadric phase sequences are similar to those of Chu [7].

Example 1: For $N = 5$

$$\begin{align*}
a_1 &= 5^{-1/2}(1, \omega_5^1, \omega_5^2, \omega_5^3, \omega_5^4), \\
a_2 &= 5^{-1/2}(1, \omega_5^2, \omega_5^3, \omega_5^4, \omega_5^1), \\
a_3 &= 5^{-1/2}(1, \omega_5^3, \omega_5^1, \omega_5^4, \omega_5^2), \\
a_4 &= 5^{-1/2}(1, \omega_5^4, \omega_5^2, \omega_5^1, \omega_5^3), \\
a_5 &= 5^{-1/2}(1, 1, 1, 1, 1), \\
b_1 &= 5^{-1/2}(1, \omega_5^2, \omega_5^1, \omega_5^3, \omega_5^4), \\
b_2 &= 5^{-1/2}(1, \omega_5^4, \omega_5^3, \omega_5^2, \omega_5^1), \\
b_3 &= 5^{-1/2}(1, 1, \omega_5^3, \omega_5^1, \omega_5^4), \\
b_4 &= 5^{-1/2}(1, \omega_5^3, 1, \omega_5^1, \omega_5^4), \\
b_5 &= 5^{-1/2}(1, \omega_5^1, \omega_5^4, \omega_5^3, 1), \\
max(3C) = \max(3C_2) &= 5^{-1/2} \text{ where } \\
3C_2 &= \{a_1, a_2, \ldots, a_4\}, \\
3C_2 &= \{b_1, b_2, b_3, b_4, b_5\}.
\end{align*}$$

The sequence $a_5$ is not used because of its constant autocorrelation; indeed the period of $a_5$ is one, not five. $3C_2$ has all sidelobes $A_{3C_2}(\tau), \tau \neq 0$, equal to zero, and all cross correlation magnitudes $|A_{3C_2}(\tau)|, \lambda \neq \mu, \mu = \omega^{\tau - 1}$, let $B_{3C_2}$ denote the correlation between $b_\lambda$ and $b_\mu$, the following holds

$$B_{3C_2}(\tau) = \begin{cases} 1, & \text{if } \lambda = \mu, \tau = 0, \\ 0, & \text{if } \lambda \neq \mu, \tau = 0, \\ 5^{-1/2}, & \text{otherwise}. \end{cases}$$

The family $3C_2$ generalizes to all odd integers, while $3C_2$ generalizes to all primes $> 5$, yielding sequence families which meet the bound $N^{-1/2}$ for correlation magnitudes. For odd $N \geq 3$, define $3C_p$ by

$$3C_p = \{a_1, a_2, \ldots, a_{p-1}\},$$

where $p$ is the smallest prime divisor of $N$.

Theorem 1: For odd $N \geq 3$, $3C_p$ is a family of $p-1$ quadric phase sequences with $\max(3C_p) = N^{-1/2}$, where $p$ is the smallest prime divisor of $N$. In particular, the correlation coefficients $A_{3C_p}(\tau), 0 < \tau < N-1, 1 < \lambda, \mu < p-1$, satisfy

$$|A_{3C_p}(\tau)| = \begin{cases} 1, & \text{for } \lambda = \mu, \tau = 0, \\ 0, & \text{for } \lambda \neq \mu, \tau = 0, \\ N^{-1/2}, & \text{otherwise}. \end{cases}$$

For $p$ an odd prime let

$$3C_p = \{b_1, b_2, \ldots, b_p\}.$$

Theorem 2: For every prime $p \geq 5$, $3C_p$ is a family of $p$ cubic phase sequences with $\max(3C_p) = p^{-1/2}$. In particular the correlation coefficients $B_{3C_p}(\tau), 0 < \tau < p-1, 1 < \lambda, \mu < p$, satisfy

$$|B_{3C_p}(\tau)| = \begin{cases} 1, & \text{for } \lambda = \mu, \tau = 0, \\ 0, & \text{for } \lambda \neq \mu, \tau = 0, \\ p^{-1/2}, & \text{otherwise}. \end{cases}$$

Theorems 1 and 2 are proved by manipulation and evaluation of certain exponential sums. Using the definitions of $A_{3C_p}, a_\lambda$, and $a_\mu$, one obtains

$$A_{3C_p}(\tau) = \sum_{k=0}^{n-1} a_\lambda(k+\tau)a_\mu(k)^{*}$$

$$= \frac{1}{N} \sum_{k=0}^{n-1} \omega_N^{(k+\tau)\lambda} \omega_N^{-\mu k^2}$$

$$= \frac{1}{N} \omega_N^{\lambda^2} \sum_{k=0}^{n-1} \omega_N^{(\lambda^2-\mu)k^2 + 2\tau k}.$$ 

Similarly

$$B_{3C_p}(\tau) = \frac{1}{N} \omega_N^\lambda \sum_{k=0}^{n-1} \omega_N^{\lambda^2 k^2 + (\lambda - \mu + 3\tau)k}.$$
It follows that
\[ |A_{\lambda\mu}(\tau)| = \frac{1}{N} |Q_N(\lambda - \mu, 2\lambda\tau)|, \] (2)
\[ |B_{\lambda\mu}(\tau)| = \frac{1}{N} |Q_N(3\tau, \lambda - \mu + 3\tau^2)|, \] (3)
where
\[ Q_N(\eta, \sigma) = \sum_{k=0}^{N-1} \omega_N^{\eta k^2 + \sigma k}. \] (4)
Hence the magnitudes of the correlations can be determined from the values \[ |Q_N(\eta, \sigma)|. \]

Lemma 1: Suppose \( N \) is odd and \( \delta = \gcd(\eta, N) \), the greatest common divisor of \( \eta \) and \( N \). Then
\[ |Q_N(\eta, \sigma)|^2 = \left\{ \begin{array}{ll}
N\delta, & \text{if } \delta \text{ divides } \sigma \\
0, & \text{if } \delta \text{ does not divide } \sigma.
\end{array} \right. \] (5)
Proof: By definition
\[ |Q_N(\eta, \sigma)|^2 = Q_N(\eta, \sigma)(Q_N(\eta, \sigma))^* = \sum_{k=0}^{N-1} \left( \sum_{r=0}^{N-1} \omega_N^{\eta k^2 + \sigma k} \right)^2 = \sum_{k,r} \omega_N^{(k^2-\sigma)+\sigma(r-k)}, \]
where the pair \((k, r)\) runs through the set \( Z_N \times Z_N \). Thus the pair \((k, s)\) also runs through \( Z_N \times Z_N \), where \( s = k - r \). Using this change of summation indices one obtains
\[ |Q_N(\eta, \sigma)|^2 = \sum_{k,r} \omega_N^{(k^2-\sigma)+\sigma(r-k)} = \sum_{k=0}^{N-1} \omega_N^{\eta k^2 + \sigma k}, \]
with the summation over those values of \( k \) for which \( 2\eta k \equiv \sigma (\text{mod} N) \) and \( 0 \leq k < N - 1 \). At this point we use the fact that \( N \) is odd. Since \( \gcd(2, N) = 1 \), \( 1, \eta \equiv 0 \) (mod \( N \)) whenever \( 2\eta k \equiv 0 \) (mod \( N \)). Thus
\[ \omega_N^{\eta k^2 + \sigma k} = \omega_N^{\sigma k}, \]
if \( 2\eta k \equiv 0 \) (mod \( N \)).
It follows that
\[ |Q_N(\eta, \sigma)|^2 = N \sum_{k=0}^{N-1} \omega_N^{\sigma k}, \]
summing over the values of \( s \) for which \( \eta s \equiv 0 \) (mod \( N \)), and \( 0 < s < N - 1 \). The set of \( s \) in \( Z_N \) for which \( \eta s \equiv 0 \) (mod \( N \)) is just \( \{0, m, 2m, \ldots, (\delta - 1)m\} \) where \( \delta = \gcd(\eta, N) \) and \( m = N/\delta \). Therefore
\[ |Q_N(\eta, \sigma)|^2 = N \left[ \frac{1 + \omega_N^{m\sigma} + \omega_N^{2m\sigma} + \cdots + \omega_N^{\delta \sigma}}{\delta} \right] = \left\{ \begin{array}{ll}
N\delta, & \text{if } \sigma m \equiv 0 \text{ (mod } \delta) \\
0, & \text{if } \sigma m \not\equiv 0 \text{ (mod } \delta) \}
\end{array} \right. \]
Since \( \sigma m \equiv 0 \) (mod \( \delta \)) if and only if \( \delta \) divides \( \sigma \), the lemma is proved.

Proofs of Theorems 1 and 2: For \( \alpha_1 \) and \( \alpha_2 \) in \( \mathbb{Z}_N \), \( \lambda \) and \( \mu \) are relatively prime to \( N \). Moreover \( \lambda - \mu \) is also relatively prime to \( N \) except when \( \lambda = \mu \). Therefore the values of \[ |A_{\lambda\mu}(\tau)| \] given in Theorem 1 follow from application of (5) to (2).
For \( \tau \neq 0, \) \( 3\tau \) is relatively prime to \( p \) when \( p > 5 \). Therefore \[ |B_{\lambda\mu}(\tau)| = 2 \] whenever \( \tau \neq 0 \). It also follows from (3) and (5) that \( B_{\lambda\mu}(0) = 0 \) whenever \( \lambda = \mu \). This proves Theorem 2.

The possibilities of enlarging the family \( \mathbb{G}_N \) or of using the cubic phase sequence \( b_1, b_2, \ldots \) for composite \( N \) deserve some discussion. As before \( p \) denotes the smallest prime divisor of \( N \). If \( \gcd(\lambda, N) = d \), then \[ |A_{\lambda\mu}(m)| = \begin{cases} 1, & \text{if } m = N/d \end{cases} \]
in this case \[ |A_{\lambda\mu}(d)| = \begin{cases} (d/N)^{1/2}, & \text{if } \gcd(d, \lambda, N)/p. \end{cases} \]
Therefore, in order for \( \max(\mathbb{G}_N) \) not to exceed \( N^{-1/2} \), \( \mathbb{G}_N \) contains \( p \) distinct sequences \( \alpha_1, \alpha_2, \ldots \) with \( \lambda \) and \( \lambda - \mu \) relatively prime to \( N \). Of course there will be suitable families of \( p - 1 \) sequences other than \( \{\alpha_1, \alpha_2, \ldots, \alpha_{p-1}\} \). For example \( \max(\delta) = 35^{-1/2} \) when \( \delta = \{\alpha_4, \alpha_5, \alpha_6, \alpha_7\}, N = 35 \).

For any cubic phase sequence \( b_1, b_2, \ldots \) for \( \mathbb{G}_N \) is divisible by \( p \) but not by three. Thus the autocorrelations exceed \( N^{-1/2} \) for all \( b_1 \). This is similar to the behavior of the character sequences of [2].

IV. POWER RESIDUE SEQUENCES

Let \( \gamma \) denote a primitive root in the finite field \( Z_p \) where \( p = MN + 1 \). Let \( \beta = \gamma^p \), so that \( \beta \) and \( \gamma \) are primitive \( N \)th and \( (p - 1) \)th roots of unity in \( Z_p \), respectively. The \( N \) distinct powers of \( \beta \) (mod \( p \)) form a subgroup of \( Z_p^* \), the multiplicative group of nonzero elements of \( Z_p \). Denoting this subgroup by \( \mathbb{C}_N \), the set \( Z_p^* \) is partitioned by the \( N \) cosets of \( \mathbb{C}_N \). Moreover the\( \mathbb{E}_N \) elements \( \gamma, \gamma^2, \ldots, \gamma^{N-1} \) are coset representatives:
\[ Z_p^* = \mathbb{C}_N \cup \gamma^\eta \mathbb{C}_N \cup \cdots \cup \gamma^{N-1} \mathbb{C}_N. \]
The \( \lambda \)th \( (M, N) \) power residue sequence \( y_\lambda(k) \) is defined by
\[ y_\lambda(k) = \sum_{s=0}^{N-1} \omega_N^{\lambda k s} \text{ when } \lambda \text{ is divisible by } p \text{ but not by three.} \]

Example 2: For \( p = 19, M = 5, N = 6, \) and \( \gamma = 2 \), one obtains three distinct \( (3, 6) \) power residue sequences:
\begin{align*}
y_0(k) & = \sum_{s=0}^{5} \omega_N^{2 ks} \text{ when } k \equiv 0 \text{ (mod } N) \\
y_1(k) & = \sum_{s=0}^{5} \omega_N^{2 ks} \text{ when } k \equiv 1 \text{ (mod } N) \\
y_2(k) & = \sum_{s=0}^{5} \omega_N^{2 ks} \text{ when } k \equiv 2 \text{ (mod } N). \end{align*}
For \( \lambda = 2, p = 19, N = 6, \) and \( \gamma = 2 \), one obtains three distinct \( (3, 6) \) power residue sequences:
\begin{align*}
y_{0,1}(k) & = \sum_{s=0}^{5} \omega_N^{2 ks} \text{ when } k \equiv 0 \text{ (mod } N) \\
y_{0,2}(k) & = \sum_{s=0}^{5} \omega_N^{2 ks} \text{ when } k \equiv 1 \text{ (mod } N) \\
y_{1,2}(k) & = \sum_{s=0}^{5} \omega_N^{2 ks} \text{ when } k \equiv 2 \text{ (mod } N). \end{align*}

In general let \( \mathbb{G}_{M,N} = \{ y_{\lambda_1, \lambda_2}, \ldots, y_{\lambda_M, \lambda_N} \} \) and
\[ Y_{\lambda\mu}(\tau) = \sum_{k=0}^{N-1} y_{\lambda\mu}(k + \tau) y_{\lambda\mu}(k)^*, \]
for \( 0 < \lambda, \mu < M - 1 \) and \( 0 < s < N - 1 \), where \( p = MN + 1 \) is prime.

Lemma 2: The nonpeak correlations for the power residue family \( \mathbb{G}_{M,N} \) all assume one of the \( M \) values \( \lambda_1, \lambda_2, \ldots, \lambda_{M-1} \), where
\[ s_{\lambda} = \frac{1}{N-1} \sum_{k=0}^{N-1} y_{\lambda}(k). \]
In particular
\[ Y_{\lambda\mu}(\tau) = \left\{ \begin{array}{ll}
1, & \text{if } \lambda = \mu \text{ and } \tau = 0 \\
\eta, & \text{otherwise,}
\end{array} \right. \]
where η is the unique residue (mod M), 0 < η < M - 1, such that \( \gamma^{-\eta} (\gamma^\beta - \gamma^r) = \gamma^r \) for some \( r \). That is, \( \gamma^\eta \) and \( \gamma^\beta - \gamma^r \) are in the same coset in \( Z^*_M \) of the group \( C_N \) generated by \( \gamma = \gamma^\eta \).

**Proof:** By definition of \( Y_{\alpha}(r), y_\alpha \) and \( y_\mu \),

\[
Y_{\alpha}(r) = \sum_{k=0}^{N-1} y_\alpha(k + r) y_\mu(k) \tag{1}
\]

\[
= \frac{1}{N} \sum_{k=0}^{N-1} \omega^\alpha y_\mu(k) y^{r+k} \tag{2}
\]

\[
= \frac{1}{N} \sum_{k=0}^{N-1} \omega^\alpha \omega^\gamma y^{r+k} \tag{3}
\]

where \( \alpha = \gamma^\beta - \gamma^r \). The exponents in the sum run through the set \( \alpha C_N \). If \( \alpha \equiv 0 \pmod{p} \), then \( \alpha C_N = \gamma^\eta C_N \) for a unique \( \eta \) satisfying \( 0 < \eta < M - 1 \). Therefore

\[
Y_{\alpha}(r) = \frac{1}{N} \sum_{k=0}^{N-1} \omega^\alpha y_\mu(k) \tag{4}
\]

\[
= \frac{1}{N} \sum_{k=0}^{N-1} \omega^\gamma y^{r+k} \tag{5}
\]

\[
= \omega^\gamma \sum_{k=0}^{N-1} y_\mu(k) \tag{6}
\]

whenever \( \alpha \) is in \( Z^*_M \). This leaves only the case \( \alpha \equiv 0 \pmod{p} \). Here \( \gamma^\beta \equiv y_\mu \) and \( \gamma^r = y_\mu^{-1} \). Since \( y^0, y^1, \ldots, y^{M-1} \) are distinct coset representatives for \( C_N \), it follows that \( \mu = \lambda \eta \) and \( \beta = \eta \). Thus, if \( \alpha \equiv 0 \pmod{p} \), then the correlation in question is a peak \( Y_{\alpha}(0) \). This proves Lemma 2.

**Example 3:** The set \( D = \{1,2,4\} \) is a \((7,3,1)\) cyclic difference set in \( Z_7 \):

- \( 1 = 2 - 1 \), \( 4 = 1 - 4 \), \( 2 = 4 - 2 \), \( 5 = 2 - 4 \), \( 3 = 4 - 1 \), \( 6 = 1 - 2 \).

**Example 4:** The set \( D = \{0,1,3,9\} \) is a \((13,4,1)\) cyclic difference set in \( Z_{13} \).

The fundamental theory of cyclic difference sets is presented in [8] and [9]. An elementary counting argument shows that a necessary condition for the existence of a cyclic \((V,K,\Lambda)\) difference set is that

\[
K^2 - K = \Lambda(V - 1). \tag{7}
\]

Further necessary conditions on the parameters, \( V, K, \) and \( \Lambda \) can be proved by deeper algebraic and number theoretic techniques [8], [9].

Of primary interest here are \((p,N,\Lambda)\) cyclic difference sets \( D \) with \( p = MN + 1 \) a prime, and \( D = C_N \), the multiplicative group of nonzero \( M \)th powers in \( Z^*_p \). The \((7,3,1)\) difference set \((1,2,4)\) of Example 3 is \( C_2 \), the set of nonzero quadratic residues (second powers) in \( Z^*_7 \). For the associated pair of \((2,3)\) power residue sequences:

\[
s_0 = -1 - \sqrt{3} / 6, \tag{8}
\]

\[
s_1 = (1 - \sqrt{3}) / 6, \tag{9}
\]

\[
max(\|s_2\|) = \|s_0\| = \|s_1\| = \sqrt{2} / 3. \tag{10}
\]

The set \((0,1,3,9)\) of Example 4 is \( C_2 \) augmented by \( 0 \). For \( \gamma = 2 \) in \( Z_{13} \), the relevant parameters for the \((4,3)\) power residue sequences are

\[
s_0 = s^2_0 = 0.217 + 0.174j, \tag{11}
\]

\[
s_1 = s^2_0 = -0.384 + 0.574j, \tag{12}
\]

\[
|s_0| = |s_1| = 0.278 = ((5 - \sqrt{13}) / 18)^{1/2}, \tag{13}
\]

\[
max(\|s_2\|) - |s_0| - |s_1| = 0.691 = ((5 + \sqrt{13}) / 18)^{1/2}. \tag{14}
\]

The magnitudes of \( s_0, 0 < \lambda < 3 \), are not all equal because \( C_2 \) is not a cyclic difference set in \( Z_{13} \).

Suppose \( C_2 \) is a cyclic \((p,N,\Lambda)\) difference set in \( Z_p \), \( p = MN + 1 \). The \( N^2 \) exponents in (6) include zero exactly \( N \) times and each nonzero element of \( Z_p \) exactly \( \Lambda \) times. Thus (6) becomes

\[
|s_\lambda|^2 = N^{-2} \left( N + \Lambda \sum_{k=1}^{p-1} \theta^k \right) \tag{15}
\]

\[
= N^{-2} (N - \Lambda), \tag{16}
\]

since \( \theta \) is a complex (primitive) \( p \)th root of one. Substituting \( (p,N,\Lambda) \) for \((V,K,\Lambda)\) in (7) yields

\[
N^2 - N = \Lambda(N-1) = MN \tag{17}
\]

and

\[
\Lambda = (N-1) / M. \tag{18}
\]

From (8) and (9) it follows that

\[
|s_\lambda|^2 = N^{-1/2} (1 - 1 / M + 1 / MN)^{1/2}. \tag{19}
\]

This proves the following theorem.

**Theorem 3:** Suppose \( p = MN + 1 \) is prime and the set \( C_N \) of nonzero \( M \)th powers forms a cyclic \((p,N,\Lambda)\) difference set in the additive group \( Z_p \). Then the set \( \mathcal{D}_{M,N} \) of \((M,N)\) power residue sequences contains \( M \) distinct sequences \( y_\lambda \) of period \( N \) for which

\[
Y_{\lambda}(r) = \begin{cases} 1, & \text{if } \lambda = \mu \text{ and } \tau = 0 \text{,} \\ 1 - \frac{1}{M} + \frac{1}{MN}^{1/2}, & \text{otherwise.} \end{cases} \tag{20}
\]

The only known infinite class of pairs \((M,N)\) to which Theorem 3 applies is

\[
\mathcal{D} = \{(2,N) : N \text{ is odd, } 2N + 1 \text{ is prime}\}. \tag{21}
\]

Each member of \( \mathcal{D} \) gives a pair \( \mathcal{D}_{2,N} \) of power residue sequences of period \( N \) satisfying

\[
max(\|s_2\|) = N^{1/2} (1 + 1 / 2N)^{1/2} \approx (2N)^{-1/2}. \tag{22}
\]
The first nontrivial case arises from the $(7, 3, 1)$ cyclic difference of Example 3:

\[ y_0 = 3^{-1/2}(\omega_7 + \omega_7^2 + \omega_7^3), \]
\[ y_1 = 3^{-1/2}(\omega_7^3 + \omega_7^4 + \omega_7^5). \]

The difference sets associated with $\mathcal{H}$ are the Paley–Hadamard quadratic residue sets in the finite fields $\mathbb{Z}_p$, $p \equiv 3 \pmod{4}$. The other known power residue difference sets to which Theorem 3 applies are for $M = 4$ or $8$. If $p = 4^m + 1$, $n$ odd, then $\mathcal{E}_n$ is a cyclic set in $\mathbb{Z}_p^*, N = n^2$. Each of these sets yields a family of four sequences of period $N$. The appropriate values of $N$ less than 10,000 are $3^2$, $5^2$, $7^2$, $11^2$, $13^2$, $23^2$, $31^2$, $41^2$, $43^2$, $59^2$, $61^2$, $67^2$, $73^2$, $75^2$, and $85^2$. The only known cases with $M = 8$ are for $p = 8n^2 + 1 = 64m^2 + 9$, $n$ and $m$ odd. The first two such primes are 73 and 140 411 704 393 18, $p = 1241$.

A comparison of (1) and (10) shows that $\max(\mathcal{A}_{4,M,N})$ is nearly minimal whenever $\mathcal{C}_N$ is a difference set; in particular

\[ \max(\mathcal{A}_{4,M,N}) \leq \left[ \frac{1}{MN(M - 1)} \right]^{1/2} B(M, N). \]

It is possible for $\max(\mathcal{A}_{4,M,N})$ to be less than $N^{-1/2}$ when $\mathcal{C}_N$ is not a different set. When $p = 1 \pmod{4}$, $\mathcal{C}_N$ is not a difference set for $N = (p - 1)/2$. In this case

\[ s_0 = \frac{(-1 + \sqrt{p})}{(p - 1)}, \]
\[ s_1 = \frac{(-1 - \sqrt{p})}{(p - 1)}, \]
\[ \max(\mathcal{A}_{4,M,N}) = |s_1| = \frac{(1 + \sqrt{p})}{(p - 1)}, \]

\[ \left( \frac{2}{p} \right) = N^{-1/2}, \]

whenever $p > 13$, $p \equiv 1 \pmod{4}$. Other examples with $\mathcal{C}_N$ not a different set and $M > 2$ are $\max(\mathcal{A}_{4,27}) = 0.1878$, $\max(\mathcal{A}_{4,69}) = 0.1201$, $\max(\mathcal{A}_{4,87}) = 0.0994$, $\max(\mathcal{A}_{4,93}) = 0.1016$, $\max(\mathcal{A}_{4,127}) = 0.0814$.

V. SUMMARY

Three types of families of complex periodic sequences have been discussed which possess desirable correlation properties: quadric phase, cubic phase, and power residue. In each normalized sequence of period $N$ all elements have magnitude $N^{-1/2}$.

Quadric and cubic phase sequences nearly meet the Welch bound (1). For every odd number $N$, there is a family of $p - 1$ quadric phase sequences which has correlation maximum equal to $N^{-1/2}$, where $p$ is the smallest prime divisor of $N$. Furthermore the autocorrelation sidelobes of each quadric phase sequence are all zero. Cubic phase sequences have nonzero autocorrelation sidelobes and meet the bound $N^{-1/2}$ only when $N$ is prime.

Families of $M$ power residue sequences, each of period $N$, have been constructed for $MN + 1 = p$, a prime number. These sequences are derived from the multiplicative group $\mathcal{C}_N$ of nonzero $M$th powers in the finite field $\mathbb{Z}_p$. When $\mathcal{C}_N$ is a cyclic difference set in the additive group $\mathbb{Z}_p^*$, the resulting power residue sequences nearly meet the Welch bound. For every prime $p = 3 \pmod{4}$ the group $\mathcal{C}_p$ is a Paley–Hadamard difference set giving rise to a pair of sequences of period $N$ with correlation magnitudes slightly exceeding $(2N^{-1/2})$, $N = (p - 1)/2$. For very large $p \equiv 1 \pmod{4}$, the analogous pair of sequences of period $N = (p - 1)/2$ also has correlation magnitudes near $(2N^{-1/2})$.

Attention has been focused here on meeting the Welch bound for small (i.e., $M < N$) families of periodic sequences. Generalizations of the techniques employed here will produce additional interesting sequence families. Other power residue sequences for which $\mathcal{C}_N$ is not a difference set possess correlation magnitudes near $N^{-1/2}$. Quadric and cubic phase sequences are defined by certain second and third degree phase polynomials, respectively. More general phase polynomials would yield larger families of sequences. For example, the $p^2$ quartics $k^2 + \lambda x^2 + \mu x$, $0 < \lambda, \mu < p - 1$, define $p^2$ cyclically distinct sequences of period $p$. Computer tests indicate that for $p = 2 \pmod{3}$, these quartic families have correlation magnitudes less than $2p^{-1/2}$.

ACKNOWLEDGMENT

The author is grateful to Bruce McClung for assistance with the computer tests on quartic phase sequences mentioned in Section V. The helpful suggestions of two anonymous referees are also appreciated.

NOTE ADDED IN PROOF

Recent results of Sarwate [10] appeared after submission of this correspondence for publication. Theorem 1 above is essentially Theorem 3 of [10]. For odd $N$ the Frank–Zadoff–Chu sequence $\mu(2N)$ of [10] differs from the quartic phase sequence $\phi_N$ by only the normalizing scalar $N^{-1/2}$.

REFERENCES


BURST-ERROR CORRECTING CONVOLUTIONAL CODES WITH SHORT CONSTRAINT LENGTH

WILLIAM E. RODGERS, MEMBER, IEEE, AND ROBERT B. LACKEY

Abstract—A new class of B1 codes which have an information rate of $(b-1)/b$ for $b = 2, 3, 4, \ldots$, is presented. These codes correct error bursts up to $b$ bits long when followed by a guard space of $3b^2 - 2b - 1$ bits. It is assumed that a hard decision is made on the first sub-block of $b$ bits after one constraint length of the code is received and then feedback is used to modify the syndrome bits. One simplified decoding scheme is described which uses simple logic for error correction. A detailed example is pre-