



Fig. 4. Evaluation of the lower bound for $M=5$ and $P_e=0.05$. Dashed line is $\underline{\text{co}}(R_z^1, R_z^5)(d)$.

Upper Bound: $R^*(d) \leq \underline{\text{co}}(R_z^1, R_z^M)(d)$.

IV. EVALUATION OF THE UPPER AND LOWER BOUND

The importance of the upper and lower bound lies in the fact that they can be shown to agree for a large range of P_e and M . $R_z^2(d), \dots, R_z^{M-1}(d)$ were evaluated for $M=3, 4, 5, \dots, 10$ and $M=100$ with $P_e=0.005, 0.05$, and 0.5 using a computer program to find the minimum of the convex function in (20) over the convex set \mathcal{d}_j . For these values of M and P_e , it was found that $\underline{\text{co}}(R_z^1, R_z^2, \dots, R_z^M)(d) = \underline{\text{co}}(R_z^1, R_z^M)(d)$ so that the upper and lower bounds agree and $R^*(d) = \underline{\text{co}}(R_z^1, R_z^M)(d)$. As an example, $R_z^1(d), R_z^2(d), \dots, R_z^5(d)$ are shown in Fig. 4 for $M=5$ and $P_e=0.05$. The dashed line is $\underline{\text{co}}(R_z^1, R_z^5)(d)$ which can be seen to equal $\underline{\text{co}}(R_z^1, R_z^2, \dots, R_z^5)(d)$. We conjecture that $R^*(d) = \underline{\text{co}}(R_z^1, R_z^M)(d)$ for any $M \geq 2$ and P_e satisfying $0 < P_e \leq 1/2$.

When $R^*(d) = \underline{\text{co}}(R_z^1, R_z^M)(d)$, the optimum coding-decoding procedure is to have the decoder ignore side information and use only source information for low distortion; to have the decoder ignore source information and use only side information for distortion P_e ; and to time-share the two schemes for intermediate values of distortion. It is an interesting open problem to characterize the class of correlated sources for which the optimum performance is obtained by time-sharing strictly source information with strictly side information. In general, there exist correlated sources for which the optimum coding-decoding scheme is not a time-sharing scheme; for example, this is true when the source has $p(x|y)=1$ for some x, y .

REFERENCES

- [1] A. D. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 1-10, Jan. 1976.
- [2] K. M. Mackenthun, Jr., "Noiseless coding of error detection information," submitted to *IEEE Trans. Inform. Theory*.

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

$$B(M, N) \triangleq \left(\frac{M-1}{MN-1} \right)^{1/2}. \quad (1)$$

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 ϕ -function [3]. For N a prime, their sequences have autocorrelation sidelobes of magnitude $1/(N-1)$ and cross correlations of magnitude zero and $N^{1/2}/(N-1)$. For composite N the autocorrelation sidelobes may reach $(\phi(d))^{-1}$ 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 $2^{1/2}N^{-1/2}$ for $m \equiv 2 \pmod{4}$ 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 , $p=MN+1$. 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].

Manuscript received March 20, 1979; revised September 17, 1979.

The author is with the Naval Weapons Center, Code 3133, China Lake, CA 93555.

II. BASIC DEFINITIONS

Let \mathcal{K} denote a family $\{h_\lambda : 1 \leq \lambda \leq M\}$ of complex sequences of period N . The k th element of h_λ is $h_\lambda(k)$, and one period of h_λ is $(h_\lambda(0), h_\lambda(1), \dots, h_\lambda(N-1))$. 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 τ th correlation coefficient between h_λ and h_μ is given by

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

where $h_\mu(k)^*$ is the complex conjugate of $h_\mu(k)$. The arguments $k+\tau$ and k in h_λ and h_μ can be reduced modulo N to one of the integers $0, 1, \dots, N-1$. 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 $H_{\lambda\lambda}(0)$ are one. The measure of correlation magnitude of primary interest is

$$\max(\mathcal{C}) = \max\{|H_{\lambda\mu}(\tau)| : \lambda \neq \mu \text{ or } \tau \neq 0\}.$$

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

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

Every h_λ will be a sequence of roots of unity scaled by $N^{-1/2}$,

$$h_\lambda(k) = N^{-1/2} \omega_n^{f(\lambda, k)},$$

where $\omega_n = \exp(2\pi j/n)$ and f is a function from $Z_M \times Z_N$ into Z_n . For the sequences of Section III $n = N$, while for those of Section IV $n = MN+1 = p$.

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

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

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

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

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

III. QUADRIC AND CUBIC PHASE SEQUENCES

For N an odd integer greater than two, the λ th quadric phase sequence a_λ is defined by

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

The λ th cubic phase sequence b_λ is defined by

$$b_\lambda(k) \triangleq N^{-1/2} \omega_N^{\lambda k^3 + \lambda k}.$$

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

Example 1: For $N=5$

$$a_1 = 5^{-1/2}(1, \omega_5, \omega_5^4, \omega_5^4, \omega_5),$$

$$a_2 = 5^{-1/2}(1, \omega_5^2, \omega_5^3, \omega_5^3, \omega_5^2),$$

$$a_3 = 5^{-1/2}(1, \omega_5^3, \omega_5^2, \omega_5^2, \omega_5^3),$$

$$a_4 = 5^{-1/2}(1, \omega_5^4, \omega_5, \omega_5, \omega_5^4),$$

$$a_5 = 5^{-1/2}(1, 1, 1, 1, 1),$$

$$b_1 = 5^{-1/2}(1, \omega_5^2, 1, 1, \omega_5^3),$$

$$b_2 = 5^{-1/2}(1, \omega_5^3, \omega_5^2, \omega_5^3, \omega_5^2),$$

$$b_3 = 5^{-1/2}(1, \omega_5^4, \omega_5^4, \omega_5, \omega_5),$$

$$b_4 = 5^{-1/2}(1, 1, \omega_5, \omega_5^4, 1),$$

$$b_5 = 5^{-1/2}(1, \omega_5, \omega_5^3, \omega_5^2, \omega_5^4).$$

$\max(\mathcal{Q}_5) = \max(\mathcal{B}_5) = 5^{-1/2}$ where

$$\mathcal{Q}_5 = \{a_1, a_2, a_3, a_4\},$$

$$\mathcal{B}_5 = \{b_1, b_2, b_3, b_4, b_5\}.$$

The sequence a_5 is not used because of its constant autocorrelation; indeed the period of a_5 is one, not five. \mathcal{Q}_5 has all sidelobes $A_{\lambda\lambda}(\tau), \tau \neq 0$, equal to zero, and all cross correlation magnitudes $|A_{\lambda\mu}(\tau)|, \lambda \neq \mu$, equal to $5^{-1/2}$. Letting $B_{\lambda\mu}$ denote the correlation between b_λ and b_μ , the following holds

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

The family \mathcal{Q}_5 generalizes to all odd integers, while \mathcal{B}_5 generalizes to all primes ≥ 5 , yielding sequence families which meet the bound $N^{-1/2}$ for correlation magnitudes. For odd $N \geq 3$, define \mathcal{Q}_N by

$$\mathcal{Q}_N \triangleq \{a_1, a_2, \dots, a_{p-1}\},$$

where p is the smallest prime divisor of N .

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

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

For p an odd prime let

$$\mathcal{B}_p \triangleq \{b_1, b_2, \dots, b_p\}.$$

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

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

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

$$\begin{aligned} A_{\lambda\mu}(\tau) &= \sum_{k=0}^{N-1} a_\lambda(k+\tau) a_\mu(k)^* \\ &= \frac{1}{N} \sum_{k=0}^{N-1} \omega_N^{\lambda(k+\tau)^2} \omega_N^{-\mu k^2} \\ &= \frac{1}{N} \omega_N^{\lambda \tau^2} \sum_{k=0}^{N-1} \omega_N^{(\lambda-\mu)k^2 + 2\lambda\tau k}. \end{aligned}$$

Similarly

$$B_{\lambda\mu}(\tau) = \frac{1}{N} \omega_N^{\tau^3 + \lambda\tau} \sum_{k=0}^{N-1} \omega_N^{3\tau k^2 + (\lambda-\mu+3\tau^2)k}.$$

It follows that

$$|A_{\lambda\mu}(\tau)| = \frac{1}{N} |Q_N(\lambda - \mu, 2\lambda\tau)|, \quad (2)$$

$$|B_{\lambda\mu}(\tau)| = \frac{1}{N} |Q_N(3\tau, \lambda - \mu + 3\tau^2)|, \quad (3)$$

where

$$Q_N(\eta, \sigma) \triangleq \sum_{k=0}^{N-1} \omega_N^{\eta k^2 + \sigma k}. \quad (4)$$

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 η and N . Then

$$|Q_N(\eta, \sigma)|^2 = \begin{cases} N\delta, & \text{if } \delta \text{ divides } \sigma \\ 0, & \text{if } \delta \text{ does not divide } \sigma. \end{cases} \quad (5)$$

Proof: By definition

$$\begin{aligned} |Q_N(\eta, \sigma)|^2 &= Q_N(\eta, \sigma) (Q_N(\eta, \sigma))^* \\ &= \left(\sum_{k=0}^{N-1} \omega_N^{\eta k^2 + \sigma k} \right) \left(\sum_{r=0}^{N-1} \omega_N^{-\eta r^2 - \sigma r} \right) \\ &= \sum_{k,r} \omega_N^{\eta(k^2 - r^2) + \sigma(k - r)}, \end{aligned}$$

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

$$\begin{aligned} |Q_N(\eta, \sigma)|^2 &= \sum_{k,r} \omega_N^{(k-r)(\eta(k+r) + \sigma)} \\ &= \sum_{k,s} \omega_N^{s(\eta(2k-s) + \sigma)} \\ &= \sum_{s=0}^{N-1} \omega_N^{-\eta s^2 - \sigma s} \left(\sum_{k=0}^{N-1} \omega_N^{2\eta s k} \right). \end{aligned}$$

Since ω_N is a primitive N th root of one,

$$\sum_{k=0}^{N-1} \omega_N^{2\eta s k} = \begin{cases} N, & \text{if } 2\eta s \equiv 0 \pmod{N} \\ 0, & \text{otherwise.} \end{cases}$$

Therefore

$$|Q_N(\eta, \sigma)|^2 = N \sum_s \omega_N^{-\eta s^2 - \sigma s},$$

with the summation over those values of s for which $2\eta s \equiv 0 \pmod{N}$, and $0 \leq s \leq N-1$. At this point we use the fact that N is odd. Since $\gcd(2, N) = 1$, $\eta s \equiv 0 \pmod{N}$ whenever $2\eta s \equiv 0 \pmod{N}$. Thus

$$\omega_N^{-\eta s^2 - \sigma s} = \omega_N^{-\sigma s}, \quad \text{if } 2\eta s \equiv 0 \pmod{N}.$$

It follows that

$$|Q_N(\eta, \sigma)|^2 = N \sum_s \omega_N^{-\sigma s},$$

summing over the values of s for which $\eta s \equiv 0 \pmod{N}$, and $0 \leq s \leq N-1$. The set of s in Z_N for which $\eta s \equiv 0 \pmod{N}$ is just $\{0, m, 2m, \dots, (\delta-1)m\}$ where $\delta = \gcd(\eta, N)$ and $m = N/\delta$. Therefore

$$\begin{aligned} |Q_N(\eta, \sigma)|^2 &= N [1 + \omega_N^{-\sigma m} + \omega_N^{-2\sigma m} + \dots + \omega_N^{-(\delta-1)\sigma m}] \\ &= \begin{cases} N\delta, & \text{if } \sigma m \equiv 0 \pmod{N} \\ 0, & \text{if } \sigma m \not\equiv 0 \pmod{N} \end{cases} \end{aligned}$$

Since $\sigma m \equiv 0 \pmod{N}$ if and only if δ divides σ , the lemma is proved.

Proofs of Theorems 1 and 2: For a_λ and a_μ in \mathcal{C}_N , λ and μ 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 $\tau \neq 0$, 3τ is relatively prime to p when $p \geq 5$. Therefore $|B_{\lambda\mu}(\tau)|^2 = N$ whenever $\tau \neq 0$. It also follows from (3) and (5) that $B_{\lambda\mu}(0) = 0$ whenever $\lambda \neq \mu$. This proves Theorem 2.

The possibilities of enlarging the family \mathcal{C}_N or of using the cubic phase sequence b_1, b_2, \dots for composite N deserve some discussion. As before p denotes the smallest prime divisor of N . If $\gcd(\lambda, N) = d$, then $|A_{\lambda\lambda}(m)| = 1$, where $m = N/d$. Therefore λ should be relatively prime to N for every a_λ in \mathcal{C}_N . If \mathcal{C}_N contains p distinct sequences a_λ , each λ relatively prime to N , then there must be two sequences a_λ, a_μ in \mathcal{C}_N with $\lambda \equiv \mu \pmod{p}$. In this case $|A_{\lambda\mu}(d)| = (d/N)^{1/2}$, where $d = \gcd(\lambda - \mu, N) \geq p$. Therefore, in order for $\max(\mathcal{C}_N)$ not to exceed $N^{-1/2}$, \mathcal{C}_N must contain at most $p-1$ sequences a_λ , with all λ and $\lambda - \mu$ relatively prime to N . Of course there will be suitable families of $p-1$ sequences other than $\{a_1, a_2, \dots, a_{p-1}\}$. For example $\max(\mathcal{C}) = 35^{-1/2}$ when $\mathcal{C} = \{a_4, a_8, a_{12}, a_{16}\}$, $N = 35$.

For any cubic phase sequence b_λ , $|B_{\lambda\lambda}(p)| = (p/N)^{1/2}$ when N is divisible by p but not by three. Thus the autocorrelations exceed $N^{-1/2}$ for all b_λ . This is similar to the behavior of the character sequences of [2].

IV. POWER RESIDUE SEQUENCES

Let γ denote a primitive root in the finite field Z_p where $p = MN + 1$. Let $\beta = \gamma^M$, so that β and γ are primitive N th and $(p-1)$ th roots of unity in Z_p respectively. The N distinct powers of $\beta \pmod{p}$ form a subgroup of Z_p^* , the multiplicative group of nonzero elements of Z_p . Denoting this subgroup by \mathcal{C}_N , the set Z_p^* is partitioned by the M cosets of \mathcal{C}_N . Moreover the M elements $1, \gamma, \gamma^2, \dots, \gamma^{M-1}$ are coset representatives:

$$Z_p^* = \mathcal{C}_N \cup \gamma \mathcal{C}_N \cup \gamma^2 \mathcal{C}_N \cup \dots \cup \gamma^{M-1} \mathcal{C}_N.$$

The λ th (M, N) power residue sequence y_λ is defined by

$$y_\lambda(k) \triangleq N^{-1/2} \omega_p^{\gamma^\lambda \beta^k}.$$

Example 2: For $p = 19$, $M = 3$, $N = 6$, and $\gamma = 2$, one obtains three distinct $(3, 6)$ power residue sequences:

$$\begin{aligned} y_0 &= 6^{-1/2} (\omega_{19}^8, \omega_{19}^7, \omega_{19}^{18}, \omega_{19}^{11}, \omega_{19}^{12}) \\ y_1 &= 6^{-1/2} (\omega_{19}^2, \omega_{19}^{16}, \omega_{19}^{14}, \omega_{19}^{17}, \omega_{19}^3, \omega_{19}^5) \\ y_2 &= 6^{-1/2} (\omega_{19}^4, \omega_{19}^{13}, \omega_{19}^9, \omega_{19}^{15}, \omega_{19}^6, \omega_{19}^{10}). \end{aligned}$$

For $\mathcal{C}_{3,6} = \{y_0, y_1, y_2\}$, $\max(\mathcal{C}_{3,6}) = 0.418$. Indeed all 51 nonpeak correlations $Y_{\lambda\mu}(\tau)$ assume one of three values

$$s_\lambda = 6^{-1/2} \sum_{k=0}^5 y_\lambda(k), \quad 0 \leq \lambda \leq 2,$$

$$s_0 = -0.204, \quad s_1 = 0.418, \quad s_2 = -0.381.$$

In general let $\mathcal{C}_{M,N} = \{y_0, y_1, \dots, y_{M-1}\}$ and

$$Y_{\lambda\mu}(\tau) \triangleq \sum_{k=0}^{N-1} y_\lambda(k + \tau) y_\mu(k)^*,$$

for $0 \leq \lambda, \mu \leq M-1$ and $0 \leq \tau \leq N-1$, where $p = MN + 1$ is prime.

Lemma 2: The nonpeak correlations for the power residue family $\mathcal{C}_{M,N}$ all assume one of the M values s_0, s_1, \dots, s_{M-1} , where

$$s_\lambda \triangleq N^{-1/2} \sum_{k=0}^{N-1} y_\lambda(k).$$

In particular

$$Y_{\lambda\mu}(\tau) = \begin{cases} 1, & \text{if } \lambda = \mu \text{ and } \tau = 0 \\ s_\eta, & \text{otherwise,} \end{cases}$$

where η is the unique residue (mod M), $0 \leq \eta \leq M-1$, such that $\gamma^{-\eta}(\gamma^\lambda \beta^\tau - \gamma^\mu) = \beta^r$ for some r . That is, γ^η and $\gamma^\lambda \beta^\tau - \gamma^\mu$ are in the same coset in $Z_p^\#$ of the group \mathcal{C}_N generated by $\beta = \gamma^M$.

Proof: By definition of $Y_{\lambda\mu}(\tau)$, y_λ and y_μ ,

$$\begin{aligned} Y_{\lambda\mu}(\tau) &= \sum_{k=0}^{N-1} y_\lambda(k+\tau) y_\mu(k)^* \\ &= \frac{1}{N} \sum_{k=0}^{N-1} \omega_p^{\gamma^\lambda \beta^{k+\tau}} \omega_p^{-\gamma^\mu \beta^k} \\ &= \frac{1}{N} \sum_{k=0}^{N-1} \omega_p^{\alpha \beta^k}, \end{aligned}$$

where $\alpha = \gamma^\lambda \beta^\tau - \gamma^\mu$. The exponents in the sum run through the set $\alpha \mathcal{C}_N$. If $\alpha \not\equiv 0 \pmod{p}$, then $\alpha \mathcal{C}_N = \gamma^\eta \mathcal{C}_N$ for a unique η satisfying $0 \leq \eta \leq M-1$. Therefore

$$\begin{aligned} Y_{\lambda\mu}(\tau) &= \frac{1}{N} \sum_{k=0}^{N-1} \omega_p^{\gamma^\eta \beta^k} \\ &= N^{-1/2} \sum_{k=0}^{N-1} y_\eta(k) \\ &= s_\eta, \end{aligned}$$

whenever α is in $Z_p^\#$. This leaves only the case $\alpha \equiv 0 \pmod{p}$. Here $\gamma^\lambda \beta^\tau \equiv \gamma^\mu$ and $\beta^\tau \equiv \gamma^{\mu-\lambda}$. Since $\gamma^0, \gamma^1, \dots, \gamma^{M-1}$ are distinct coset representatives for \mathcal{C}_N , it follows that $\mu = \lambda$, and $\beta^\tau \equiv 1$. Thus, if $\alpha \equiv 0 \pmod{p}$, then the correlation in question is a peak $Y_{\lambda\lambda}(0)$. This proves Lemma 2.

$\max(\mathcal{Q}_{M,N})$ is just the largest of the M numbers $|s_0|, |s_1|, \dots, |s_{M-1}|$. From the definitions of s_λ and $y_\lambda(k)$ we have

$$\begin{aligned} |s_\lambda|^2 &= \frac{1}{N} \left(\sum_{k=0}^{N-1} y_\lambda(k) \right) \left(\sum_{r=0}^{N-1} y_\lambda(r) \right)^* \\ &= \frac{1}{N} \sum_{k,r} y_\lambda(k) (y_\lambda(r))^* \\ &= N^{-2} \sum_{k,r} \omega_p^{\gamma^\lambda \beta^k} \omega_p^{-\gamma^\lambda \beta^r} \\ &= N^{-2} \sum_{k,r} \theta_\lambda^{\beta^k - \beta^r}, \end{aligned}$$

where $\theta_\lambda = \exp(2\pi j \gamma^\lambda / p)$, and the index pair (k, r) runs through the N^2 pairs in $Z_N \times Z_N$. Equivalently

$$|s_\lambda|^2 = N^{-2} \sum \{ \theta_\lambda^{\mu-\xi} : (\mu, \xi) \in \mathcal{C}_N \times \mathcal{C}_N \}; \quad (6)$$

that is the exponent $\beta^k - \beta^r$ runs through the N^2 differences $\mu - \xi$, $\mu \in \mathcal{C}_N$, $\xi \in \mathcal{C}_N$, as (k, r) runs through $Z_N \times Z_N$. In the exceptional cases where the $N^2 - N$ nonzero differences are uniformly distributed over the $p-1$ residue in $Z_p^\#$, all s_λ have the same magnitude, and $\max(\mathcal{Q}_{M,N})$ is nearly optimal. This occurs when \mathcal{C}_N is a difference set in the additive group Z_p .

A cyclic (V, K, Λ) difference set is a subset \mathcal{D} of the cyclic group Z_V satisfying the following: \mathcal{D} contains K elements; and for every nonzero z in Z_V , $z = \mu - \xi$ for exactly Λ distinct pairs (μ, ξ) in $\mathcal{D} \times \mathcal{D}$.

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

$$\begin{array}{ll} 1=2-1, & 4=1-4, \\ 2=4-2, & 5=2-4, \\ 3=4-1, & 6=1-2. \end{array}$$

Example 4: The set $\mathcal{D} = \{0, 1, 3, 9\}$ 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, Λ) dif-

ference set is that

$$K^2 - K = \Lambda(V-1). \quad (7)$$

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

Of primary interest here are (p, N, Λ) cyclic difference sets \mathcal{D} with $p = MN + 1$ a prime, and $\mathcal{D} = \mathcal{C}_N$, the multiplicative group of nonzero M th powers in $Z_p^\#$. The $(7, 3, 1)$ difference set $\{1, 2, 4\}$ of Example 3 is \mathcal{C}_3 , the set of nonzero quadratic residues (second powers) in $Z_7^\#$. For the associated pair of $(2, 3)$ power residue sequences:

$$s_0 = (-1 + j\sqrt{7})/6,$$

$$s_1 = (-1 - j\sqrt{7})/6,$$

$$\max(\mathcal{Q}_{2,3}) = |s_0| = |s_1| = \sqrt{2}/3.$$

The set $\{0, 1, 3, 9\}$ of Example 4 is \mathcal{C}_3 augmented by $\{0\}$. For $\gamma = 2$ in Z_{13} , the relevant parameters for the $(4, 3)$ power residue sequences are

$$s_0 = s_2^* = 0.217 + 0.174j,$$

$$s_1 = s_3^* = -0.384 + 0.575j,$$

$$|s_0| = |s_2| = 0.278 = ((5 - \sqrt{13})/18)^{1/2},$$

$$\max(\mathcal{Q}_{4,3}) = |s_1| = |s_3| = 0.691 = ((5 + \sqrt{13})/18)^{1/2}.$$

The magnitudes of s_λ , $0 \leq \lambda \leq 3$, are not all equal because \mathcal{C}_3 is not a cyclic difference set in Z_{13} .

Suppose \mathcal{C}_N is a cyclic (p, N, Λ) 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 Λ times. Thus (6) becomes

$$\begin{aligned} |s_\lambda|^2 &= N^{-2} \left(N + \Lambda \sum_{k=1}^{p-1} \theta_\lambda^k \right) \\ &= N^{-2} (N - \Lambda), \end{aligned} \quad (8)$$

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

$$N^2 - N = \Lambda(p-1) = \Lambda MN,$$

and

$$\Lambda = (N-1)/M. \quad (9)$$

From (8) and (9) it follows that

$$|s_\lambda| = N^{-1/2} \left(1 - \frac{1}{M} + \frac{1}{MN} \right)^{1/2}$$

This proves the following theorem.

Theorem 3: Suppose $p = MN + 1$ is prime and the set \mathcal{C}_N of nonzero M th powers forms a cyclic (p, N, Λ) difference set in the additive group Z_p . Then the set $\mathcal{Q}_{M,N}$ of (M, N) power residue sequences contains M distinct sequences y_λ of period N for which

$$|Y_{\lambda\mu}(\tau)| = \begin{cases} 1, & \text{if } \lambda = \mu \text{ and } \tau = 0 \\ N^{-1/2} \left(1 - \frac{1}{M} + \frac{1}{MN} \right)^{1/2}, & \text{otherwise.} \end{cases} \quad (10)$$

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

$$\mathcal{P} = \{(2, N) : N \text{ is odd, } 2N+1 \text{ is prime}\}.$$

Each member of \mathcal{P} gives a pair $\mathcal{Q}_{2,N}$ of power residue sequences of period N satisfying

$$\max(\mathcal{Q}_{2,N}) = N^{-1/2} \left(\frac{1}{2} + \frac{1}{2N} \right)^{1/2} \approx (2N)^{-1/2}.$$

The first nontrivial case arises from the (7,3,1) cyclic difference of Example 3:

$$y_0 = 3^{-1/2}(\omega_7, \omega_7^2, \omega_7^4), \\ y_1 = 3^{-1/2}(\omega_7^3, \omega_7^6, \omega_7^5).$$

The difference sets associated with \mathcal{P} are the Paley-Hadamard quadratic residue sets in the finite fields $Z_p, p \equiv 3 \pmod{4}$.

The other known power residue differences sets to which Theorem 3 applies are for $M=4$ or 8. If $p=4n^2+1, n$ odd, then \mathcal{C}_N is a cyclic set in $Z_p, N=n^2$. Each of these sets yields a family of four sequences of period N . The appropriate values of N less than 10 000 are $3^2, 5^2, 7^2, 13^2, 17^2, 23^2, 27^2, 33^2, 37^2, 45^2, 55^2, 63^2, 65^2, 67^2, 73^2, 75^2$, 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 [8, p. 124].

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

$$\max(\mathcal{Q}_{M,N}) < \left[1 + \frac{1}{MN(M-1)} \right]^{1/2} B(M,N).$$

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

$$s_0 = (-1 + \sqrt{p})/(p-1), \\ s_1 = (-1 - \sqrt{p})/(p-1), \\ \max(\mathcal{Q}_{2,N}) = |s_1| = (1 + \sqrt{p})/(p-1) \\ < \left(\frac{2}{p-1} \right)^{1/2} = N^{-1/2},$$

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

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 Z_p . When \mathcal{C}_N is a cyclic difference set in the additive group Z_p , the resulting power residue sequences nearly meet the Welch bound. For every prime $p \equiv 3 \pmod{4}$ the group \mathcal{C}_N 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., $M \leq N$) families of periodic sequences. Generali-

zations 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 $k^4 + \lambda k^2 + \mu k, 0 \leq \lambda, \mu \leq p-1$, define p^2 cyclically distinct sequences of period p . Computer tests indicate that for $p \equiv 2 \pmod{3}$, 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 $u^{(2N)}$ of [10] differs from the quadric phase sequence a_λ by only the normalizing scalar $N^{1/2}$.

REFERENCES

- [1] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 397-399, May 1974.
- [2] R. A. Scholtz and L. R. Welch, "Group characters: Sequences with good correlation properties," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 537-545, Sept. 1978.
- [3] W. J. LeVeque, *Topics in Number Theory*. Reading, MA: Addison-Wesley, 1956.
- [4] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 619-621, Oct. 1967.
- [5] N. B. Chakrabarti and M. Tomlinson, "Design of sequences with specified autocorrelation and cross correlation," *IEEE Trans. Commun.*, vol. COM-24, pp. 1246-1252, Nov. 1976.
- [6] E. Landau, *Elementary Number Theory*. New York: Chelsea, 1958. (Translated from the German by Jacob E. Goodman.)
- [7] D. C. Chu, "Polyphase codes with good periodic correlation properties," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 531-532, July 1972.
- [8] L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics, No. 182. Berlin, Heidelberg, New York: Springer-Verlag, 1971.
- [9] M. Hall, Jr., *Combinatorial Theory*. Waltham, MA: Blaisdell, 1967.
- [10] D. V. Sarwate, "Bounds on crosscorrelation and autocorrelation of sequences," *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 720-724, Nov. 1979.

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 $b=2,3,4,\dots$ 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-

Manuscript received March 16, 1977; revised August 3, 1979.
W. E. Rodgers was with the Department of Electrical Engineering, Ohio State University, Columbus, OH. He is now with the Aerospace and Missile Systems Group 262/C38, Hughes Aircraft Company, 8433 Fallbrook Ave., Canoga Park, CA 91304.

R. B. Lackey is with the Department of Electrical Engineering, Ohio State University, 2015 Neil Ave., Columbus, OH 43210.