CORRELATION PARAMETERS
FOR PERIODIC SEQUENCES--
PROPERTIES, BOUNDS,
AND EFFICIENT
COMPUTATIONAL METHODS

M.B. PURSLEY
D.V. SARWATE

APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED.

UNIVERSITY OF ILLINOIS - URBANA, ILLINOIS
**Title:** Correlation Parameters for Periodic Sequences - Properties, Bounds, and Efficient Computational Methods

**Authors:** M. B. Pursley and D. V. Sarwate

**Publication Date:** April, 1976

**Pages:** 23

**Abstract:**

The selection of sets of sequences with good correlation properties is an important problem in many areas of communication theory. In this paper we investigate several autocorrelation and cross-correlation parameters such as those which characterize the performance of phase-coded spread-spectrum multiple-access communication systems. Although algorithms have been proposed for selecting sequences for multiple-access applications, the amount of computation required is often prohibitive. We provide new analytical results which permit significant reduction in the amount of computation needed to obtain sequence sets with good correlation properties.
Correlation Parameters for Periodic Sequences --
Properties, Bounds, and Efficient Computational Methods

by M. B. Pursley and D. V. Sarwate*

April 16, 1976

Abstract

The selection of sets of sequences with good correlation properties is an important problem in many areas of communication theory. In this paper we investigate several autocorrelation and cross-correlation parameters such as those which characterize the performance of phase-coded spread-spectrum multiple-access communication systems. Although algorithms have been proposed for selecting sequences for multiple-access applications, the amount of computation required is often prohibitive. We provide new analytical results which permit significant reduction in the amount of computation needed to obtain sequence sets with good correlation properties.

*The authors are with the Coordinated Science Laboratory and the Department of Electrical Engineering, University of Illinois at Urbana-Champaign, Urbana, Illinois 61801. This work is supported in part by the Joint Services Electronics Program (U.S. Army, U.S. Navy, and U.S. Air Force) under Contract DAAB-07-72-C-0259.
I. Introduction

One of the important problems in multiple-access communications is the selection of a set of periodic sequences with small cross-correlation and out-of-phase autocorrelation. A number of investigators have identified important correlation parameters that should be considered in the choice of such a set and algorithms have been proposed for finding sets which are reasonably good with respect to one or more of these parameters. For most systems of interest, the proposed algorithms require an excessive amount of computation and, as a result, are not often used in practice. In this paper we present analytical results on correlation parameters of sequences, and we point out how these results can be used in the selection of sets of sequences for such applications as spread-spectrum multiple-access (SSMA) communications.

In Section II we briefly describe the phase-coded SSMA system which is the main application to which our results are addressed, and we discuss the correlation parameters that are needed in the design and analysis of such a system. The analytical results are stated and proved in Section III and applied to the efficient calculation of correlation parameters in Section IV. In Section IV we also obtain quantitative results on the computation required for such calculations and on the computational saving achieved by applying the ideas of Section III. We also discuss the application of the Fast Fourier Transform algorithm to the calculation of the important correlation parameters.
II. Important Correlation Parameters

In order to provide motivation for the choice of correlation parameters considered in this paper we will describe a typical phase-coded SSMA system. The system has $K$ transmitters which are not time or phase synchronous and it has one correlation receiver for each transmitter. The $K$ signals are to be transmitted over the same radio-frequency (RF) channel using a common center frequency $\omega_c = 2\pi f_c$. Generalizations to unequal center frequencies are possible but are not considered here since the main feature of the system is to allow the $K$ asynchronous signals to share the same RF bandwidth.

The $k^{th}$ user's data signal $b_k(t)$ is a sequence of unit amplitude, positive and negative, rectangular pulses of duration $T$. The $k^{th}$ user is assigned a code waveform $a_k(t)$ which consists of a periodic sequence of unit amplitude, positive and negative rectangular pulses of duration $T_c$. If $a^{(k)}$ is a sequence of elements of $\{+1, -1\}$ then we can represent $a_k(t)$ as

$$a_k(t) = \sum_{j=-\infty}^{\infty} a^{(k)}_j p_{T_c}(t - jT_c)$$

where $p_{T_c}(t) = 1$ for $0 \leq t < T_c$ and $p_{T_c}(t) = 0$ otherwise. For the moment we assume that each sequence $a^{(k)}$ has period $p = T/T_c$ so that there is one code period $a^{(k)}_0, a^{(k)}_1, ..., a^{(k)}_{p-1}$ per data symbol. This assumption is not really necessary and, in fact in Section III we require only $a^{(k)}_j = a^{(k)}_{j+p}$ for all $j \in \mathbb{Z}$ ($\mathbb{Z}$ denotes the set of all integers). This allows us to analyze SSMA systems in which there are multiple code periods per data symbol.
The data signal $b_k(t)$ is modulated onto the phase-coded carrier $c_k(t)$ given by

$$c_k(t) = \sqrt{2P} \sin (\omega_c t + \psi_k + (\pi/2) a_k(t)) = \sqrt{2P} a_k(t) \cos (\omega_c t + \psi_k)$$

which produces the signal

$$s_k(t) = \sqrt{2P} \sin (\omega_c t + \psi_k + (\pi/2) a_k(t) b_k(t)) = \sqrt{2P} a_k(t) b_k(t) \cos (\omega_c t + \psi_k).$$

In the above expressions $\psi_k$ represents the phase of the $k^{th}$ carrier and $P$ represents the common signal power. The results can easily be modified for unequal power levels. The received signal $r(t)$ is given by

$$r(t) = n(t) + \sum_{k=1}^{K} \sqrt{2P} a_k(t - \tau_k) b_k(t - \tau_k) \cos (\omega_c t + \phi_k),$$

where $\phi_k = \psi_k - \omega \tau_k$, and $n(t)$ is the channel noise process which we assume to be a white Gaussian process with two-sided spectral density $N_0/2$. Since we are concerned with relative phase shifts modulo $2\pi$ and relative time delays modulo $T$, there is no loss in generality in assuming $\theta_i = 0$ and $\tau_i = 0$ and considering only $0 \leq \tau_k < T$ and $0 \leq \theta_k < 2\pi$ for $k \neq i$.

If the received signal $r(t)$ is the input to a correlation receiver matched to $s_i(t)$, the output is $Z_i = \int_0^T r(t) a_i(t) \cos \omega_c t \, dt$. In all that follows we assume $\omega_c \gg T^{-1}$ since the frequency response of a realistic hardware implementation of the correlation receiver is such that the double frequency component of $r(t) \cos \omega_c t$ will be negligible under this condition.
The condition $\omega_c \gg T^{-1}$ is always satisfied in a practical SSMA communication system. The data signal $b_k(t)$ can be expressed as

$$b_k(t) = \sum_{\ell=0}^{\infty} b_{k,\ell} P_T(t - \ell T)$$

where $b_{k,\ell} \in \{+1, -1\}$.

At this point there are a number of different system performance parameters that could be considered. The three that we will be concerned with are the maximum interference at the output of the $i^{th}$ correlation receiver due to the presence of the $k^{th}$ signal; the signal-to-noise ratio at the output of the correlation receiver where $b_{k,\ell}, \tau_k$ and $\phi_k$ are assumed to be random variables for $k \neq i$ and the $K - 1$ interfering signals are treated as noise; and the error probability for the $i^{th}$ correlation receiver where we again treat $b_{k,\ell}, \tau_k$, and $\phi_k$ as random variables. The first of these has recently been investigated by Massey and Uhran [1], the second by Pursley [2], and the third by Yao [3].

The key correlation parameters for binary phase-coded SSMA communications can be given in terms of the pairwise aperiodic cross-correlation functions for the binary sequence set $\{a^{(k)}|1 \leq k \leq K\}$. The aperiodic cross-correlation function for two binary sequences $a^{(k)}$ and $a^{(i)}$ of period $p$ is given by

$$c_{k,i}(\ell) = \begin{cases} 
\sum_{j=0}^{p-1-%231} a_{j}^{(k)} a_{j+\ell}^{(i)}, & 0 \leq \ell \leq p-1 \\
\sum_{j=0}^{p-1+%231} a_{j}^{(k)} a_{j+\ell}^{(i)}, & 1-p \leq \ell < 0 
\end{cases}$$

1Throughout the paper the term "binary sequence" will refer to a sequence of elements of $\{+1, -1\}$ unless otherwise noted.
and \( C_{k,i}(p) = C_{k,i}(-p) = 0 \). The aperiodic autocorrelation function for \( a^{(k)} \) is \( C_{k,k}(*) \) which will be denoted by \( C_k(*) \). The usual periodic cross-correlation function is

\[
\theta_{k,i}(\ell) = \sum_{j=0}^{p-1} a^{(k)} \cdot a^{(i)}_{j+\ell}, \ell \in \mathbb{Z}.
\]

Therefore, \( \theta_{k,i}(\ell) = C_{k,i}(\ell) + C_{k,i}(\ell - p) \) for \( 0 \leq \ell < p \). The periodic autocorrelation function \( \theta_{k,k}(\cdot) \) will be denoted by \( \theta_k(\cdot) \).

From the work of Massey and Uhran [1] it is clear that the odd cross-correlation \( \hat{\theta}_{k,i}(\ell) = C_{k,i}(\ell) - C_{k,i}(\ell - p) \) is at least as important as the periodic cross-correlation \( \theta_{k,i}(\ell) \) for the asynchronous phase-coded SSMA system. In addition, Massey and Uhran point out the role of the odd autocorrelation \( \hat{\theta}_i(\ell) = C_i(\ell) - C_i(\ell - p) \) in determining the performance of such systems when multipath distortion is present. They show that the maximum magnitude of the periodic and odd cross-correlation and the maximum magnitude of the out-of-phase periodic and odd autocorrelation are the key parameters needed to determine the maximum interference at the \( i^{th} \) correlation receiver due to the presence of the other \( K-1 \) signals and the multipath signals. They discuss methods for selecting a set of sequences for which these parameters are small and they note that the aperiodic correlation parameters are very sensitive to shifts in the sequences. As a result, application of an algorithm which finds an optimum shift for each of the \( K \) sequences will typically produce significant improvements in the aperiodic correlation parameters. However, algorithms proposed to date, including some which find good but nevertheless suboptimal shifts, require excessive computation for values of \( K \) and \( p \) of interest. In Sections III and IV we discuss more efficient algorithms for this purpose.
Taking an entirely different point of view we can treat the phase shifts, time delays, and data symbols as a collection of mutually independent random variables and compute the signal-to-noise ratio \( \text{SNR}_1 \) defined by

\[
\text{SNR}_1 = \left[ \text{Var}[z_i] \right]^{-\frac{1}{2}} \text{E}[z_i|b_{i,o} = +1]
\]

It has been shown [2] that

\[
\text{E}[z_i|b_{i,o} = +1] = \sqrt{p/2} T
\]

and

\[
\text{Var}[z_i] = \frac{P T^2}{12 p^3} \sum_{k=1}^{K} r_{k,i} + \frac{N T}{4}
\]

where

\[
r_{k,i} = \sum_{\ell=0}^{p-1} \left( C_{k,i}(\ell-p) + C_{k,i}(\ell-p)C_{k,i}(\ell+1-p) + C_{k,i}(\ell+1-p) + C_{k,i}(\ell) + C_{k,i}(\ell)C_{k,i}(\ell+1) + C_{k,i}(\ell+1) \right).
\]

Notice that \( r_{k,i} \) depends not only on the set of values taken on by the aperiodic cross-correlation function but also on the order in which these values occur. For most applications the approximation

\[
r_{k,i} \approx \tilde{r}_{k,i} = 2 \sum_{\ell=1-p}^{p-1} C_{k,i}(\ell),
\]

which results from neglecting the terms \( C_{k,i}(\ell-p)C_{k,i}(\ell+1-p) \) and \( C_{k,i}(\ell)C_{k,i}(\ell+1) \), is quite satisfactory even for moderate values of \( p \). A more complete discussion of the signal-to-noise ratio parameter and quantitative results on \( \text{SNR}_1 \) for Gold codes [4] of period 511 can be found in [2].
Recently, Yao [3] has applied moment space bounds [5] to the same phase-coded SSMA system that we described at the beginning of this section. For application of these bounds, the maximum periodic and odd cross-correlations and the parameters $r_{k,i}$ must be computed. In addition, these bounds require the evaluation of the fourth moment of $Z_i$, which can also be determined from the aperiodic cross-correlation functions [3]. For the cases considered in [3] it is shown that the error probability for the $i^{th}$ receiver is approximately $1 - \Phi(\text{SNR}_i)$ where $\Phi$ is the standard (i.e., zero mean, unit variance) Gaussian distribution function. This has been experimentally verified in the past.
III. Identities and Bounds for Correlation Parameters

In this section, we present several useful analytical results which can be used to reduce the computation required to evaluate the correlation parameters. These lead to more efficient algorithms for obtaining sets of sequences with small cross-correlation. As pointed out by Welch [6], the sampling theorem guarantees that the most general signal sets that need to be considered are sequences of complex numbers. We develop our results for such sequences since little is gained by restricting attention to binary sequences.

Let $a^*$ denote the complex conjugate of $a$. If $x$ and $y$ are complex sequences such that $x_j = x_{j+p}$ and $y_j = y_{j+p}$ for all $j \in \mathbb{Z}$, then we define

$$C_{x,y}(\ell) = \begin{cases} \sum_{j=0}^{p-1-l} x_j y_{j+l}^* , & 0 \leq \ell \leq p-1 \\ \sum_{j=0}^{p-1+p-l} x_j y_{j-l}^* , & 1-p \leq \ell < 0 \end{cases}$$

and $C_{x,y}(p) = C_{x,y}(-p) = 0$. Under the condition that $p$ is the least common multiple of the periods of $x$ and $y$, $C_{x,y}(\cdot)$ is the aperiodic cross-correlation function for $x$ and $y$. We denote the function $C_{x,x}(\cdot)$ by $c_x(\cdot)$ and note that

$$C_{x,y}(-\ell) = [c_y(x(\ell))]^*$$
$$C_x(-\ell) = [c_x(\ell)]^*$$

**Proposition 1:**

$$\sum_{\ell=1-p}^{p-1} |C_{x,y}(\ell)|^2 = \sum_{\ell=1-p}^{p-1} c_x(\ell)[c_y(\ell)]^*$$
Proof: If \( u \) and \( v \) are any complex-valued sequences of period \( p' \) then

\[
\sum_{\ell=0}^{p'-1} |\theta_{u,v}(\ell)|^2 = \sum_{\ell=0}^{p'-1} \theta_u(\ell)[\theta_v(\ell)]^* \tag{2}
\]

where \( \theta_{u,v}(\cdot) \) is the usual periodic cross-correlation function for sequences \( u \) and \( v \), and \( \theta_u(\cdot) \) and \( \theta_v(\cdot) \) are the periodic autocorrelation functions. The proof of (2) is omitted since it is a minor modification of the proof of Gold's Proposition 2 [7]. Let \( p' \geq 2p-1 \) and define \( u_j = x_j \) and \( v_j = y_j \) for \( 0 \leq j \leq p-1 \) and \( u_j = v_j = 0 \) for \( p \leq j < p' \). If we are only interested in proving the proposition we can let \( p' = 2p-1 \) as in Welch [6]. By letting \( p' \geq 2p-1 \) we can simultaneously prove the proposition and establish a result which will be used in Section IV. We let \( u_{j+mp'} = u_j \) and \( v_{j+mp'} = v_j \) for \( m \in \mathbb{Z} \) and \( 0 \leq j \leq p'-1 \) so that \( u \) and \( v \) satisfy the conditions for (2). It is easy to verify that

\[
\theta_{u,v}(\ell) = \begin{cases} 
C_{x,y}(\ell) & 0 \leq \ell \leq p-1 \\
0 & p \leq \ell \leq p'-p \\
C_{x,y}(\ell-p') & p'-p+1 \leq \ell \leq p'-1
\end{cases}
\]

and, similarly

\[
\theta_u(\ell) = \begin{cases} 
C_x(\ell) & 0 \leq \ell \leq p-1 \\
0 & p \leq \ell \leq p'-p \\
C_x(\ell-p') & p'-p+1 \leq \ell \leq p'-1
\end{cases}
\]

Using (2), we have

\[
\sum_{\ell=1-p}^{p-1} |C_{x,y}(\ell)|^2 = \sum_{\ell=0}^{p'-1} |\theta_{u,v}(\ell)|^2 = \sum_{\ell=0}^{p'-1} \theta_u(\ell)[\theta_v(\ell)]^* \\
= \sum_{\ell=0}^{p'-1} \theta_u(\ell)[\theta_v(\ell)]^* \\
= \sum_{\ell=1-p}^{p-1} C_x(\ell)[C_y(\ell)]^*
\]
The following corollary to Proposition 1 is established by applying Cauchy's inequality to the sum \( \sum_{\ell=1-p}^{p-1} |c_x(\ell)c_y(\ell)| \).

**Corollary 1:**

\[
\sum_{\ell=1-p}^{p-1} |c_x(\ell)c_y(\ell)|^2 \leq \left( \sum_{\ell=1-p}^{p-1} |c_x(\ell)|^2 \right)^{1/2} \left( \sum_{\ell=1-p}^{p-1} |c_y(\ell)|^2 \right)^{1/2} \tag{3}
\]

Of course, Cauchy's inequality can also be applied to \( \sum_{\ell=0}^{p-1} \theta_x(\ell)\theta_y(\ell) \) to give

\[
\sum_{\ell=0}^{p-1} |\theta_x(\ell)\theta_y(\ell)|^2 \leq \left( \sum_{\ell=0}^{p-1} |\theta_x(\ell)|^2 \right)^{1/2} \left( \sum_{\ell=0}^{p-1} |\theta_y(\ell)|^2 \right)^{1/2} \tag{4}
\]

Equation (4) is satisfied with equality if and only if \( \theta_x(\bullet) = \alpha \theta_y(\bullet) \) for some \( \alpha \). If \( x \) and \( y \) are binary sequences, then \( \theta_x(0) = \theta_y(0) = p \) and therefore (4) is satisfied with equality if and only if the two binary sequences \( x \) and \( y \) have identical periodic autocorrelation functions. In particular, all pairs of binary m-sequences of period \( p \) satisfy (4) with equality, both sides of (4) having value \( p^2 + p - 1 \). However, the same is not true for (3).

Equation (3) is satisfied with equality if and only if \( c_x(\bullet) = \alpha c_y(\bullet) \) for some \( \alpha \). For instance, this condition is met whenever \( y_j = \beta x_{p-1-j} \) for all \( j \in \mathbb{Z} \) with \( |\beta|^2 = \alpha \). We get some interesting results from this when \( x \) and \( y \) are binary sequences of period \( p \) (which we will assume is the case in the remainder of this paragraph). Since \( c_x(0) = c_y(0) = p \), equality holds in (3) if and only if \( c_x(\ell) = c_y(\ell) \) for \( 0 \leq \ell \leq p-1 \). Since \( |c_x(\ell)| > 0 \) whenever \( p - |\ell| \) is odd, the right side of (3) has value at least \( p^2 + p - 1 \) when \( p \) is odd and \( p^2 + p \) when \( p \) is even. These minimum values
are achieved if and only if both $x$ and $y$ are Barker sequences [8], [9].

A bit more can be said when $p$ is odd. If $x$ and $y$ are any Barker sequences of odd period $p$, $C_x(\ell) = C_y(\ell) = 0$ for odd $\ell$ and $C_x(\ell) = C_y(\ell) = (-1)^{(p-1)/2}$ for even $\ell$ [9]. Therefore, both sides of (3) have value $p^2 + p - 1$ if and only if $x$ and $y$ are Barker sequences.

The next proposition shows that it is easy to find $C_{x,y}(\cdot)$ from $C_{x,y}(\cdot)$ if $\hat{y}$ is a shifted version of $y$ (i.e., $\hat{y}_j = y_{j+1}$ for all $j \in \mathbb{Z}$).

**Proposition 2:**

$$C_{x,y}(\ell) = \begin{cases} C_{x,y}(\ell+1) + x_{p-\ell-1}y_0^* & 0 \leq \ell \leq p-1 \\ C_{x,y}(\ell+1) - x_{-\ell-1}y_0^* & 1-p \leq \ell < 0 \end{cases}$$

**Proof:** For $0 \leq \ell < p-1$

$$C_{x,y}(\ell) = \sum_{j=0}^{p-1-\ell} x_j y_{j+1+\ell}^* = \sum_{j=0}^{p-1-(\ell+1)} x_j y_{j+(\ell+1)}^* + x_{p-\ell-1}y_0^*$$

$$= C_{x,y}(\ell+1) + x_{p-\ell-1}y_0^*.$$ Since $C_{x,y}(p) = 0$ we have

$$C_{x,y}(\ell) = C_{x,y}(\ell+1) + x_{p-\ell-1}y_0^* \quad 0 \leq \ell \leq p-1.$$
For \(1-p \leq \lambda < 0\)

\[
C_{x,y}(\lambda) = \sum_{j=0}^{p-1-\lambda} x_{j-l} y_{j+\lambda} = \sum_{j=1}^{p-1+(\lambda+1)} x_{j-l} y_{j}^* \\
= \sum_{j=0}^{p-1+(\lambda+1)} x_{j-l} y_{j}^* - x_{-\ell-1} y_{0}^* \\
= C_{x,y}(\lambda+1) - x_{-\ell-1} y_{0}^*
\]

An application of Proposition 2 to the odd cross-correlation function \(\theta_{x,y}(*)\) gives the corresponding result

\[
\theta_{x,y}(\lambda) = \theta_{x,y}(\lambda+1) + 2x_{p-\ell-1} y_{0}^*, \quad 0 \leq \lambda < p-1.
\]

The next proposition shows that we can find \(C_{x}(\lambda)\) from \(C_{x}(*)\) where \(\hat{x}_j = x_{j+1}\) for all \(j \in \mathbb{Z}\).

**Proposition 3:**

\[
C_{x}(\lambda) = \begin{cases}
C_{x}(\lambda) - x_{0} x_{\lambda}^* + x_{p-\lambda} x_{0}^* & 0 \leq \lambda \leq p-1 \\
C_{x}(\lambda) - x_{-\lambda} x_{0}^* + x_{0} x_{p+\lambda}^* & 1-p \leq \lambda < 0
\end{cases}
\]

**Proof:** If \(0 \leq \lambda < p-1\)

\[
C_{x}(\lambda) = \sum_{j=0}^{p-1-\lambda} \hat{x}_{j} \hat{x}_{j+\lambda}^* \\
= \sum_{j=0}^{p-1-\lambda} x_{j+1} x_{j+1+\lambda}^* \\
= x_{0} x_{\lambda}^* + \sum_{j=1}^{p-1-\lambda} x_{j} x_{j+\lambda}^* + x_{p-\lambda} x_{0}^* - x_{0} x_{\lambda}^* \\
= C_{x}(\lambda) - x_{0} x_{\lambda}^* + x_{p-\lambda} x_{0}^*
\]

The proof for negative values of \(\lambda\) is similar.
In the next section we consider only binary sequences. Consequently it is worthwhile to mention that if \( x \) and \( y \) are binary sequences, Proposition 1 implies
\[
\sum_{\ell=1}^{p-1} c_{x,y}(\ell) = p^2 + 2 \sum_{\ell=1}^{p-1} c_x(\ell) c_y(\ell).
\]
If Cauchy's inequality is applied to \( \sum_{\ell=1}^{p-1} c_x(\ell) c_y(\ell) \) we see that
\[
\sum_{\ell=1}^{p-1} c_{x,y}^2(\ell) \leq p^2 + 2 \left( \sum_{\ell=1}^{p-1} c_x^2(\ell) \right)^{\frac{1}{2}} \left( \sum_{\ell=1}^{p-1} c_y^2(\ell) \right)^{\frac{1}{2}}
\]
which is a tighter bound than the bound provided by Corollary 1. We also obtain the following lower bound from Cauchy's inequality
\[
\sum_{\ell=1}^{p-1} c_{x,y}^2(\ell) \geq p^2 - 2 \left( \sum_{\ell=1}^{p-1} c_x^2(\ell) \right)^{\frac{1}{2}} \left( \sum_{\ell=1}^{p-1} c_y^2(\ell) \right)^{\frac{1}{2}}
\]
so that the bounds in (6) and (7) are both very tight when the sum of the squares of the autocorrelation values is small when compared with \( p^2 \), which is true for Barker sequences of lengths 11 or 13 for example.
IV. Computation of Correlation Parameters

In this section, we discuss how the results of Section III can be used to compute the various correlation parameters for binary sequences in a more efficient manner, and estimate the computation required in each case. Thus, $C_{k,i}(\ell)$ can be computed using $p-|\ell|$ comparisons and $p-|\ell|$ additions and the $2p-1$ values of $C_{k,i}(\cdot)$ can be computed using $p^2$ comparisons and $p^2$ additions. Autocorrelation functions $C_{i}(\cdot)$, however, require only $\frac{1}{2}p(p-1)$ comparisons and $\frac{1}{2}p(p-1)$ additions because of the symmetry displayed in (1), and because $C_{i}(0)$ is always $p$ and need not be computed.

In Section II, it was pointed out that $\sum r_{k,i}$ is the crucial correlation parameter for determining the $i^{th}$ user's signal-to-noise ratio. The expression for $r_{k,i}$ can easily be manipulated to give

$$r_{k,i} = \sum_{\ell=1-p}^{p-1} C_{k,i}(\ell)[C_{k,i}(\ell) + C_{k,i}(\ell) + C_{k,i}(\ell+1)].$$

Thus $r_{k,i}$ can be computed from $C_{k,i}(\cdot)$ using $2p-1$ multiplications and $3(2p-1)$ additions. If there are $K$ users, we have to compute $\binom{K}{2}$ cross-correlation functions and $r_{k,i}$'s in order to compute $\sum_{k\neq i} r_{k,i}$ for all $i$.

If $\sum \tilde{r}_{k,i}$ is used as an approximation to $\sum r_{k,i}$, we still require $2p-1$ multiplications to compute $\tilde{r}_{k,i}$ from $C_{k,i}(\cdot)$, though the number of additions is reduced to $2p-1$. However, using Proposition 1, we have
\[ r_{\bar{k}, i} = \frac{p-1}{2} \sum_{\ell=1-p}^{p-1} C_{k,i}(\ell) = \frac{p-1}{2} \sum_{\ell=1-p}^{p-1} C_k(\ell)C_i(\ell) \]

\[ = 2p^2 + 4 \sum_{\ell=1}^{p-1} C_k(\ell)C_i(\ell) \]

If \( C_k(*) \) and \( C_i(*) \) are known, \( r_{\bar{k}, i} \) can be computed in \( p \) multiplications and \( p \) additions, which is smaller by a factor of 2 than the computation required to find \( r_{\bar{k}, i} \) from \( C_k,i(*) \). The importance of Proposition 1, however, lies in the fact that only \( K \) autocorrelation functions, rather than \( \binom{K}{2} \) cross-correlation functions, need to be computed in order to find \( r_{\bar{k}, i} \) for all \( k < i \), and the resulting computational saving is more than a factor of \( K-1 \). In fact, if it is desired to compute \( r_{\bar{k}, i} \) for all \( k \leq i \) (in order to obtain information on both the cross-correlation and autocorrelation), Proposition 1 provides a method which requires \( \binom{K}{2} p^2 \) fewer comparisons and additions than the direct method of computing \( r_{\bar{k}, i} \) for all \( k \leq i \).

In the proof of Proposition 1, it was seen that the aperiodic cross-correlation function for two sequences of period \( p \) can be expressed as the periodic cross-correlation function for two other sequences of period \( p' \geq 2p-1 \). We can compute this periodic cross-correlation function by finding the discrete Fourier transforms of the two sequences of period \( p' \), multiplying them in the transform domain and then computing the inverse discrete Fourier transform of the product \( C_{12} \). These transforms can be computed by the Fast Fourier Transform (FFT) algorithm which requires \( \frac{1}{2} p' \log_2 p' \) complex multiplications and \( p' \log_2 p' \) complex additions if \( p' \) is a power of 2. In many cases of interest in the multiple-access
communication problem, \( p \) is of the form \( 2^m - 1 \) and thus \( p' \) can be chosen to be \( 2p+2 \). If we compute the \( \binom{K}{2} \) cross-correlation functions in order to compute the \( \tilde{r}_{k,i} \)'s, we require \( K(p+1) \log_2(2p+2) + \binom{K}{2}(2p+2) + \binom{K}{2}(p+1) \log_2(2p+2) \) complex multiplications and \( K(2p+2) \log_2(2p+2) \) complex additions. If Proposition 1 is used, we need compute only the \( K \) autocorrelation functions which requires \( 2K(p+1) \log_2(2p+2) + K(2p+2) \) complex multiplications and \( 2K(2p+2) \log_2(2p+2) \) complex additions and the computational saving is more than a factor of \( K/4 \).

In comparing FFT methods with non-FFT methods, it should be remembered that complex multiplications actually consist of 4 real multiplications and 2 real additions while complex additions consist of two real additions. Thus, the FFT method uses \( 4(2p+2) \log_2(2p+2) + 4(2p+2) \) real multiplications and \( 6(2p+2) \log_2(2p+2) + 2(2p+2) \) real additions to compute an autocorrelation function while the direct method uses \( \frac{1}{2} p(p-1) \) binary comparisons and \( \frac{1}{2} p(p-1) \) integer additions. On a computer, real (i.e., floating point) additions and multiplications require more time than integer additions. Hence, the FFT method is not faster than the direct method unless \( p \) is quite large. One other method based on the FFT is the use of Parseval's theorem to deduce the sum of the squares of the cross-correlation functions from the sum of the squares of the magnitudes of their discrete Fourier transforms. It can be shown that this method requires \( 2K(2p+2) \log_2(2p+2) + 4K(2p+2) + \binom{K}{2}(2p+2) \) real multiplications and \( 3K(2p+2) \log_2(2p+2) + 2K(2p+2) + \binom{K}{2}(2p+2) \) real additions. Here also, a savings in computation is not necessarily
achieved by resorting to a FFT, unless p is quite large. It should also be pointed out that this method does not provide the values of the autocorrelation functions $C_i(\cdot)$ which are also of considerable interest in the multiple-access communication problem.

Next, let us consider the problem of finding the auto-optimal shift $l$ of a given sequence (i.e., a shift of the sequence for which the maximum magnitude of the out-of-phase odd autocorrelation is as small as possible). $C_i(\cdot)$ can be computed using $\frac{1}{2} p(p-1)$ comparisons and $\frac{1}{2} p(p-1)$ additions and $\hat{\theta}_i(\cdot)$ requires $\frac{1}{2}(p-1)$ further additions (since $\hat{\theta}_i(0) = p$ and $\hat{\theta}_i(l) = -\hat{\theta}_i(p-l)$). Thus, computing $\hat{\theta}_i(\cdot)$ for $p$ shifts of the sequence requires $\frac{1}{2} p^2(p-1)$ comparisons and $\frac{1}{2} p(p^2-1)$ additions. However, using Proposition 3, it is easy to see that

$$\hat{\theta}_x(l) = \hat{\theta}_x(l) - 2x_0 x_l^* + 2x_{p-l}^* x_0^*.$$  

Hence, only 2 comparisons and 2 additions are necessary to update $\hat{\theta}_i(l)$, and such updates are necessary for $(p-1)/2$ values of $l$ only. Thus, a total of $\frac{1}{2}(3p-2)(p-1)$ comparisons and $\frac{1}{2}(p-1)(3p-1)$ additions is necessary to find the auto-optimal shift and this is better by a factor of $p/3$ over the direct method.

This idea can be generalized to finding the best shifts of $K$ sequences where the various cross-correlation parameters are chosen as the criteria. Unfortunately, there are $p^K$ shifts to be considered which requires a prohibitive amount of computation. One suboptimal scheme, investigated by Sywyk [11], is as follows. First, the $K$ sequences are ordered in some arbitrary manner, and the auto-optimal shift of the first sequence is found. For $i = 2, 3, \ldots K$, we choose that shift of the $i^{th}$ sequence
which minimizes $\hat{c}$ where

$$
\hat{c} = \max_{1 \leq k \leq i} \max_{l} \hat{c}_{k, i}(l)
$$

Thus, we have to compute $(i-1)$ cross-correlation functions for $p$ shifts of the $i$th sequence. Since we require $p^2$ comparisons and $p^2$ additions to compute $C_{k, i}(\cdot)$ and a further $p-1$ addition to compute $\hat{c}_{k, i}(\cdot)$, the total computation required is $(i-1)p^3$ comparisons and $(i-1)p(p^2+p-1)$ additions. However, after computing the cross-correlation functions once, one can use (5) to update each using $p$ comparisons and $p$ additions. The total computation required for the $i$th sequence by the use of this method is $(i-1)p(2p-1)$ comparisons and $(i-1)(2p^2-1)$ additions which is better by a factor of $p/2$ over the direct method.

This scheme can also be used with other correlation parameters. For example, one can choose that shift of the $i$th sequence which minimizes the parameter $\hat{r}_i = \sum_{k=1}^{k=i-1} r_{k, i}$ which measures the effect of the 1st, 2nd, ..., $(i-1)$th users' signals on $\text{SNR}_i$. Since $\hat{r}_{i, k} = r_{k, i}$, this is equivalent to choosing that shift of the $i$th sequence which minimizes the average effect of the $i$th user's signal on $\text{SNR}_{k}$, $k = 1, 2, ..., i-1$. Thus, the direct method requires $(i-1)p^3$ comparisons and $(i-1)p^3$ additions to compute $C_{k, i}(\cdot)$ for $p$ shifts of the $i$th sequence. On the other hand, Proposition 2 allows us to update each $C_{k, i}(\cdot)$ using $p$ comparisons (since only $p$ distinct symbols from the $k$th sequence need to be compared with the zeroth symbol of the $i$th sequence) and $2p-1$ additions. Thus, a total
of \((i-1)p(2p-1)\) comparisons and \((i-1)(3p^2-3p+1)\) additions is required to compute all the \(C_{k,i}(\cdot)\) for \(p\) shifts of the \(i^{th}\) sequence. This is a computational saving of a factor of \(\frac{1}{2}p\) for comparisons and \(p/3\) for additions. In both cases, the same amount of computation is required to find \(r_i\) from the \(C_{k,i}(\cdot)\).

If one minimizes \(\tilde{r}_i = \sum_{k=1}^{i-1} \tilde{r}_{k,i}\) instead of \(r_i\), further savings in computation are possible. While dealing with the \(i^{th}\) sequence, we need to compute \(C_{i}(\cdot)\) only, since \(C_{k}(\cdot), 1 \leq k < i\), would be available from previous computations. Computing \(C_{i}(\cdot)\) for \(p\) shifts of the \(i^{th}\) sequence requires \(\frac{1}{2}p^2(p-1)\) comparisons and \(\frac{1}{2}p^2(p-1)\) additions. However, using Proposition 3, we can update \(C_{i}(\cdot)\) using \(p-1\) comparisons and \(p-1\) additions, and thus, a total of \(\frac{1}{2}(p-1)(3p-2)\) comparisons and \(\frac{1}{2}(p-1)(3p-2)\) additions is required to find \(C_{i}(\cdot)\) for \(p\) shifts of the \(i^{th}\) sequence. The saving in computation is a factor of \(p/3\) over the direct method. The major computational advantage in using \(\tilde{r}_i\) as an approximation to \(r_i\) lies in the fact that only one autocorrelation function, rather than \((i-1)\) cross-correlation functions, need to be computed when the \(i^{th}\) sequence is being examined. Over \(K\) sequences, the computational saving is a factor of \(K-1\).
V. Discussion

In this paper we have presented results which are useful in the study and selection of sequences with good correlation properties. We should point out that the following generalization of Proposition 1 and Corollary 1 can be established. For $T > 0$, let $L_T$ be the space of all complex-valued functions of a real variable which satisfy $x(t + T) = x(t)$ for each $t$ and $\int_{[0,T]} |x(t)|^2 \mu(dt) < \infty$ where $\mu$ is a measure on the real line. If for each $x \in L_T$ and $y \in L_T$ we define $C_{x,y}(T) = C_{x,y}(-T) = 0$ and

$$C_{x,y}(\tau) = \begin{cases} \int_{[0,T-\tau]} x(t)y^*(t+\tau) \mu(dt), & 0 \leq \tau < T \\ \int_{[0,T+\tau]} x(t-\tau)y^*(t) \mu(dt), & -T < \tau < 0 \end{cases}$$

then

$$\int_{[-T,T]} |C_{x,y}(\tau)|^2 \mu(d\tau) = \int_{[-T,T]} C_{x,x}(\tau)C_{y,y}^*(\tau) \mu(d\tau) \leq \left[ \int_{[-T,T]} |C_{x,x}(\tau)|^2 \mu(d\tau) \right]^{\frac{1}{2}} \left[ \int_{[-T,T]} |C_{y,y}(\tau)|^2 \mu(d\tau) \right]^{\frac{1}{2}}.$$

This gives Proposition 1 and Corollary 1 as a special case when $\mu(Z) = 1$ and $\mu(Z^C) = 0$.

We have also indicated how these results can be employed to reduce the amount of computation required to calculate the key correlation...
parameters. Some of these results are currently being used by H. F. A. Roefs, as part of his Ph.D. research on multiple-access communications at the Coordinated Science Laboratory. In addition to application of the analytical results of Section III to computational problems, Proposition 1 and Corollary 1 can be employed to investigate aperiodic cross-correlation properties of certain classes of sequences which have been studied from the point of view of their aperiodic autocorrelation properties [8]-[10]. Our brief discussion of Barker sequences in Section III gives an indication of what might result from such an investigation.
References


