channel measurement information," *IEEE Trans. Inform. Theory*, pp. 170-182, Jan. 1972.
[24] R. M. Fano, *The Transmission of Information*. Cambridge, MA: M.I.T. Press and Wiley, 1961.
[25] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes," *Inform. Contr.*, vol. 3, pp. 68-79, 279-290; and *Math. Rev.*, vol. 22, p. 3619, 1960.
[26] A. Hocquenghem, "Codes correcteurs d'Erreurs," *Chiffres* (Paris), vol. 2, pp. 147-156; and *Math. Rev.*, vol. 22, p. 652, 1959.
[27] V. D. Goppa, "A new class of linear error-correcting codes," *Probl. Peredach. Inform.*, vol. 6, no. 3, pp. 24-30, Sept., 1970.
[28] ——, "Rational representation of codes and (L, g) codes," *Probl. Peredach. Inform.*, vol. 7, no. 3, pp. 41-49, Sept. 1971.
[29] E. R. Berlekamp, "Goppa codes," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 590-592, Sept. 1973.
[30] N. J. Patterson, "The Algebraic Decoding of Goppa Codes," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 203-207, Mar. 1975.
[31] Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa, "A method for solving key equations for decoding goppa codes," *Inform. Contr.*, vol. 27, pp. 87-99, 1975.
[32] W. W. Peterson, *Error-Correcting Codes*. Cambridge, MA: M.I.T. Press, 1961.

Crosscorrelation Properties of Pseudorandom and Related Sequences

DILIP V. SARWATE, SENIOR MEMBER, IEEE
AND MICHAEL B. PURSLEY, SENIOR MEMBER, IEEE

Invited Paper

Abstract—Binary maximal-length linear feedback shift register sequences (m-sequences) have been successfully employed in communications, navigation, and related systems over the past several years. For the early applications, m-sequences were used primarily because of their excellent periodic autocorrelation properties. For many of the recent systems applications, however, the crosscorrelation properties of such sequences are at least as important as the autocorrelation properties, and the system performance depends upon the aperiodic correlation in addition to the periodic correlation. This paper presents a survey of recent results and provides several new results on the periodic and aperiodic crosscorrelation functions for pairs of m-sequences and for pairs of related (but not maximal-length) binary shift register sequences. Also included are several recent results on correlation for complex-valued sequences as well as identities relating the crosscorrelation functions to autocorrelation functions. Examples of problems in spread-spectrum communications are employed to motivate the choice of correlation parameters that are considered in the paper.

Manuscript received June 25, 1979; revised January 11, 1980. This work was supported in part by the National Science Foundation under Grant ENG78-06630, the Army Research Office under Grant DAAG-29-78-G-0114, and the Joint Services Electronics Program under Contract N00014-79-C-0424.

The authors are with the Coordinated Science Laboratory and the Department of Engineering, University of Illinois, Urbana, IL 61801.

I. Introduction

THERE are a large number of problems in systems engineering that require sets of signals which have one or both of the following two properties:

i) each signal in the set is easy to distinguish from a time-shifted version of itself;
ii) each signal in the set is easy to distinguish from (a possibly time-shifted version of) every other signal in the set.

The first property is important for such applications as ranging systems, radar systems, and spread-spectrum communications systems. The second is important for simultaneous ranging to several targets, multiple-terminal system identification, and code-division multiple-access communications systems.

The signals employed in the kinds of applications mentioned above are usually required to be periodic. This is primarily because of the simplifications in system implementation that

0018-9219/80/0500-0593$00.75

typically result from the use of periodic signals. Consequently, we restrict attention to periodic signals throughout the paper. In order to simplify the presentation, we consider only those sets of signals which have the property that for some T, $x(t) = x(t+T)$ for all t and for each signal x in the set. The most common example is a set of signals of common period T; however, all that is required is that T be an integer multiple of the period of each signal in the set.

One of the most common and most useful measures of distinguishability is the mean-squared difference. For our purposes, two signals are easy to distinguish if and only if the mean-squared difference between them is large, and we will require not only that $x(t)$ is easy to distinguish from $y(t)$ but also that $-x(t)$ is easy to distinguish from $y(t)$. Both $+x(t)$ and $-x(t)$ must be considered whenever modulation processes are involved, such as when binary data is modulated onto $x(t)$ or when $x(t)$ is modulated onto a carrier signal. Thus the measure of distinguishability is the quantity

$$T^{-1}\int_0^T [y(t) \pm x(t)]^2\, dt$$

$$= T^{-1}\left\{\int_0^T [y^2(t)+x^2(t)]\, dt \pm 2\int_0^T x(t)y(t)\, dt\right\}. \quad (1.1)$$

The first integral on the right-hand side of (1.1) is the energy in $x(t)$, $0 \leqslant t \leqslant T$, plus the energy in $y(t)$, $0 \leqslant t \leqslant T$. Thus for fixed signal energy, $y(t)$ is easy to distinguish from both $+x(t)$ and $-x(t)$ if and only if the magnitude of the quantity

$$r = \int_0^T x(t)y(t)\, dt \quad (1.2)$$

is small. For communications, navigation, and radar systems with correlation receivers or matched filters, r represents the output of the filter matched to the signal $y(t)$ when the input is $x(t)$. In a multiple-access communications system, for example, $x(t)$ and $y(t)$ may represent the signals assigned to two different transmitters, in which case the parameter r is a measure of the crosstalk interference between the two signals.

Properties i) and ii) require distinguishability of $x(t)$ and $y(t+\tau)$ for all $\tau \in [0, T]$ if $x(t)$ and $y(t)$ are different signals, and for all $\tau \in (0, T)$ if $x(t)$ and $y(t)$ are the same. Consequently, it is the magnitude of the *crosscorrelation function*

$$r_{x,y}(\tau) = \int_0^T x(t)y(t+\tau)\, dt \quad (1.3)$$

that is of interest. In writing (1.2) and (1.3), we have assumed that $x(t)$ and $y(t)$ are real-valued signals. The necessary modification for complex-valued signals is to replace $y(t)$ by its complex conjugate.

Due in part to the relative simplicity of their generation, the signals of interest for most applications are periodic signals which consist of sequences of elemental time-limited pulses. These pulses are all of the same shape, so that the signal can be written as

$$x(t) = \sum_{n=-\infty}^{\infty} x_n \varphi(t - nT_c) \quad (1.4)$$

where $\varphi(t)$ is the basic pulse waveform and T_c is the time duration of this pulse. If $x(t) = x(t+T)$ for all t, then T must be a multiple of T_c, and the sequence (x_n) must be periodic with a period which is a divisor of $N = T/T_c$.

Suppose $x(t)$ and $y(t)$ are periodic signals as described above, $x(t)$ is given by (1.4), and $y(t)$ is given by

$$y(t) = \sum_{n=-\infty}^{\infty} y_n \varphi(t - nT_c). \quad (1.5)$$

Then it is easy to show that the parameter r of (1.2) is given by

$$r = \lambda \sum_{n=0}^{N-1} x_n y_n \quad (1.6)$$

where the constant λ is

$$\lambda = \int_0^{T_c} \varphi^2(t)\, dt. \quad (1.7)$$

For example, if $\varphi(t) = p_{T_c}(t)$, the unit amplitude rectangular pulse of duration T_c which starts at $t = 0$, then $\lambda = T_c$. In general, according to (1.6), the inner product of the continuous-time periodic signals $x(t)$ and $y(t)$ is proportional to the inner product of the corresponding vectors $(x_0, x_1, \cdots, x_{N-1})$ and $(y_0, y_1, \cdots, y_{N-1})$. Furthermore, if $\tau = lT_c$ then (1.6) generalizes to

$$r_{x,y}(\tau) = \lambda \sum_{n=0}^{N-1} x_n y_{n+l} \quad (1.8)$$

which is the constant λ of (1.7) multiplied by the inner product of $(x_0, x_1, \cdots, x_{N-1})$ and $(y_l, y_{l+1}, \cdots, y_{l+N-1})$. Since the sequence (y_n) has a period which divides N, then

$$(y_l, y_{l+1}, \cdots, y_{l+N-1}) = (y_l, y_{l+1}, \cdots, y_{N-1}, y_0, \cdots, y_{l-1}). \quad (1.9)$$

The right-hand side of (1.9) is the lth cyclic shift of the original vector $(y_0, y_1, \cdots, y_{N-1})$.

The above discussion motivates the consideration of the *periodic crosscorrelation function* for sequences (x_n) and (y_n) which is defined by

$$\theta_{x,y}(l) = \sum_{n=0}^{N-1} x_n y_{n+l}. \quad (1.10)$$

From (1.8) we see that $r_{x,y}(\tau) = \lambda \theta_{x,y}(l)$ whenever $\tau = lT_c$. In addition, for arbitrary values of τ, $r_{x,y}(\tau)$ can be determined from the periodic crosscorrelation function. For instance, if $\varphi(t) = p_{T_c}(t)$ then for $0 \leqslant \tau < T$,

$$r_{x,y}(\tau) = T_c\, \theta_{x,y}(l') + (\tau - l'T_c)[\theta_{x,y}(l'+1) - \theta_{x,y}(l')] \quad (1.11)$$

where l' is the largest integer such that $l'T_c \leqslant \tau$. It is also worth pointing out that for any choice of elemental pulse $\varphi(t)$,

$$\max\{|r_{x,y}(\tau)| : 0 \leqslant \tau \leqslant T\} = \lambda \max\{|\theta_{x,y}(l)| : 0 \leqslant l \leqslant N-1\}.$$

Since the periodic crosscorrelation parameters for the continuous-time signals $x(t)$ and $y(t)$ of (1.4) and (1.5) are completely determined by the crosscorrelation function, the signal design problem described at the beginning of the paper

reduces to the problem of finding sets of periodic sequences with the following two properties:

1′) for each sequence $x = (x_n)$ in the set, $|\theta_{x,x}(l)|$ is small for $1 \leqslant l \leqslant N - 1$;
2′) for each pair of sequences $x = (x_n)$ and $y = (y_n)$, $|\theta_{x,y}(l)|$ is small for all l.

Sequences which have these properties (and in some cases also have other important properties) are the subject of this paper. We refer to such sequences as *pseudorandom and related sequences* for reasons which are given below.

The study of pseudorandom and related sequences spans more than twenty-five years. During this time, results have been obtained on structural properties, correlation functions, methods of generation, and applications to various electronic systems problems such as those previously mentioned. Some of the recent applications have required additional and more detailed examinations of certain properties of pseudorandom and related sequences. For instance, the increased interest in spread-spectrum communications has led to a corresponding increased interest in *aperiodic* correlation parameters for such sequences in addition to the periodic correlation parameters mentioned above. Similarly, the use of code-division multiple-access communications techniques has resulted in the necessity of a deeper study of crosscorrelation properties of periodic sequences. This paper is primarily concerned with the aperiodic and periodic crosscorrelation properties of pseudorandom and related sequences. The particular correlation parameters considered are those that are motivated by recent applications in such areas as spread-spectrum and code-division multiple-access communications.

In much of the literature on periodic sequences, the terms pseudorandom sequence, pseudonoise (PN) sequence, and maximal-length linear feedback shift-register sequence (m-sequence) are used synonymously. However, during the last ten years or so there has been an increased tendency to employ the terms pseudorandom sequence or pseudonoise sequence as generic names for sequences from some imprecisely defined large class that includes certain nonmaximal-length linear feedback shift-register sequences in addition to the m-sequences. For example, communications engineers quite commonly lump together m-sequences and Gold sequences [35] under the title "PN sequences." In the title and introduction of this paper, we refer to the large class mentioned above as the class of pseudorandom and related sequences. However, we do not use this generic name elsewhere in the paper. In order to avoid a potential source of confusion, in Sections II-V we make a clear distinction between the maximal-length sequences and various types of related nonmaximal-length sequences such as those described in [35], [52], and [66].

The sequences that have received the most attention in the literature are the binary maximal-length linear feedback shift-register sequences which we refer to as m-sequences. As the name suggests, these are precisely the sequences of maximum possible period (which is $N = 2^n - 1$) from an n-stage binary shift register with linear feedback. One of the key features of an m-sequence is its autocorrelation function $\theta_{x,x}(0) = N$ and $\theta_{x,x}(l) = -1$ for $1 \leqslant l < N$ (Property V of Section III), which is the "best" possible autocorrelation function for a binary sequence of period $N = 2^n - 1$. Here "best" refers to the minimum possible values of $|\theta_{x,x}(l)|$ for $1 \leqslant l < N$ (i.e., minimum autocorrelation sidelobes). It is this ideal periodic autocorrelation property that was exploited in most of the early applications of m-sequences.

In the present paper, we consider a number of different correlation parameters (including the periodic autocorrelation) for several classes of periodic sequences. With respect to binary sequences, we discuss the periodic crosscorrelation functions for pairs of m-sequences and for pairs of related linear feedback shift-register sequences. The key results on crosscorrelation are considerably less widely known and understood than the autocorrelation results, yet the former are more important for many applications. Included in the nonmaximal-length sequences considered are the Gold sequences [35] and the Kasami sequences [51], [52]. We present a representative cross section of results ranging from the classical well-known properties to the more recent or less widely disseminated results which have already proved to be important in the design of practical systems.

After introducing the periodic correlation functions in Section II, we discuss the basic correlation properties of periodic sequences. Bounds and identities are given which relate various periodic correlation parameters, and Fourier transforms of periodic sequences and of their correlation functions are briefly discussed. In Section III, after a brief look at binary shift-register sequences in general, we discuss the properties of m-sequences and their correlation functions. Our treatment is tutorial in nature and we have avoided explicit use of the theory of finite fields. This necessarily means that some of the finer details are lacking and that, in some instances, our treatment is more laborious and less elegant than it might have otherwise been. We hope, however, that our approach will make this section accessible to a broader audience. In Section IV, we present a collection of results on the periodic crosscorrelation functions for sets of pseudorandom and related sequences. Primary consideration is given to sets of m-sequences, sets of sequences which are sums of m-sequences (e.g., the Gold sequences), and the large and small sets of Kasami sequences. Finally, in Section V, aperiodic correlation functions are discussed. In this section aperiodic correlation identities are given for general periodic sequences, and aperiodic correlation data is given to illustrate the application of many of the results.

Applications in the analysis and design of spread-spectrum multiple-access communication systems (e.g., [12], [56], [72], [80]–[84], [102], [118], [133]) and spread-spectrum communications systems for multipath channels (e.g., [12], [71], [72]) provide the primary motivation for the work surveyed in the paper. However, the results on periodic correlation are also applicable to multiple-terminal system identification (e.g., [14], [16], [17], [29]) where signals with good correlation properties are needed as test signals. In addition, there are numerous applications to ranging, synchronization, data scrambling, holography, and spectrometry.

II. Periodic Correlation Functions for Complex-Valued Sequences

In this section we discuss the periodic correlation functions (autocorrelation and crosscorrelation) for general complex-valued periodic sequences. We avoid placing restrictions on the structure of the sequences, so that the results are applicable to general problems in signal design and analysis (perhaps via representations in terms of complex signals and orthogonal expansions). Of particular interest are applications of the results for complex-valued sequences to spread-spectrum com-

munications, especially quadriphase spread-spectrum multiple-access communications [83].

The results summarized in this section consist primarily of identities for periodic correlation functions and bounds on periodic correlation parameters. The correlation parameters considered include peak periodic correlation and mean-squared periodic correlation. In addition, Fourier transforms of sequences and Fourier transforms of periodic correlation functions are discussed.

A. Definitions and Basic Properties

Let $\mathbb{C}$ denote the set of complex numbers, and $\mathbb{C}^N$ the set of all vectors with N complex components. Elements of $\mathbb{C}^N$ are denoted by x, y, z, etc., where $x = (x_0, x_1, \cdots, x_{N-1})$ with $x_i \in \mathbb{C}$ for $0 \leq i < N$. The *inner product* $\langle x, y \rangle$ of two vectors x and y is defined by $\langle x, y \rangle = x_0 y_0^* + x_1 y_1^* + \cdots + x_{N-1} y_{N-1}^*$ where a^* denotes the complex conjugate of a. Note that $\langle x, x \rangle$ is a positive real number for all nonzero $x \in \mathbb{C}^N$. The *norm* $\|x\|$ of x is the positive square root of $\langle x, x \rangle$, and Σx denotes $x_0 + x_1 + \cdots + x_{N-1}$.

Let T denote the operator which shifts vectors cyclically to the left by one place, that is $Tx = (x_1, x_2, \cdots, x_{N-1}, x_0)$. If T is applied k times to x, the result is $T^k x$. We see that $T^k x = (x_k, x_{k+1}, \cdots, x_{N-1}, x_0, x_1, \cdots, x_{k-1})$ for $0 \leq k < N$, while $T^N x = x$. For larger values of k, $T^k x = T^{k'} x$ where $k' \equiv k \bmod N$. Similarly the operator T^{-1} shifts vectors cyclically to the right by one place, and it is easy to see that $T^{-k} x = T^{N-k} x$ for $0 \leq k < N$, and $T^{-N} x = x$. We also have that $\|T^k x\| = \|x\|$ and $\Sigma(T^k x) = \Sigma x$. The *period* of x is defined to be the least positive integer M such that $T^M x = x$. Although $T^i x \neq T^j x$ for $0 \leq i < j < M$, the vectors $x, Tx, T^2 x, \cdots, T^{M-1} x$ are *cyclically equivalent*; that is, they are cyclic shifts of each other. Generally M can be any divisor of N, but in most cases of interest, we will have $M = N$.

Let $\mathbb{Z}$ denote the set of all integers. Given $x \in \mathbb{C}^N$, we can generate an (infinitely long) periodic sequence x by repeating the vector x over and over again. More formally, given $x = (x_0, x_1, x_2, \cdots, x_{N-1})$ we define x, the periodic sequence generated by x by

$$x = \cdots, x_{-2}, x_{-1}, x_0, x_1, x_2, \cdots, x_{N-1}, x_N, \cdots$$

where $x_{mN+i} = x_i$ for all nonzero integers m and all i in the range $0 \leq i \leq N-1$. The left cyclic shift operator T on vectors x can be extended to the sequences x where it becomes a left shift operator which we also denote by T. Thus the vector $T^k x$ generates the periodic sequence $T^k x$ where $(T^k x)_i = x_{i+k}$ for all integers i. The *period* of the sequence x is just M, the period of x; it is the least positive integer such that $x_i = x_{i+M}$ for all i. The sequences $x, Tx, T^2 x, \cdots, T^{M-1} x$ are called *phases* of x; they are generated by cyclically equivalent vectors.

If $x = (x_0, x_1, \cdots, x_{N-1})$ is a vector of length N, the *reverse* of x is the vector

$$w = (x_{N-1}, \cdots, x_1, x_0).$$

That is, $w_i = x_{N-1-i}$ for $0 \leq i \leq N-1$. The sequence w which is generated by the vector w is called the *reverse sequence* for x. It satisfies $w_i = x_{N-1-i}$ for each integer i; moreover, for each k in the range $0 \leq k \leq N-1$.

$$(T^k w)_i = (T^{-k} x)_{N-1-i} = (T^{N-k} x)_{N-1-i}$$

so that each phase of w is the reverse of some phase of x. For this reason we refer to each of the phases of w as a *reciprocal* of x. The reciprocals of x are precisely the sequences generated by the vectors which are cyclically equivalent to w. One of the reciprocal sequences for x is of particular interest in the theory of shift-register sequences, and it will be discussed further in Section III-B. This is the sequence $v = T^{N-1} w$, which is the phase of w with the property

$$v_i = (Tx)_{N-1-i} = x_{-i}$$

for each i.

For vectors x and y of length N we define the *periodic crosscorrelation function* $\theta_{x,y}(\cdot)$ by

$$\theta_{x,y}(l) = \langle x, T^l y \rangle, \qquad l \in \mathbb{Z}. \tag{2.1a}$$

If x and y are the sequences generated by x and y, respectively, then (2.1a) is equivalent to

$$\theta_{x,y}(l) = \sum_{i=0}^{N-1} x_i y_{i+l}^*, \qquad l \in \mathbb{Z}. \tag{2.1b}$$

It is easy to verify that for each $l \in \mathbb{Z}$,

$$\theta_{x,y}(l) = \theta_{x,y}(l+N) \tag{2.2}$$

and

$$\theta_{x,y}(-l) = [\theta_{y,x}(l)]^*. \tag{2.3}$$

Applying the Cauchy inequality $|\langle u, v \rangle| \leq \|u\| \cdot \|v\|$ to (2.1a) we get

$$\begin{aligned} |\theta_{x,y}(l)| &= |\langle x, T^l y \rangle| \\ &\leq \|x\| \cdot \|T^l y\| \\ &= \|x\| \cdot \|y\|. \end{aligned}$$

Hence,

$$|\theta_{x,y}(l)| \leq \|x\| \cdot \|y\|. \tag{2.4}$$

It is also easy to show that

$$\sum_{l=0}^{N-1} \theta_{x,y}(l) = (\Sigma x)(\Sigma y)^*. \tag{2.5}$$

The *periodic autocorrelation function* $\theta_x(\cdot)$ for the sequence x is just $\theta_{x,x}(\cdot)$. Notice that $\theta_x(0) = \langle x, x \rangle$ is a positive real number, except when $x = \mathbf{0}$. From (2.1)–(2.4), we see that for each $l \in \mathbb{Z}$, $\theta_x(l) = \theta_x(l+N)$, $\theta_x(-l) = [\theta_x(l)]^*$, and

$$|\theta_x(l)| \leq \|x\|^2 = \langle x, x \rangle = \theta_x(0).$$

From (2.5), we see that

$$\sum_{l=0}^{N-1} \theta_x(l) = |\Sigma x|^2. \tag{2.6}$$

At times, it is convenient to use the alternative notation $\theta(x, y)(\cdot)$ for $\theta_{x,y}(\cdot)$, and $\theta(x)(\cdot)$ for $\theta_x(\cdot)$. As an example, consider the crosscorrelation function for x and $T^k y$. It is very easy to show that

$$\theta(x, T^k y)(l) = \theta(x, y)(l+k). \tag{2.7}$$

Similarly, for all i, j, and k

$$\theta(T^i x, T^j y)(l) = \theta(x, y)(l+j-i) \tag{2.8}$$

and

$$\theta(T^k x)(l) = \theta(x)(l). \tag{2.9}$$

Two sequences x and y are said to be uncorrelated if $\theta_{x,y}(l) =$

0 for all l, and a sequence x of period M is said to have a *two-valued* autocorrelation function if $\theta_x(l)$ equals some constant other than $\theta_x(0)$ for all $l \not\equiv 0 \bmod M$. Since $\theta_x(l) = [\theta_x(-l)]^*$, this constant must be real.

B. Correlation Identities

We now discuss some useful but not very well known identities involving crosscorrelation functions. Let $w, x, y, z \in \mathbb{C}^N$ and let w, x, y, z be the corresponding sequences. The four crosscorrelation functions $\theta_{w,x}$, $\theta_{y,z}$, $\theta_{w,y}$, and $\theta_{x,z}$ are related through the following identity

$$\sum_{l=0}^{N-1} \theta_{w,y}(l)[\theta_{x,z}(l+n)]^* = \sum_{l=0}^{N-1} \theta_{w,x}(l)[\theta_{y,z}(l+n)]^*. \tag{2.10}$$

A proof of this result is given in [87], and an alternative proof via discrete Fourier transforms is presented in Section II-D. We note the following special cases of this result. Setting $z = y$ in (2.10), we obtain

$$\sum_{l=0}^{N-1} \theta_{w,y}(l)[\theta_{x,y}(l+n)]^* = \sum_{l=0}^{N-1} \theta_{w,x}(l)[\theta_y(l+n)]^*. \tag{2.11}$$

Setting $w = x$ in (2.11) gives

$$\sum_{l=0}^{N-1} \theta_{x,y}(l)[\theta_{x,y}(l+n)]^* = \sum_{l=0}^{N-1} \theta_x(l)[\theta_y(l+n)]^* \tag{2.12}$$

and setting $n = 0$ in (2.12) gives

$$\sum_{l=0}^{N-1} |\theta_{x,y}(l)|^2 = \sum_{l=0}^{N-1} \theta_x(l)[\theta_y(l)]^*. \tag{2.13}$$

A version of (2.13) can be found in papers published in the mid-1960's by Gold [37] and by Stalder and Cahn [115]. However, since the more general (2.12) occurs as an *exercise* in a well-known textbook [13] published at about the same time, the basic result is undoubtedly much older. The provenance of all these results is not as important or as interesting as their *utility*. These identities provide a remarkable variety of bounds, computational techniques, and sequence construction techniques which we have discussed in some detail in [86], [87], [94], [95], and [105].

As an example of sequence construction techniques, consider the following. For given x and y, (2.1) defines a mapping from $\mathbb{Z}$ into $\mathbb{C}$, that is, a complex-valued sequence. From (2.2), it is clear that this sequence (which we may denote by $\theta_{x,y}$) is periodic. We can thus interpret (2.10) to mean that the crosscorrelation *function* for the *sequences* $\theta_{w,y}$ and $\theta_{x,z}$ equals the crosscorrelation *function* for the *sequences* $\theta_{w,x}$ and $\theta_{y,z}$. Now, if w and x are uncorrelated sequences, (2.10) implies that $\theta_{w,y}$ and $\theta_{x,z}$ are also uncorrelated sequences for any other sequences y and z. Indeed, from (2.11) it is clear that y and z may be identical. Thus, starting from two uncorrelated sequences, we can produce two new uncorrelated sequences. Turning to (2.12), we interpret this identity to mean that the autocorrelation *function* for the *sequence* $\theta_{x,y}$ equals the crosscorrelation *function* for the *sequences* θ_x and θ_y. If x and y are sequences of period M with a two-valued autocorrelation function, then $\theta_{x,y}$ (and also $\theta_{y,x}$) is a sequence of period M with a two-valued autocorrelation function. For further details on such methods, see [105].

C. Bounds on Correlation Functions

Let us now discuss a variety of bounds on crosscorrelation and autocorrelation functions. We have already exhibited the bound (2.4) which we rewrite as

$$|\theta_{x,y}(l)| \leq [\theta_x(0)\theta_y(0)]^{1/2}. \tag{2.14}$$

If we apply the Cauchy inequality to the right-hand side of the correlation identity (2.13) we obtain [86]

$$\sum_{l=0}^{N-1} |\theta_{x,y}(l)|^2 \leq \left(\sum_{l=0}^{N-1} |\theta_x(l)|^2\right)^{1/2} \left(\sum_{l=0}^{N-1} |\theta_y(l)|^2\right)^{1/2}. \tag{2.15}$$

A tighter upper bound, as well as a lower bound, can be obtained if we first rewrite (2.13) as

$$\sum_{l=0}^{N-1} |\theta_{x,y}(l)|^2 = \theta_x(0)\theta_y(0) + \sum_{l=1}^{N-1} \theta_x(l)[\theta_y(l)]^* \tag{2.16}$$

and then apply the Cauchy inequality to the sum on the right-hand side of (2.16). We obtain [87]

$$\sum_{l=0}^{N-1} |\theta_{x,y}(l)|^2 \leq \theta_x(0)\theta_y(0) + \left(\sum_{l=1}^{N-1} |\theta_x(l)|^2\right)^{1/2} \left(\sum_{l=1}^{N-1} |\theta_y(l)|^2\right)^{1/2} \tag{2.17}$$

and

$$\sum_{l=0}^{N-1} |\theta_{x,y}(l)|^2 \geq \theta_x(0)\theta_y(0) - \left(\sum_{l=1}^{N-1} |\theta_x(l)|^2\right)^{1/2} \left(\sum_{l=1}^{N-1} |\theta_y(l)|^2\right)^{1/2} \tag{2.18}$$

The above discussion provides bounds on the mean-square values of correlation functions. Maximum values of these functions can be bounded in a similar fashion. For a set $\mathfrak{X}$ of periodic sequences define θ_c, the *peak crosscorrelation magnitude*, by

$$\theta_c = \max \{|\theta_{x,y}(l)|: 0 \leq l \leq N-1, x \in \mathfrak{X}, y \in \mathfrak{X}, x \neq y\} \tag{2.19}$$

and θ_a, the *peak out-of-phase autocorrelation magnitude*, by

$$\theta_a = \max \{|\theta_x(l)|: 1 \leq l \leq N-1, x \in \mathfrak{X}\}. \tag{2.20}$$

In [95] it is shown that if $\mathfrak{X}$ contains K sequences then

$$\left(\frac{\theta_c^2}{N}\right) + \frac{N-1}{N(K-1)}\left(\frac{\theta_a^2}{N}\right) \geq 1. \tag{2.21}$$

The special case $K = 2$ of (2.21) can be found in [115] and [87]. Note that (2.21) implies

$$\theta_{\max} \triangleq \max \{\theta_a, \theta_c\} \geq N\left[\frac{K-1}{NK-1}\right]^{1/2} \tag{2.22}$$

which is a result due to Sidelnikov [108] and Welch [129].

For further details, for tighter bounds in the case $K > N$, and for sequences satisfying these bounds with equality see [95], [101], [108], and [129].

Finally, we remark that in stating these bounds, we have not restricted the periods of the sequences in any way (other than the implicit restriction that all periods are divisors of N). Although the bounds are valid in general, they are not particularly useful unless all of the sequences have period N. For example, if any of the sequences in the set $\mathfrak{X}$ has period less than N, then $\theta_a = N$. This changes (2.21) into the rather disappointing $\theta_c^2 \geqslant 1 - N(N-1)/(K-1)$, which is a trivial lower bound for most values of N and K of interest.

D. Fourier Transforms

Given the periodic sequence x, we define its discrete Fourier transform (DFT) to be the sequence X which is given by

$$X_k = \frac{1}{N} \sum_{i=0}^{N-1} x_i \exp(-j 2\pi ki/N), \qquad k \in \mathbf{Z} \tag{2.23}$$

where $j = \sqrt{-1}$. The sequence x is called the inverse DFT of X and we have

$$x_i = \sum_{k=0}^{N-1} X_k \exp(j 2\pi ki/N), \qquad i \in \mathbf{Z}. \tag{2.24}$$

As we mentioned earlier, one can think of the crosscorrelation function $\theta_{x,y}(\cdot)$ as a periodic sequence. Let $\Theta_{x,y}(\cdot)$ denote the DFT of $\theta_{x,y}(\cdot)$. It is well known [13] that

$$\Theta_{x,y}(k) = NX_{-k}(Y_{-k})^* \tag{2.25}$$

and

$$\Theta_x(k) = N|X_{-k}|^2$$

where Y is the DFT of y. This can be used to provide an alternative proof of the correlation identities (2.10)–(2.13). For example, the left-hand side of (2.10) defines the nth element of a sequence u (say) and the right-hand side defines the nth element of a sequence v. U and V, the DFT's of u and v, are easily computed via (2.25) and we have

$$\begin{aligned} U_k &= N\Theta_{w,y}(-k)[\Theta_{x,z}(-k)]^* \\ &= N[NW_kY_k^*][NX_kZ_k^*]^* \\ &= N[NW_kX_k^*][NY_kZ_k^*]^* \\ &= N\Theta_{w,x}(-k)[\Theta_{y,z}(-k)]^* \\ &= V_k. \end{aligned}$$

Hence, $u = v$, which establishes (2.10). The proof of (2.10) that is given in [87] involves changing the order of summation several times, and is equally simple.

III. Binary Maximal-Length Sequences

The mathematical study of maximal-length sequences (m-sequences) seems to have started in the mid-1950's. According to Golomb [41], the theory of m-sequences was being developed and applied around this time by Gilbert, Golomb, Welch, and Zierler. The details of this theory have been well documented by Golomb [41], Selmer [104], and Zierler [134], and in the recent survey by MacWilliams and Sloane [69]. Much of the early research was concerned with the autocorrelation properties and the "noise-like" aspects of m-sequences. However, some attention was given to the problem of selecting sets of m-sequences with good crosscorrelation properties and by the late 1960's several theoretical and experimental results were known. Even at the present time, however, the key crosscorrelation properties of m-sequences are considerably less widely known than the autocorrelation properties, and yet the former are more important in many applications. Here, we shall assume that the reader is familiar with m-sequences and their basic properties (some of which are stated in Section III-B), and we shall concentrate on the crosscorrelation properties. In this section, we shall restrict attention to binary sequences. This is primarily because binary sequences are more commonly employed in communications and related applications than nonbinary sequences. In addition, the restriction to binary sequences simplifies much of the discussion in this section. The reader interested in the crosscorrelation properties of nonbinary m-sequences will find almost all of the known results in [45].

A. Properties of Binary Shift-Register Sequences

Let $h(x) = h_0x^n + h_1x^{n-1} + \cdots + h_{n-1}x + h_n$ denote a binary polynomial of degree n where $h_0 = h_n = 1$ and the other h_i's take on values 0 and 1. It is convenient and conventional to represent such a polynomial by a binary vector $h = (h_0, h_1, \cdots, h_n)$, and to express this vector in octal notation (see e.g., [79], [84]). For example, the polynomials $x^4 + x + 1$ and $x^5 + x^2 + 1$ are represented by the binary vectors 10011 and 100101, respectively, and the octal notation for these polynomials is 23 and 45, respectively. A binary sequence u is said to be a *sequence generated by* $h(x)$ if for all integers j

$$h_0u_j \oplus h_1u_{j-1} \oplus h_2u_{j-2} \oplus \cdots \oplus h_nu_{j-n} = 0. \tag{3.1}$$

Here $\oplus$ denotes addition modulo 2 (i.e., the EXCLUSIVE-OR operation). Replacing j by $j+n$ in (3.1), and using the fact that $h_0 = 1$, we obtain

$$u_{j+n} = h_nu_j \oplus h_{n-1}u_{j+1} \oplus \cdots \oplus h_1u_{j+n-1}.$$

From this it follows that the sequence u can be generated by an n-stage binary linear feedback shift register which has a feedback tap connected to the ith cell if $h_i = 1$, $0 < i \leqslant n$. Since $h_n = 1$, there is always such a connection for the nth cell. For example, the shift register in Fig. 1(a) corresponds to $h(x) = x^5 + x^2 + 1$ while that in Fig. 1(b) corresponds to $h(x) = x^5 + x^4 + x^3 + x^2 + 1$ (i.e., the polynomial 75). Note that the cells are numbered from right to left.

A shift register can generate several different sequences, one of which is the all-zeros sequence. Of course, only the nonzero sequences are of interest and henceforth we shall reserve u to denote a nonzero solution to (3.1). The following properties of shift register sequences are well known. If u is a sequence generated by $h(x)$, then for all integers i, T^iu is also a sequence generated by $h(x)$; that is, different phases of the same sequence can be generated by the same shift register. Similarly, if u and v are generated by $h(x)$, then so is $u \oplus v$, where $u \oplus v$ denotes the sequence whose ith element is $u_i \oplus v_i$. Finally, the period of u is at most $2^n - 1$, where n is the number of cells in the shift register, or equivalently, the degree of $h(x)$.

In most practical applications, a binary sequence is actually transmitted as a sequence of unit amplitude, positive and negative pulses. This pulse sequence is obtained by replacing each 1 by a −1 and each 0 by a +1 in the original sequence. Conventionally, such pulse sequences are also called binary sequences since they are two-valued. Since it is sometimes necessary to distinguish between a $\{0, 1\}$-valued binary sequence and the

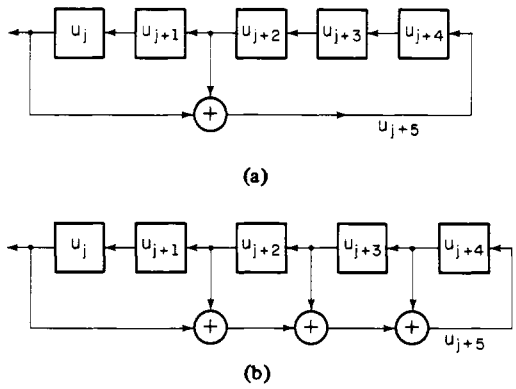

Fig. 1. Maximal-length linear feedback shift-registers. (a) Shift-register polynomial $x^5 + x^2 + 1$ (octal representation 45). (b) Shift-register polynomial $x^5 + x^4 + x^3 + x^2 + 1$ (octal representation 75).

corresponding $\{+1, -1\}$-valued binary sequence, we introduce the function $\chi(\cdot)$ defined by $\chi(0) = +1$, $\chi(1) = -1$ or equivalently $\chi(\alpha) = (-1)^\alpha$ for $\alpha \in \{0, 1\}$. If u denotes an arbitrary $\{0, 1\}$-valued sequence, then $\chi(u)$ denotes the corresponding $\{+1, -1\}$-valued sequence, where the ith element of $\chi(u)$ is just $\chi(u_i)$. Clearly, if u is of period N, then so is $\chi(u)$. We can think of u and $\chi(u)$ as being generated (in the sense of Section II-A) by the vectors u and $\chi(u)$ of length N. Notice that $T^i(\chi(u)) = \chi(T^i u)$ and

$$\Sigma\chi(u) = \chi(u_0) + \chi(u_1) + \cdots + \chi(u_{N-1}) = N - 2wt(u) \tag{3.2}$$

where $wt(u)$ denotes the Hamming weight of u, that is, the number of ones in u.

Since binary sequences u and v are conventionally implemented as the sequences $\chi(u)$ and $\chi(v)$, the correlation functions of $\chi(u)$ and $\chi(v)$ are the ones that normally arise in system analyses. It is conventional to define the periodic cross-correlation function $\theta_{u,v}(\cdot)$ to be equal to $\theta_{\chi(u),\chi(v)}(\cdot)$. Thus we have

$$\begin{aligned}\theta_{u,v}(l) \triangleq \theta_{\chi(u),\chi(v)}(l) &= \sum_{i=0}^{N-1} \chi(u_i)\chi(v_{i+l}) \\ &= \sum_{i=0}^{N-1} (-1)^{u_i}(-1)^{v_{i+l}} \\ &= \sum_{i=0}^{N-1} (-1)^{u_i \oplus v_{i+l}} \\ &= \sum_{i=0}^{N-1} \chi(u_i \oplus v_{i+l}).\end{aligned}$$

Applying (3.2), we get

$$\theta_{u,v}(l) = N - 2wt(u \oplus T^l v). \tag{3.3}$$

Let A_l denote the number of places in which the vectors u and $T^l v$ agree. Obviously this is the same as the number of places in which the vectors $\chi(u)$ and $T^l(\chi(v))$ agree. Then $D_l = N - A_l$ is the number of places in which the vectors u and $T^l v$ (or $\chi(u)$ and $T^l(\chi(v))$) differ. It is easy to see that $D_l = wt(u \oplus T^l v)$, and we have

$$\theta_{u,v}(l) = A_l - D_l.$$

This alternative expression for $\theta_{u,v}(l)$ is quite common in the engineering literature. It is very useful because it can be applied for either of the two binary alphabets, $\{0, 1\}$ or $\{+1, -1\}$.

The periodic autocorrelation function $\theta_u(\cdot)$ is just $\theta_{u,u}(\cdot)$ and we have

$$\theta_u(l) = N - 2wt(u \oplus T^l u). \tag{3.4}$$

The correlation functions for binary sequences have all the properties discussed in Section II. In addition, note that $\theta_{u,v}(l)$ is always an integer, and this integer is odd (even) if N is odd (even).

B. Properties of Binary Maximal-Length Sequences

The period of a sequence u generated by the polynomial $h(x)$ cannot exceed $2^n - 1$ where n is the degree of $h(x)$. If u has this maximal period $N = 2^n - 1$, it is called a maximal-length sequence or m-sequence, and $h(x)$ is called a primitive binary polynomial of degree n. This definition is equivalent to an alternative definition [41] based on "randomness properties." The m-sequence u enjoys the following well-known properties.

Property I: The period of u is $N = 2^n - 1$.

Property II: There are exactly N nonzero sequences generated by $h(x)$, and they are just the N different phases of u; namely $u, Tu, T^2u, \cdots, T^{N-1}u$.

Property III: Given distinct integers i and j, $0 \leq i, j < N$, there is a unique integer k, distinct from both i and j, such that $0 \leq k < N$ and

$$T^i u \oplus T^j u = T^k u.$$

A sequence of period N is an m-sequence if and only if it has Property III [41], [134], which is commonly known as the shift-and-add property. As before let u denote the binary vector of length N which generates u in the sense of Section II-A.

Property IV: $wt(u) = 2^{n-1} = \frac{1}{2}(N + 1)$.

Properties III and IV together with (3.4) give the following well known property.

Property V:

$$\theta_u(l) = \begin{cases} N, & \text{if } l \equiv 0 \bmod N \\ -1, & \text{if } l \not\equiv 0 \bmod N. \end{cases}$$

Thus binary m-sequences have two-valued autocorrelation functions.

Among the N sequences generated by $h(x)$ there is exactly one which has Property VI below. This unique sequence [134], which we denote by $\tilde{u}$, is called a *characteristic* m-sequence, or the *characteristic phase* of the m-sequence u. As before, u will continue to denote an arbitrary nonzero sequence generated by $h(x)$.

Property VI: $\tilde{u}_i = \tilde{u}_{2i}$ for all $i \in \mathbb{Z}$.

Let q denote a positive integer, and consider the sequence v formed by taking every qth bit of u (i.e., $v_i = u_{qi}$ for all $i \in \mathbb{Z}$). The sequence v is said to be a *decimation* by q of u, and will be denoted by $u[q]$. Let gcd (a, b) denote the greatest common divisor of the integers a and b.

Property VII: Assume that $u[q]$ is not identically zero. Then, $u[q]$ has period $N/\text{gcd}(N, q)$, and is generated by the polynomial $\hat{h}(x)$ whose roots are the qth powers of the roots of $h(x)$.

Since Property VII may be unfamiliar to some readers (it is not discussed in [69], for example), we give a simple illustration of how to use tables of polynomials to find $\hat{h}(x)$ for a

given $h(x)$ and decimation q. Let $n = 6$ and $N = 63$. A table of binary polynomials [79, appendix C] contains the following entry

DEGREE 6 1 103 *F* 3 127 *B* 5 147 *H* 7 111 *A*
9 015 11 155 *E* 21 007

The letters *E*, *F*, and *H* mean (among other things) that the polynomials 103, 147, and 155 are primitive while *A* and *B* indicate nonprimitive polynomials. Now suppose that the *m*-sequence u is generated by the polynomial 103. Then, $u[3]$ is generated by the polynomial 127. $u[5]$ is generated by 147, $u[7]$ is generated by 111, etc. According to Property VII, $u[3]$ has period $63/\gcd(63,3) = 21$, and thus is not an *m*-sequence; while $u[5]$ has period 63 and is an *m*-sequence. The corresponding polynomials 127 and 147 are clearly indicated as nonprimitive and primitive, respectively.

Clearly, $v = u[q]$ has period N if and only if $\gcd(N, q) = 1$. In this case, the decimation is called a *proper* decimation, and the sequence v is an *m*-sequence of period N generated by the primitive binary polynomial $\hat{h}(x)$. We remark that if, instead of u, we decimate $T^i u$ by q, we will get some phase $T^j v$ of v; that is, regardless of which of the *m*-sequences generated by $h(x)$ we choose to decimate, the result will be an *m*-sequence generated by $\hat{h}(x)$. In particular, decimating $\tilde{u}$, the characteristic phase of u, gives $\tilde{v}$, the characteristic phase of v.

What *m*-sequences do we get upon properly decimating u by q? First note that we need only consider values of q less than N since $u[q] = u[q \bmod N]$. Clearly, $u[1] = u$. Now, from Property VI it is clear that $\tilde{u}[2] = \tilde{u}$. Hence, $u[2] = T^k u$ for some k, from which it can be shown [134] that $\tilde{u} = T^{2k} u$. More generally, $\tilde{u}[2^j] = \tilde{u}$ and we get that $u[2^j] = T^i u$ for some i which depends on j. This result can be generalized further as follows.

Property VIII: Suppose $\gcd(N, q) = 1$. If $v = u[q]$, then for all $j \geq 0$,

$$\tilde{u}[2^j q] = \tilde{u}[2^j q \bmod N] = \tilde{v}$$

and

$$u[2^j q] = u[2^j q \bmod N] = T^i v$$

for some i which depends on j.

Property VIII is also valid for $j < 0$ provided $2^j q$ is an integer. Hence, proper decimation by odd integers q gives all of the *m*-sequences of period N. However, the following decimation by an even integer is of interest. Let $v = u[N - 1]$. Then $v_t = u_{(N-1)t} = u_{-t}$, that is v is just a reciprocal of u as defined in Section II-A. Note that u need not be in characteristic phase. The *m*-sequence v is generated by the *reciprocal polynomial* of $h(x)$, that is, $\hat{h}(x) = x^n h(x^{-1}) = h_n x^n + h_{n-1} x^{n-1} + \cdots + h_0$. From Property VIII we see that a different phase of v is produced if we decimate u by $\frac{1}{2}(N - 1) = 2^{n-1} - 1$ instead of $(N - 1)$. Other proper decimations lead to other *m*-sequences. We illustrate some of these by the following examples.

Example 1: Let $n = 5$ and $N = 31$. Since N is a prime, $\gcd(N, q) = 1$ for all q, $1 \leq q \leq N - 1$. Thus every decimation will give an *m*-sequence. The table in [79] contains the entry

DEGREE 5 1 45 *E* 3 75 *G* 5 67 *H*

If u is an *m*-sequence generated by the polynomial 45, then $v = u[3]$ is generated by the polynomial 75, as are $u[6]$, $u[12]$, $u[24]$, and $u[17]$, which are just different phases of v. Similarly, $w = u[5]$ is generated by the polynomial 67, as are

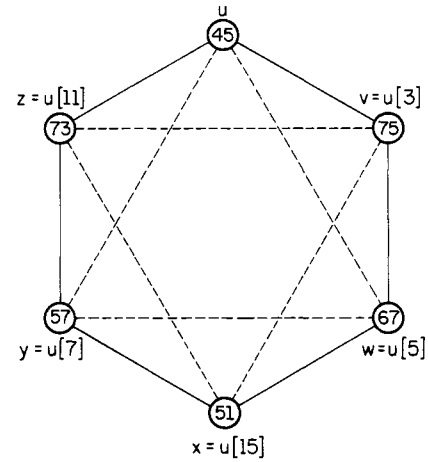

Fig. 2. Decimation relations for *m*-sequences of period 31. When traversed clockwise, solid lines and dotted lines correspond to decimations by 3 and 5, respectively.

$u[10]$, $u[20]$, $u[9]$, and $u[18]$, which are just different phases of w. Next, let us consider $y = u[7]$ as well as $u[14]$, $u[28]$, $u[25]$, and $u[19]$, all of which are generated by the same primitive polynomial. The table contains no entry corresponding to 7, so a little manipulation is necessary to find the polynomial. Note that $u_{14t} = u_{(14+31)t} = u_{45t} = u_{15(3t)} = v_{15t}$ since $v = u[3]$. Since $15 = \frac{1}{2}(N - 1)$, we find that $v[15]$ is generated by the *reciprocal* of polynomial 75 which is 57. Hence, y is generated by the polynomial 57. Similarly, consider $z = u[11]$, as well as $u[22]$, $u[13]$, $u[26]$, and $u[21]$, which are all generated by the same polynomial. But, $u_{13t} = u_{(13+62)t} = u_{75t} = u_{15(5t)} = w_{15t}$; i.e., $u[13] = w[15]$, and hence z is generated by the reciprocal of polynomial 67 which is 73. Lastly, $x = u[15]$ as well as $u[30]$, $u[29]$, $u[27]$, and $u[23]$ are all generated by the reciprocal of polynomial 45 which is 51. What about decimations of the other *m*-sequences? Some results were obtained in the course of the above discussion, for example $v[15] = u[14] = y[2]$. Next note that $v[3]$ is just $u[9]$ which, as we found above, is generated by the polynomial 67, while $v[5]$ is just $u[15]$ and is generated by the polynomial 51. Continuing in this manner, we can find the results of decimating all six sequences u, v, w, x, y, z by all possible integers q. These relationships are summarized in Fig. 2 where the six primitive binary polynomials of degree 5 are marked on the vertices of the hexagon. Each side of the hexagon corresponds to a decimation by 3 if traversed clockwise, and to a decimation by 11 if traversed counterclockwise. Thus, if an *m*-sequence generated by the polynomial 51 is decimated by 3 we get an *m*-sequence generated by the polynomial 57; while if it is decimated by 11, we get an *m*-sequence generated by the polynomial 67. The dotted lines correspond to decimation by 5 if traversed clockwise and 7 if traversed counterclockwise. Finally, traversing a diameter (these are not drawn on the figure) corresponds to decimation by 15, which, as we have discussed above, gives a reciprocal sequence.

The next example is included primarily to illustrate nonproper decimations (i.e., decimations by q where $\gcd(N, q) > 1$).

Example 2: Let $n = 6$ and $N = 63$. The polynomials of degree 6 were listed earlier. The reader may verify by calculations similar to those in Example 1 that if u denotes an *m*-sequence generated by the polynomial 103, then $v = u[5]$, $w = u[11]$,

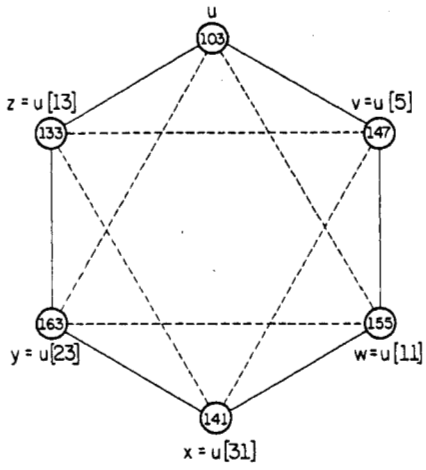

Fig. 3. Decimation relations for m-sequences of period 63. When traversed clockwise, solid lines and dotted lines correspond to decimations by 5 and 11, respectively.

$x = u[31]$, $y = u[23]$, and $z = u[13]$ are generated by the polynomials 147, 155, 141, 163, and 133, respectively. The relationships between these m-sequences are summarized on Fig. 3 which superficially is very similar to Fig. 2. However, each side of the hexagon now corresponds to decimation by 5 clockwise and 13 counterclockwise, while each dotted line corresponds to decimation by 11 clockwise and 23 counterclockwise. The unmarked diameters correspond to decimation by 31 which produces a reciprocal sequence. Let us now consider nonproper decimations.

Decimation by 7: According to Property VII, $u[7]$ has period 9 and is generated by the polynomial 111. Decimating any other phase of u by 7 will also give a sequence of period 9 generated by the polynomial 111, *but* this sequence *need not* be some phase of $u[7]$. In order to show this, for $0 \leqslant i < 7$, let $b^{(i)}$ denote the sequence obtained by decimating $T^i\tilde{u}$ by 7, where $\tilde{u}$ is the characteristic phase of u. The corresponding vectors $b^{(i)}$ (which, we take to be vectors of length 63 rather than 9) are easily found. Note that

$$b^{(0)} = (\tilde{u}_0, \tilde{u}_7, \tilde{u}_{14}, \cdots, \tilde{u}_{56}, \tilde{u}_{63}, \tilde{u}_{70}, \cdots, \tilde{u}_{434})$$
$$= (\tilde{u}_0, \tilde{u}_7, \tilde{u}_{14}, \cdots, \tilde{u}_{56}, \tilde{u}_0, \tilde{u}_7, \cdots, \tilde{u}_{56}).$$

Similarly,

$$b^{(1)} = (\tilde{u}_1, \tilde{u}_8, \tilde{u}_{15}, \cdots, \tilde{u}_{57}, \tilde{u}_1, \tilde{u}_8, \cdots, \tilde{u}_{57})$$
$$b^{(2)} = (\tilde{u}_2, \tilde{u}_9, \tilde{u}_{16}, \cdots, \tilde{u}_{58}, \tilde{u}_2, \tilde{u}_9, \cdots, \tilde{u}_{58})$$
$$\vdots$$
$$b^{(6)} = (\tilde{u}_6, \tilde{u}_{13}, \tilde{u}_{20}, \cdots, \tilde{u}_{62}, \tilde{u}_6, \tilde{u}_{13}, \cdots, \tilde{u}_{62}).$$

It is easy to see that decimating $T^{7k+l}\tilde{u}$ by 7, where $k > 0$ and $0 \leqslant i < 7$, gives $T^k b^{(l)}$. Also, we can think of $\tilde{u}$ as being formed by the *interleaving* or interlacing of the seven sequences $b^{(0)}, b^{(1)}, \cdots, b^{(6)}$. What happens if we decimate the other m-sequences by 7? Note that $b^{(0)} = \tilde{u}[7] = \tilde{u}[14] = \tilde{u}[28] = \tilde{u}[56] = \tilde{u}[49] = \tilde{u}[35]$. Since $\tilde{v} = \tilde{u}[5]$, $\tilde{v}[7] = \tilde{u}[35] = b^{(0)}$. Similarly, $\tilde{w}[7] = \tilde{u}[77] = \tilde{u}[14] = b^{(0)}$. Continuing in this manner, we get that $\tilde{x}[7]$, $\tilde{y}[7]$, and $\tilde{z}[7]$ are all equal to $b^{(0)}$. Decimating other phases of these other m-sequences produces various phases of the sequences $b^{(l)}$, $0 \leqslant i < 7$. For example, decimating $T\tilde{v}$ by 7 results in the sequence $Tb^{(3)}$. The conclusion is that no matter which m-sequence of period 63 we choose to decimate by 7, the result is a sequence generated by the polynomial 111. Alternatively, every m-sequence of period 63 can be formed by interleaving appropriate phases of the seven sequences $b^{(l)}$, $0 \leqslant i < 7$.

Decimation by 3 and by 15: As we remarked earlier, $u[3]$ has period 21 and is generated by the nonprimitive polynomial 127. We define sequences $c^{(l)}$ analogously to the $b^{(i)}$'s; that is, $c^{(0)} = \tilde{u}[3]$, and $c^{(l)}$ is obtained by decimating $T^i\tilde{u}$ by 3. The corresponding vectors of length 63 are

$$c^{(0)} = (\tilde{u}_0, \tilde{u}_3, \tilde{u}_6, \cdots, \tilde{u}_{60})$$
$$c^{(1)} = (\tilde{u}_1, \tilde{u}_4, \tilde{u}_7, \cdots, \tilde{u}_{61})$$
$$c^{(2)} = (\tilde{u}_2, \tilde{u}_5, \tilde{u}_8, \cdots, \tilde{u}_{62})$$

and the result of decimating $T^{3k+l}\tilde{u}$ by 3 is just $T^k c^{(l)}$. Next, note that $c^{(0)} = \tilde{u}[3] = \tilde{u}[6] = \tilde{u}[12] = \tilde{u}[24] = \tilde{u}[48] = \tilde{u}[33]$. Hence decimating $\tilde{w} = \tilde{u}[11]$ by 3 gives $\tilde{u}[33] = c^{(0)}$, as does decimating $\tilde{y} = \tilde{u}[23]$. On the other hand, $\tilde{v} = u[5]$ and hence $\tilde{v}[3] = \tilde{u}[15] = \tilde{u}[60]$ which is just a reciprocal of $c^{(0)}$. Thus $\tilde{v}[3]$ is generated by the reciprocal of polynomial 127, which is 165. Upon working out the details, one can conclude that decimating any phase of u, w, or y by 3 gives sequences $c^{(0)}$, $c^{(1)}$, $c^{(2)}$ in some phase, while decimating them by 15 gives some phase of $d^{(0)}$, $d^{(1)}$, $d^{(2)}$ which are reciprocals of $c^{(0)}$, $c^{(1)}$, $c^{(2)}$, respectively. On the other hand, decimating any phase of v, x, or z by 3 gives some phase of $d^{(0)}$, $d^{(1)}$, $d^{(2)}$, while decimating them by 15 gives some phase of $c^{(0)}$, $c^{(1)}$, $c^{(2)}$.

Decimation by 9, by 27, and by 21: The sequence $u[9]$ has period 7 and is generated by the polynomial 015 (i.e., $x^3 + x^2 + 1$). This is a *primitive* polynomial of degree 3 which generates an m-sequence of period $2^3 - 1 = 7$. We obtain after some manipulation that any phase of u, w, or y when decimated by 9 gives some phase of e, an m-sequence generated by 015; while decimating v, x, or z by 9 gives some phase of f, an m-sequence generated by the *reciprocal* of $x^3 + x^2 + 1$, which is $x^3 + x + 1$. On the other hand, decimating u, w, or y by 27 gives some phase of f while decimating v, x, or z by 27 gives some phase of e. We will leave it to the reader to verify that decimation by 21 of any of the m-sequences of period 63 gives an m-sequence of period 3 generated by the polynomial $x^2 + x + 1$. One *caveat* is in order. Decimating certain phases of the m-sequences $u, v, \cdots, z$ by 9, 27, or 21 results in the all-zeros sequence which has period 1. Property VII is no longer applicable in such cases and all our statements above should be qualified to exclude such decimations.

This long example concludes our discussion of m-sequences *per se*. For many other interesting and useful properties of m-sequences, the reader is referred to [41], [69], [104], and [134].

C. Crosscorrelation Functions for Maximal-Length Sequences

Let u and v denote m-sequences of period $N = 2^n - 1$ and let $v = u[q]$. Many useful properties of the crosscorrelation function $\theta_{u,v}(\cdot)$ follow immediately from results stated earlier in this paper. We have that $\theta_{u,v}(l) = \theta_{u,v}(l + N)$ and $|\theta_{u,v}(l)| \leqslant N$ for all l. Furthermore, $\theta_{u,v}(l)$ is always an *odd* integer. In fact Helleseth [45] proves that for all l, $\theta_{u,v}(l) + 1$ is a multiple of 8 (that is, $\theta_{u,v}(l) \equiv -1 \bmod 8$), except when u and v are generated by reciprocal polynomials, in which case $\theta_{u,v}(l) + 1$ is a multiple of 4. From (2.5), (3.2), and Property IV, it fol-

lows that

$$\sum_{l=0}^{N-1} \theta_{u,v}(l) = +1. \tag{3.5}$$

Hence, for large N the *average* value of $\theta_{u,v}(\cdot)$ is very nearly zero. Similarly, Property V and the correlation identity (2.13) give

$$\sum_{l=0}^{N-1} [\theta_{u,v}(l)]^2 = N^2 + N - 1$$

$$= 2^{2n} - 2^n - 1. \tag{3.6}$$

Notice that (3.5) and (3.6) are independent of the decimation q; indeed these equations are valid even if $v = T^i u$ for some i. From (3.6), it follows that the *mean-square* value of $\theta_{u,v}(\cdot)$ is very nearly 2^n, and that $|\theta_{u,v}(l)|$ exceeds $2^{n/2} - 1$ for at least one value of l. The latter bound is quite weak. In Section IV, we show that a bound due to Sidelnikov [108] implies that for at least one integer l,

$$|\theta_{u,v}(l)| > -1 + 2^{(n+1)/2}. \tag{3.7}$$

Earlier, Kasami [52, theorem 13] proved (3.7) for odd n.

Let us now consider the crosscorrelation function of $\tilde{u}$ and $\tilde{v}$, the characteristic phases of u and v. Since $u = T^i \tilde{u}$ and $v = T^j \tilde{v}$ for some i and j, we see from (2.8) that

$$\theta(u, v)(l) = \theta(T^i \tilde{u}, T^j \tilde{v})(l)$$

$$= \theta(\tilde{u}, \tilde{v})(l - i + j).$$

Hence it suffices to study $\theta(\tilde{u}, \tilde{v})(\cdot)$ because, if necessary, we can always find $\theta(u, v)(\cdot)$ from $\theta(\tilde{u}, \tilde{v})(\cdot)$. This is very convenient because $\theta(\tilde{u}, \tilde{v})(\cdot)$ satisfies a relation similar to Property VI of m-sequences, namely,

$$\theta(\tilde{u}, \tilde{v})(l) = \theta(\tilde{u}, \tilde{v})(2l). \tag{3.8}$$

In order to verify this, it is convenient to use x_l and y_l to denote $\chi(\tilde{u}_l)$ and $\chi(\tilde{v}_l)$, respectively. Then,

$$\theta(\tilde{u}, \tilde{v})(l) = \sum_{i=0}^{N-1} x_i y_{i+l}$$

$$= x_0 y_l + \sum_{i=1}^{(N-1)/2} (x_i y_{i+l} + x_{i+(N-1)/2} y_{i+(N-1)/2+l}).$$

But $x_l = x_{2l}$ and $y_l = y_{2l}$. Hence,

$$\theta(\tilde{u}, \tilde{v})(l) = x_0 y_{2l} + \sum_{i=1}^{(N-1)/2} (x_{2i} y_{2i+2l} + x_{2l-1+N} y_{2l-1+N+2l})$$

$$= x_0 y_{2l} + \sum_{i=1}^{(N-1)/2} (x_{2i} y_{2i+2l} + x_{(2l-1)} y_{(2l-1)+2l})$$

$$= \sum_{i=0}^{N-1} x_i y_{i+2l}$$

$$= \theta(\tilde{u}, \tilde{v})(2l).$$

Obviously, equation (3.8) generalizes to

$$\theta(\tilde{u}, \tilde{v})(l) = \theta(\tilde{u}, \tilde{v})(2^j l) = \theta(\tilde{u}, \tilde{v})(2^j l \bmod N), \qquad \text{for all } j \geq 0.$$

It follows that in order to determine $\theta(\tilde{u}, \tilde{v})(\cdot)$ completely, it is sufficient to know the value of $\theta(\tilde{u}, \tilde{v})(l)$ for a few selected integers l. For example, if $N = 31$, knowing $\theta(\tilde{u}, \tilde{v})(l)$ for $l = 0, 1, 3, 5, 7, 11$, and 15, suffices to determine $\theta(\tilde{u}, \tilde{v})(l)$ for all l. This approach was taken by Gold and Kopitzke [39] in their experimental determination of crosscorrelation functions for m-sequences of periods up to 8191. Their tables give the values of $\theta(\tilde{u}, \tilde{v})(l)$ only for selected values of l. Furthermore, for each $N = 2^n - 1$, the Gold-Kopitzke tables tabulate $\theta(\tilde{u}, \tilde{v})(\cdot)$ for a fixed $\tilde{u}$ and all possible choices for $\tilde{v}$. This information is sufficient to find $\theta(\tilde{x}, \tilde{y})$ for any m-sequences $\tilde{x}, \tilde{y}$ by means of the following technique. First find the decimation of $\tilde{u}$ that produces $\tilde{x}$, and the decimation of $\tilde{x}$ that produces $\tilde{y}$. Suppose that $\tilde{x} = \tilde{u}[r]$ and $\tilde{y} = \tilde{x}[q]$, and let $\tilde{v} = \tilde{u}[q]$. Then,

$$\theta(\tilde{x}, \tilde{y})(rl) = \theta(\tilde{u}, \tilde{v})(l)$$

and

$$\theta(\tilde{x}, \tilde{y})(l) = \theta(\tilde{u}, \tilde{v})(r'l) \tag{3.9}$$

where $rr' \equiv 1 \bmod N$. As an illustration, consider the six m-sequences of period 31 whose decimation relations are diagramed in Fig. 2. If we wish to find $\theta(\tilde{w}, \tilde{z})(\cdot)$, we note that $\tilde{w} = \tilde{u}[5]$ and $\tilde{z} = \tilde{w}[15]$. Also, $\tilde{x} = \tilde{u}[15]$. Hence we have that $\theta(\tilde{w}, \tilde{z})(5l) = \theta(\tilde{u}, \tilde{x})(l)$ and $\theta(\tilde{w}, \tilde{z})(l) = \theta(\tilde{u}, \tilde{x})(25l)$. In this manner, we can obtain the crosscorrelation function for any pair of m-sequences of periods up to 8191 from the Gold-Kopitzke tables.

D. Crosscorrelation Spectra

For many applications it is not necessary to know the value $\theta_{u,v}(l)$ for each l. For instance it may be sufficient to have tight bounds on $|\theta_{u,v}(l)|$ or to know the set of values taken on by $\theta_{u,v}(l)$. Frequently, we do not need to know more than the set of crosscorrelation values together with the number of integers l $(0 \leq l < N)$ for which $\theta_{u,v}(l) = c$ for each c in this set. This is referred to as the *spectrum* of the crosscorrelation function $\theta_{u,v}$ or as the *crosscorrelation spectrum* for the pair of sequences (u, v). In many cases the crosscorrelation spectrum is much easier to evaluate than the crosscorrelation function if judicious use is made of analytical results such as those stated below. The spectrum is of course much easier to tabulate than the function.

Some general properties of crosscorrelation spectra are as follows. First, we see from (2.8) that the crosscorrelation spectrum for the pair (u, v) is the same as for the pair $(T^i u, T^j v)$. In particular for any m-sequences u and v, the crosscorrelation spectrum for (u, v) is the same as that for $(\tilde{u}, \tilde{v})$, the characteristic phases of (u, v). A second useful result is implicit in (3.9): the crosscorrelation spectrum for two m-sequences which are related through a given decimation q is the *same* as the crosscorrelation spectrum for any other pair of m-sequences related through the same decimation q. In short, the crosscorrelation *spectrum* depends *only* upon q and *not upon* the individual m-sequences. Furthermore, from (2.3) it can be seen that decimations q and q', where $qq' \equiv 1 \bmod N$ give rise to the same crosscorrelation spectrum.

What do such crosscorrelation spectra look like? First notice that (3.5) implies that $\theta_{u,v}(\cdot)$ must take on positive as well as negative values. According to Property V, an *autocorrelation* spectrum is *two valued*

$$N \text{ occurs } 1 \text{ time}$$

$$-1 \text{ occurs } N - 1 \text{ times.}$$

Golomb [41] has observed that if u and v are generated

different primitive polynomials, then $\theta_{u,v}(\cdot)$ takes on at least *three values* (for a proof, see [45]). Theorem 1 below exhibits specific decimations which produce three-valued crosscorrelation spectra except when n is a power of 2. This result is a composite one; various parts of it were proved by Gold [37], Kasami [51], [52], Solomon, and Welch (see [42] and [77]). It also occurs in a different guise in [53] and [70].

Theorem 1: Let u and v denote m-sequences of period $2^n - 1$. If $v = u[q]$, where either $q = 2^k + 1$ or $q = 2^{2k} - 2^k + 1$, and if $e = \gcd(n, k)$ is such that n/e is odd, then the spectrum of $\theta_{u,v}$ is three valued and

$$\begin{array}{lll} -1 + 2^{(n+e)/2} & \text{occurs } 2^{n-e-1} + 2^{(n-e-2)/2} & \text{times} \\ -1 & \text{occurs } 2^n - 2^{n-e} - 1 & \text{times} \\ -1 - 2^{(n+e)/2} & \text{occurs } 2^{n-e-1} - 2^{(n-e-2)/2} & \text{times.} \end{array}$$

Of course, the same spectrum is obtained if instead of $v = u[q]$, we let $u = v[q]$. Notice that if e is large, $\theta_{u,v}(l)$ takes on large values but only very few times while if e is small, $\theta_{u,v}(l)$ takes on smaller values more frequently. In most instances, small values of e are desirable. If we wish to have $e = 1$ then clearly n must be odd in order that n/e be odd. When n is odd, we can take $k = 1$ or $k = 2$ (and possibly other values of k as well), and obtain that $\theta(u, u[3])$, $\theta(u, u[5])$ and $\theta(u, u[13])$ all have the three-valued spectrum given in Theorem 1 (with $e = 1$). Suppose next that $n \equiv 2 \bmod 4$. Then, n/e is odd if e is even and a divisor of n. Letting $k = 2$, we obtain that $\theta(u, u[5])$ and $\theta(u, u[13])$ both have the three-valued spectrum given in Theorem 1 (with $e = 2$). To summarize the above, let us define $t(n)$ as

$$t(n) = 1 + 2^{\lfloor (n+2)/2 \rfloor} \tag{3.10}$$

where $\lfloor \alpha \rfloor$ denotes the integer part of the real number α. Then if $n \not\equiv 0 \bmod 4$, there exist pairs of m-sequences with three-valued crosscorrelation functions, where the three values are -1, $-t(n)$, and $t(n) - 2$.

A crosscorrelation function taking on these values is called a *preferred three-valued crosscorrelation function* and the corresponding pair of m-sequences (polynomials) is called a *preferred pair* of m-sequences (polynomials) [39]. We mention that decimations other than those specified by Theorem 1 can also lead to preferred three-valued crosscorrelation functions. Several examples of such decimations are given by Niho [77] who experimentally investigated crosscorrelation spectra for $n \leqslant 17$. On the basis of his data, Niho has conjectured that several decimations of the form $2^i + 2^j \pm 1$ also lead to preferred three-valued crosscorrelation functions [77].

Next consider the case where n is a multiple of 4 (i.e., $n \equiv 0 \bmod 4$). If $n = 2^i m$ where $m > 1$ is odd, then we must take e in Theorem 1 to be at least $2^i \geqslant 4$ in order to get a three-valued crosscorrelation spectrum. Thus Theorem 1 provides no preferred pairs of m-sequences, and Niho's results [77] reveal no counterexample to the conjecture that none exist when n is a multiple of 4. If n is a power of 2, then Theorem 1 cannot be used at all to construct three-valued correlation spectra, and no counterexample is known to the conjecture that none exist [45]. Curiously enough, when $n \equiv 0 \bmod 4$, there exist decimations which give *four-valued* spectra which are (in one sense at least) considerably better than the *three-valued* spectra. The following theorem due to Niho [77] gives the details.

Theorem 2: Let u and v denote m-sequences of period $2^n - 1$ where n is a multiple of 4. If $v = u[-1 + 2^{(n+2)/2}] = u[t(n) - 2]$, then $\theta_{u,v}$ has a four-valued spectrum and

$$\begin{array}{lll} -1 + 2^{(n+2)/2} & \text{occurs } (2^{n-1} - 2^{(n-2)/2})/3 & \text{times} \\ -1 + 2^{n/2} & \text{occurs } 2^{n/2} & \text{times} \\ -1 & \text{occurs } 2^{n-1} - 2^{(n-2)/2} - 1 & \text{times} \\ -1 - 2^{n/2} & \text{occurs } (2^n - 2^{n/2})/3 & \text{times.} \end{array}$$

Since $n \equiv 0 \bmod 4$, the best three-valued crosscorrelation spectrum provided by Theorem 1 has correlation magnitudes as large as $1 + 2^{(n+e)/2}$ where $e \geqslant 4$. The correlation magnitudes in Theorem 2 are bounded by $-1 + 2^{(n+2)/2} = t(n) - 2$, and are much smaller.

Next, let us suppose that u and v are reciprocal m-sequences (i.e., are generated by reciprocal polynomials). For this case, Dowling and McEliece [23] have shown that for all l,

$$|\theta_{u,v}(l)| \leqslant 2^{(n+2)/2}. \tag{3.11}$$

The fact that $\theta_{u,v}(l) + 1$ must be a multiple of 4 can be used to improve (3.11) slightly. When n is even, we obtain

$$-t(n) + 4 \leqslant \theta_{u,v}(l) \leqslant t(n) - 2.$$

When n is odd, the right-hand side of (3.11) is not an integer, and the improved bound, while being easy to compute for any given n, is a messy analytical expression that we prefer to omit. It is conjectured that the improved version of (3.11) is a tight bound. Niho [77] experimentally determined the crosscorrelation spectra for $n \leqslant 18$ and found that not only is the bound tight but also that $\theta_{u,v}$ takes on every integer value (congruent to -1 modulo 4) which satisfies the bound (3.11). Earlier Dowling and McEliece [23] had noted the occurrence of this phenomenon for $n \leqslant 8$. We remark that when n is even, the correlation magnitudes are bounded by $t(n) - 2$ which is slightly smaller than $t(n)$, the bound for preferred pairs of sequences. This, together with Theorem 2, clearly indicates that one should not necessarily insist on having three-valued spectra if the goal is to minimize the peak crosscorrelation.

Let θ_c (which was defined in (2.19)) denote the maximum crosscorrelation magnitude for a given pair of m-sequences u and v of period $2^n - 1$, $n \geqslant 3$. We summarize the results stated above as follows.

1) When n is odd, or when $n \equiv 2 \bmod 4$, $\theta_c = t(n)$ for preferred pairs of m-sequences.

2) When n is even, $\theta_c = t(n) - 2$ for reciprocal pairs of m-sequences.

3) When n is a multiple of 4, $\theta_c = t(n) - 2$ for the pairs of m-sequences specified in Theorem 2.

We remark that when n is odd, the bound (3.7), together with the fact that θ_c is an odd integer, implies that $\theta_c \geqslant t(n)$ for *any* pair of m-sequences. The preferred pairs thus achieve the minimum possible value of θ_c when n is odd. When n is even, the lower bound (3.7) is smaller than $t(n) - 2$ by a factor of approximately $\sqrt{2}$. On the basis of all the known analytical results [45], [77] and experimental data [39], [77], it can be conjectured that when n is even, the lower bound is weak, and that $\theta_c \geqslant t(n) - 2$ for *any* pair of m-sequences.

IV. Sets of Binary Sequences with Small Crosscorrelation

In the previous section, we gave many examples of pairs of sequences for which the periodic crosscorrelation function is relatively small in magnitude. However, for the vast majority of applications, more than two sequences are needed. For

TABLE I
SET SIZES AND CROSSCORRELATION BOUNDS FOR THE SETS OF ALL M-SEQUENCES AND FOR MAXIMAL CONNECTED SETS

n	$N = 2^n - 1$	Number of m-sequences	θ_c for set of all m-sequences	M_n	$t(n)$
3	7	2	5	2	5
4	15	2	9	0	9
5	31	6	11	3	9
6	63	6	23	2	17
7	127	18	41	6	17
8	255	16	95	0	33
9	511	48	113	2	33
10	1023	60	383	3	65
11	2047	176	287	4	65
12	4095	144	1407	0	129
13	8191	630	$\geqslant$ 703	4	129
14	16383	756	$\geqslant$ 5631	3	257
15	32767	1800	$\geqslant$ 2047	2	257
16	65535	2048	$\geqslant$ 4095	0	513

instance, large sets of sequences are needed for typical code-division multiple-access communications systems. It is not uncommon for thirty or more to be required, and for certain random access and hybrid systems the number of sequences required could easily exceed a few hundred.

In this section, we consider large sets of periodic sequences which have good periodic correlation as measured by the peak periodic correlation parameters θ_c and θ_a (defined in (2.19) and (2.20)). The sizes of these sets range from a small fraction of the period N (for m-sequences) to much larger than N (for Kasami sequences). All of the sequences discussed are derivable from m-sequences, and they can be generated by linear feedback shift registers of relatively short length compared with the period.

A. Maximal Connected Sets of m-Sequences

Our first topic is a natural extension of the concept of a preferred pair of m-sequences. Recall from the previous section that a preferred pair of m-sequences is a pair of m-sequences of period $N = 2^n - 1$ which has the preferred three-valued crosscorrelation function. The values taken on by the preferred three-valued crosscorrelation function are -1, $-t(n)$, and $t(n) - 2$, where

$$t(n) = 1 + 2^{\lfloor (n+2)/2 \rfloor}.$$

The pair of primitive polynomials that generate a preferred pair of m-sequences is called a preferred pair of polynomials. In discussions of the properties of preferred pairs (such as the one below) it makes no difference whether we consider the m-sequences themselves or the polynomials which generate them.

A connected set of m-sequences is a collection of m-sequences which has the property that each pair in the collection is a preferred pair. A largest possible connected set is called a *maximal connected set* [39] and the size of such a set is denoted by M_n. Gold and Kopitzke [39] have experimentally determined M_n for $5 \leqslant n \leqslant 13$. From the data in [77], it is also possible to find the values of M_n for $n \leqslant 16$. Note that $M_2 = M_1 = 0$ since there is only one m-sequence for each of the periods $2^2 - 1$ and $2^1 - 1$. Listed in Table I are the values of M_n and the peak periodic crosscorrelation magnitudes $t(n)$ for a maximal connected set for $3 \leqslant n \leqslant 16$. For purposes of comparison, Table I also lists the size of the set of *all* m-sequences of each period, and the peak periodic crosscorrelation magnitude θ_c for this set. As remarked earlier, it appears that preferred pairs do not exist when n is a multiple of 4; hence it is conjectured that $M_{4k} = 0$ not only for $k \leqslant 4$ but for all integers k. Note that Theorem 2 enables us to construct a pair of m-sequences with four-valued crosscorrelation function bounded by $t(n) - 2$ wherever n is a multiple of 4. Hence, the table gives $t(n)$ for these values of n as well.

To illustrate a procedure for constructing a maximal connected set, let us return to Example 1 in which we consider m-sequences of period 31. In the discussion following Theorem 1, we noted that when n is odd, both $\{u, u[3]\}$ and $\{u, u[5]\}$ are preferred pairs of m-sequences. Recall that on Fig. 2, the solid lines denote decimations by 3 while dotted lines denote decimations by 5. We redraw Fig. 2 as Fig. 4, and note that *every* line on Fig. 4 connects a preferred pair. There are no other preferred pairs (the pairs of polynomials *not* connected by lines on Fig. 4 are reciprocals of each other). Thus the problem of finding a maximal connected set is just the problem of finding a largest subset of the six vertices on Fig. 4 such that every pair of vertices from the subset is connected by a line. It is easy to see that $M_5 = 3$, and that each triangle on Fig. 4 corresponds to a maximal connected set. Notice that there are eight maximal connected sets, and that each m-sequence belongs to four of them. For example, the maximal connected sets containing u are $\{u, v, w\}$, $\{u, v, z\}$, $\{u, w, y\}$, and $\{u, y, z\}$.

This graphical analogy is quite useful in thinking about the problem of maximal connected sets. Consider a graph in which each vertex represents an m-sequence, and two vertices are connected by an edge if and only if the corresponding m-sequences are a preferred pair. In graph-theoretic terminology, a connected set is a clique, and a maximal connected set is a maximal clique. The problem of finding cliques is known to be intractable for graphs in general. In this application, however, the graphs are highly symmetric and generally very sparse, and the problem is easily solved.

Let us now consider m-sequences of period 63 which were discussed in Example 2. Since $n \equiv 2 \bmod 4$, both $\{u, u[5]\}$ and $\{u, u[13]\}$ are preferred pairs. It is easily verified from the data in [39] or [77] that decimation by 11, 23, or 31 does not give preferred pairs. The graph to be considered is thus Fig. 5. It is not possible to find a set of more than two

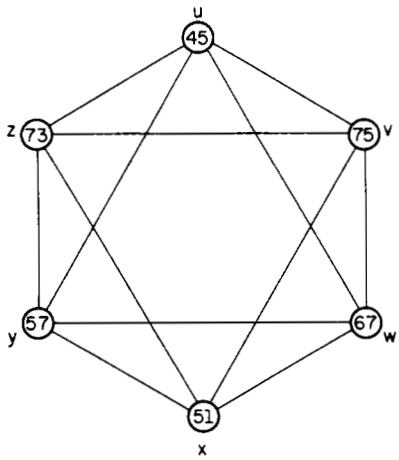

Fig. 4. Preferred pairs of m-sequences of period 31. The vertices of every triangle form a maximal connected set.

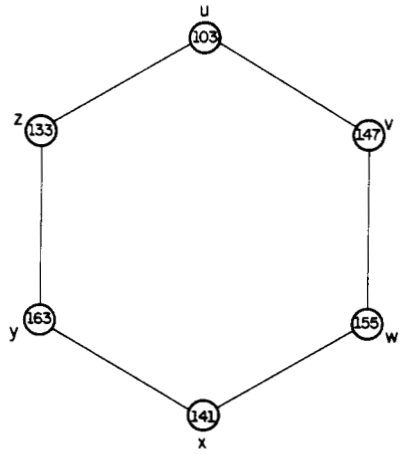

Fig. 5. Preferred pairs of m-sequences of period 63. Every pair of adjacent vertices is a maximal connected set.

vertices on Fig. 5 such that every pair of vertices from the set is connected by a line. Thus $M_6 = 2$, there are six maximal connected sets, and each m-sequence belongs to two of them. For example, the maximal connected sets containing w are $\{v, w\}$ and $\{w, x\}$.

Next, let us consider the eighteen m-sequences of period 127. Here $\{u, u[q]\}$ is a preferred pair for ten values of q, namely 3, 5, 9, 11, 13, 15, 23, 27, 29, and 43. We use Fig. 6 to illustrate these preferred pairs. The sides of the polygon in Fig. 6 correspond to decimation by 3 when traversed clockwise, and to decimation by 43 when traversed counterclockwise. The lines emanating from the vertex marked u indicate the ten preferred pairs that contain u. Note that similar sets of lines emanating from other vertices are not shown. Fig. 6 is also useful for exhibiting all the maximal connected sets. Every set of six consecutive vertices around the perimeter of the polygon is a maximal connected set. For example, {271, 367, 345, 221, 361, 375} is a maximal connected set of polynomials. There are eighteen maximal connected sets, and each m-sequence belongs to six of them.

Maximal connected sets of m-sequences are useful in those applications which require only a few sequences with excellent crosscorrelation and autocorrelation properties. However, most applications (such as spread-spectrum multiple-access communications, for example) require much larger sets of sequences. Unfortunately, large sets of m-sequences generally have quite poor crosscorrelation properties, and thus are inadequate for such applications. For example, a maximal connected set of m-sequences of period 127 contains six sequences and has peak periodic crosscorrelation magnitude $\theta_c = 17$. On the other hand, *any set* of seven or more such sequences has a relatively large peak periodic crosscorrelation value of $\theta_c = 41$. As another example, there are 48 m-sequences of period 511. A maximal connected set contains 2 m-sequences, and $\theta_c = 33$ for this set. On the other hand, *any set* containing 3 or more m-sequences must have $\theta_c \geq 55$. Similarly, there are 176 m-sequences of period 2047. A maximal connected set contains 4 sequences, and $\theta_c = 65$ for this set. On the other hand, any set containing 5 or more sequences must have $\theta_c \geq 113$. We remark that if the m-sequences are not carefully selected, peak periodic crosscorrelation magnitudes much larger than those quoted above can occur. The worst case peak periodic crosscorrelation magnitudes for m-sequences are given in Table I.

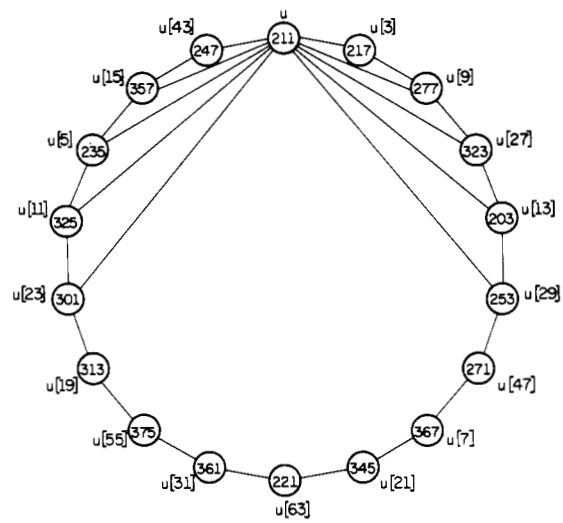

Fig. 6. Preferred decimations for m-sequences of period 127. Every set of six consecutive vertices is a maximal connected set.

As pointed out by these examples, only very small sets of m-sequences can have good periodic crosscorrelation properties. It is therefore desirable to obtain larger sets of sequences of period $N = 2^n - 1$ which have the same bound $\theta_c \leq t(n)$ on the peak periodic crosscorrelation as for the maximal connected sets. Since the larger sets must contain some non-maximal-length sequences, then their peak periodic autocorrelation θ_a must exceed 1.

B. Gold Sequences

One important class of periodic sequences which provides larger sets of sequences with good periodic crosscorrelation is the class of Gold sequences. A set of Gold sequences of period $N = 2^n - 1$, consists of $N + 2$ sequences for which $\theta_c = \theta_a = t(n)$. A set of Gold sequences can be constructed from appropriately selected m-sequences as described below.

Suppose a shift register polynomial $f(x)$ factors into $h(x)\hat{h}(x)$ where $h(x)$ and $\hat{h}(x)$ have no factors in common. Then the set of all sequences generated by $f(x)$ is just the set of all sequences of the form $a \oplus b$ where a is some sequence generated by $h(x)$, b is some sequence generated by $\hat{h}(x)$, and we do not make the usual restriction that a and b are nonzero sequences [134], [136]. Now suppose that $h(x)$ and $\hat{h}(x)$ are two dif-

ferent primitive binary polynomials of degree n that generate the m-sequences u and v, respectively, of period $N = 2^n - 1$. If y denotes a nonzero sequence generated by $f(x) = h(x)\hat{h}(x)$, then, from the above and Property II of m-sequences, we get that either

$$y = T^i u \tag{4.1}$$

or

$$y = T^j v \tag{4.2}$$

or

$$y = T^i u \oplus T^j v \tag{4.3}$$

where $0 \leqslant i, j \leqslant N - 1$, and where, as before, $T^i u \oplus T^j v$ denotes the sequence whose kth element is $u_{i+k} \oplus v_{j+k}$. From this it follows that y is some phase of some sequence in the set $G(u, v)$ defined by

$$G(u, v) \triangleq \{u, v, u \oplus v, u \oplus Tv, u \oplus T^2 v, \cdots, u \oplus T^{N-1} v\}. \tag{4.4}$$

Note that $G(u, v)$ contains $N + 2 = 2^n + 1$ sequences of period N. Next let us consider the crosscorrelation function for two distinct sequences $y, z \in G(u, v)$. Since both these sequences are generated by $f(x)$, so is the sequence $y \oplus T^l z$. If $y \oplus T^l z$ is of the form (4.1) or (4.2), we get from Property IV that $wt(y \oplus T^l z) = (N + 1)/2$, while if $y \oplus T^l z$ is of the form (4.3) then $wt(y \oplus T^l z) = wt(T^i u \oplus T^j v) = wt(u \oplus T^{j-i} v)$. Consequently, $\theta_{y,z}(l) = N - 2wt(y \oplus T^l z)$ either equals -1 or equals $N - 2wt(u \oplus T^{j-i} v) = \theta_{u,v}(j - i)$. A similar analysis can be carried out for the autocorrelation function $\theta_y(\cdot)$ and shows that the set of values taken on by the correlation functions for sequences in $G(u, v)$ is just the set of values taken on by the correlation functions for u and v. More importantly, the peak correlation parameters θ_c and θ_a for $G(u, v)$ satisfy

$$\theta_c = \theta_a = \max \{|\theta_{u,v}(l)| : 0 \leqslant l \leqslant N - 1\}. \tag{4.5}$$

In other words, given a pair of m-sequences u and v with peak periodic crosscorrelation magnitude M, we can construct a set of $N + 2$ sequences with peak periodic crosscorrelation magnitude and peak out-of-phase periodic autocorrelation magnitude equal to M.

In the late 1960's, Gold [35], [37], published the construction (4.4) and proved (4.5). In particular, he showed that if $\{u, v\}$ is *any* preferred pair of m-sequences then $G(u, v)$ has peak correlation parameters $\theta_c = \theta_a = t(n)$. In this case, the crosscorrelation functions for sequences belonging to $G(u, v)$ take on the three preferred values only. Gold also proved that if n is odd, then $\{u, u[2^k + 1]\}$ is a preferred pair of m-sequences, provided $\gcd(n, k) = 1$. This result is, of course, a special case of Theorem 1. At about the same time, Kasami [51], [52] proved Theorem 1 for all decimations of the form $q = 2^k + 1$. One implication of this result is that $\{u, u[t(n)]\}$ is a preferred pair of m-sequences whenever $n \not\equiv 0 \bmod 4$. Consequently, $G(u, u[t(n)])$ has peak correlation parameters $\theta_c = \theta_a = t(n)$, and the correlation functions for sequences in $G(u, u[t(n)])$ take on the preferred three values. In the literature following the pioneering work of Gold and Kasami, some authors have defined Gold sequences as the set $G(u, u[t(n)])$ only. While this has mnemonic value (the decimation and the correlation bound are both given by $t(n)$), it is clear [35, sec. IV] that $G(u, v)$ should be called a set of Gold sequences whenever $\{u, v\}$ is *any* preferred pair of m-sequences. We summarize the above discussion as follows.

Theorem 3: Let $\{u, v\}$ denote a preferred pair of m-sequences of period $N = 2^n - 1$ generated by the primitive binary polynomials $h(x)$ and $\hat{h}(x)$ respectively. Then the set $G(u, v)$ defined in (4.4) is called a set of Gold sequences. For $y, z \in G(u, v)$, $\theta_{y,z}(l) \in \{-1, -t(n), t(n) - 2\}$ for all integers l, and $\theta_y(l) \in \{-1, -t(n), t(n) - 2\}$ for all $l \not\equiv 0 \bmod N$. Every sequence in $G(u, v)$ can be generated by the polynomial $f(x) = h(x)\hat{h}(x)$. Note that the nonmaximal-length sequences belonging to $G(u, v)$ also can be generated by adding together (term by term, modulo 2) the outputs of the shift registers corresponding to $h(x)$ and $\hat{h}(x)$. The maximal-length sequences belonging to $G(u, v)$ are, of course, the outputs of the individual shift registers.

We now compare the parameter $\theta_{\max} = \max \{\theta_a, \theta_c\}$ for a set of Gold sequences to a bound due to Sidelnikov [108] which states that for any set of N or more *binary* sequences of period N

$$\theta_{\max} > (2N - 2)^{1/2}. \tag{4.6}$$

(Note that (2.22), which applies to *complex-valued* sequences in general, provides a much weaker lower bound on $\theta_{\max}$.) For $N = 2^n - 1$, equation (4.6) implies that

$$\theta_{\max} > -1 + 2^{(n+1)/2}. \tag{4.7}$$

When n is odd, the right-hand side of (4.7) equals $t(n) - 2$. Since $\theta_{\max}$ must be an odd integer, we obtain that for *any* set of N or more binary sequences of period $N = 2^n - 1$, n odd,

$$\theta_{\max} \geqslant t(n). \tag{4.8}$$

Since $\theta_{\max} = t(n)$ for Gold sequences, we conclude that they form an *optimal* set with respect to the bounds (4.6)–(4.8) when n is odd. When n is even, the right-hand side of (4.7) is not an integer, and is smaller than $t(n)$ by a factor of approximately $\sqrt{2}$. Although the bound itself probably is weak, Gold sequences are not optimal in this case. As discussed in Section III, reciprocal m-sequences, as well as the m-sequences of Theorem 2, have peak periodic crosscorrelation equal to $t(n) - 2$. Using such pairs of m-sequences in (4.4) gives sets of $N + 2$ sequences with $\theta_{\max} = t(n) - 2$ as compared to $\theta_{\max} = t(n)$ for Gold sequences. As a final remark, we note that a pair of m-sequences for which (3.7) is not satisfied implies the existence (via (4.4)) of a set of sequences for which (4.7) is not satisfied. Thus the Sidelnikov bound implies (3.7) as claimed earlier.

C. Gold-like and Dual-BCH Sequences

We now discuss two relatively unknown classes of sequences which have parameters very similar to those of Gold sequences. Both classes are obtained via the following construction. Let n be even and let q be an integer such that $\gcd(q, 2^n - 1) = 3$. Let u denote an m-sequence of period $N = 2^n - 1$ generated by $h(x)$, and let $v^{(k)}$, $k = 0, 1, 2$, denote the result of decimating $T^k u$ by q. Property VII of m-sequences implies that the $v^{(k)}$ are sequences of period $N' = N/3$ which are generated by the polynomial $\hat{h}(x)$ whose roots are qth powers of the roots of $h(x)$. From the theory of shift register sequences, if y denotes a nonzero sequence generated by $f(x) = h(x)\hat{h}(x)$, then either

$$y = T^i u \tag{4.9}$$

or

$$y = T^j v^{(k)} \tag{4.10}$$

or

$$y = T^i u \oplus T^j v^{(k)} \tag{4.11}$$

where $0 \leqslant i \leqslant N-1$, $0 \leqslant j \leqslant N'-1$, and $0 \leqslant k \leqslant 2$. Noting that sequences of the form (4.10) are of period $N/3$, we see that any sequence of period N generated by $f(x)$ is some phase of some sequence in the set $H_q(u)$ defined by

$$\begin{aligned} H_q(u) = \{&u, u \oplus v^{(0)}, u \oplus Tv^{(0)}, \cdots, u \oplus T^{N'-1}v^{(0)}, \\ &u \oplus v^{(1)}, u \oplus Tv^{(1)}, \cdots, u \oplus T^{N'-1}v^{(1)}, \\ &u \oplus v^{(2)}, u \oplus Tv^{(2)}, \cdots, u \oplus T^{N'-1}v^{(2)}\}. \end{aligned} \tag{4.12}$$

Note that $H_q(u)$ contains $N+1 = 2^n$ sequences of period N.

We apply this construction to exhibit sets of sequences that we call the Gold-like sequences. Suppose that u is an m-sequence of period $2^n - 1$ generated by $h(x)$. Then, according to Property VII of m-sequences, $u[t(n)]$ is generated by $\hat{h}(x)$, where the roots of $\hat{h}(x)$ are $t(n)$th powers of the roots of $h(x)$. In [35], Gold proved that for any sequence y generated by $f(x) = h(x)\hat{h}(x)$,

$$2^{n-1} - 2^{\lfloor n/2 \rfloor} \leqslant wt(y) \leqslant 2^{n-1} + 2^{\lfloor n/2 \rfloor}. \tag{4.13}$$

For $n \not\equiv 0 \bmod 4$, $\hat{h}(x)$ is a primitive polynomial and (4.1)–(4.4) are applicable. For the set $G(u, v)$ thus constructed, it is easy to show that (4.13) implies $\theta_{\max} = t(n)$. Indeed, in this case, $G(u, v)$ is a set of Gold sequences and the correlation functions take on the three preferred values -1, $-t(n)$ and $t(n) - 2$. For $n \equiv 0 \bmod 4$, $\gcd(t(n), 2^n - 1) = 3$ and consequently (4.9)–(4.12) must be used. However, (4.13) is still valid provided the vectors $v^{(k)}$ are taken to be of length N rather than $N/3$ (see Example 2). Consequently it can be shown that for the set $H_{t(n)}(u)$, $\theta_{\max} = t(n)$. We call $H_{t(n)}(u)$ a set of Gold-like sequences. The correlation functions for the sequences belonging to $H_{t(n)}(u)$ take on values in the set $\{-1, -t(n), t(n) - 2, -s(n), s(n) - 2\}$ where $s(n)$ is defined (for even n only) by

$$\begin{aligned} s(n) &= 1 + 2^{n/2} \\ &= \tfrac{1}{2}(t(n) + 1). \end{aligned} \tag{4.14}$$

The latter result is due to Kasami [51], [52]. We remark that *all* of Kasami's results are stated in terms of weight spectra; that is, in terms of the number of sequences y generated by $f(x)$ such that $wt(y) = i$ for $0 \leqslant i \leqslant N$. In presenting them here, we have rewritten them in terms of correlation spectra. For example, according to Theorem 11 of [52], the nonzero sequences generated by $f(x)$ have weights 2^{n-1} and $2^{n-1} \pm 2^{\lfloor n/2 \rfloor}$ when $n \not\equiv 0 \bmod 4$, while if $n \equiv 0 \bmod 4$, weights $2^{n-1} \pm 2^{\lfloor n/2 \rfloor - 1}$ also occur. Using (3.3) and (3.4), it is easy to see that the corresponding correlation values are as quoted above.

Dual-BCH sequences are generated by the polynomial $f(x) = h(x)\hat{h}(x)$ where $u[3]$ is generated by the polynomial $\hat{h}(x)$. When n is odd, $\hat{h}(x)$ is a primitive polynomial and (4.1)–(4.4) are applicable. The set $G(u, u[3])$ thus obtained is a set of Gold sequences since decimation by 3 is a preferred decimation when n is odd. When n is even, $\gcd(3, 2^n - 1) = 3$ and consequently (4.9)–(4.12) are applicable. For the set $H_3(u)$, $\theta_{\max} = t(n)$ and the correlation functions take on values in the set $\{-1, -t(n), t(n) - 2, -s(n), s(n) - 2\}$ [52]. The reason for the name dual-BCH is that the set $\{y : y$ is a sequence generated by $f(x)\}$ is the dual code of a double-error-correcting BCH code [9], [52], [70]. If we generalize this idea by considering the dual of a t-error-correcting BCH code, then a set of N^{t-1} or more sequences can be constructed for which

$$\theta_{\max} \leqslant 1 + (t-1)2^{(n+2)/2}.$$

Further details may be found in [4], [70], and [129].

D. Kasami Sequences

Let n be even and let u denote an m-sequence of period $N = 2^n - 1$ generated by $h(x)$. Consider the sequence $w = u[s(n)] = u[2^{n/2} + 1]$. It follows from Property VII that w is a sequence of period $2^{n/2} - 1$ which is generated by the polynomial $h'(x)$ whose roots are the $s(n)$th powers of the roots of $h(x)$. Furthermore, since $h'(x)$ can be shown to be a polynomial of degree $n/2$, w is an *m-sequence* of period $2^{n/2} - 1$. Now consider the sequences generated by the polynomial $h(x)h'(x)$ of degree $3n/2$. Clearly, any such sequence must be of one of the forms $T^i u$, $T^j w$, $T^i u \oplus T^j w$, $0 \leqslant i < 2^n - 1$, $0 \leqslant j < 2^{n/2} - 1$. Thus any sequence y of period $2^n - 1$ generated by $h(x)h'(x)$ is some phase of some sequence in the set $K_s(u)$ defined by

$$K_s(u) \triangleq \{u, u \oplus w, u \oplus Tw, \cdots, u \oplus T^{2^{n/2}-2}w\}. \tag{4.15}$$

We have called this set of sequences the *small set of Kasami sequences* in honor of Kasami who discovered that the correlation functions for sequences belonging to $K_s(u)$ take on values in the set $\{-1, -s(n), s(n) - 2\}$ [51], [52]. Consequently, for the set $K_s(u)$,

$$\begin{aligned} \theta_{\max} &= s(n) \\ &= 1 + 2^{n/2}. \end{aligned} \tag{4.16}$$

Notice that $\theta_{\max}$ for the set $K_s(u)$ is approximately one half of the value of $\theta_{\max}$ achieved by the sets of sequences discussed previously. On the other hand, $K_s(u)$ contains only $2^{n/2} = (N+1)^{1/2}$ sequences, while the sets discussed previously contain $N+1$ or $N+2$ sequences. We remark that Welch's bound (2.22) when applied to a set of $2^{n/2}$ sequences of period $2^n - 1$ implies that

$$\theta_{\max} > -1 + 2^{n/2}. \tag{4.17}$$

For *binary* sequences, the fact that $\theta_{\max}$ is an odd integer can be used to improve (4.17) to

$$\theta_{\max} \geqslant 1 + 2^{n/2}. \tag{4.18}$$

Comparing (4.16) and (4.18), we see that the small set of Kasami sequences is an optimal collection of binary sequences with respect to the bound (4.18). In fact, since (4.17) applies for complex-valued sequences, one cannot obtain values for $\theta_{\max}$ for complex-valued sequences that are significantly smaller than the value $s(n)$ which is achieved by the set $K_s(u)$ of binary sequences.

Now let $\hat{h}(x)$ denote the polynomial which generates the sequence $u[t(n)]$. As we noted earlier, the polynomial $h(x)\hat{h}(x)$ generates the set of Gold sequences $G(u, u[t(n)])$ if $n \not\equiv 0 \bmod 4$, while if $n \equiv 0 \bmod 4$, $h(x)\hat{h}(x)$ generates the set of Gold-like sequences $H_{t(n)}(u)$. Now all the sequences generated by $f(x) = h(x)\hat{h}(x)h'(x)$ are of the form $a \oplus b \oplus c$ where a, b, and c are generated by $h(x)$, $h(x)$ and $h'(x)$ respectively. In order to exhibit the sequences of period N generated by $f(x)$, we use the notation $z \oplus \mathfrak{T}$ (where z is a

sequence and $\mathfrak{X}$ a collection of sequences) to denote the set $\{z \oplus y : y \in \mathfrak{X}\}$.

Theorem 4: Let n be even and let $h(x)$ denote a primitive binary polynomial of degree n that generates the m-sequence u. Let $w = u[s(n)]$ denote an m-sequence of period $2^{n/2} - 1$ generated by the primitive polynomial $h'(x)$ of degree $n/2$, and let $\hat{h}(x)$ denote the polynomial of degree n that generates $u[t(n)]$. Then, the set of sequences of period N generated by $h(x)\hat{h}(x)h'(x)$, called the *large set of Kasami sequences* and denoted by $K_L(u)$, is as follows:

i) if $n \equiv 2 \bmod 4$, then

$$K_L(u) = G(u, v) \bigcup \left[\bigcup_{i=0}^{2^{n/2}-2} \{T^i w \oplus G(u, v)\} \right] \quad (4.19)$$

where $v = u[t(n)]$, and $G(u, v)$ is defined in (4.4).

ii) if $n \equiv 0 \bmod 4$, then

$$K_L(u) = H_{t(n)}(u) \bigcup \left[\bigcup_{i=0}^{2^{n/2}-2} \{T^i w \oplus H_{t(n)}(u)\} \right]$$

$$\bigcup \{v^{(j)} \oplus T^k w : 0 \leqslant j \leqslant 2,\ 0 \leqslant k < (2^{n/2} - 1)/3\} \quad (4.20)$$

where $v^{(j)}$ is the result of decimating $T^j u$ by $t(n)$ and $H_{t(n)}(u)$ is defined in (4.12). In either case, the correlation functions for $K_L(u)$ take on values in the set $\{-1, -t(n), t(n)-2, -s(n), s(n)-2\}$ and $\theta_{\max} = t(n)$. If $n \equiv 2 \bmod 4$, $K_L(u)$ contains $2^{n/2}(2^n + 1)$ sequences while if $n \equiv 0 \bmod 4$, $K_L(u)$ contains $2^{n/2}(2^n + 1) - 1$ sequences.

The large set of Kasami sequences contains both the small set of Kasami sequences and a set of Gold (or Gold-like) sequences as subsets. More interestingly, the correlation bound $\theta_{\max} = t(n)$ is the *same* as that for the latter subset. As a historical remark, we note that in an unpublished report Massey and Uhran [71], who were aware of Gold's results [35] but not of Kasami's results [51], [52], exhibited the sets of sequences that we have called the Gold-like sequences and the small and large sets of Kasami sequences. They also derived the bound on $\theta_{\max}$, but did not find the sets of values taken on by the correlation functions. In [96], we translated Kasami's results on weight spectra into results on correlation spectra, and first used the term Kasami sequence; later we discovered that some of these results were already known to Massey and Uhran [71].

E. Other Sets of Sequences

Thus far, we have discussed the construction of sets of sequences of period $2^n - 1$. For periods other than $2^n - 1$, the sizes of the sequence sets as well as the corresponding values of $\theta_{\max}$ vary considerably as a function of N (e.g., [7], [66]). For example McEliece [66] shows that one can obtain 3, 23, 45, and 11 sequences of periods 85, 89, 91, and 93, respectively. The corresponding values of $\theta_{\max}$ are 11, 23, 19, and 29. One very interesting general class in [66] is as follows. Let $n = 2m$, let u denote an m-sequence of period $2^n - 1$, and let $\hat{h}(x)$ denote the polynomial which generates $u[2^m - 1]$. Then $\hat{h}(x)$ is of degree $2m$ and it generates a set of $(2^m - 1)$ sequences of period $2^m + 1$ for which

$$\theta_{\max} \leqslant 1 + 2\lfloor 2^{m/2} - \tfrac{1}{2} \rfloor.$$

If m is even, this bound becomes $\theta_{\max} \leqslant t(m) - 2$. In this case, the parameters for this set of sequences are very similar to the parameters of the set $G(y, z)$ where y and z are reciprocal m-sequences of period $2^m - 1$ (m even). Note that $G(y, z)$ contains $2^m + 1$ sequences of period $2^m - 1$, while the set of sequences generated by $\hat{h}(x)$ contains $2^m - 1$ sequences of period $2^m + 1$. Each sequence set can be generated by a polynomial of degree $2m$, and $\theta_{\max} \leqslant t(m) - 2$ for each set.

F. Examples

For $N = 31$, 63, 65, 127, and 255, we consider specific polynomials that generate the various classes of sequences that have been discussed above.

Example 3: Consider the case $n = 5$, $N = 31$, and $t(n) = 9$. The preferred pairs of m-sequences of period 31 are exhibited in Fig. 4. According to Theorem 3, each preferred pair gives rise to a set of Gold sequences, and thus there are 12 different sets of Gold sequences of period 31. Each set contains 33 sequences, and the correlation functions for these sequences take on the values 7, −1, and −9. The sets $G(u, v)$, $G(v, w)$, $G(z, u)$, $G(u, w)$, $G(w, y)$, and $G(y, u)$ are generated by the polynomials 3551, 2303, 3667, 3013, 3735, and 2563, respectively, while $G(x, y)$, $G(y, z)$, $G(w, x)$, $G(x, z)$, $G(z, v)$, and $G(v, x)$, are generated by the respective *reciprocals* of these polynomials. Alternatively, it is possible to generate these sets by summing the sequences generated by two polynomials of degree 5. For example, $G(u, v)$ can be obtained by summing the sequences generated by the polynomials 45 and 75 (i.e., by the shift registers in Fig. 1).

Two distinct m-sequences of period 31 either form a preferred pair or are reciprocals of each other. In the latter case, one can use (4.4) to construct a set of 33 sequences whose correlation functions take on the six values 11, 7, 3, −1, −5, and −9 (see Section III-D). An example of such a set is $G(v, y)$ which is generated by the polynomial 3373. Note that $\theta_{\max} = 11$ for $G(v, y)$ while $\theta_{\max} = 9$ for all the Gold sequence sets.

Example 4: Consider the case $n = 6$, $N = 63$, $t(n) = 17$, and $s(n) = 9$. The preferred pairs of m-sequences of period 63 are exhibited in Fig. 5, and we see that there are 6 sets of Gold sequences. Each set contains 65 sequences of period 63, and the correlation functions for these sequences take on the values 15, −1, and −17. The sets $G(u, v)$, $G(w, x)$ and $G(y, z)$ are generated by the polynomials 14551, 13215, and 14375 while $G(x, y)$, $G(z, u)$, and $G(v, w)$ are generated by the respective reciprocals of these polynomials. Next suppose that we apply (4.4) to a pair of reciprocal m-sequences such as u and x. Since n is even, $\theta_{\max}$ for the set $G(u, x)$ equals 15 (see Section IV-B). In fact, the correlation functions take on all integer values congruent to −1 mod 4 in the range from −13 to +15. Since n is even, we can construct sets of dual-BCH sequences. Each such set has 64 sequences of period 63, and the correlation functions take on the values 15, 7, −1, −9, and −17. Now, in Example 2, we had found that decimating u, w, or y by 3 gives sequences $c^{(i)}$ generated by 127 while decimating v, x, or z by 3 gives sequences $d^{(i)}$ generated by 165. It follows that the dual-BCH sets $H_3(u)$, $H_3(w)$, and $H_3(y)$ are generated by the polynomials 12471, 16223, and 15251, respectively, while the sets $H_3(x)$, $H_3(z)$, and $H_3(v)$ are generated by the respective reciprocals of these polynomials.

Since n is even, we can also construct small and large sets of Kasami sequences. In Example 2, we saw that decimating u, w, or y by $s(n) = 9$ gives an m-sequence e of period 7 generated by 15, while decimating v, x, or z by 9 gives an m-sequence f generated by 13. Consequently, the small sets of Kasami se-

TABLE II
POLYNOMIALS GENERATING VARIOUS CLASSES OF SEQUENCES OF PERIODS 31, 63, 65, 127, AND 255

N	Polynomial	Const.	No.	Values taken on by the Correlation Functions	Remarks
31	3551	G	33	7, −1, −9	Gold sequences
	2373	G	33	11, 7, 3, −1, −5, −9	Reciprocal m-sequences
63	14551	G	65	15, −1, −17	Gold sequences
	14343	G	65	15, 11, 7, 3, −1, −5, −9, −13	Reciprocal m-sequences
	12471	H_3	64	15, 7, −1, −9, −17	Dual-BCH sequences
	1527	K_S	8	7, −1, −9	Small set of Kasami sequences
	133605	K_L	520	15, 7, −1, −9, −17	Large set of Kasami sequences
65	10761		63	15, 11, 7, 3, −1, −5, −9, −13	See Section IV-E
127	41567	G	129	15, −1, −17	Gold sequences
255	231441	G	257	31, 15, −1, −17	m-sequences of Theorem 2
	264455	G	257	31, ..., 15, 11, 7, 3, −1, −5, −9, −13, −17, ..., −29	Reciprocal m-sequences
	326161	H_{33}	256	31, 15, −1, −17, −33	Gold-like sequences
	267543	H_3	256	31, 15, −1, −17, −33	Dual-BCH sequences
	11367	K_S	16	15, −1, −17	Small set of Kasami sequences
	6031603	K_L	4111	31, 15, −1, −17, −33	Large set of Kasami sequences

quences $K_S(u)$, $K_S(w)$, and $K_S(y)$ are generated by the polynomials 1527, 1261, and 1047, respectively, while the sets $K_S(x)$, $K_S(z)$, and $K_S(v)$ are generated by the respective reciprocal polynomials. Each small set of Kasami sequences contains 8 sequences for which the correlation functions take on the values 7, −1, and −9. Similarly, the large sets of Kasami sequences $K_L(u)$, $K_L(w)$, and $K_L(y)$ are generated by the polynomials 133605, 174321, and 136341, respectively, while $K_L(x)$, $K_L(z)$, and $K_L(v)$ are generated by the respective reciprocal polynomials. Each set contains 520 sequences for which the correlation functions take on the values 15, 7, −1, −9, and −17.

Example 5: Let $n = 2m = 12$, and let u denote an m-sequence of period $2^n - 1 = 4095$. As described in Section IV-E, $u[63]$ is a sequence of period 65 which is generated by the polynomial $\hat{h}(x)$ of degree 12. It can be shown that regardless of which of the 144 m-sequences of period 4095 is taken to be u, $\hat{h}(x)$ must be one of the four polynomials 10761, 12345, 13535, and 15353. Each of these four polynomials generates a set of 63 sequences of period 65. According to the data in [7], the correlation functions for these sequences take on values congruent to −1 mod 4 in the range from −13 to +15, and thus $\theta_{\max} = t(m) - 2 = 15$. A closely comparable set of sequences is the set $G(u, x)$ of the previous example.

Example 6: Let $n = 7$, $N = 127$, and $t(n) = 17$. There are 90 preferred pairs of m-sequences of period 127, and consequently 90 sets of Gold sequences. Each set contains 129 sequences and the correlation functions for these sequences take on the values 15, −1, and −17. Analogously to Examples 3 and 4, the 90 sets of Gold sequences are generated by 45 polynomials of degree 14 and their reciprocals. For example, $G(u, u[3])$ is generated by the polynomial 41567 and $G(u[31], u[55])$ is generated by 50515.

Example 7: Let $n = 8$, $N = 255$, $t(n) = 33$, and $s(n) = 17$. There are no preferred pairs of m-sequences, and hence no Gold sequences, of period 255. However, it is possible to use (4.4) to construct sets of 257 sequences for which $\theta_{\max} = t(n) - 2 = 31$. For example, if u and v are m-sequences and $v = u[31]$, then Theorem 2 and (4.5) together imply that $\theta_{\max} = 31$ for the set $G(u, v)$. Furthermore, for the sequences belonging to $G(u, v)$ the correlation functions take on the four values 31, 15, −1, and −17. Similarly, if w is a reciprocal of u, then $\theta_{\max} = 31$ for the set $G(u, w)$ also. However, in this case, the correlation functions take on all integer values congruent to −1 mod 4 in the range from −29 to +31. If u is generated by the polynomial 435, then $G(u, w)$ is generated by the polynomial 264455 while $G(u, v)$ is generated by 231441.

Although there are no Gold sequences of period 255, one can construct $H_{33}(u)$ which is a set of Gold-like sequences. Similarly $H_3(u)$ is a set of dual-BCH sequences. Both sets contain 256 sequences. As noted earlier, $H_{33}(u)$ is a subset of $K_L(u)$, the large set of Kasami sequences which contains 4111 sequences. For *all three* sets, $\theta_{\max} = 33$, and the correlation functions for sequences in each set take on the five values 31, 15, −1, −17, and −33. The set $K_L(u)$ also has $K_S(u)$, the small set of Kasami sequences, as a subset. The latter contains only 16 sequences; however, $\theta_{\max} = 17$ and the correlation functions take on the three values 15, −1, and −17. The sets $H_{33}(u)$, $H_3(u)$, $K_L(u)$, and $K_S(u)$ are generated by the polynomials 326161, 267543, 6031603, and 11367, respectively.

Finally, we summarize the above examples in Table II. The first column in the table gives the period of the sequences in the set. The polynomial that generates the set is listed in the second column while the third column indicates which of the various constructions was used to obtain the set. In the fourth column we give the numbers of sequences in the set, while the fifth column gives the values taken on by the correlation functions. Further remarks are given in the last column. The sets listed in Table II are *not* unique; sets of sequences with similar properties are mentioned in Examples 3–7.

V. APERIODIC CORRELATION FUNCTIONS FOR COMPLEX-VALUED SEQUENCES

For many of the important applications of periodic sequences, each sequence is modulated in some manner by a data signal. Perhaps the most common form of this modulation is the scheme whereby a binary data signal determines the polarity of a binary sequence, which can be viewed as binary amplitude modulation or binary amplitude-shift keying. Such a scheme is used, for instance, in direct-sequence spread-spectrum communications systems. However, for many systems there is more than one of these modulated signals being transmitted at the same time and in the same frequency band. In general, the only way to make the signals distinguishable at the receiver is to assign each transmitter a unique sequence, called a *signature sequence*. As we will see, however, uniqueness is not

nearly enough; the set of signature sequences must have good correlation properties. To illustrate this fact, we consider an example which is very simple, yet it brings out the fundamental concepts that arise in a binary direct-sequence spread-spectrum system.

Consider a binary communications system in which the binary data sequence $\{b_n\} = \cdots, b_{-1}, b_0, b_1, b_2, \cdots$ is an arbitrary sequence of +1's and −1's. The binary signature sequence y is generated by a vector $y = (y_0, y_1, \cdots, y_{N-1})$ where each y_i is either +1 or −1. The sequence y can be written as

$$\begin{aligned} y &= \cdots; y_{1-N}, y_{2-N}, \cdots, y_{-1}; y_0, y_1, \cdots, y_{N-1}; \\ &\quad y_N, y_{N+1}, \cdots, y_{2N-1}; \cdots \\ &= \cdots; y; y; y; \cdots . \end{aligned} \tag{5.1}$$

The data and signature sequences are combined to give

$$\hat{y} = \cdots; b_{-1}y; b_0 y; b_1 y; \cdots . \tag{5.2}$$

In other words, $\hat{y}$ is the sequence which has as its ith element $\hat{y}_i = b_n y_k$ for all i such that $i = nN + k$ for k in the range $0 \leqslant k \leqslant N-1$.

Consider for the moment an idealized binary system without channel noise and with only one transmitted signal. The data symbol b_n is transmitted as $\hat{y}_n = b_n y$. A synchronous correlation receiver forms the inner product $\langle \hat{y}_n, y \rangle$, where $\hat{y}_n$ represents the received vector in this noiseless system and y is the signature sequence which is stored at the receiver. Notice that

$$\langle \hat{y}_n, y \rangle = b_n \langle y, y \rangle = b_n \theta_y(0). \tag{5.3}$$

Thus, in the absence of noise, the data sequence is recovered at the output of the correlation receiver.

Now suppose that there are two transmitters in this idealized system and that we are interested in receiving the data $\{b_n\}$ in the presence of another signal. This other signal is a sequence $\hat{x}$ which is formed from the data sequence $\{b'_n\}$ and the signature sequence x (generated by a binary vector $x = (x_0, x_1, \cdots, x_{N-1})$) in exactly the same manner as $\hat{y}$ was formed from $\{b_n\}$ and y. The two transmitters are not required to be synchronized; moreover, there may be different transmission delays for the two signals. If a correlation receiver is synchronized to the sequence y, and if the sequence x is delayed by an amount l $(1 \leqslant l \leqslant N-1)$ relative to y, then for a noiseless additive channel the received sequence is $\hat{y} + T^{-l}\hat{x}$ where (cf. (5.2))

$$\hat{x} = \cdots; b'_{-1}x; b'_0 x; b'_1 x; \cdots \tag{5.4}$$

Thus the output of a correlation receiver which is in synchronism with y is given by

$$z_n = \langle \hat{y}_n, y \rangle + \left[b'_{n-1} \sum_{i=0}^{l-1} x_{N-l+i} y_i + b'_n \sum_{i=l}^{N-1} x_{i-l} y_i \right]. \tag{5.5}$$

The first term represents the desired signal and the term in brackets represents the interference due to the presence of another transmitted signal in the channel.

Notice in (5.5), the last l elements of x are correlated against the first l elements of y, and the first $N-l$ elements of x are correlated against the last $N-l$ elements of y. Also notice that if $m = l - N$ then

$$\sum_{i=0}^{l-1} x_{N-l+i} y_i = \sum_{i=0}^{N-1+m} x_{i-m} y_i \tag{5.6}$$

and $1 \leqslant l \leqslant N-1$ implies $1-N \leqslant m \leqslant -1$. Furthermore, if we let $j = i - l$ we see that

$$\sum_{i=l}^{N-1} x_{i-l} y_i = \sum_{j=0}^{N-1-l} x_j y_{j+l} \tag{5.7}$$

for $0 \leqslant l \leqslant N-1$. Due to the fact that these two types of correlations occur commonly in spread-spectrum multiple-access communications systems, they have been studied extensively in the recent literature. By convention, these two types of correlations are combined to form a single correlation function which is known as the *aperiodic crosscorrelation function* for sequences x and y. For general complex-valued sequences x and y, the aperiodic crosscorrelation function $C_{x,y}$ is defined as

$$C_{x,y}(l) = \begin{cases} \displaystyle\sum_{j=0}^{N-1-l} x_j y^*_{j+l}, & 0 \leqslant l \leqslant N-1 \\ \displaystyle\sum_{j=0}^{N-1+l} x_{j-l} y^*_j, & 1-N \leqslant l < 0 \\ 0, & |l| \geqslant N. \end{cases} \tag{5.8}$$

Notice that except for the complex conjugation in (5.8), the sums that appear in the definition of $C_{x,y}(l)$ are just the sums of (5.6) and (5.7).

From the definition of $C_{x,y}$, we see that (5.5) can be rewritten as

$$z_n = b_n \theta_y(0) + [b'_{n-1} C_{x,y}(l-N) + b'_n C_{x,y}(l)] \tag{5.9}$$

where we have used (5.3), (5.6) with $m = l - N$, and (5.7). The interference term in (5.9) arises in considerably more general systems as well, such as continuous-time phase-coded spread-spectrum multiple-access systems (see [81, p. 797]). Notice that (5.9) is valid for $0 \leqslant l \leqslant N-1$.

As illustrated by the simple example given above, the aperiodic crosscorrelation function plays a key role in the design and analysis of periodic sequences for certain multiple-access communications systems. For phase-coded (or direct-sequence) spread-spectrum multiple-access communications, this role is discussed more thoroughly in [5], [72], [80], and [81]. The restriction to discrete-time noiseless channels in the above discussion is for illustrative purposes only; such restrictions are not made in the analysis of spread-spectrum systems (e.g., [81], [12]).

A. Properties of Aperiodic Correlation Functions

In this section we will summarize the important properties of the aperiodic crosscorrelation function defined in (5.8). Analogous to our notational convention for periodic correlation (Section II-A), we will often employ the alternative notation $C(x,y)(\cdot)$ for the aperiodic crosscorrelation function $C_{x,y}(\cdot)$. For the aperiodic autocorrelation function, we often use $C_x(\cdot)$ or $C(x)(\cdot)$ instead of $C_{x,x}(\cdot)$.

We first note that (5.8) implies

$$C_{x,y}(0) = \sum_{j=0}^{N-1} x_j y^*_j = \langle x, y \rangle = \theta_{x,y}(0). \tag{5.10}$$

In particular if $x = y$ then (5.10) becomes

$$C_x(0) = \sum_{j=0}^{N-1} x_j x_j^* = \sum_{j=0}^{N-1} |x_j|^2 = \|x\|^2 = \theta_x(0).$$

It is clear from the definition that some relationship must exist between the functions $C_{x,y}$ and $C_{y,x}$. Specifically, for any l,

$$C_{x,y}(-l) = [C_{y,x}(l)]^*. \tag{5.11}$$

This is analogous to (2.3) of Section II-A. The most commonly used form of this result is for the special case $x = y$ which is the following identity for aperiodic autocorrelation

$$C_x(-l) = [C_x(l)]^*. \tag{5.12}$$

The next three properties that will be considered are concerned with the influence on the aperiodic correlation function of the application of some kind of transformation to the sequences in question. The transformations considered are the shifting of one sequence, the changing of the signs of alternate elements of the sequences, and the reversal of the sequences. In all three cases the results have important implications regarding related correlation functions which are discussed in the next subsection.

The first transformation is the shift or delay of one sequence y with respect to the other sequence x. Specifically, the aperiodic crosscorrelation function $C(x, Ty)$ is related to the aperiodic crosscorrelation function $C(x, y)$ by

$$C(x, Ty)(l) = \begin{cases} C(x,y)(l+1) + x_{N-l-1}y_0^*, & 0 \leq l \leq N-1 \\ C(x,y)(l+1) - x_{-l-1}y_0^*, & 1-N \leq l < 0 \end{cases} \tag{5.13}$$

and the aperiodic autocorrelation $C(Tx)$ is related to the aperiodic autocorrelation function $C(x)$ by

$$C(Tx)(l) = \begin{cases} C(x)(l) - x_0 x_l^* + x_{N-l}x_0^*, & 0 \leq l \leq N-1 \\ C(x)(l) - x_{-l}x_0^* + x_0 x_{N+l}^*, & 1-N \leq l < 0. \end{cases} \tag{5.14}$$

These results have applications to the selection of sequences with small aperiodic crosscorrelation and autocorrelation. Given a set of sequences it is often desired to find the best phase (i.e., the best starting point or best cyclic shift) for each sequence ([72], [84]). The set of optimal phases is determined according to some parameter of the aperiodic crosscorrelation and/or autocorrelation functions for the sequences in the set. For certain parameters, the optimization requires computation of the crosscorrelation function $C(T^n x, T^m y)$ and/or the autocorrelation function $C(T^n x)$ for all phases n and m of all sequences x and y. Equations (5.13) and (5.14) can be used to compute these functions sequentially.

The next transformation considered is that of sign reversal of alternate elements of the sequences. That is, for a given pair of complex-valued sequences x and y we define vectors u and v by

$$u_i = (-1)^i x_i, \qquad 0 \leq i \leq N-1 \tag{5.15a}$$

$$v_i = (-1)^i y_i, \qquad 0 \leq i \leq N-1. \tag{5.15b}$$

Let u and v be the sequences generated by the vectors u and v, and recall that

$$C_{u,v}(l) = \begin{cases} \sum_{n=0}^{N-1-l} u_n v_{n+l}^*, & 0 \leq l \leq N-1 \\ \sum_{n=0}^{N-1+l} u_{n-l} v_n^*, & 1-N \leq l < 0 \end{cases}$$

and $C_{u,v}(l) = 0$ for $|l| \geq N$. Notice that for $0 \leq l \leq N-1$

$$C_{u,v}(l) = \sum_{n=0}^{N-1-l} x_n y_{n+l}^* (-1)^{2n+l} = (-1)^l \sum_{n=0}^{N-1-l} x_n y_{n+l}^*.$$

Therefore

$$C_{u,v}(l) = (-1)^l C_{x,y}(l), \qquad 0 \leq l \leq N-1.$$

Similarly, if $1-N \leq l < 0$,

$$C_{u,v}(l) = \sum_{n=0}^{N-1+l} x_{n-l} y_n^* (-1)^{2n-l} = (-1)^{-l} \sum_{n=0}^{N-1+l} x_{n-l} y_n^*$$
$$= (-1)^{-l} C_{x,y}(l).$$

Consequently,

$$C_{u,v}(l) = (-1)^{|l|} C_{x,y}(l) \tag{5.16}$$

for all l. Notice that if

$$u_i = (-1)^{i+1} x_i, \qquad v_i = (-1)^{i+1} y_i, \qquad 0 \leq i < N,$$

then (5.16) still holds.

A special case of (5.16) is the well-known result that if u and x are as in (5.15a) then

$$C_u(l) = (-1)^{|l|} C_x(l).$$

One application of this result is to show that if x is a Barker sequence (i.e., $|C_x(l)| \leq 1$ for $l \neq 0$) then u is also a Barker sequence (e.g., see [126]). An application of the more general identity (5.16) will be given in the next subsection.

Another fact about Barker sequences is that the reverse of a Barker sequence is also a Barker sequence [126]. More generally, suppose that x and y are any complex-valued sequences and that w and z are the corresponding *reverse* sequences as defined in Section II-A; that is, w and z are generated by vectors w and z which are defined by

$$w_i = x_{N-1-i}, \qquad 0 \leq i < N \tag{5.17a}$$

and

$$z_i = y_{N-1-i}, \qquad 0 \leq i < N. \tag{5.17b}$$

Then for $0 \leq l < N$,

$$C_{w,z}(l) = \sum_{i=0}^{N-1-l} w_i z_{i+l}^* = \sum_{i=0}^{N-1-l} x_{N-1-i} y_{N-1-i-l}^*$$
$$= \sum_{k=0}^{N-1-l} x_{k+l} y_k^* = \left[\sum_{k=0}^{N-1-l} y_k x_{k+l}^* \right]^*$$
$$= [C_{y,x}(l)]^*. \tag{5.18}$$

The same type of argument shows that (5.18) also holds for negative values of l. It then follows from (5.11) that for all l

$$C_{w,z}(l) = [C_{y,x}(l)]^* = C_{x,y}(-l). \tag{5.19}$$

Hence the set of aperiodic crosscorrelation values for the reverse sequences is the same as the set of aperiodic crosscorrelation values for the original sequences; however, the values occur in opposite order for the reverse sequences.

Suppose that w is the reverse of the sequence x as expressed by (5.17a). Setting $y = x$ and $z = w$ in (5.19), we obtain the autocorrelation identity

$$C_w(l) = [C_x(l)]^* = C_x(-l). \tag{5.20}$$

Stated simply, this is just the observation that the aperiodic autocorrelation values for the reverse of a complex-valued sequence are just the original aperiodic autocorrelation values taken in opposite order.

Some of the above aperiodic correlation identities take on useful special forms in the case where the sequences x and y are *real-valued sequences*. In all cases, of course, the complex conjugation can be omitted from the correlation functions because they are real. However, in certain cases the special form leads to a stronger result. Some of these are listed below. *If x and y are real-valued sequences then*

$$C_{x,y}(-l) = C_{y,x}(l) \tag{5.21a}$$

$$C_x(-l) = C_x(l) \tag{5.21b}$$

and if w is the reverse of x

$$C_w(l) = C_x(l). \tag{5.21c}$$

Notice in particular that the aperiodic autocorrelation function for a real-valued sequence and the aperiodic autocorrelation function for its reverse are identical. An application of this fact to asynchronous binary direct-sequence spread-spectrum multiple-access systems results from noticing that the signal-to noise ratio as defined in [81] depends only upon the aperiodic autocorrelation functions of the binary signature sequences [87]. Hence, the signal-to-noise ratio is invariant with respect to reversals of some or all of the signature sequences. As a consequence, the assignment of a sequence to one user and the reverse of the sequence to another has the same effect on the signal-to-noise ratio as the assignment of the same sequence to two different users; clearly this should be avoided. Some numerical data on the magnitude of the resulting interference is given in [84].

The aperiodic correlation functions satisfy identities analogous to those presented in Section II-B. As before, let $w, x, y, z \in \mathbb{C}^N$ and let w, x, y, z be the corresponding sequences. It can be shown that the four crosscorrelation functions $C_{w,x}$, $C_{y,z}$, $C_{w,y}$, and $C_{x,z}$ are related through the following identity [87]

$$\sum_{l=1-N}^{N-1} C_{w,y}(l)[C_{x,z}(l+n)]^* = \sum_{l=1-N}^{N-1} C_{w,x}(l)[C_{y,z}(l+n)]^*. \tag{5.22}$$

The special cases (5.23)–(5.25) given below can be derived from (5.22) in exactly the same manner as (2.11)–(2.13) were derived from (2.10). We have

$$\sum_{l=1-N}^{N-1} C_{w,y}(l)[C_{x,y}(l+n)]^* = \sum_{l=1-N}^{N-1} C_{w,x}(l)[C_y(l+n)]^* \tag{5.23}$$

$$\sum_{l=1-N}^{N-1} C_{x,y}(l)[C_{x,y}(l+n)]^* = \sum_{l=1-N}^{N-1} C_x(l)[C_y(l+n)]^* \tag{5.24}$$

and

$$\sum_{l=1-N}^{N-1} |C_{x,y}(l)|^2 = \sum_{l=1-N}^{N-1} C_x(l)[C_y(l)]^*. \tag{5.25}$$

Using (5.12), we can write (5.25) as

$$\sum_{l=1-N}^{N-1} |C_{x,y}(l)|^2 = C_x(0)C_y(0) + 2\,\mathrm{Re} \sum_{l=1}^{N-1} C_x(l)[C_y(l)]^* \tag{5.26}$$

where Re α denotes the real part of the complex number α.

Bounds similar to those obtained in Section II-C can be obtained for the aperiodic correlation functions also, which is not very surprising in view of the fact that the bounds are based on similar identities. We have the bound

$$|C_{x,y}(l)| \leq [C_x(0)C_y(0)]^{1/2} \tag{5.27}$$

which is analogous to (2.14). The bounds (analogous to (2.17) and (2.18)) that are obtained by applying the Cauchy inequality to (5.26) are

$$\sum_{l=1-N}^{N-1} |C_{x,y}(l)|^2 \leq C_x(0)C_y(0) + 2\left(\sum_{l=1}^{N-1} |C_x(l)|^2\right)^{1/2}\left(\sum_{l=1}^{N-1} |C_y(l)|^2\right)^{1/2} \tag{5.28}$$

and

$$\sum_{l=1-N}^{N-1} |C_{x,y}(l)|^2 \geq C_x(0)C_y(0) - 2\left(\sum_{l=1}^{N-1} |C_x(l)|^2\right)^{1/2}\left(\sum_{l=1}^{N-1} |C_y(l)|^2\right)^{1/2} \tag{5.29}$$

For a set $\mathfrak{X}$ of periodic sequences the peak aperiodic crosscorrelation magnitude C_c is defined by

$$C_c = \max\{|C_{x,y}(l)|: 0 \leq l \leq N-1, x \in \mathfrak{X}, y \in \mathfrak{X}, x \neq y\} \tag{5.30}$$

and the peak aperiodic autocorrelation magnitude is

$$C_a = \max\{|C_x(l)|: 1 \leq l \leq N-1, x \in \mathfrak{X}\}. \tag{5.31}$$

In [95] it is shown that if $\mathfrak{X}$ contains K sequences then

$$\frac{(2N-1)}{N}\left(\frac{C_c^2}{N}\right) + \frac{2(N-1)}{N(K-1)}\left(\frac{C_a^2}{N}\right) \geq 1. \tag{5.32}$$

The special case $K = 2$ of (5.32) can be found in [87]. Note that (5.32) implies

$$N^{-1}C_{\max}^2 = N^{-1}\max\{C_c^2, C_a^2\} \geq \frac{N(K-1)}{(2NK-K-1)} \tag{5.33}$$

which is a result due to Welch [129]. For further details and for tighter bounds in the case $K > N$, see [95] and [129]. Related results for mean-squared aperiodic correlation parameters can be found in [94].

B. Related Correlation Functions and Their Properties

Two important correlation functions which are derived from the aperiodic correlation function are the *periodic* (or even) and the *odd correlation functions*. The periodic crosscorrelation function for complex-valued sequences x and y is defined in Section II-A, where several of its important properties are given. The odd crosscorrelation function for such sequences is defined below. In this section, we take the point of view that the aperiodic correlation function is the basic correlation function, and we show how its properties carry over to the periodic and odd correlation functions.

It follows from (5.6)-(5.8), with the obvious modifications of (5.6) and (5.7) for complex-valued sequences, that for $0 \leqslant l \leqslant N-1$ and $m = l - N$,

$$C_{x,y}(l) + C_{x,y}(m) = \sum_{i=l}^{N-1} x_{i-l} y_i^* + \sum_{i=0}^{l-1} x_{i-l} y_i^*$$

since $x_{N-l+i} = x_{i-l}$. Therefore, from (2.1) it is seen that if $0 \leqslant l < N$ then

$$\theta_{x,y}(l) = C_{x,y}(l) + C_{x,y}(l-N) \tag{5.34}$$

for complex-valued sequences x and y. Notice that if $b'_{n-1} = b'_n$ in (5.9) then

$$z_n = b_n \theta_y(0) + b'_n \theta_{x,y}(l).$$

On the other hand, if $b'_{n-1} = -b'_n$ then

$$z_n = b_n \theta_y(0) + b'_n [C_{x,y}(l) - C_{x,y}(l-N)]. \tag{5.35}$$

Because of this fact, it is convenient to define the *odd crosscorrelation function* for complex-valued sequences x and y as

$$\hat{\theta}_{x,y}(l) = C_{x,y}(l) - C_{x,y}(l-N) \tag{5.36}$$

for $0 \leqslant l < N$. Thus equation (5.35) becomes

$$z_n = b_n \theta_y(0) + b'_n \hat{\theta}_{x,y}(l). \tag{5.37}$$

Notice that if $\{b'_n\}$ is a sequence of independent, identically distributed, binary random variables, then $P(b'_{n-1} \neq b'_n) = \frac{1}{2}$ so that the situation which results in (5.37) occurs one half of the time on the average. The conclusion is that for spread-spectrum multiple-access systems, the odd crosscorrelation function is as important as the periodic crosscorrelation function. However, the odd crosscorrelation function has received considerably less attention in the literature and almost no attention prior to 1969. The odd crosscorrelation function was first studied by Massey and Uhran [71] who pointed out its importance to spread-spectrum multiple-access systems. More recent results can be found in [72], [84], [86], [87], and [95].

The name "odd crosscorrelation" function is appropriate because the function $\hat{\theta}_{x,y}$ is such that

$$\begin{aligned} \hat{\theta}_{x,y}(N-l) &= C_{x,y}(N-l) - C_{x,y}(-l) \\ &= [C_{y,x}(l-N) - C_{y,x}(l)]^* \\ &= -[\hat{\theta}_{y,x}(l)]^*. \end{aligned} \tag{5.38}$$

This is in contrast to the periodic (or even) crosscorrelation function which satisfies

$$\begin{aligned} \theta_{x,y}(N-l) &= C_{x,y}(N-l) + C_{x,y}(-l) \\ &= [C_{y,x}(l-N) + C_{y,x}(l)]^* \\ &= +[\theta_{y,x}(l)]^* \end{aligned} \tag{5.39}$$

for $0 \leqslant l < N$. Notice that $\theta_{x,y}(-l) = \theta_{x,y}(N-l)$ and that

$$\begin{aligned} \theta_{x,y}(0) = \hat{\theta}_{x,y}(0) &= C_{x,y}(0) \\ &= \sum_{k=0}^{N-1} x_k y_k^* = \langle x, y \rangle. \end{aligned} \tag{5.40}$$

The odd autocorrelation function $\hat{\theta}_x$ for the complex-valued sequence x is defined by $\hat{\theta}_x(l) = \hat{\theta}_{x,x}(l)$, $0 \leqslant l < N$. For the odd and periodic autocorrelation functions, (5.38)-(5.40) become

$$\hat{\theta}_x(N-l) = -[\hat{\theta}_x(l)]^* \tag{5.41}$$

$$\theta_x(N-l) = [\theta_x(l)]^* \tag{5.42}$$

and

$$\begin{aligned} \hat{\theta}_x(0) = \theta_x(0) &= C_x(0) \\ &= \sum_{k=0}^{N-1} x_k x_k^* = \|x\|^2. \end{aligned} \tag{5.43}$$

The importance of the odd autocorrelation function $\hat{\theta}_x$ can be illustrated by a simple example which is a minor modification of the example given at the beginning of Section V. Suppose that the sequences x and y in this example are the same and that $b_k = b'_k$ for all k. Then the quantity z_n in (5.5) is the output of a correlation receiver which is in synchronism with y when the input is $\hat{y} + T^{-l}\hat{y}$. More generally, if the received signal is $\hat{y} + \beta T^{-l}\hat{y}$ where β is a real number such that $|\beta| \leqslant 1$ then the received signal $\hat{y} + \beta T^{-l}\hat{y}$ consists of a desired signal component plus a delayed attenuated version of the desired signal component. Such a signal can arise in certain multipath channels.

If $x = y$ and $b'_k = b_k$ for all k then (5.9) becomes

$$z_n = b_n \theta_y(0) + [b_{n-1} C_y(l-N) + b_n C_y(l)].$$

More generally, if the received signal is $\hat{y} + \beta T^{-l}\hat{y}$, then

$$z_n = b_n \theta_y(0) + \beta [b_{n-1} C_y(l-N) + b_n C_y(l)]. \tag{5.44}$$

If $b_n = b_{n-1}$, then (5.44) becomes

$$z_n = b_n [\theta_y(0) + \beta\, \theta_y(l)]. \tag{5.45}$$

On the other hand, if $b_n = -b_{n-1}$, equation (5.44) is equivalent to

$$z_n = b_n [\theta_y(0) + \beta \hat{\theta}_y(l)]. \tag{5.46}$$

As before, it is clear that for certain applications the odd correlation function is as important as the periodic correlation function.

Another situation in which the odd autocorrelation function plays a major role is in the acquisition by the receiver of the epoch of the signature sequence from the received signal. Here the odd autocorrelation function comes into play even if there is no interfering signal present at the receiver. For such applications, the sequences should be selected such that $\theta_y(l)$ and $\hat{\theta}_y(l)$ are both small for $0 < l < N$.

Since the periodic and odd crosscorrelation functions are derived from the aperiodic crosscorrelation function, many of

the properties of $C_{x,y}$ carry over to $\theta_{x,y}$ and $\hat{\theta}_{x,y}$. In particular, we will examine the implications of (5.13)-(5.16) and (5.22). Other aperiodic correlation properties given in Section V-A have corresponding implications. Analogous to our notational conventions regarding $C_{x,y}$ and $\theta_{x,y}$, the notation $\hat{\theta}(x,y)(\cdot)$ will often be used in place of $\hat{\theta}_{x,y}(\cdot)$. Similarly, $\hat{\theta}(x)(\cdot)$ will often be used for $\hat{\theta}_x(\cdot)$.

The first property of the odd crosscorrelation function is a consequence of (5.13); it is very useful in the problem of evaluating $\hat{\theta}(T^n x, T^m y)(l)$ for all phases n and m and for all l. The motivation for such an evaluation is discussed in the next subsection. The key result is that for any sequences x and y, $\hat{\theta}(x, Ty)(\cdot)$ can be computed from $\hat{\theta}(x,y)(\cdot)$ by the relationship

$$\hat{\theta}(x, Ty)(l) = \hat{\theta}(x,y)(l+1) + 2x_{N-l-1}y_0^* \tag{5.47}$$

which follows easily from (5.13) and (5.36). On the other hand, equations (5.13) and (5.34) imply that

$$\theta(x, Ty)(l) = \theta(x,y)(l+1) \tag{5.48}$$

which is just a special case of (2.7).

It follows from (2.8) that the periodic crosscorrelation spectrum (see Section III-D) for the pair $(T^n x, T^m y)$ is independent of the phases n and m of the sequences. However, from (5.47) one might suspect that the spectrum of the odd crosscorrelation function *does* depend on the phases of the sequences, and this is in fact true. It follows that by careful selection of phases, the maximum odd crosscorrelation can be reduced without changing the maximum periodic crosscorrelation. Further discussion of this point and some specific examples will be given in the next subsection.

For autocorrelation functions the results that are analogous to (5.47) and (5.48) are

$$\hat{\theta}(Tx)(l) = \hat{\theta}(x)(l) - 2x_0x_l^* + 2x_{N-l}x_0^* \tag{5.49}$$

$$\theta(Tx)(l) = \theta(x)(l). \tag{5.50}$$

These facts follow from (5.14) and the specializations of (5.34) and (5.36) to the case $x = y$. As with the periodic crosscorrelation spectrum, the periodic autocorrelation spectrum does not depend on the phase n of the sequence x. However, the spectrum of the odd autocorrelation function does depend on the sequence phase. Therefore, as discussed further in the next subsection, proper selection of the phase of a sequence will yield significant reductions in the maximum odd autocorrelation with no change in the periodic autocorrelation function.

If for a given x and y, u and v are defined as in equations (5.15), then (5.16) and (5.36) imply that for $0 \leq l < N$

$$\begin{aligned}\hat{\theta}_{u,v}(l) &= C_{u,v}(l) - C_{u,v}(l-N) \\ &= (-1)^l C_{x,y}(l) - (-1)^{N-l} C_{x,y}(l-N) \\ &= (-1)^l [C_{x,y}(l) - (-1)^N C_{x,y}(l-N)].\end{aligned}$$

Therefore, if N is odd (5.34) implies

$$\hat{\theta}_{u,v}(l) = (-1)^l \theta_{x,y}(l). \tag{5.51}$$

Similarly, equations (5.16) and (5.34) imply

$$\theta_{u,v}(l) = (-1)^l [C_{x,y}(l) + (-1)^N C_{x,y}(l-N)]$$

so that if N is odd (5.36) implies

$$\theta_{u,v}(l) = (-1)^l \hat{\theta}_{x,y}(l). \tag{5.52}$$

Thus, whenever N is odd, reversal of the signs of alternate elements of the vectors x and y produces an interchange of the periodic and odd crosscorrelation magnitudes. By letting $x = y$ (and hence $u = v$), it is seen that the same is true of periodic and odd autocorrelation magnitudes. Implications of this fact will be discussed in the next subsection.

Lastly, we discuss correlation function identities and bounds for the odd correlation functions. The odd correlation function identity analogous to (2.10) and (5.22) is

$$\begin{aligned}\sum_{l=0}^{N-1-n} \hat{\theta}_{w,y}(l)[\hat{\theta}_{x,z}(l+n)]^* - \sum_{l=N-n}^{N-1} \hat{\theta}_{w,y}(l)[\hat{\theta}_{x,z}(l+n-N)]^* \\ = \sum_{l=0}^{N-1-n} \hat{\theta}_{w,x}(l)[\hat{\theta}_{y,z}(l+n)]^* \\ - \sum_{l=N-n}^{N-1} \hat{\theta}_{w,x}(l)[\hat{\theta}_{y,z}(l+n-N)]^*\end{aligned} \tag{5.53}$$

which is valid for $0 \leq n \leq N-1$. (Note that for $n = 0$, the second sum on both sides of (5.53) is to be set equal to zero.) Equation (5.53) looks quite different from (2.10) and the reader may wonder whether replacing θ by $\hat{\theta}$ throughout (2.10) produces a valid result. It does not. The correct analogy between the three identities is drawn by interpreting the various identities in terms of correlation *functions* for sequences, much as we did in Section II-B. We can express (2.10) as

$$\theta[\theta_{w,y}, \theta_{x,z}](\cdot) = \theta[\theta_{w,x}, \theta_{y,z}](\cdot).$$

Since both sides of (5.23) are zero for $|n| > 2N-2$, we can express (5.23) as

$$C[C_{w,y}, C_{x,z}](\cdot) = C[C_{w,x}, C_{y,z}](\cdot).$$

Equation (5.53) is now seen to be

$$\hat{\theta}[\hat{\theta}_{w,y}, \hat{\theta}_{x,z}](\cdot) = \hat{\theta}[\hat{\theta}_{w,x}, \hat{\theta}_{y,z}](\cdot)$$

which is analogous to the previous identities. The special cases of (5.53) can be succinctly expressed as

$$\hat{\theta}[\hat{\theta}_{w,y}\hat{\theta}_{x,y}](\cdot) = \hat{\theta}[\hat{\theta}_{w,x}, \hat{\theta}_y](\cdot)$$

and

$$\hat{\theta}[\hat{\theta}_{x,y}](\cdot) = \hat{\theta}[\hat{\theta}_x, \hat{\theta}_y](\cdot).$$

As a special case of this last identity, we obtain

$$\sum_{l=0}^{N-1} |\hat{\theta}_{x,y}(l)|^2 = \sum_{l=0}^{N-1} \hat{\theta}_x(l)[\hat{\theta}_y(l)]^* \tag{5.54}$$

which was proved in [86].

Bounds on the odd correlation functions are easily described. Notice that (5.54) is just (2.13) with the θ's replaced by the $\hat{\theta}$'s. All the periodic correlation bounds of Section II-C are based on (2.13). It follows easily that all of the results of Section II-C are applicable to odd correlation functions if we replace θ by $\hat{\theta}$ everywhere in Section II-C (see also [86], [87], [94], and [95]). In [95] a set of sequences $\mathfrak{X}$ of odd period N is constructed which satisfies $\theta_c = N^{1/2}$, $\theta_a = 0$. If each $x \in \mathfrak{X}$ is modified to form a sequence u as defined by (5.15a), then for the new collection $\mathfrak{X}'$, we have $\hat{\theta}_c = N^{1/2}$, $\hat{\theta}_a = 0$. This occurs because of the interchange of the periodic and odd correlation functions as given by (5.51) and (5.52).

TABLE III
AUTOCORRELATION PARAMETERS FOR AUTO-OPTIMAL PHASES OF ONE SET OF GOLD SEQUENCES OF PERIOD 31 (SHIFT REGISTER 3551)

Number of Sequences	$M(x)$	$\hat{M}(x)$	$\min\{M(x), \hat{M}(x)\}$
2	1	7	1
1	7	5	5
5	9	5	5
21	9	7	7
4	9	9	9

C. Optimal Phases of Periodic Sequences

The illustrative examples of the previous subsection motivate the consideration of the maximum values of the magnitudes of the sidelobes of the periodic and odd autocorrelation functions (the sidelobes are the out-of-phase autocorrelations). For a given sequence x, let $M(x)$ and $\hat{M}(x)$ denote the maximum sidelobe magnitudes for the periodic and odd autocorrelation, respectively; that is,

$$M(x) = \max\{|\theta_x(l)| : 1 \leqslant l < N\} \tag{5.55a}$$

and

$$\hat{M}(x) = \max\{|\hat{\theta}_x(l)| : 1 \leqslant l < N\} \tag{5.55b}$$

It is important to notice that $l = 0$ is excluded in equations (5.55). Notice also that $M(x) \leqslant \theta_x(0)$ and $\hat{M}(x) \leqslant \hat{\theta}_x(0)$.

For a set $\mathfrak{X}$ of sequences, it is convenient to define parameters θ_a and $\hat{\theta}_a$ which are measures of the maximum periodic and odd autocorrelation sidelobes where the maximum is taken over all sequences in the set. The parameter θ_a, which is defined by (2.20), can be written as

$$\theta_a = \max\{M(x) : x \in \mathfrak{X}\}. \tag{5.56a}$$

Similarly, the parameter $\hat{\theta}_a$ can be defined by (2.20) with θ replaced by $\hat{\theta}$, and it satisfies

$$\hat{\theta}_a = \max\{\hat{M}(x) : x \in \mathfrak{X}\}. \tag{5.56b}$$

For certain applications such as the simple multipath communication example that led to (5.46), it is desirable to make the odd autocorrelation sidelobes as small as possible. As pointed out in the previous subsection, the odd autocorrelation depends upon the phase of the sequence. Let $\hat{\theta}_{AO}(x)$ denote the minimum value of $\hat{M}(T^n x)$, where the minimum is over all phases n of the sequence x. For many sequences there is more than one phase which achieves this minimum; therefore, it is useful to consider the number of times $\hat{\theta}(T^n x)(l)$ achieves its maximum value. For a sequence u let $\hat{L}(u)$ be the number of values of l, $1 \leqslant l < N$, for which $\hat{\theta}(u)(l) = \hat{M}(u)$. A phase n of a sequence x is an *auto-optimal* (AO) phase ([71], [72], [84]) if $\hat{M}(T^n x) = \hat{\theta}_{AO}(x)$ and if $\hat{L}(T^n x) \leqslant \hat{L}(T^k x)$ for all phases k for which $\hat{M}(T^k x) = \hat{\theta}_{AO}(x)$. In general, AO phases are not unique [90].

Suppose x is a real-valued sequence and w is the reverse sequence (i.e., w is given by (5.17a)). It follows from (5.21c) that $\hat{\theta}_w(l) = \hat{\theta}_x(l)$ for each l. Since the reverse of $T^k x$ is simply $T^{-k}w = T^{N-k}w$, then $\hat{\theta}_{AO}(x) = \hat{\theta}_{AO}(w)$. Furthermore, if n is an AO phase of x then $N - n$ is an AO phase of w. The sequence w is a reciprocal of x (in particular, $(T^{-1}w)_i = x_{-i}$); consequently, if x is a shift-register sequence then w is generated by the reciprocal of the polynomial that generates x. It follows that if we know the AO phases of all of the sequences generated by a given polynomial, then we can easily deduce the AO phases of all of the sequences generated by the reciprocal polynomial. Moreover, since $\hat{\theta}_{AO}(T^k w) = \hat{\theta}_{AO}(w) = \hat{\theta}_{AO}(x)$ then the maximum magnitude of the odd autocorrelation function for the AO phase of a sequence is the same as for the AO phase of each of its reciprocals.

In order to determine $\hat{\theta}_{AO}(x)$ or to find an AO phase for a given sequence x, the odd autocorrelation function for $T^n x$ must be computed for each n ($0 \leqslant n < N$). Equation (5.49) is very useful in such computations, since it permits efficient sequential computation of the functions $\hat{\theta}(T^n x)$. We will next give some examples where this type of computation has been carried out. These examples will give an indication of the relative magnitudes of various autocorrelation parameters.

For the first example, consider the 33 Gold sequences of period 31 which are obtained from the shift register polynomial 3551 and are described in Example 3. For this set of sequences $\theta_a = 9$. Furthermore, $M(x) = 1$ for two sequences x (the two m-sequences), $M(x) = 7$ for one sequence, and $M(x) = 9$ for the remaining 30 sequences. This is in fact true for any set of Gold sequences of period 31. Although some phases of certain of these sequences can give odd autocorrelation peaks as large as 21, a somewhat surprising result is that *for this set of Gold sequences*, $\hat{\theta}_{AO}(x) < 9$ for 29 of the 33 sequences and $\hat{\theta}_{AO}(x) = 9$ for the remaining four sequences [90]. Thus most of the *auto-optimal* sequences in this set have smaller peak odd autocorrelation than periodic autocorrelation; in fact, $\hat{\theta}_{AO}(x) < M(x)$ for 27 of the 33 sequences. A summary of the autocorrelation data for AO phases of these sequences is given in Table III. This table is valid only for the set of Gold sequences generated by the shift register 3551. The *odd* autocorrelation parameters are different for other sets of Gold sequences of period 31.

As an illustration of the usefulness of the interchange of periodic and odd correlation (i.e., (5.51) and (5.52)), we apply this interchange to the set $\mathfrak{X}$ of Gold sequences of period 31 that is described above. Consider a set $\mathfrak{X}'$ sequences which is derived from this set of Gold sequences as follows. First, *all* sequences are put in AO phases. The two m-sequences are included in $\mathfrak{X}'$. Next, (5.15a) is applied to each of the remaining 31 sequences in $\mathfrak{X}$, and the new sequences are included in $\mathfrak{X}'$. The resulting set $\mathfrak{X}'$ is a set of 33 sequences of period 31 for which $M(x) = 9$ for four sequences and $M(x) < 9$ for the remaining 29 sequences. The actual periodic correlation values appear in the right-hand column of Table III. Thus the set $\mathfrak{X}'$ has better peak periodic autocorrelation parameters than the original Gold sequences. Notice that for either set $\mathfrak{X}$ or $\mathfrak{X}'$, $\hat{\theta}_a = \theta_a = 9$.

In Table IV we present data on the maximum odd autocorrelation for the AO phases of the six sets of Gold sequences of period 31 which are generated by the polynomials listed in Example 3. For convenience, let $\hat{\eta}_{AO}(i)$ be the number of sequences x in a given set for which $\hat{\theta}_{AO}(x) = i$. For Gold sequences of period 31 it turns out that $\hat{\theta}_{AO}(x)$ is either 5, 7, or 9; consequently, $\hat{\eta}_{AO}(i) = 0$ if $i \notin \{5, 7, 9\}$. The values of $\hat{\eta}_{AO}(i)$ for $i \in \{5, 7, 9\}$ are shown in Table IV for each of the six sets.

In the first column these six sets are listed using the notation of Example 3. The second column gives the octal representation of the shift register which generates the set of sequences. As an illustration consider the set $G(u, v)$ of Gold sequences

TABLE IV
NUMBER OF SEQUENCES x FOR WHICH $\hat{\theta}_{AO}(x) = 5$, 7, AND 9 FOR EACH OF SIX SETS OF GOLD SEQUENCES OF PERIOD 31

Set	Polynomial	$\hat{\eta}_{AO}(5)$	$\hat{\eta}_{AO}(7)$	$\hat{\eta}_{AO}(9)$
$G(u, v)$	3551	6	23	4
$G(v, w)$	2303	8	21	4
$G(z, u)$	3667	7	22	4
$G(u, w)$	3013	5	25	3
$G(w, y)$	3735	7	24	2
$G(y, u)$	2563	5	25	3

which are generated by the shift register corresponding to polynomial 3551. For this set there are 6 sequences which when shifted to their AO phases have a peak odd autocorrelation of 5. Similarly, for the AO phases of 23 sequences the maximum odd autocorrelation magnitude is 7, and for the AO phases of 4 sequences the maximum is 9. These results are also valid for the set $G(x, y)$ since it is generated by the polynomial 2267 which is the reciprocal of 3551. This follows from our earlier remarks on the odd autocorrelation properties of AO phases of reciprocal sequences.

One of the conclusions to be drawn from Table IV is that the odd autocorrelation parameters are not in general the same for the various sets of Gold sequences. The differences are even more pronounced if consideration is given to additional parameters such as the mean-squared aperiodic autocorrelation or the number $\hat{L}(T^n x)$ for the AO phase of each sequence x in the set.

Next consider the Gold sequences of period 63 that are generated by the 12 stage shift register 14551. For this set it is well known that $\theta_a = 17$. However, Roefs [90] found that with these sequences in their AO phases, $\hat{\theta}_a = 15$. Furthermore, $\hat{\theta}_{AO}(x)$ is 9 for 2 of these sequences, 11 for 24 sequences, 13 for 23 sequences, and 15 for 16 sequences. Hence, a fairly large subset of these sequences can be extracted if it is desired to have $\hat{\theta}_a = 13$ or $\hat{\theta}_a = 11$.

As a final example to illustrate autocorrelation parameters, consider the set of all m-sequences of period 127. In [84] the correlation parameters are given for one set of AO phases of these sequences. Since these are m-sequences, then of course $\theta_a = 1$ regardless of the sequence phases. For any set of AO phases, $\hat{M}(x)$ is 19 for 4 sequences, 17 for 12 sequences, and 15 for 2 sequences.

As illustrated in the previous subsection, the periodic and odd *crosscorrelation* functions play a key role for applications to multiple-access communications. For such applications, it is desirable to have a set of sequences for which the periodic and odd crosscorrelation magnitudes are small. The parameter θ_c defined by (2.19) is the maximum periodic crosscorrelation magnitude for a set of sequences. Let $\hat{\theta}_c$ be the maximum odd crosscorrelation magnitude; that is, $\hat{\theta}_c$ is defined by (2.19) with θ replaced by $\hat{\theta}$.

As in the case of the odd autocorrelation, it is possible to alter the odd crosscorrelation values by changing the phases of the sequences. However, considerably more computation is required to find the optimal phases for minimizing the odd crosscorrelation. Even if (5.47) is employed, the number of computations required to minimize $\hat{\theta}_c$ may be prohibitive. Notice that for a set of K sequences of period N, there are a total of N^K different sets of phases for the sequences. Moreover, for each set of phases, there are $\frac{1}{2}K(K-1)$ crosscorrelation functions to be evaluated. As a result, suboptimal search procedures and *ad hoc* techniques are typically employed. Fortunately, suboptimal procedures usually provide significant reductions in the maximum crosscorrelation. For instance, consider the Gold sequences of period 31 which are generated by the polynomial 3551. In their AO phases these sequences have correlation parameters $\theta_a = \hat{\theta}_a = \theta_c = 9$ and $\hat{\theta}_c = 21$. It is fairly easy to modify the phases of the sequences in this set to achieve $\hat{\theta}_c = 17$ with no change in $\hat{\theta}_a$ (of course θ_a and θ_c are invariant under shifts). It is possible to omit a few sequences and obtain a subset with $\hat{\theta}_c = 15$ and $\hat{\theta}_a = 7$ or a somewhat larger subset with $\hat{\theta}_c = 15$ and $\hat{\theta}_a = 9$. For the Gold sequences of period 31 which are generated by polynomial 3667 it is possible to modify the phases to achieve $\hat{\theta}_c = 15$ and $\hat{\theta}_a = 9$ for the *entire* set of 33 sequences.

Although there are no analytical results which give the values of $\hat{\theta}_c$ for the standard sets of sequences such as m-sequences and Gold sequences, Massey and Uhran have obtained bounds on $\hat{\theta}_c$ for such sets [71], [72]. For *all* of the sets of sequences in Section IV which have $\theta_{max} = t(n)$, their bound is

$$\hat{\theta}_c \leq 2^{n-1} + 2^{\lfloor n/2 \rfloor} + 1 \tag{5.57}$$

and for the small set of Kasami sequences ($\theta_{max} = s(n)$) their bound becomes

$$\hat{\theta}_c \leq 2^{n-1} + 2^{(n-2)/2} + 1. \tag{5.58}$$

For $n = 5$, (5.57) implies that $\hat{\theta}_c \leq 21$ for each set of phases of each set of Gold sequences of period 31. As mentioned above, we know that $\hat{\theta}_c = 21$ for the Gold sequences of period 31, and thus (5.57) is tight in this case. However, (5.57) does not give a tight bound in general (e.g., it is not tight for $n = 7$) nor does (5.58). Furthermore, there is a more fundamental difficulty with any such bound. Bounds which are valid for each set of phases of the sequences cannot take into account that the phases can be selected to give much smaller values of $\hat{\theta}_c$. For example, we pointed out above that it is possible to obtain $\hat{\theta}_c = 15$ for one set of Gold sequences of period 31, whereas the bound is $\hat{\theta}_c = 21$.

VI. CONCLUDING REMARKS

In this paper we have presented results on a number of problems that are concerned with periodic and aperiodic autocorrelation and crosscorrelation for periodic sequences. The choice of topics covered here was of course based on our own interests and experience; we have included the results that we have found most useful in our work. Some of the important topics that we were unable to include in the paper are the partial correlation of periodic sequences, the design of multilevel sequences for frequency hopping patterns, combination sequences, statistical analysis of aperiodic correlation for periodic sequences,

and correlation parameters for random sequences. Some results on partial correlation can be found in [8], [26], [63], [82], and [127]; and results on frequency hopping patterns are given in [60], [88], [89], [98], and [111]. Representative references on combination sequences are [40, ch. 6], [74], [75], and [121]. For statistical analyses of aperiodic correlation parameters for periodic sequences see [90], and for consideration of random sequences consult [76], [91], and [99].

Along with the list of references, we have provided a selected bibliography which contains papers on several topics related to the subject of this paper. We have followed the practice of including an unpublished technical report only if, because of its technical content or historical importance, it is of special significance to the subject of this paper. For most of the unpublished reports listed, we have provided an accession number. We have included a few Ph.D. dissertations that contain significant contributions to the main topic of this paper. These are typically available from two sources: University Microfilms International or as technical reports from the university that granted the degree. Unfortunately, this is not true of M.S. theses, so we have not included in the bibliography any of the large number of relevant M.S. theses.

Acknowledgment

We wish to thank R. J. McEliece, G. W. Swenson, Jr., E. Szilléry, M. E. Van Valkenburg, W. J. Williams, N. Zierler, and an anonymous reviewer for their advice and encouragement during the preparation of this paper.

References and Selected Bibliography

[1] M. H. Ackroyd, "Synthesis of efficient Huffman sequences," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-8, pp. 2-6, 1972.
[2] ——, "Huffman sequences with approximately uniform envelopes or cross-correlation functions," *IEEE Trans. Inform. Theory*, vol. IT-23, pp. 620-623, 1977.
[3] J. M. Aein and J. W. Schwartz, Eds., "Multiple-access to a communication satellite with a hard-limiting repeater—Volume II: Proceedings of the IDA multiple access summer study," Inst. Defense Analyses, Rep. R-108, (AD 465789), 1965.
[4] D. R. Anderson,"A new class of cyclic codes," *SIAM J. Appl. Math.*, vol. 16, pp. 181-197, 1968.
[5] D. R. Anderson and P. A. Wintz, "Analysis of a spread-spectrum multiple-access system with a hard limiter," *IEEE Trans. Commun. Technol.*, vol. COM-17, pp. 285-290, 1969.
[6] R. H. Barker, "Group synchronizing of binary digital systems," in *Communication Theory*. London, England: Butterworth, 1953.
[7] L. D. Baumert and R. J. McEliece, "Weights of irreducible cyclic codes," *Inform. Cont.*, vol. 20, pp. 158-175, 1972.
[8] N. E. Bekir, R. A. Scholtz, and L. R. Welch, "Partial-period correlation properties of PN sequences," in *1978 National Telecommunications Conf. Rec.*, vol. 3, pp. 35.1.1-4, 1978.
[9] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.
[10] G. S. Bloom and S. W. Golomb, "Applications of numbered undirected graphs," *Proc. IEEE*, vol. 65, pp. 562-570, 1977.
[11] A. M. Boehmer, "Binary pulse compression codes," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 156-167, 1967.
[12] D. E. Borth and M. B. Pursley, "Analysis of direct sequence spread-spectrum multiple-access communication over Rician fading channels," *IEEE Trans. Commun.*, vol. COM-27, pp. 1566-1577, 1979.
[13] R. N. Bracewell, *The Fourier Transform and Its Applications*. New York: McGraw-Hill, 1965.
[14] P. A. N. Briggs and K. R. Godfrey, "Pseudorandom signals for the dynamic analysis of multivariable systems," *Proc. Inst. Elec. Eng.*, vol. 113, pp. 1259-1267, 1966.
[15] ——, "New class of pseudorandom ternary sequences," *Electron. Lett.*, vol. 4, pp. 438-439, 1968.
[16] ——, "Design of uncorrelated signals," *Electron. Lett.*, vol. 12, pp. 555-556, 1976.
[17] P. A. N. Briggs, P. H. Hammond, M. T. G. Hughes, and G. O. Plumb, "Correlation analysis of process dynamics using pseudo-random binary test perturbation," *Proc. Inst. Mech. Eng.*, vol. 179, pt. 3H, pp. 37-51, 1965.
[18] D. Calabro and J. Paolillo, "Synthesis of cyclically orthogonal binary sequences of the same least period," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 756-758, 1968.
[19] J. R. Caprio, "Strictly complex impulse-equivalent codes and subsets with very uniform distribution," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 695-706, 1969.
[20] N. B. Chakrabarti and M. Tomlinson, "Design of sequences with specified autocorrelation and cross-correlation," *IEEE Trans. Commun.*, vol. COM-24, pp. 1246-1252, 1976.
[21] D. C. Chu, "Polyphase codes with good periodic correlation properties," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 531-532, 1972.
[22] G. R. Cooper and R. W. Nettleton, "A spread-spectrum technique for high-capacity mobile communications," *IEEE Trans. Veh. Technol.*, vol. VT-27, pp. 264-275, 1978.
[23] T. A. Dowling and R. J. McEliece, "Cross-correlation of reverse maximal-length shift register sequences," JPL Space Programs Summary 37-53, vol. 3, pp. 192-193, 1968.
[24] R. L. Frank, "Polyphase codes with good nonperiodic correlation properties," *IEEE Trans. Inform. Theory*, vol. IT-9, pp. 43-45, 1963.
[25] R. Frank and S. Zadoff, "Phase shift codes with good periodic correlation properties," *IRE Trans. Inform. Theory*, vol. IT-8, pp. 381-382, 1962.
[26] S. Fredricsson, "Pseudo-randomness properties of binary shift register sequences," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 115-120, 1975.
[27] R. M. Gagliardi, "Rapid acquisition signal design in a multiple-access environment," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-10, pp. 359-363, 1974.
[28] K. R. Godfrey, "Three-level m-sequences," *Electron. Lett.*, vol. 2, pp. 241-243, 1966.
[29] ——, "The theory of the correlation method of dynamic analysis and its application to industrial processes and nuclear power plants," *Meas. Contr.*, vol. 2, pp. T65-T72, 1969.
[30] M. J. E. Golay, "Complementary series," *IRE Trans. Inform. Theory*, vol. IT-7, pp. 82-87, 1961.
[31] ——, "A class of finite binary sequences with alternate auto-correlation values equal to zero," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 449-450, 1972.
[32] ——, "Notes on impulse equivalent pulse trains," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 718-721, 1975.
[33] R. Gold, "Characteristic linear sequences and their coset functions," *SIAM J. Appl. Math.*, vol. 14, pp. 980-985, 1966.
[34] ——, "Study of correlation properties of binary sequences," AF Avionics Lab., Wright-Patterson AFB, OH, Tech. Rep. AFAL-TR-66-234, (AD 488858), 1966.
[35] ——, "Optimal binary sequences for spread spectrum multiplexing," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 619-621, 1967.
[36] ——, "Study of correlation properties of binary sequences," AF Avionics Lab., Wright-Patterson AFB, OH, Tech. Rep. AFAL-TR-67-311 (AD 826367), 1967.
[37] ——, "Maximal recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 154-156, 1968.
[38] ——, "Study of multistate PN sequences and their application to communication systems," Rockwell International Corp. Rep. (AD A025137), 1976.
[39] R. Gold and E. Kopitzke, "Study of correlation properties of binary sequences," Interim Tech. Rep. 1, vols. 1-4, Magnavox Res. Lab., Torrance, CA (AD 470696-9), 1965.
[40] S. W. Golomb, Ed., *Digital Communications with Space Applications*. Englewood Cliffs, NJ: Prentice-Hall, 1964.
[41] ——, *Shift Register Sequences*. San Francisco, CA: Holden-Day, 1967.
[42] ——, "Theory of transformation groups of polynomials over GF(2) with applications to linear shift register sequences," *Inform. Sci.*, vol. 1, pp. 87-109, 1968.
[43] S. W. Golomb and R. A. Scholtz, "Generalized Barker sequences," *IEEE Trans. Inform. Theory*, vol. IT-11, pp. 533-537, 1965.
[44] R. C. Heimiller, "Phase shift pulse codes with good periodic correlation properties," *IRE Trans. Inform. Theory*, vol. IT-7, pp. 254-257, 1961.
[45] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discrete Math.*, vol. 16, pp. 209-232, 9176.
[46] D. A. Huffman, "The generation of impulse-equivalent pulse trains," *IRE Trans. Inform. Theory*, vol. IT-8, pp. S10-S16, 1962.
[47] D. L. Huffman, "A modification of Huffman's impulse-equivalent pulse trains to increase signal energy utilization," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 559-561, 1974.
[48] *IEEE Trans. Commun.: Special Issue on Spread Spectrum Com-*

munications, vol. COM-25, 1977.
[49] G. A. Kabatyanskii and V. I. Levenshtein, "Bounds for packings on a sphere and in space," *Probl. Peredach. Inform.*, vol. 14, pp. 3–25, Jan. 1978, (in Russian). English translation in *Probl. Inform. Transmission*, vol. 14, pp. 1–17, 1978.
[50] J. Kaiser, J. W. Schwartz, and J. M. Aein, "Multiple access to a communication satellite with a hard-limiting repeater. Volume I: Modulation techniques and their applications," Inst. Defense Analyses, Rep. R-108, (AD 457945), 1965.
[51] T. Kasami, "Weight distribution formula for some class of cyclic codes," Coordinated Science Lab., Univ. Illinois, Urbana. Tech. Rep. R-285 (AD 632574), 1966.
[52] ——, "Weight distribution of Bose–Chaudhuri–Hocquenghem codes," in *Combinatorial Mathematics and Its Applications*. Chapel Hill, NC: Univ. of North Carolina Press, 1969 (also Coordinated Science Lab. Univ. Illinois, Urbana, Tech. Rep. R-317, 1966). Reprinted in E. R. Berlekamp, Ed., *Key Papers in the Development of Coding Theory*. New York: IEEE Press, 1974.
[53] A. M. Kerdock, F. J. MacWilliams, and A. M. Odlyzko, "A new theorem about the Mattson–Solomon polynomial and some applications," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 85–89, 1974.
[54] E. L. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 732–736, 1976.
[55] Y. I. Kotov, "Correlation functions of composite sequences constructed from m-sequences," *Radio Eng. Electron. Phys.*, vol. 19, pp. 128–130, 1974.
[56] I. L. Lebow, K. L. Jordan, and P. R. Drouilhet, Jr., "Satellite communications to mobile platforms," *Proc. IEEE*, vol. 59, pp. 139–159, 1971.
[57] J. Lee and D. R. Smith, "Families of shift-register sequences with impulsive correlation properties," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 255–261, 1974.
[58] A. Lempel, "Analysis and synthesis of polynomials and sequences over GF(2)," *IEEE Trans. Inform. Theory*, vol. IT-17, pp. 297–303, 1971.
[59] ——, M. Cohn, and W. L. Eastman, "A class of balanced binary sequences with optimal autocorrelation properties," *IEEE Trans. Inform. Theory*, vol. IT-23, pp. 38–42, 1977.
[60] A. Lempel and H. Greenberger, "Families of sequences with optimal Hamming correlation properties," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 90–94, 1974.
[61] R. M. Lerner, "Signals having good correlation functions," *WESCON Conv. Rec.*, 1961.
[62] K. N. Levitt and J. K. Wolf, "On the interleaving of two-level periodic binary sequences," *Proc. N. E. C.*, pp. 644–649, 1965.
[63] J. H. Lindholm, "An analysis of the pseudo-randomness properties of subsequences of long m-sequences," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 569–576, 1968.
[64] J. Lindner, "Binary sequences up to length 40 with best possible autocorrelation function," *Electron. Lett.*, vol. 11, p. 507, 1975.
[65] R. J. McEliece, "On periodic sequences from $GF(q)$," *J. Combinatorial Theory*, series A, vol. 10, pp. 80–91, 1971.
[66] ——, "Correlation properties of sets of sequences derived from irreducible cyclic codes," *Inform. Contr.*, to be published.
[67] R. J. McEliece and H. Rumsey, Jr., "Euler products, cyclotomy, and coding," *J. Number Theory*, vol. 4, pp. 302–311, 1972.
[68] F. J. MacWilliams, "An example of two cyclically orthogonal sequences with maximum period," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 338–339, 1967.
[69] F. J. MacWilliams and N. J. A. Sloane, "Pseudo-random sequences and arrays," *Proc. IEEE*, vol. 64, pp. 1715–1729, 1976.
[70] ——, *The Theory of Error-Correcting Codes*. Amsterdam, the Netherlands: North-Holland, 1977.
[71] J. L. Massey and J. J. Uhran, Jr., "Final report for multipath study," Contract NAS5-10786, Univ. Notre Dame, Notre Dame, IN, 1969.
[72] ——, "Sub-baud coding," in *Proc. 13th Annu. Allerton Conf. Circuit and System Theory*, pp. 539–547, 1975.
[73] K. A. Meshkovskii, "A new class of pseudorandom sequences of binary signals," *Probl. Peredach. Inform.*, vol. 9, pp. 117–119, July 1973 (in Russian). English translation in *Probl. Inform. Transmission*, vol. 9, pp. 267–269, 1973.
[74] L. B. Milstein, "Some statistical properties of combination sequences," *IEEE Trans. Inform. Theory*, vol. IT-23, pp. 254–258, 1977.
[75] L. B. Milstein and R. R. Ragonetti, "Combination sequences for spread spectrum communications," *IEEE Trans. Commun.*, vol. COM-25, pp. 691–696, 1977.
[76] J. W. Moon and L. Moser, "On the correlation function of random binary sequences," *SIAM J. Appl. Math.*, vol. 16, no. 2, pp. 340–343, 1968.
[77] Y. Niho, "Multi-valued cross-correlation functions between two maximal linear recursive sequences," Ph.D. dissertation, Dep. Elec. Eng., Univ. Southern California (also USC EE Rep. 409), 1972.
[78] M. I. Pelekhatyi and E. A. Golubev, "Autocorrelative properties of certain types of binary sequences," *Probl. Peredach. Inform.*, vol. 8, pp. 92–99, Jan. 1972 (in Russian). English translation in *Probl. Inform. Transmission*, vol. 8, pp. 71–76, 1972.
[79] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd ed. Cambridge, MA: M.I.T. Press, 1972.
[80] M. B. Pursley, "Evaluating performance of codes for spread spectrum multiple access communications," in *Proc. 12th Annu. Allerton Conf. Circuit and System Theory*, pp. 765–774, 1974.
[81] ——, "Performance evaluation for phase-coded spread-spectrum multiple-access communication—Part I: System analysis," *IEEE Trans. Commun.*, vol. COM-25, pp. 795–799, 1977.
[82] ——, "On the mean-square partial correlation of periodic sequences," in *Proc. 1979 Conf. Information Sciences and Systems* (John Hopkins Univ., Baltimore, MD), pp. 377–379, 1979.
[83] M. B. Pursley and F. D. Garber, "Quadriphase spread-spectrum multiple-access communications," in *IEEE Int. Conf. Communications, Conf. Rec.*, vol. 1, pp. 7.3.1–7.3.5, 1978.
[84] M. B. Pursley and H. F. A. Roefs, "Numerical evaluation of correlation parameters for optimal phases of binary shift-register sequences," *IEEE Trans. Commun.*, vol. COM-27, pp. 1597–1604, 1979.
[85] M. B. Pursley and D. V. Sarwate, "Bounds on aperiodic cross-correlation for binary sequences," *Electron. Lett.*, vol. 12, pp. 304–305, 1976.
[86] ——, "Evaluation of correlation parameters for periodic sequences," *IEEE Trans. Inform. Theory*, vol. IT-23, pp. 508–513, 1977.
[87] ——, "Performance evaluation for phase-coded spread-spectrum multiple-access communication—Part II: Code sequence analysis," *IEEE Trans. Commun.*, vol. COM-25, pp. 800–803, 1977.
[88] I. S. Reed, "kth order near-orthogonal codes," *IEEE Trans. Inform. Theory*, vol. IT-17, pp. 116–117, 1971.
[89] I. S. Reed and H. Blasbalg, "Multipath tolerant ranging and data transfer techniques for air-to-ground and ground-to-air links," *Proc. IEEE*, vol. 58, pp. 422–429, 1970.
[90] H. F. A. Roefs, "Binary sequences for spread-spectrum multiple-access communication," Ph.D. dissertation, Dep. Elec. Eng., Univ. Illinois, Urbana, (also Coordinated Science Lab. Rep. R-785), Aug. 1977.
[91] H. F. A. Roefs and M. B. Pursley, "Correlation parameters of random binary sequences," *Electron. Lett.*, vol. 13, pp. 488–489, 1977.
[92] H. F. A. Roefs, D. V. Sarwate, and M. B. Pursley, "Periodic correlation functions for sums of pairs of m-sequences," in *Proc. 1977 Conf. Information Sciences and Systems* (Johns Hopkins Univ., Baltimore, MD), pp. 487–492, 1977.
[93] D. V. Sarwate, "Comments on 'A class of balanced binary sequences with optimal autocorrelation properties'," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 128–129, 1978.
[94] ——, "Crosscorrelation properties of sequences with applications to spread-spectrum multiple-access communication," in *Proc. AFOSR Workshop in Communication Theory and Applications*, Provincetown, MA, pp. 88–91, 1978.
[95] D. V. Sarwate, "Bounds on crosscorrelation and autocorrelation of sequences," *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 720–724, 1979.
[96] D. V. Sarwate and M. B. Pursley, "Applications of coding theory to spread-spectrum multiple-access satellite communications," in *Proc. 1976 IEEE Canadian Communications and Power Conf.*, pp. 72–75, 1976.
[97] ——, "New correlation identities for periodic sequences," *Electron. Lett.*, vol. 13, no. 2, pp. 48–49, 1977.
[98] ——, "Hopping patterns for frequency hopped multiple-access communication," in *IEEE Int. Conf. Communications, Conf. Rec.*, pp. 7.4.1–7.4.3, 1978.
[99] K. S. Schneider and R. S. Orr, "Aperiodic correlation constraints on large binary sequence sets," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 79–84, 1975.
[100] M. R. Schroeder, "Synthesis of low-peak-factor signals and binary sequences with low autocorrelation," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 79–84, 1970.
[101] R. A. Scholtz and L. R. Welch, "Group characters: Sequences with good correlation properties," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 537–545, 1978.
[102] J. W. Schwartz, J. M. Aein, and J. Kaiser, "Modulation techniques for multiple access to a hard-limiting satellite repeater," *Proc. IEEE*, vol. 54, pp. 763–777, 1966.
[103] G. Seguin, "Binary sequences with specified correlation properties," Ph.D. dissertation, Dep. Elec. Eng., Univ. Notre Dame, Notre Dame, IN (also Tech. Rep. 7103), 1971.
[104] E. S. Selmer, "Linear recurrence relations over finite fields," Dep. Math., Univ. Bergen, Bergen, Norway, 1966.
[105] D. A. Shedd and D. V. Sarwate, "Construction of sequences with good correlation properties," *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 94–97, 1979.
[106] V. M. Sidelnikov, "Some k-valued pseudo-random sequences and nearly equidistant codes," *Probl. Peredach. Inform.*, vol. 5,

pp. 16-22, Jan. 1969 (in Russian). English translation in *Probl. Inform. Transmission*, vol. 5, pp. 12-16, 1969.
[107] ——, "Cross correlation of sequences," *Probl. Kybern.*, vol. 24, pp. 15-42, 1971 (in Russian).
[108] ——, "On mutual correlation of sequences," *Soviet Math. Dokl.*, vol. 12, pp. 197-201, 1971.
[109] N. I. Smirnov, "Applications of *m*-sequences in asynchronous radio systems," *Telecommun. Radio Eng.*, vol. 24, no. 10, pp. 26-35 (translated from the Russian journal *Elektrosvayz*), 1970.
[110] N. I. Smirnov and N. A. Golubkov, "Correlation properties of segments of *m*-sequences," *Telecommun. Radio Eng.*, vol. 28, no. 6, pp. 123-125 (translation from the Russian journal *Elektrosvayz*), 1973.
[111] G. Solomon, "Optimal frequency hopping sequences for multiple-access," in *Proc. 1973 Symp. Spread Spectrum Communications*, vol. 1, (AD 915852), pp. 33-35, 1973.
[112] G. Solomon and R. J. McEliece, "Weights of cyclic codes," *J. Combinatorial Theory*, vol. 1, pp. 459-475, 1966.
[113] U. Somaini and M. H. Ackroyd, "Uniform complex codes with low autocorrelation sidelobes," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 689-691, 1974.
[114] R. Spann, "A two-dimensional correlation property of pseudorandom maximal-length sequences," *Proc. IEEE*, vol. 53, p. 1257, 1963.
[115] J. E. Stalder and C. R. Cahn, "Bounds for correlation peaks of periodic digital sequences," *Proc. IEEE*, vol. 52, pp. 1262-1263, 1964.
[116] J. J. Stiffler, "Rapid acquisition sequences," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 221-225, 1968.
[117] ——, *Theory of Synchronous Communications*. Englewood Cliffs, NJ: Prentice-Hall, 1971,
[118] I. G. Stiglitz, "Multiple-access considerations—A satellite example," *IEEE Trans. Commun.*, vol. COM-21, pp. 577-582, 1973.
[119] Y. Sugiyama, S. Hirasawa, M. Kasahara, and T. Namekawa, "The construction of sequences by interleaving method," *Electron. Commun. Japan*, vol. 55-A, pp. 35-42, 1972.
[120] Y. Taki, H. Miyakawa, M. Hatori, and S. Namba, "Even-shift orthogonal sequences," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 295-300, 1969.
[121] R. C. Titsworth, "Optimal ranging codes," *IEEE Trans. Space Electron. Telem.*, vol. SET-10, pp. 19-30, 1964.
[122] C.-C. Tseng and C. L. Liu, "Complementary sets of sequences," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 644-652, 1972.
[123] R. Turyn, "The correlation function of a sequence of roots of 1," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 524-525, 1967.
[124] ——, "Sequences with small correlation," in *Error Correcting Codes*, H. B. Mann, Ed. New York: Wiley, 1968.
[125] ——, "Four-phase Barker codes," *IEEE Transactions on Information Theory*, vol. IT-20, pp. 366-371, 1974.
[126] R. Turyn and J. Storer, "On binary sequences," *Proc. Amer. Math. Soc.*, vol. 12, pp. 394-399, 1961.
[127] S. Wainberg and J. K. Wolf, "Subsequences of pseudorandom sequences," *IEEE Trans. Commun.*, vol. COM-18, pp. 606-612, 1970.
[128] G. D. Weathers, E. R. Graf, and G. R. Wallace, "The subsequence weight distribution of summed maximal length digital sequences," *IEEE Trans. Commun.*, vol. COM-22, pp. 997-1004, 1974.
[129] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 397-399, 1974.
[130] L. Weng, "Decomposition of *m*-sequences and its applications," *IEEE Trans. Inform. Theory*, vol. IT-17, pp. 457-463, 1971.
[131] M. Willett, "The index of an *m*-sequence," *SIAM J. Appl. Math.*, vol. 25, pp. 24-27, 1973.
[132] M. Willett, "Characteristic *m*-sequences," *Math. Comput.*, vol. 30, pp. 306-311, 1976.
[133] K. Yao, "Error probability of asynchronous spread spectrum multiple access communications systems," *IEEE Trans. Commun.*, vol. COM-25, pp. 803-809, 1977.
[134] N. Zierler, "Linear recurring sequences," *J. Soc. Industrial and Applied Mathematics*, vol. 7, pp. 31-48, 1959.
[135] ——, "Linear recurring sequences and error-correcting codes," in *Error Correcting Codes*, H. B. Mann, Ed. New York: Wiley, 1968.
[136] N. Zierler and W. H. Mills, "Products of linear recurring sequences," *J. Algebra*, vol. 27, pp. 147-157, 1973.