CDMA SEQUENCES AND TECHNIQUES

by

Ian F. Blake and Jon W. Mark

Department of Electrical Engineering
University of Waterloo
Waterloo, Ontario, Canada
N21 3G1

December 1978

This work was supported by the Department of Supply
and Services of Canada under Project No. 808-01

TABLE OF CONTENTS

FORWORD

This report contains a state-of-the-art survey of Spread Spectrum Multiple Access (SSMA) techniques in general, but Code Division Multiple Access (DCMA) in particular. Specifically, Section 1 describes CDMA signaling concepts and techniques, Section 2 discusses sequences and their correlation properties, and Section 3 considers the synchronization aspect of CDMA signaling.

Two salient features that are necessary for the successful operation of a CDMA system are: 1) the code sequences must possess a very wide signal spectrum and 2) the code must be susceptible to rapid acquisition. The first feature calls for long sequences which possess noise-like properties while the second feature favours short sequences. Thus, these two features represent conflicting requirements. Successful CDMA operation requires simultaneous satisfaction of both features. Hence certain suitable compromise has to be incorporated; this is the direction which is currently under investigation.

1. CDMA TECHNIQUES

1.1 Introduction

Multiple access communication arises in situations where many users attempt simultaneous transmission through a common communication channel or share a common central resource facility. The satellite channel having ample bandwidth and a wide geographical coverage is a natural environment for multiple access communication. Ground-radio networks and terrestial data bus in which user terminals are attached through communication adapters are also candidates for multiple access. Conventional multiple access schemes are frequency-division multiple access (FDMA) and time-division multiple access (TDMA) in which fixed frequency bands or time slots are allocated to the users. When the number of users is large FDMA (TDMA) can run into a problem in bandwidth (time slot) allocation. The effectiveness of both FDMA and TDMA is thus greatly reduced. Also in an environment in which data generation is random and bursty, either FDMA or TDMA would be inefficient in that a large fraction of the frequency band (or time slot) may be idle over a certain period of time. Other multiple access schemes are demand-assignment multiple access (DAMA) and random multiple access (RMA). DAMA itself has many derivatives. Two of the more prominent schemes are Polling [Konheim and Meister, 1974] and reservation scheduling [Mark, 1978]. With random multiple access the transmissions by various users will add to produce a composite signal. Unless there are specific properties which are built into a relationship amongst the various signals so that each intended user can discriminate against unwanted signals, the composite signal just appears as noise to all concerned. Thus, simultaneous trans-

mission by two or more users can lead to destructive interference and retransmission must take place. A scheme, known as the ALOHA system [Abramson, 1970] developed by a group of researchers at the University of Hawaii, uses this transmission strategy.

When the different user signals are coded so that they form an orthogonal set, then intended users can extract their own wanted signals with only negligibly small interference. That is, unwanted signals will appear as wideband noise; the power spectra of unwanted signals spread over a wide frequency band, hence the term spread spectrum. When the various singals are coded to form an orthogonal set, or an almost orthogonal set, which is characterized by a low cross-correlation function, the mode of spread spectrum multiple access is called code-division multiple access (CDMA). It is with respect to sequences possessing good cross-correlation properties, and hence suitable for CDMA application, that the present study is directed.

Spread spectrum as a research discipline spans a rather wide cross-section of the communication field [Dixon, 1975]. To date spread spectrum multiple access (SSMA) systems have been used mainly in military systems under various names as frequency hopping [Nossen, 1974], pseudonoise systems [Lefande, 1970], jamming systems [Ross, 1974], etc. By far the two most widely discussed spread spectrum code signals are the following: i) Direct sequence (DS) signal with chip time (digit duration) T_c, and ii) noncoherent frequency hopping (FH) signal with frequency separation Δf. The essential ingredient in these two techniques is the code use to spread the bandwidth of unwanted signals; hence DS and FH are known as code-division multiple access (CDMA) techniques.

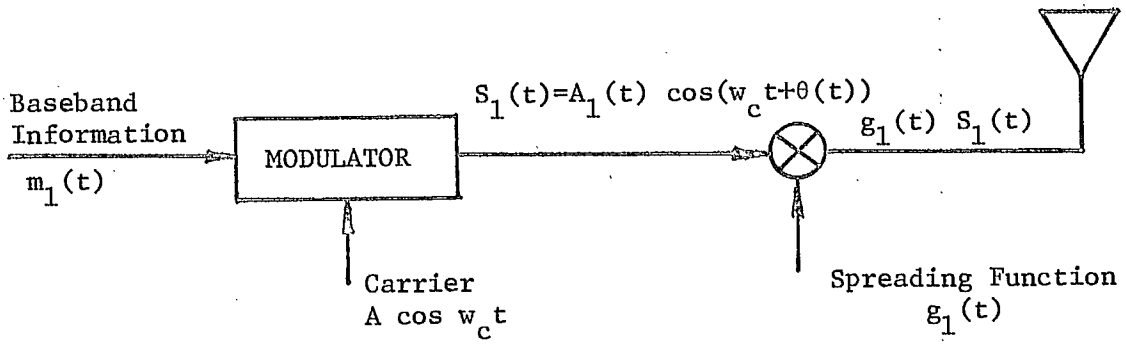
In the remaining portion of this section we present a brief

exposition of DS and FH as spread spectrum techniques. A survey of the codes or sequences together with their correlation properties is given in Section 2. As in all other aspects of communication, synchronization represents a prominent and indispensible feature in SSMA. Section 3 presents a survey of synchronization techniques which pertain to CDMA applications.

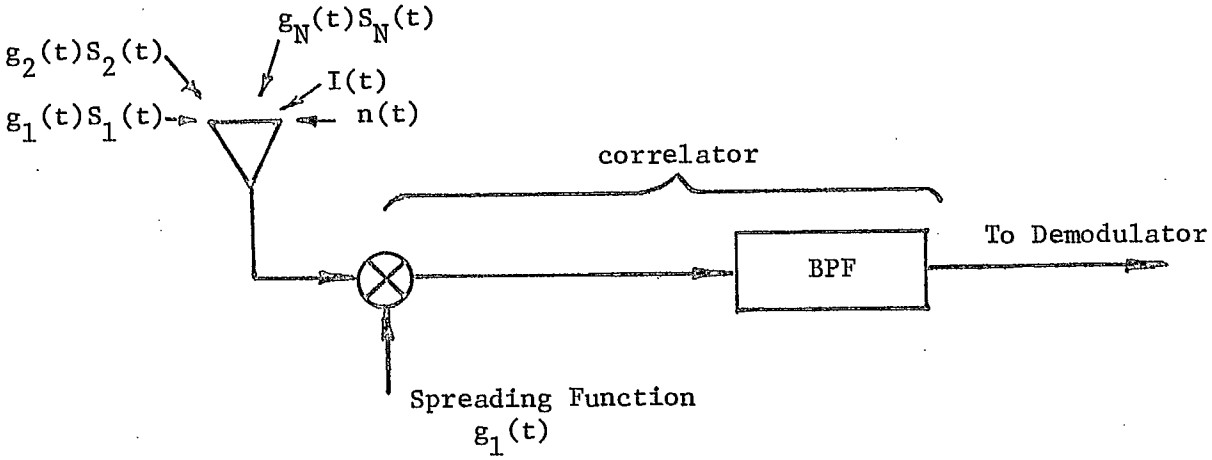
1.2 Basic Concept of Spread Spectrum

Under normal communication situations in which the information is to be conveyed over a certain distance, the baseband information is modulated onto a carrier to avoid excessive propagation attenuation. When there is more than one user involved, simultaneous transmission by many users over a common channel will result in interference. Superposition of a code, which is known only to the intended receiver, will permit extraction of the wanted information provided that the code and the encoding process have the following properties: 1) at the receiver, signals from unwanted users will look like noise, and 2) the superposed code is transparent to the baseband information signal, i.e., removal of the code at the receiver will not perturb the baseband information. Property 1 is a code design problem, which we will deal with in Section 2. Property 2 is an encoding problem which we discuss below.

Generation of the transmitted signal in a multiple access environment thus involves two steps: conventional modulation of baseband information onto a carrier and subsequent encoding of a superposable orthogonal code. At the receiving end the process is reversed: removal of the code and demodulation to reproduce the baseband information. The basic concept of spread spectrum communication is depicted in Fig. 1.1 [Utlaut, 1978].



(a) Transmitter



(b) Receiver

Fig. 1.1 Basic Spread Spectrum Concept

In Fig. 1.1, $S_1(t)$ is the wanted signal, $S_i(t)$, i = 2,3,...,N are the (N-1) unwanted signals, I(t) is other interference and n(t) is additive noise. The intended user will have $g_1(t)$ as its despreading function, which is identical to the spreading function employed to protect the identity of baseband information $m_1(t)$. Let $\langle x,y \rangle$ denote the inner product of the variables x and y. It is desired that $\langle g_1(t), g_1(t) \rangle = 1$ and $\langle g_1(t), g_i(t), i \neq 1 \rangle = 0$, i.e., $\{g_i(t)\}_{i=1}^{N}$ is a set of N orthonormal functions, and that the spectra of $g_1(t)\ I(t)$ and $g_1(t)\ n(t)$ will be wide compared to the baseband information bandwidth. It is possible that the interferer I(t)

may itself be narrowband, so that it is necessary that the spreading function $g_1(t)$ be of very wideband, since the bandwidth of $g_1(t)$ I(t) is given by the sum of the bandwidth of $g_1(t)$ and that of I(t). In CDMA the spreading function $g_1(t)$ is the code which has a bandwidth $B_c >> B_m$, where B_m is the information bandwidth. The processing gain G_p is thus given by the ratio: $G_p = B_c/B_m$, so that the output signal-to-noise ratio is related to the input signal-to-noise ratio as follows: $(S/N)_o = G_p(S/N)_i$. For design consideration the signal-to-noise ratio equation is insufficient, i.e., it is impractical for the signal to be G_p(dB) below the interferer, since we must take into account a certain minimum output signal-to-noise ratio requirement to yield the identity of the information and the losses incurred by the processor. Let $(S/N)_o$ be this output signal-to-noise ratio requirement and L be the processing loss. The interference margin M_i is defined as [Dixon, 1965].

$$M_i = G_p + (L + (S/N)_o) \text{ dB}.$$

1.3 Direct Sequence (DS) Signaling

By a sequence it is meant that its elements assume values from a finite alphabet. While the alphabet size of the sequences discussed in Section 2 is arbitrary, for spread spectrum applications the most interesting sequences are those drawn from an alphabet of 2 elements, i.e., in GF(2). In this section we are concerned with binary spreading sequences or codes. While we can employ the spread spectrum signal generation as depicted in Fig. 1.1, in which the information is modulated onto a carrier and the modulated signal is then subsequently encoded by modulating the code onto this RF signal, it is better to first combine the information signal and the spreading sequence before modulation. If the original

information is an analog waveform, combining the information with the spreading code requires first digitizing the analog waveform and encoding the result into a PCM signal. Combining the PCM signal with the spreading code can then be accomplished using a modulo 2 operation which has the property that

$$(c \oplus a) \oplus c = a$$

Thus, if "c" is the code and "a" is the PCM information signal, removal of the code from the composite sequence $c \oplus a$ can be accomplished by modulo 2 adding to it the code c. It is in this context the spreading code is transparent to the information signal.

The process of combining the information sequence "a" with the code "c" is called code modification. The code "c" itself is referred to as the unmodified code. Modulation of the composite sequence $c \oplus a$ onto the carrier can be done using a variety of modulation schemes, such as pam and fsk. However, phase-shift keying (psk) is preferred on account of 1) the modulated signal has a constant envelope so that for the bandwidth used, the transmitted power is maximized, and 2) psk is equivalent to double sideband suppressed carrier modulation, so that it is easier to generate the psk than fsk signal. In fact psk can be accomplished using balanced modulation as depicted in Fig. 1.2.

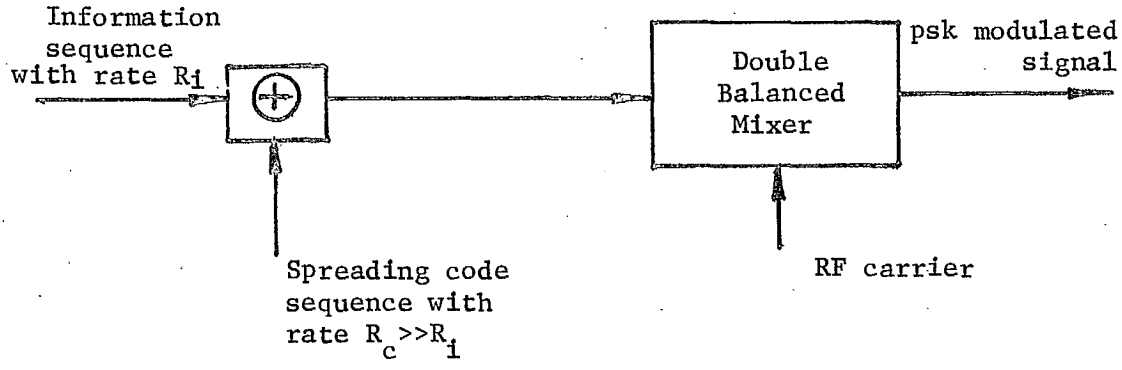


Fig. 1.2 Direct Sequence Signaling with psk Modulation

Binary psk is also known as phase reversal modulation. Whenever the composite code c⊕a has a transition from ONE to ZERO or from ZERO to ONE, the carrier changes phase by π radians. The phase-shift keying process is illustrated in Fig. 1.3. If an unmodified code is used at the

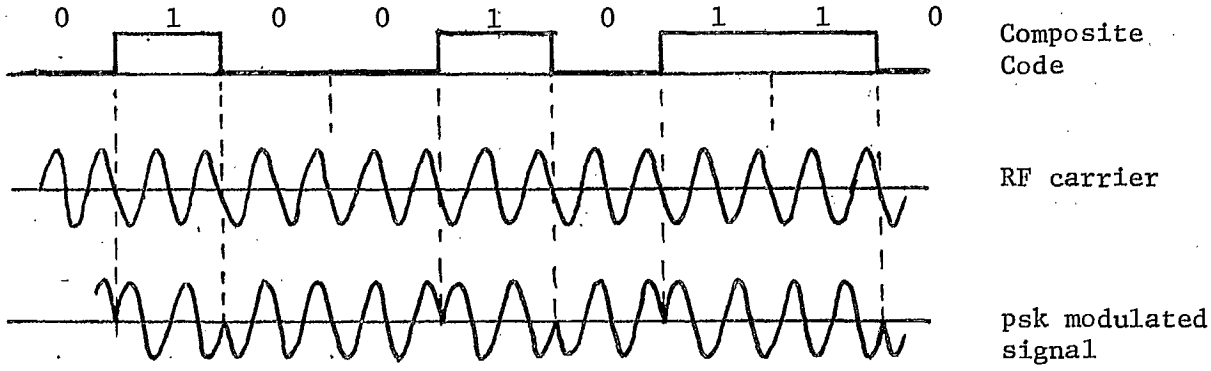


Fig. 1.3 psk Waveform

receiver to balance demodulate the psk signal, the recovered signal will be an information sequence modulated psk, which is at the same carrier frequency as the incoming psk signal. Such a code removal process is known as in-line correlation, the object of which is to reject interfering signals. Since the recovered signal is at the same carrier frequency as the input psk, a narrowband interfering signal could conceivably leak through the correlator, defeating the purpose of spreading the spectrum. A process which generates an output at a center frequency different from the carrier frequency of the input psk is known as an heterodyne correlator. The essential feature of an heterodyne correlator is that the signal used for despreading is at a carrier frequency $f_c + f_{IF}$, where f_c is the carrier of the incoming psk and f_{IF} is a chosen IF frequency. The reference signal is itself a psk in which the modulating signal is the code sequence and the local carrier is $f_c + f_{IF}$. The code removal process is depicted in Fig. 1.4, in which the reference signal is assumed to be synchronized

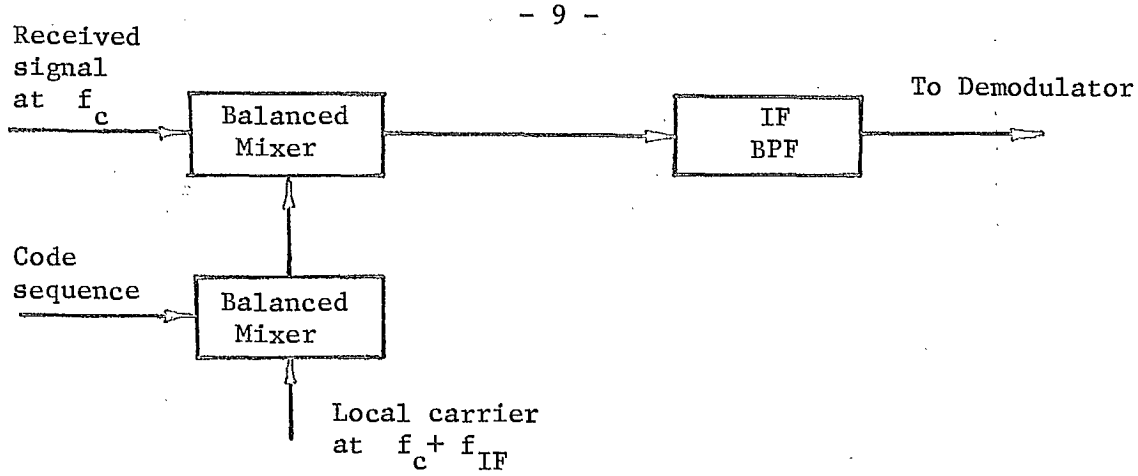


Fig. 1.4 Heterodyne Correlator to Remove Code Sequence

with the incoming RF signal. We postpone discussions of synchronization techniques and the effect of synchronization errors on correlation to Section 3.

1.4 Frequency Hopping (FH) Signaling:

The principle behind frequency hopping (FH) signaling is the same as in direct sequence (DS) signaling; FH differs from DS only in the manner with which FH or DS is implemented. Thus, as with DS there is no restriction on the choice of modulation. The code sequence is used to randomly switch the carrier frequency instead of directly modulating the carrier. A functional block diagram of the transmitter and receiver of an FH signaling system is depicted in Fig. 1.5. Basically, when the local oscillator (frequency synthesizer) in the receiver is switched with a synchronized replica of the transmitted code, the frequency hops on the received signal will be removed, leaving the original modulated signal untouched. An offset f_{IF} frequency is applied at the receiver for the same reason that f_{IF} is used for code removal in DS signaling.

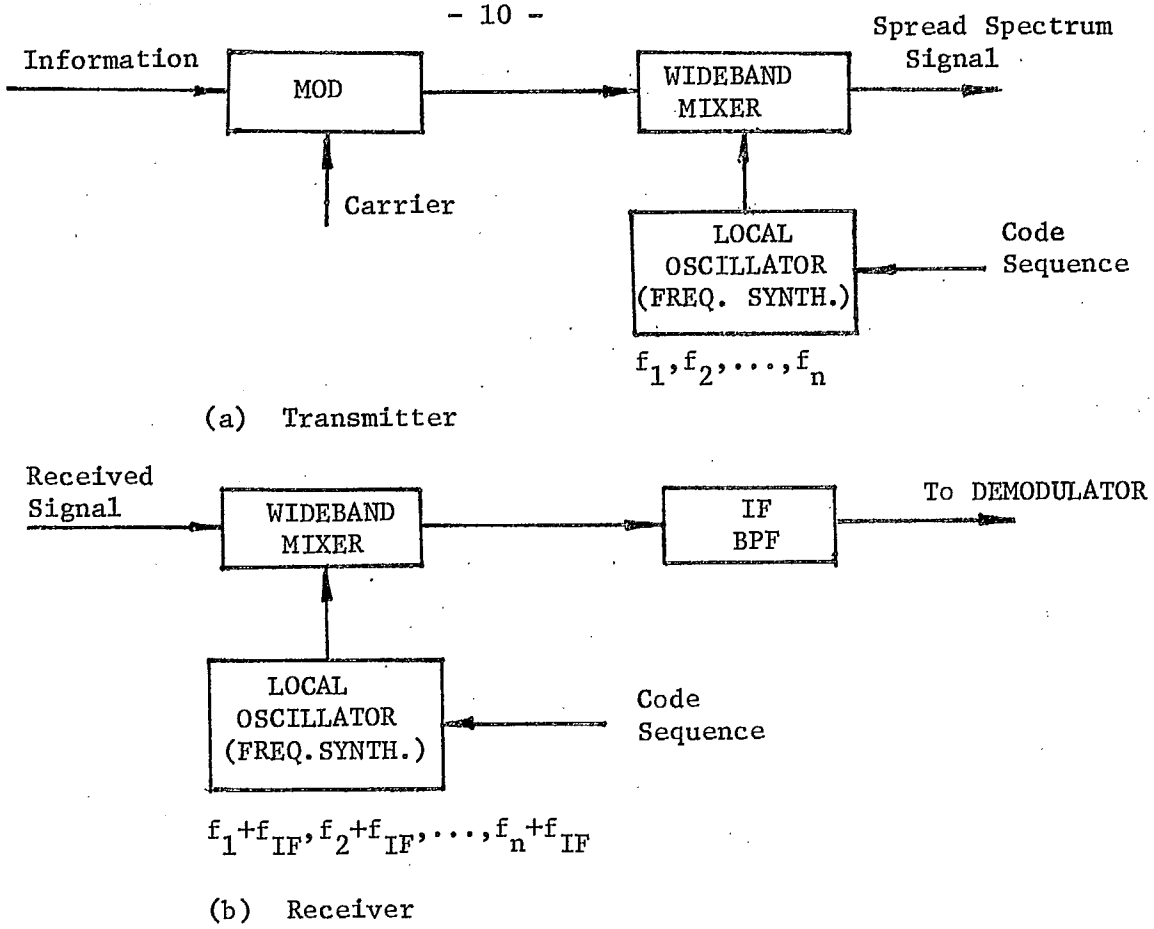


Fig. 1.5 Functional Block Diagram of a Frequency Hopping Signaling System.

Let Δf be the frequency separation between discrete frequencies and N be the number of available frequency choices. If the channel spacing is contiguous, i.e., nonoverlapping, the spread spectrum bandwidth is $B_{RF} = N \Delta f$. The processing gain is then $G_p = B_{RF}/B_m$, where B_m is the bandwidth of the information. If the frequency separation is chosen such that $\Delta f = B_m$, then $G_p = N$, which is the number of channels used. A DS signal requires a high code rate R_c in order to attain a high processing gain since the bandwidth of the code is $B_c = 2R_c$. A frequency hopping signal, however, does not require a high hopping rate. Moreover, it is desirable that the frequency-hopping rate be the same as the information rate. If the frequency-hopping rate is greater than the information rate, it tends

to spread the spectrum to exceed the received information bandwidth. However, there may result in a residual phase modulation which may seriously degrade the performance of subsequent demodulation of the information. On the other hand, if the frequency-hopping rate is less than the information rate, interference from unwanted signals will tend to be coherent. However, the occurrence of interference will tend to be intermittent with periods of one hop suffering heavy interference and long periods of many hops being free of interference. This latter feature is dependent on the correlation property of the code and the code length.

With frequency hopping it is difficult to maintain carrier coherence across the wideband. Thus the signal presented to the demodulator may change phase each time the system hops to a new frequency. Therefore, coherent demodulation is not suitable for FH signaling. Instead simple envelope detection, which does not care about input phase shifts and can respond quickly to pulsed signals, is most often used.

1.5 FH/DS Signaling:

Hybrid FH/DS signaling extends the spectrum spreading range attainable by FH or DS alone. Basically FH/DS signaling consists of a direct sequence modulated signal whose center frequency hops periodically. The hybrid FH/DS signaling procedure is depicted in Fig. 1.6.

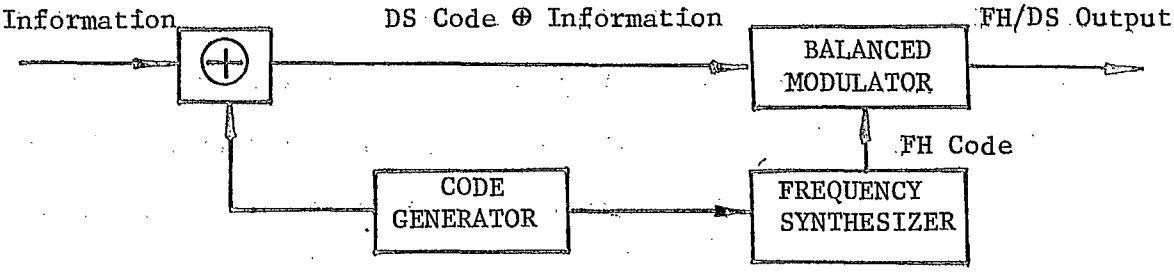


Fig. 1.6 Hybrid FH/DS Signaling

The DS code rate is normally much faster than the rate of frequency hopping. Therefore many bits of the DS code will occur in a single frequency channel. Also, the number of channels available is usually much smaller than the number of code bits so that in the course of a complete code length all the frequency channels will have been used many times. The pattern of their use is random depending on the randomness of the code itself.

As in DS signaling removal of the code in a hybrid signaling system also employs heterodyne correlation, the difference being in that the reference signal is also hybrid FH/DS. A hybrid FH/DS receiver is illustrated in Fig. 1.7.

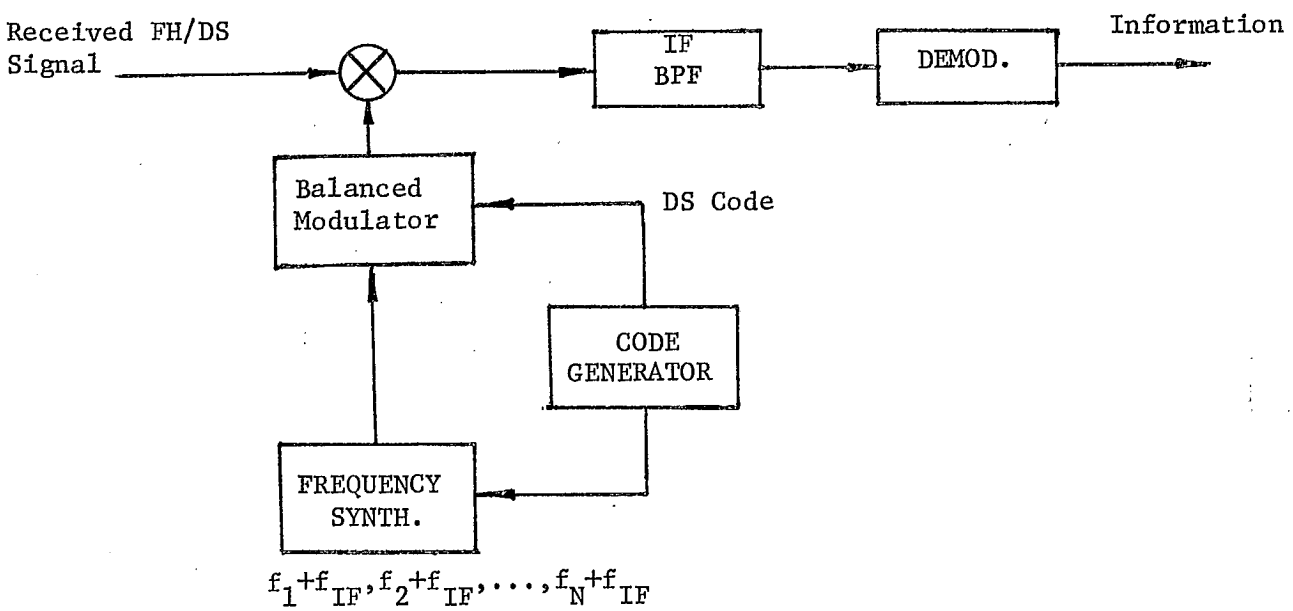


Fig. 1.7 Hybrid FH/DS Receiver

The processing gain of a hybrid FH/DS signal in dB is given by the sum of the processing gains of the FH and the DS signals, i.e.,

$$G_p(\text{FH/DS}) = G_p(\text{FH}) + G_p(\text{DS})$$

$$= 10 \log_{10}(\text{number of channels}) + 10 \log_{10} \frac{B_c}{B_m} \text{ dB.}$$

To achieve the same processing gain as FH/DS, a DS signal must have a very high code rate or the FH signal must have a huge number of channels. Because of a reduction in the number of channels and in the code rate, FH/DS offers simpler implementation possibilities.

1.6 Summary:

To attain a reasonably large processing gain the code rate has to be high compared to the information rate and the code length must be large. For SSMA applications long codes are essential.

Although multi-level codes, which lead to m-ary psk signaling, are interesting in themselves, the simplicity with which binary psk offers overrides any advantage multi-level codes may have over binary codes in SSMA applications [Judge, 1962; Aein, 1964; Gold, 1967].

References

Abramason, N. (1970, "The ALOHA System - Another Alternative for Computer Communication," AFIPS Conf. Proc., Fall Joint Computer Conference, 37, pp. 281-285.

Aein, J.M. (Dec. 1964), "Multiple Access to a Hard-Limiting Communication-Satellite Repeater," IEEE Trans. Space Electron. Telem., Vol. SET-10, pp. 159-167.

Cohen, A.R., Heller, J.A., and Viterbi, A.J., (Oct. 1971), "A New Coding Technique for Asynchronous Multiple Access Communication," IEEE Trans. Commun., Vol. COM-19, No. 5, Part II, pp. 849-855.

Dixon, R.C. (1976) ed., Spread Spectrum Techniques, IEEE Press.

Dixon, R.C. (1976), Spread Spectrum Systems, John Wiley.

Gold, R. (Oct. 1976), "Optimal Binary Sequences for Spread Spectrum Multiplexing," IEEE Trans. Inform. Theory, Vol. IT-13, pp.619-621.

Judge, W.J. (May 1962), "Multiplexing Using Quasiorthogonal Binary Functions," AIEE Trans. Commun. Electron., Vol. 81, pp. 81-83.

Kleinrock, L. and Tobagi, F.A. (Dec. 1965), "Packet Switching in Radio Channels: Part I - Carrier Sense Multiple-Access Nodes and Their Throughput - Delay Characteristics," IEEE Trans. Commun., Vol. COM-23, No. 12, pp. 1400-1416.

Konheim, A.G. and Meister, B. (July 1974), "Waiting Lines and Times in a System with Polling," Journal of the Association for Computing Machinery, Vol. 21, No. 3, pp. 470-490.

Lefande, R.A. (Oct. 1970), "Effects of Phase Nonlinearities on Phase Shift Keyed Pseudo Noise/Spread Spectrum Communication Systems," IEEE Trans. Commun. Technol., Vol. COM-18, No. 5, pp. 685-686.

Mark, J.W. (Sept. 1978), "Global Scheduling Approach to Conflict-Free Multiaccess via a Data Bus," IEEE Trans. Commun., Vol. COM-26, No. 9, pp. 1342-1352.

Nossen, E.J. (Apr.-May, 1974), "Fast Frequency-Hopping Synthesizers," RCA Eng. Vol. 19, No. 6, pp. 81-85.

Ross, G.N. (1974), "Digital Control of Active Jamming Systems," IEEE Proc. Nat'l. Aerospace Electron. Conf., Dayton, Ohio.

Utlaut, W.F. (Sept. 1978), "Spread Spectrum: Principles and Possible Application to Spectrum Utilization and Allocation," IEEE Commun. Society Magazine, Vol. 16, No. 5, pp. 21-30.

2. SEQUENCES AND THEIR CORRELATION PROPERTIES

2.1. Introduction

The purpose of this section is to survey the design and analysis of sequences or sets of sequences with small autocorrelation and crosscorrelation values. While much of the interest is focussed on sequences over the alphabet $\{\pm 1\}$, other alphabets are also considered. In particular the alphabet consisting of the k^{th} roots of unity for some integer k has been of interest since this corresponds to the phase coding of signals.

There are no proofs of any of the results included here and the construction of the sequences is described in varying amounts of detail, depending more on the author's interest in them rather than in their assessment of their importance.

There is a wide variation in the literature for the notation of these problems and in the next section we establish our own notation for use throughout the report. Thus readers going from this report to the original articles will have some translation to do. Some general bounds and properties of the periodic and aperiodic correlation functions are also given in the next section. Section 2.3 considers Barker sequences and the existence problem for them. Maximum length sequences are discussed at some length in Section 2.4. While the basic properties of such sequences have been known for some time, recent work has considerably extended this knowledge particularly on the cross correlation properties of distinct sequences. A few of these new results are mentioned. In Section 2.5 the construction of multiphase sequences with desirable correlation properties is considered and in Section 2.6 the construction of sequences (both binary and multiphase) which produce correlation functions with certain properties. At

times these two approaches are quite ambiguous and so there is considerable overlap. There is an obvious connection between the design of sequences with good correlation properties and the design of error correcting codes with good distance properties. This connection is briefly explored in Section 2.7. Section 2.8 considers the complementary sequences of Golay and their extensions.

An annotated bibliography has been included as the Appendix as a ready reference for readers interested in the contents of a particular paper. More detailed comments on the paper will be normally found in the text but often scattered among various sections and perhaps difficult to locate. The duplication involved in this approach was felt to be worth the convenience. Likewise, all references are by author and date to give the reader an immediate indication of the historical perspective of the results.

2.2. The Periodic and Aperiodic Correlation Functions

Let $\underline{x}^{\nu} = \{x_0^{\nu}, x_1^{\nu}, \ldots, x_{n-1}^{\nu}\}$, $\nu = 1, 2, \ldots, M$ be a set of M sequences of complex numbers of length n. Define the aperiodic cross-correlation function

$$c_{\nu\lambda}(\ell) = \begin{cases} \sum_{i=0}^{n-1-\ell} x_i^{\nu}\, \bar{x}_{i+\ell}^{\lambda} & \ell = 0,1,\ldots,n-1 \\ \sum_{i=0}^{n-1+\ell} x_{i-\ell}^{\nu}\, \bar{x}_i^{\lambda} & \ell = -1,-2,\ldots,-(n-1) \end{cases} \qquad \nu,\lambda = 1,2,\ldots,M$$

where the overbar indicates complex conjugation. The periodic cross-correlation function is

$$a_{\nu\lambda}(\ell) = \sum_{i=0}^{n-1} x_i^{\nu}\, \bar{x}_{i+\ell}^{\lambda} \qquad \ell = 0,1,\ldots,n-1$$

$$= c_{\nu\lambda}(\ell) + \bar{c}_{\lambda\nu}(n-\ell) = c_{\nu\lambda}(\ell) + c_{\nu\lambda}(\ell-n)$$

since it is readily verified that $\bar{c}_{\nu\lambda}(\ell) = c_{\lambda\nu}(-\ell)$. The odd cross-correlation function is defined by

$$b_{\nu\lambda}(\ell) = c_{\nu\lambda}(\ell) - c_{\nu\lambda}(\ell-n)$$

and has been shown to be of significance in the performance of binary asynchronous phase coded spread spectrum multiple access (SSMA) systems. Specifically it is important in establishing synchronization when succeeding binary symbols are different. Reference to it in the literature is limited.

The periodic, odd and aperiodic autocorrelation functions are

$$a_\nu(\ell) = a_{\nu\nu}(\ell),\ b_\nu(\ell) = b_{\nu\nu}(\ell) \text{ and } c_\nu(\ell) = c_{\nu\nu}(\ell);\ \ell = 1,2,\ldots,M$$

respectively and when only the one sequence is under consideration (M=1), the subscripts will be omitted. Notice that

$$c_\nu(-\ell) = \bar{c}_\nu(\ell) \quad \text{and} \quad a_\nu(\ell) = c_\nu(\ell) + \bar{c}_\nu(n-\ell)\ .$$

It is also easy to show that the periodic correlation function is invariant under cyclic shifts of the sequence but the odd correlation function is not.

Much of the work in this report will be concerned with sequences over finite alphabets and usually over the complex m^{th} roots of unity, for some positive integer m The aim is to design sets of sequences whose off peak autocorrelation values and whose cross correlation values for all shifts are minimized in magnitude. For this reason we define the following quantities:

$$m_a = \max_{1\le\nu\le M} \max_{1\le\ell<n} |a_\nu(\ell)|$$

and

$$m_a' = \max_{\nu\neq\lambda} \max_{0\le\ell<n} |a_{\nu\lambda}(\ell)|$$

i.e., m_a is the maximum off peak magnitude of the periodic autocorrelation function of any of the M sequences and m_a' is the maximum magnitude of any of the periodic cross correlations. The quantities m_b, m_b', m_c and m_c' denote

the odd and aperiodic autocorrelation and cross-correlation functions. The same notation will be used when there is only one sequence under consideration, M=1.

It is useful to derive some general relationships and inequalities on these quantities for later use and consider first the work of Welch (1974). For a set of M sequences of length n let

$$a_{max} = \max (m_a, m_a')$$

i.e., a_{max} is the maximum magnitude of the off peak autocorrelation values and the cross-correlation value for any shift. It can then be shown that, for any positive integer k,

$$a_{max}^{2k} \geq \frac{1}{(Mn-1)} \left[\frac{Mn}{\binom{n+k-1}{k}} - 1 \right]$$

and, in particular for k = 1,

$$a_{max} \geq \left[\frac{M-1}{Mn-1} \right]^{1/2} \tag{2.1}$$

By appending (n-1) zeroes to each of the M sequences, to give sequences of length (2n-1), the periodic correlation and cross-correlation functions of the extended sequences are the aperiodic correlations of the original sequences. Defining c_{max} for the aperiodic case in the same manner as for the periodic case the above bounds, modified by replacing n with 2n-1, become

$$c_{max}^{2k} \geq \frac{1}{((2n-1)M-1)} \left[\frac{M(2n-1)}{\binom{2n+k-2}{k}} - 1 \right]$$

and for k = 1 this inequality reduces to

$$c_{max} \geq \left[\frac{M-1}{M(2n-1)-1} \right]^{1/2} \tag{2.2}$$

Such bounds are useful in evaluating particular sets of sequences.

Pursley and Sarwate (1977a) established the following identity, in their examination of phase coded SSMA systems: if x^{μ}, x^{η}, x^{ν} and x^{λ} are four sequences of period n then

$$\sum_{\ell=0}^{n-1} a_{\mu\eta}(\ell)\, \bar{a}_{\nu\lambda}(\ell+k) = \sum_{\ell=0}^{n-1} a_{\mu\nu}(\ell)\, \bar{a}_{\eta\lambda}(\ell+k). \tag{2.3}$$

Notice that if $\mu = \nu$ and $\eta = \lambda$ and $k = 0$ the identity reduces to

$$\sum_{\ell=0}^{n-1} |a_{\mu\eta}(\ell)|^2 = \sum_{\ell=0}^{n-1} a_{\mu}(\ell)\, \bar{a}_{\eta}(\ell) \tag{2.4}$$

which is an interesting observation on the relationship between cross-correlations and autocorrelations, noted as proposition 1 in Pursley and Sarwate (1977b). For the case when $x_i = \pm 1$ equation (2.4) reduces to

$$\sum_{\ell=0}^{n-1} a_{\mu\eta}^{2}(\ell) = N^2 + \sum_{\ell=1}^{n-1} a_{\mu}(\ell)\, a_{\eta}(\ell)$$

and applying Cauchy's inequality to the right hand sum gives the bounds

$$n^2 - \left\{\sum_{\ell=1}^{n-1} a_{\mu}^{2}(\ell)\right\}^{1/2} \left\{\sum_{\ell=1}^{n-1} a_{\eta}^{2}(\ell)\right\}^{1/2} \le \sum_{\ell=0}^{n-1} a_{\mu\eta}^{2}(\ell) \le n^2 + \left\{\sum_{\ell=1}^{n-1} a_{\mu}^{2}(\ell)\right\}^{1/2} \left\{\sum_{\ell=1}^{n-1} a_{\eta}^{2}(\ell)\right\}^{1/2} \tag{2.5}$$

This equation is useful in examining the performance of a given set of sequences since we are interested in minimizing both $|a_{\mu}(\ell)|$, $\ell \neq 0$ for each sequence μ for good acquisition and synchronization, and $|a_{\mu\eta}(\ell)|$, $\mu \neq \eta$ for good discrimination between users.

The corresponding results for the aperiodic correlation function are:

$$\sum_{\ell=-(n-1)}^{(n-1)} c_{\mu\eta}(\ell)\, \bar{c}_{\nu\lambda}(\ell+k) = \sum_{\ell=-(n-1)}^{(n-1)} c_{\mu\nu}(\ell)\, \bar{c}_{\eta\lambda}(\ell+k)$$

and, for binary sequences,

$$n^2 - 2\left\{\sum_{\ell=1}^{n-1} c_\mu^2(\ell)\right\}^{1/2}\left\{\sum_{\ell=1}^{n-1} c_\eta^2(\ell)\right\}^{1/2} \le \sum_{\ell=-(n-1)}^{(n-1)} c_{\mu\eta}^2(\ell) \le n^2 + 2\left\{\sum_{\ell=1}^{n-1} c_\mu^2(\ell)\right\}^{1/2}\left\{\sum_{\ell=1}^{n-1} c_\eta^2(\ell)\right\}^{1/2}$$

In applications it is important to have both m_a and m_a' as small as possible and it is known there is a trade-off --- one cannot have a set of sequences with both m_a and m_a' arbitrarily small. Pursley (1978a, 1978b) examines this trade-off and shows (Pursley 1978b) that for any set of M sequences

$$\left(\frac{m_a'}{n}\right)^2 + \frac{n-1}{n(M-1)}\left(\frac{m_a}{n}\right)^2 \ge 1 \qquad (2.6)$$

and this relation gives a lower bound on one of the parameters m_a, m_a', when the other is given. It is also shown there that if $M \ge (n+1)^2$ then $m_a' \ge \sqrt{n}$. It is also shown that equation (2.6) is valid for the aperiodic correlation function i.e., with m_a, m_a' replaced with m_c, m_c'. As a consequence of these results it is shown that attempting to reduce the value of $(m_a')^2/n$ below 1 will imply that the set of sequences will have a substantial increase in $(m_a)^2/n$ above 0. Various sets of sequences are constructed in Pursley (1978b) and in particular a set of n sequences of length n for which $(m_a')^2/n = 0$ and $(m_a)^2/n = n$, and a set for which $(m_a')^2/n = 1$ and $(m_a)^2/n = 0$, for n odd.

In a slightly different approach Pursley (1978a) defined the quantities

$$P_{\nu\lambda} = \frac{1}{n^2}\sum_{\ell=0}^{n-1} |a_{\nu\lambda}(\ell)|^2 \qquad \nu \ne \lambda$$

and

$$Q_\nu = \frac{1}{n^2} \sum_{\ell=0}^{n-1} |a_\nu(\ell)|^2$$

and showed that

$$\sum_{\substack{\nu,\lambda \\ \nu\neq\lambda}} P_{\nu\lambda} + \sum_{\nu} Q_\nu \geq M(M-1)$$

assuming that $a_\nu(0) = n$ for each ν in the set of size M. Consequently if $\bar{P}$ and $\bar{Q}$ are the maximum values of $P_{\nu\lambda}$ and Q_ν respectively then

$$\bar{P} + (K-1)^{-1} \bar{Q} \geq 1$$

and again the tradeoff between autocorrelation and cross-correlation peaks is observed. Similar results are obtained for the aperiodic correlation case.

In the same spirit as many arguments of coding theory it is natural to ask the question "how large can a set of binary sequences of length n be if the maximum off peak aperiodic autocorrelation function is to be less than $n\alpha$ and the maximum aperiodic cross-correlation function is to be less than $n\beta$?". As in coding theory, random coding and expurgation arguments can be used to prove existence of such sets for certain parameters. Using this approach Schneider and Orr (1975) proved the following:

Theorem (Schneider and Orr, 1975). Let α and β satisfy $0 \leq \alpha \leq 1$ and $0 \leq \beta \leq 1$. There exists at least one set of binary (± 1) sequences of length n, S_n, such that $m_c < n\alpha$, $m_c' < n\beta$ and

$$|S_n| \geq \begin{cases} 0 & \text{if } H(\frac{1-\alpha}{2}) \geq 1 - \frac{\log(4n)}{n} \\ \\ \frac{1}{16n} \{\exp_2 [n(1-H(\frac{1-\beta}{2}))]\}\{1-4n \exp_2[-n(1-H(\frac{1-\alpha}{2}))]\} \end{cases}$$

As a corollary to this theorem it can be shown that there exist sets S_n such that $|S_n|$ grows exponentially with n for fixed β, providing α

does not approach zero faster than $1/\sqrt{n}$. Similarly it can be shown that there exist sets such that $|S_n|$ grows as some power of n (the power being less than unity) providing neither α nor β approaches zero faster than $1/\sqrt{n}$. Such statements are useful in evaluating sets of sequences. Seguin (1978) obtained similar results for skew symmetric binary sequences (ie., sequences for which $x_j\, x_{n-1-j} = (-1)^{j+1}$ if $4|(n+1)$ and $(-1)^j$ if $4|(n-1)$) using similar methods.

Moon and Moser (1968) showed that if $c_n' = \max_{\ell>0} c_\nu(\ell)$ where c_ν is the autocorrelation function of a sequence of length n then "for almost all" sequences of length n

$$1-\varepsilon < \frac{\log c_n'}{\frac{1}{2}\log n} < 1+\varepsilon.$$

The phrase "for almost all" sequences implies the statement is true for all but a fraction of the 2^n possible sequences, and this fraction tends to zero as n tends to infinity. In a probabilistic measure theoretic sense we would say that the probability measure of the set where

$$\left\{ \left| \frac{\log c_n'}{\frac{1}{2}\log n} - 1 \right| \geq \varepsilon \right\}$$

tends to zero as n tends to infinity if the measure is uniform on the set of all possible sequences. Roefs and Pursley (1977) are able to make the same statement with c_n' replaced by

$$c_n'' = \max_{\ell} c_{\nu\lambda}(\ell)$$

for any two sequences $\underline{x}^\nu$, $\underline{x}^\lambda$ drawn from the set of all possible 2^{2n} sequences.

In several places in the report it is necessary to transform a binary (0,1) sequence $\underline{x} = (x_0, x_1, \ldots, x_{n-1})$ into a binary (-1, +1) sequence

$\underline{y} = (y_0, y_1, \ldots, y_{n-1})$ by the transformation $\eta: 0 \to +1,\ 1 \to -1$. For this transformation of n-tuples we will use the notation $\underline{y} = \eta(\underline{x})$ and $\underline{x} = \eta^{-1}(\underline{y})$.

2.3. Barker Sequences

The original problem considered by Barker (1957) was concerned with the design of binary (±1) sequences for which the off centre aperiodic correlation is either 0 or -1. The sequences he determined are:

$n = 3 \quad + + -$

$n = 7 \quad + + + - - + -$

$n = 11 \quad + + + - - - + - - + -$

It has since become conventional to only require that $|c(\ell)| \leq 1 \ \ell \neq 0$ and, under this relaxed condition, the following sequences can be obtained (as given in Turyn and Storer (1961)):

$n = 2 \quad + +$

$n = 4 \quad + + + -;\ + + - +$

$n = 5 \quad + + + - +$

$n = 13 \quad + + + + + - - + + - + - +$.

For n odd these are in fact the only sequences with the required property (Turyn, 1961). While a complete proof of this theorem is beyond the purpose of this survey some points established in it are worth mentioning. Since we assume that $x_i = +1$ or -1, terms of the form $x_i x_{i+k}$ are also either +1 or -1 and, for any binary sequence we have

$$\prod_{i=0}^{n-1-k} x_i x_{i+k} = (-1)^{(n-k-c(k))/2} \qquad 1 \leq k < n-1 \ .$$

Multiplying two equations of this form yields

$$x_{n-k}\, x_{k+1} = (-1)^{n-k-(c(k)+c(k+1)+1)/2}, \qquad 0 \leq k \leq n-2.$$

Since the sequences under consideration are real

$$c(k) + c(n-k) = \sum_{0}^{n-1} x_i \, x_{i+k}$$

and hence

$$\prod_{0}^{n-1} x_i \, x_{i+k} = 1 = (-1)^{(n-c(k) - c(n-k)/2}$$

implying that $c(k) + c(n-k) \equiv n \pmod 4$. Now for Barker sequences $|c(k)| \leq 1$ and it follows that for such sequences $c(k) = 0$ for $(n-k)$ even and $c(k) = \pm 1$ for $(n-k)$ odd. It also follows that if $n \equiv 2 \pmod 4$ then $n = 2$ since if $n > 2$ then $c_n = c_{n-2}$ but $c_2 + c_{n-2} = 0 \not\equiv n \pmod 4$. Thus for n even a Barker sequence of length n could exist only for $n \equiv 0 \pmod 4$ and for such sequences $c(k) + c(n-k) = 0$.

If n is odd then $c(k) = 0$ for n-k even and $c(k) = (-1)^{(n-1)/2}$ for $(n-k)$ odd and hence the $c(k)$ are in fact completely determined by these conditions.

For n even there is considerable evidence that there are no Barker sequences of length greater than 4. Historically, Luenberger (1963) showed that if a binary (± 1) Barker sequence of even length n exists then n must be a perfect square. Since it was previously known there is no Barker sequence of length 16, the only other possibilities for even length Barker sequences of lengths less than 100 are for those of lengths 36 and 64. Turyn (1963) observed that a necessary condition for Barker sequences of even length n to exist is that a sequence of length n with periodic correlation function $a(k) = 0$, $k \neq 0$ exist. The nonexistence of such a periodic sequence implies the nonexistence of the corresponding Barker sequence. Everett (1966) observed that the existence of a periodic sequence with the property that $a(k) =$ constant is equivalent to the existence of a difference

set with certain parameters. In this setting the nonexistence of Barker sequences of lengths 16 and 36 was well known. Turyn himself showed that Barker sequences of lengths $n = 4N^2$ where N is the power of a prime cannot exist thus eliminating n = 64 and leaving the smallest unresolved case as n = 6,084. In fact, the existence of a periodic sequence with zero off centre correlation is equivalent to a circulant Hadamard matrix and it has long been conjectured that the only such matrix has order 4.

Turyn (1967) defines the quantity

$$b(n) = \min_{n} \max_{j>0} |c(j)|$$

where the minimum is taken over all sequences of length n. Moser and Moon (1968) showed that if the binary ±1 sequence is chosen independently and at random then the maximum off peak value of c(j) will be of the order of $\sqrt{n}$. When the constraint that $|c(j)| \leq 1$, for Barker sequences, is relaxed to, say, $|c(j)| \leq 2$ then other sequences are of course found. For example Turyn (1967) notes that there are binary sequences of lengths 21, 25 and 28 with $|c(j)| \leq 2$ but none of lengths 22, 23, 24, 26 and 27. Other results achievable when the conditions to be satisfied by the autocorrelation function are relaxed are noted in the following sections.

We also mention here that periodic sequences with off peak values of c(j) a constant, correspond to cyclic difference sets and the situation with regard to these is summarized in Turyn (1967). Again, for periodic sequences the behaviour of $\min_{n} \max_{j} |a(j)|$ is of interest and it is noted that sequences achieving the minimum do not in general arise from difference sets since such sets with the requisite values are scarce.

In section 5 sequences over alphabets of size greater than two are considered and, in particular, such sequences which satisfy a Barker type

constraint on their correlation function are constructed.

2.4. Maximum Length Sequences

An enormous amount of effort has gone into the examination of maximum length sequences ie., sequences generated by a linear shift register whose feedback function is a primitive polynomial. In this section we give a brief review of the most important properties of such sequences and then consider a few of their properties of particular relevance to this work.

Recall first that since there always exists a primitive polynomial of degree m over GF(2), there always exists a maximum length sequence of length 2^m-1, for each positive integer m. For most values of m there will exist more than one such sequence and, in this case, the cross correlation function can be of interest.

Using the notation of MacWilliams and Sloane (1976) let h(x) be a primitive polynomial over GF(2) generating the maximum length sequence $a_0,a_1,a_2,\ldots,a_{2^m-2}$. Clearly any cyclic shift of this sequence is also a maximum length sequence corresponding to a different initial condition of the shift register. If $h(x) = \sum_0^m h_i x^i$ then each such sequence satisfies the recurrence relation

$$a_{i+m} = \sum_{j=0}^{m-1} h_j a_{i+j}.$$

For a maximum length sequence of length 2^m-1 any sequence of m consecutive bits is called a window and each possible non-zero binary (0, 1) m-tuple occurs exactly once among the 2^m-1 windows.

It can be shown that in any maximum length sequence there are 2^{m-1} 1's and $2^{m-1}-1$ 0's. The modulo 2 sum of a maximum length sequence with any

of its cyclic shifts is again a cyclic shift of the sequence.

Perhaps one of the most important properties of maximum length sequences is the shape of its correlation function. If we transform the binary (0,1) sequence of the shift register output to the binary (±1) sequence $b_0, b_1, \ldots, b_{2^m-2}$ where $b_i = (-1)^{a_i}$ then the periodic correlation function of this sequence is

$$a(k) = \sum_{j=0}^{2^m-2} b_j \, b_{j+k}$$

where, as usual, the subscripts are reduced modulo 2^m-1 where necessary. It is a simple matter to show that

$$a(k) = \begin{cases} n & , \quad k = 0 \\ -1 & , \quad k = 1,2,\ldots,2^m-2 \end{cases}$$

and of course this is the best possible correlation function in the sense that no other binary sequence has a correlation function for which $\max_{k\neq 0} a(k)$ is smaller.

Since a maximal length sequence is generated deterministically it cannot be called random and yet it has certain properties that one might naturally expect of a truly random sequence. For example if we define a run in a maximal length sequence to be a maximal string of consecutive identical symbols, then in any maximal length sequence one half of the runs have length one, one quarter of the runs have length 2, one eighth of the runs have length 3 and so on. However many other tests of randomness are possible and the question as to what distinguishes a maximal length sequence from a truly random binary sequence is one of some interest. One aspect of this question will be considered later in the section. The relationship between maximum length sequences, Hadamard matrices and Hamming codes is well known and is omitted here.

If $h(x)$ is the primitive polynomial associated with a particular maximum length sequence and $h^*(x) = x^m h(1/x)$ then the generator polynomial of the sequence will be defined by $g(x) = (x^{2^m-1}+1)/h^*(x)$. The polynomial representation of any of the 2^m-1 possible cyclic shifts of the sequence can then be described by the polynomial $a(x)g(x)$ for some binary polynomial $a(x)$ of degree less than m.

We consider now some properties of sequences obtained by employing techniques such as sampling or interlacing of shift register sequences. For example if, from the maximum length sequence over GF(p), $a_0, a_1, \ldots, a_{p^m-1}$, a new sequence is defined by the equation $b_i = a_{ki}$, $(k, p^m-1) = 1$, then either another maximum length sequence is obtained or it is a cyclically shifted version of the original one. Surböck and Weinrichter (1978) consider the problem when the sampling interval k is a divisor of the period. They define an elementary sequence as one whose feedback polynomial is an irreducible polynomial. If the period of this sequence has period $q = \prod p_i^m i$, the p_i distinct primes, then the sequence can be generated by interlacing elementary sequences of period $p_i^m i$. Lempel and Eastman (1971) were concerned with a high speed construction method for maximal length sequences. If $a_o, a_1, a_2, \ldots$ is a maximum length sequence of period $p=2^n-1$ then the sequences $\{d_i^j\}$ are defined by $d_i^j = a_{ik+j}$ for a given integer k, $j = 0,1,\ldots k-1$. When $(k,p) > 1$ define δ by $\delta = \min \{m \mid 2^m k = k \bmod (p)\}$. Then sequence $\{d_i^j\}$ satisfies a linear recursion of degree δ which is necessarily some divisor of n and has period $p_k = p/(p,k)$ or some divisor of it. In such a case different "phases" may, for the same k, result in sequences which are not cyclic shifts of each other. Using these facts Lempel and Eastman (1971) show how a given maximum length sequence of rate k,R can be realized by a combination of k shift registers each of length which is a divisor of n.

In a similar vein we describe the work of Surböck and Weinrichter. Using their notation, define the D-transform of a sequence $f_0, f_1, f_2, \ldots$ over GF(p) by $F(D) = \sum_{o}^{\infty} f_i D^i$. If the feedback polynomial is N(D) then

$$F(D) = H(D)/N(D)$$

where H(D) depends on the initial state of the register. If F(D) is the product of irreducible polynomials then the sequence F(D) is the sum of the corresponding elementary sequences. Assume now that N(D) is an irreducible polynomial of degree r, the minimal polynomial of $\alpha \varepsilon GF(p^r)$ with exponent L. The corresponding elementary sequence E(D) = H(D)/N(D) has period L where $L|(p^r-1)$. If $L = (p^r-1)/t$ there exists t different elementary sequences of period L, all with the same generator polynomial N(D) but different numerators H(D). Such a collection of sequences will be called a family of elementary sequences.

Assume now that L is nonprime and that q is an arbitrary factor of L, q = L/s. It is then shown that the elementary sequence E(D) = H(D)/N(D) with period L can be constructed by interlacing shorter elementary sequences $F_i(D)$ of period q generated by the same elementary polynomial A(D) where A(D) is the minimum polynomial of α^s, α a root of N(D). The application of this result to the generation of long maximum length sequences, each generated with the same feedback polynomial, is immediate. This characterization of maximum length sequences can be used to consider applications to synchronization problems and to explain certain phenomena on the cross correlation properties of such sequences.

Milstein (1977) considers the problem of rapid acquisition of synchronization and performance using suitable sequences. In particular, it is known that given m maximum length sequences of lengths n_i, i = 1,2,...,m,

$(n_i, n_j) = 1$, $i \neq j$, a composite sequence of length $N = \prod_{i=1}^{m} n_i$ can be formed. To establish synchronization with this composite sequence it is only necessary to perform $\sum_{1}^{m} n_i$ correlations as opposed to as many as $\prod_{1}^{m} n_i$ correlations for a maximum length sequence of this length.

On the subject of the rapid acquisition of synchronization, Stiffler (1968) observes that the number Σn_i of correlations required to acquire the composite sequence is much greater than the $\log_2 N$ binary decisions theoretically required. He then constructs sequences which can be acquired in such a number of decisions for $N=2^n$. The construction of the sequences is as follows. Let $b_j = \{\sigma_j^1, \sigma_j^2, \ldots, \sigma_j^n\}$ be the binary expansion for the integer $j-1$, $j = 1,2,\ldots,2^n$ where

$$j-1 = \sum_{i=1}^{n} (1 - \frac{\sigma_j^i}{2}) 2^{i-1}$$

and the σ_j^i is either $+1$ or -1. Then the rapid acquisition binary sequence is $(\xi_1, \xi_2, \ldots, \xi_N)$, $N-2^n$, is defined by

$$\xi_j = \begin{cases} 1 & \text{if } \sum_{i=1}^{n} \sigma_j^i \geq 0 \\ -1 & \text{if } \sum_{i=1}^{n} \sigma_j^i < 0. \end{cases}$$

It is shown how the phase of such sequences can be established by making only n binary decisions.

Maximum length sequences are also referred to as pseudo-noise sequences in the literature because of their random-like properties. It turns out however that not all maximum length sequences are "equally random" and that in applications the notion of the moments of weight distributions of subsequences is important in determining the "good" sequences. Consider the set of all subsequences of length M (ie., sets of consecutive M bits)

of the binary (0,1) maximum length sequence of length $N=2^r-1$. Let A_w be the number of these sequences of length M of weight w of the binary sequence $a_0,a_1,\ldots$ and let $b_0,b_1,\ldots, b_i = 1-2a_i$, be the corresponding ±1 sequence. If

$$S_k = \sum_{i=0}^{M-1} b_{k+i}$$

then the p^{th} moment of the weight distribution is given by

$$\underline{S}^p = \frac{1}{N} \sum_{i=0}^{N-1} S_i{}^p$$

as quantity which can also be expressed as

$$\underline{S}^p = \frac{1}{N} \sum_{w=1}^{M} (M-2w)^p A_w.$$

Lindholm (1968) showed that the first two moments are

$$\underline{S}^1 = -\frac{M}{N} \quad \text{and} \quad \underline{S}^2 = M\left(1 - \frac{(M-1)}{N}\right)$$

and are independent of the particular maximum length sequence chosen. An expression for the third moment is given as

$$\underline{S}^3 = -\frac{M^3}{N} + 3! \left(\frac{N+1}{N}\right) B_3$$

where B_3 is the number of trinomials of degree less than M divisible by f(x) the primitive polynomial of the shift register. In general the k^{th} moment of the distribution depends on B_k, the number of k-term (ie., k nonzero coefficients, including the constant and leading term) polynomial of degree less than M which are divisible by f(x). With the use of these moments of the weight distribution, some basis for determining which maximum length sequence to use in a given application can be made.

Wainberg and Wolf (1970) give the first four moments of all sub-sequences of length less than 100 for the six maximum length sequences of

length $N = 2^{23}-1$ and considered the skewness properties of the distributions obtained. To assist with this task simple algorithms for the calculation of the third and fourth moments are given.

Fredricsson (1975) also considers the weight distribution of subsequences of maximum length sequences. This is compared to an ideal distribution and a lower bound on the deviation between the actual and ideal is given. Some comments on the relationship between higher order correlations and the spectral tests of random sequences. It is also shown that maximum length sequences with good weight distribution and correlation properties can only exist for long sequences and a lower bound on the required length is given.

For multiple access systems large sets of sequences with low off peak autocorrelation and crosscorrelation values are required. It is of interest to determine the crosscorrelation values of two maximum length sequences since their autocorrelation functions are, in a sense, ideal. For the remainder of the section we consider certain results on this problem.

Gold (1968) examines the problem for certain maximum length sequences, and these have a coding theory interpretation. If α is a primitive element in $GF(2^n)$ and $T(.)$ is the trace function on $GF(2^n)$ then let $x_i^{\nu} = T(\alpha^{-i})$ be a maximal length sequence. Denote by $f(x)$ the minimal polynomial of α and by $V(f)$ the space of linear sequences generated by $f(x)$ ie.,

$$V(f) = \{h(x) \mid h(x) = g(x)/f(x), \text{ degree } g < \text{degree } f\}.$$

Let $S = \eta \circ T$ denote the conversion of the binary (0,1) sequences to the binary (+1,-1) sequences and as usual, let $a_{\nu\lambda}(k)$ denote the periodic crosscorrelation function between two ± 1 sequences $\underline{x}^{\nu}$ and $\underline{x}^{\lambda}$. Gold (1968) showed that if $x_i^{\nu} = S(\alpha_{-i})$ and $x_i^{\lambda} = S((\alpha^{2^{\ell}}+1)_{-i})$, where it is assumed that η is odd and that $(\ell,\eta) = 1$, then the autocorrelation function is given by

$$a_{\nu\lambda}(k) = \begin{cases} -1 & \text{if } x_k^{\nu} = 1 \\ \text{either } -(2^{(n+1)/2}+1) \text{ or } (2^{(M+1)/2}-1) & \text{if } x_k^{\nu} = -1. \end{cases}$$

This fact was actually found by Kasami in a University of Illinois report in coding terms when he established the weight distribution of the $(2^n-1,2n)$ code generated, by linear recursion, by the polynomial $f_1(x)f_{2^{\ell}+1}(x)$ where $f_i(x)$ is the minimal polynomial of α^i. The relationship between sequences and error correcting codes is explored further in Section 2.7.. For the present purpose, to describe the results of Gold (1967), we note that the BCH bound can be described by

$$g(x) = \frac{x^{2^n-1}+1}{\ell cm\{f_1(x), f_2(x), \ldots, f_{2k}(x)\}}$$

then for any two sequences $\underline{a}$, $\underline{b}$ ε V(g), the Hamming weight of $\underline{a} + \underline{b}$ is at least 2k+1. This fact can be used to show that if the integer t is defined by

$$t = \begin{cases} 2^{(n+1)/2}+1 & n \text{ odd} \\ 2^{(n+2)/2}+1 & n \text{ even} \end{cases}$$

and if $\eta^{-1}(\underline{x}^{\nu})$ ε V (f_1) and $\eta^{-1}(\underline{x}^{\lambda})$ ε V (f_t) then $|a_{\nu\lambda}(k)| \leq t$ for all $k > 0$, where $a_{\nu\lambda}(k)$ is the correlation function of the corresponding (± 1) sequences x^{ν} and x^{λ}.

Gold (1967) further shows that if f_1 and f_t are a pair of primitive polynomials, with t as defined above, which generate maximum length sequences of length 2^n-1, then the shift register corresponding to the product polynomial $f_1(x)f_t(x)$ will generate 2^n+1 different sequences each with period 2^n-1 and such that the crosscorrelation function satisfies the relation $|a_{\nu\lambda}(k)| \leq t$. This result assumes that if n is even then $n \not\equiv 0 \pmod 4$.

A characteristic sequence of V(f), f irreducible, is a sequence

$h \in V(f)$ such that $h_{2i} = h_i$, $i = 1,2,\ldots$. Such sequences are studied extensively in Gold (1966). The concept of a coset function of a characteristic sequence is introduced and the coset functions of all maximal length sequences are obtained. These notions however lie outside the present interests.

The recent work of Helleseth (1976b) is an extensive investigation into the crosscorrelation function between two maximal linear sequences. The main interest in this work is in determining the values that the crosscorrelation function takes on and the number of times it assumes these values over a single period. Both the case of binary sequences and those over GF(p) are considered and a few of these results will be mentioned here.

Recall first that there are $\varphi(p^n-1)/n$ maximal linear sequences over GF(p) where φ is Euler's Totient function that are not equivalent under cyclic shifts. If $\{a_j\}$ is a maximum length sequence then $\{a_{dj}\}$ is a maximum length sequence if and only if $(d, p^n-1) = 1$. Furthermore, if $\{a_j\}$ and $\{b_j\}$ are two inequivalent sequences then there exists an integer d relatively prime to p^n-1 such that $b_{j+k} = a_{dj}$. Thus, so far as the crosscorrelation function is concerned, it is entirely determined by the integer d for a fixed sequence $\{a_i\}$. The crosscorrelation function between the two maximal sequences is

$$a_{ab}(t) = \sum_{j=0}^{p^n-2} \theta(a_{j-t}) \; \bar{\theta}(b_j)$$

where $\theta(x) = \xi^x$, ξ a complex p^{th} root of unity, $\xi \neq 1$. This correlation function can be expressed as

$$a_{ab}(t) = \sum_{x \in GF(p^n)^*} \xi^{Tr(cx-x^d)} = a_d(t)$$

where $c = \alpha^{-t}$, α a primitive element of $GF(p^n)$ and $\{b_j\} = \{a_{dj}\}$. Several interesting results on this crosscorrelation function are obtained and we list several of them here:

a) $a_d(t)$ is a real number.

b) The values and the number of occurrences of each value of $a_d(t)$ are independent of the choice of ξ.

c) $a_d(t) = a_{d^{-1}}(-dt)$ where d^{-1}. $d \equiv 1 \bmod (p^n-1)$.

d) $a_{dp^j}(t) = a_d(t)$

e) $a_d(p^j t) = a_d(t)$

f) $\sum_{t=0}^{p^n-2} a_d(t) = 1$

g) $a_1(t) = \begin{cases} p^n-1 & , \quad t \equiv 0 \bmod (p^n-1) \\ -1 & , \quad t \not\equiv 0 \bmod (p^n-1) \end{cases}$

h) Over one period $a_d(t)$ has at least three values if and only if $d \notin \{1,p,\ldots,p^n-1\}$.

i) $a_d(t)$ is an integer for all t if and only if $d \equiv 1 \bmod (p-1)$.

j) We have $a_d(t) \equiv -1 \bmod (\Pi)$ and, furthermore, if $a_d(t)$ is an integer then $a_d(t) \equiv -1 \bmod (p)$. ($\Pi = 1-\zeta$, ζ a pth root of unity.)

k) For binary sequences $a_d(t) \equiv -1 \bmod (4)$ and, if $d \notin \{-1,-2,\ldots, -2^{n-1}\}$ then $a_d(t) \equiv -1 \bmod (8)$.

ℓ) The number of distinct values assumed by the crosscorrelation function of two binary maximum length sequences of period $p = 2^\ell-1$ can never exceed the number of cyclotomic cosets modulo p.

The remainder of the results in this interesting paper are concerned with the correlation functions for certain values of d, the number of distinct values they assume and the multiplicities with which they assume these values. It is encyclopaedic in nature.

2.5. Multiphase Sequences and their Correlation Functions

The values and behaviour of the autocorrelation and crosscorrelation functions when the alphabet is restricted to be binary have been examined in previous sections. This section considers this behaviour when more than these two phases are allowed and we begin with the work of Welti (1960), apparently the first work on multiphase sequences.

In this work two alphabets are used: a binary alphabet $\{\alpha,\beta\}$ such that $\alpha+\alpha=\beta+\beta=\alpha$, $\alpha+\beta=\beta+\alpha=\beta$, $\alpha\alpha=\beta\beta=1$, $\alpha\beta=\beta\alpha=-1$: and a quaternary alphabet $\{\alpha,\beta,\gamma,\partial\}$, also with appropriate addition and multiplication. For any sequence A over either alphabet we define multiplication by an integer k as $k\underline{A} = (\alpha,\alpha,\ldots,\alpha)$ if k is even and as $\underline{A}$ if k is odd. The intersection of binary letters is given by the tabulation

$$\begin{bmatrix} \alpha\cap\alpha & \alpha\cap\beta \\ \beta\cap\alpha & \beta\cap\beta \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ \alpha & \beta \end{bmatrix} \quad \text{(note the non-commutativity)}$$

and the corresponding intersection of sequences is given by $\underline{A}\cap\underline{B} = (a_1\cap b_1, a_2\cap b_2,\ldots, a_n\cap b_n)$. The negative of a binary sequence interchanges α and β. The product $\underline{A}\ \underline{B} = \Sigma a_i b_i$ is the usual inner product.

To construct the class of binary sequences (from which the quaternary sequences will be obtained) let $\underline{A}_i^k$ be a sequence of length 2^k, k fixed and $i = 1,2,\ldots,k$ such that the first 2^{i-1} places contain α's, the next 2^{i-1} places contain β's and so on. Let $\underline{X}_i^k$ be a binary vector which is the binary expansion of the letter i. Define the sequence $\underline{B}_i^k$ by

$$\underline{B}_i^k = \sum_{j=1}^{k} x_j^i \underline{A}_j^k \quad , \quad i = 1,2,\ldots,2^k, \underline{x}_i^k = (x_1^i, x_2^i, \ldots, x_k^i)$$

For each k, 2^k sequences are obtained with the property that

$$\underline{B}_i^k \; \underline{B}_j^k = \begin{cases} 0 & i \neq j \\ 2^k & i = j \end{cases}$$

Now consider translating this set by the vector

$$\underline{C}^k = \sum_{j=1}^{k-1} \underline{A}_j^k \cap \underline{A}_{j+1}^k$$

to form the sequences

$$\underline{D}_i^k = \underline{B}_i^k + \underline{C}^k \qquad i = 1,2,\ldots,2^k$$

These sequences are also orthogonal and will be referred to as a D-code and k is the order of D^k and i its rank. The sequences $\underline{D}_i^k$ and $\underline{D}_j^k$ are called mates if $|i-j| = 2^{k-1}$. A mate of $\underline{D}_i^k$ will be denoted by $\underline{\tilde{D}}_i^k$ and clearly $\underline{\tilde{D}}_i^k = \underline{D}_i^k + \underline{A}_k^k$ and $\underline{D}_i^k$ and $\underline{\tilde{D}}_i^k$ agree in the leading 2^{k-1} elements and disagree in the rest. $\underline{D}_i^k$ and $\underline{D}_j^k$ are called neighbours if $|i-j| = 1$, max (i,j) odd. It can be shown that the catenation of a D sequence with its mate is a sequence of the next higher order and of the same rank. Other properties of these codes are also examined.

The quaternary sequences, called E-codes, are obtained from these D-codes. The sequence $\underline{E}_i^k$ is obtained from $\underline{D}_i^k$ by replacing even place α's and β's with γ's and ∂'s respectively, and the sequences $\underline{E}_i^k$ and $\underline{E}_j^k$ are mates or neighbours iff the corresponding D-sequences are mates or neighbours. It can be shown that the aperiodic autocorrelation of an E sequence has off peak values of zero while the crosscorrelation of any two distinct sequences is zero for all shifts. Of course this orthogonality is dependent upon the multiplication of the quaternary elements which is given in the table

$$\begin{bmatrix} \alpha\alpha & \alpha\beta & \alpha\gamma & \alpha\partial \\ \beta\alpha & \beta\beta & \beta\gamma & \beta\partial \\ \gamma\alpha & \gamma\beta & \gamma\gamma & \gamma\partial \\ \partial\alpha & \partial\beta & \partial\gamma & \partial\partial \end{bmatrix} = \begin{bmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{bmatrix}$$

Some comments on this choice of multiplication table are given by Welti (1960). It was in fact chosen to ensure the orthogonality of the constructed codes.

Frank and Zadoff (1962) commenting on earlier work by Heimiller and by Frank construct sequences of length N^2 over the complex N^2 roots of unity. In his earlier work Heimiller had required that N be a prime but this restriction is not necessary. The construction is as follows. Let ξ be a primitive N^m root of unity and construct the following array:

$$\begin{array}{cccccc} \xi & \xi^2 & \xi^3 & \cdots & \xi^N \\ \xi^2 & \xi^4 & \xi^6 & & \xi^{2N} \\ \vdots & & & & \\ \xi^N & \xi^{2N} & \xi^{3N} & \cdots & \xi^{N^2} \end{array}$$

where the indices are taken modulo N. The sequence is then formed by taking the rows of the array, one row at a time and the periodic correlation function of this sequence is an impulse function; i.e. is zero for every off centre shift.

Frank (1963) later considered a similar construction for sequences with good aperiodic correlation properties. He begins with a variant of the above array, namely

$$\begin{matrix} \xi^0 & \xi^0 & \xi^0 & \cdots & \xi^0 \\ \xi^0 & \xi^1 & \xi^2 & \cdots & \xi^{N-1} \\ \vdots & & & & \\ \xi^0 & \xi^{N-1} & \xi^{2(N-1)} & \cdots & \xi^{(N-1)^2} \end{matrix}$$

and observes that the sequence obtained from this array, row by row, has a periodic correlation which is, again, an impulse function. To obtain sequences with good aperiodic correlation functions, however, one chooses a starting point in the array and runs through the array once. However, it is suggested that simply taking the rows one at a time, beginning with the top row, as in the previous case, should yield sequences with good aperiodic correlation properties. Several specific sequences constructed in this manner are analyzed and the following observations, which are conjectured to be always true, are noted:

i) The maximum off peak value of the aperiodic correlation function is the vector sum of N/2 (or (N+1)/2 if N is odd) unit vectors in the complex plane, each vector separated by $2\pi/N$ radians.

ii) For shifts of N, the correlation function is zero (this is of course always true).

iii) For a shift of j where $|j-kN| \leq 1$ the absolute value of the correlation function is unity.

iv) The correlation function for shifts of m and N^2-m has the same magnitude.

v) The side lobe peaks are themselves individually symmetrical.

Turyn (1967) considered these observations and was able to show that if

$$c(m) = \sum_{i=0}^{N^2-1-m} x_i \, \overline{x}_{i+m}$$

then $|c(kN+r)| = |c(kN+N-r)| = |c((N-k-1)N+r)| = |c((N-k-1)N+N-r)|$ establishing the observed side lobe symmetries. More importantly he established conjecture i) above by showing that

$$|c(m)| \leq b_n = \left| \sum_{i=0}^{\lfloor \frac{N-1}{2} \rfloor} \xi^i \right|$$

an interesting property of sums of complex roots of unity. Properties ii) and iii) above were also established, i.e.

$$c(kN) = 0 \quad \text{and} \quad c(kN+1) = -\xi^{k+1} \quad (\therefore |c(kN+1)| = 1)$$

Chu (1972) constructed a class of sequences of length N over the N^{th} roots of unity for which the periodic correlation function is an impulse function. For N even the sequence is $(a_0, a_1, \ldots, a_{N-1})$ where

$$a_k = \exp(i \frac{M\pi k^2}{N}) \quad , \; k = 0,1,\ldots, N-1, \; (M,N) = 1$$

and for N odd

$$a_k = \exp(i \frac{M\pi k(k+1)}{N})$$

Golomb and Scholz (1965) were interested in constructing sequences over the complex numbers, each with magnitude unity, which satisfy the Barker constraint, namely that $|c(k)| \leq 1, k \neq 0$. If $(u_0, u_1, \ldots, u_{n-1})$ is a complex sequence, $|u_i| = 1$, with aperiodic correlation function $c_u(k)$, then the sequence

$$v_j = u_j \, e^{2\pi ij/m} \quad , \quad m \text{ any nonzero integer}$$

has the correlation function $a_v(k) = e^{-2\pi ik/m} \, c_u(k)$ and hence such a transformation preserves the "Barker property" of the original sequence.

In a similar way the transformations

$$v_j = u_j \, e^{2\pi i(j+\alpha)/x}$$

where α and x are any real numbers and

$$v_j = u_{n-j-1} \qquad \text{(sequence reversal)}$$

and

$$v_j = \overline{u}_j \qquad \text{(conjugation)}$$

also preserve the Barker property and take generalized Barker sequences to generalized Barker sequences. Using such transformations one obtains a quaternary generalized Barker sequence from a binary one. However, a quaternary generalized Barker sequence of length 15 not obtained in this manner is also given in this paper (Golomb and Scholz, 1965).

The general question of interest is, given $\rho = e^{2\pi i/\ell}$ and the alphabet $\{1,\rho,\rho^2,\ldots,\rho^{\ell-1}\}$, what are all the values ℓ such that a Barker sequence of length n over this alphabet of size ℓ can be constructed? A summary of the known results on this problem is given. The sextic alphabet (ℓ=6) is singled out as being of particular interest. There is evidence to suggest that the only value of ℓ for which generalized Barker sequence of length 6 exists is ℓ=6. Generalized Barker sequences for all lengths up to 13 were found over the sextic alphabet.

Turyn (1974) considered the properties of three phase and four phase Barker sequences. We reproduce some of these interesting properties here. It is first shown that a four phase Barker sequence of odd length has a real correlation function and that $c(j) = \pm 1$ for j odd and that $c(j) = 0$ for j even, $j \neq 0$. It follows that for any ternary Barker sequence in which $x_0 = x_1 = 1$, $x_{n-2} = -x_{n-1}$ and x_{n-2} and x_{n-1} are real.

In fact in any four phase sequence with a real correlation function but not necessarily with the Barker property $x_k = \pm x_{n-1-k}$ for all k (i.e. $x_k \bar{x}_{n-1-k}$ is real). For binary Barker sequences of odd length it is known that $x_k x_{n-1-k} = (-1)^k u$ where $u = \pm 1$ and $u \equiv n \pmod 4$. The equivalent property for four phase Barker sequences of odd length is that $x_k x_{n-1-k} = (-1)^{k+1} u$, $u = \pm 1$. More detailed properties of generalized Barker sequences and their correlation functions are derived in Turyn (1974) but these are omitted here. It is also shown that if n is a prime and if 2 is primitive (mod n) or if $n \equiv -1 \pmod 4$ and 2 is of order $(n-1)/2$ mod n, then the only four phase Barker sequences are equivalent to real ones; hence the shortest length for such a sequence (of length greater than 13) is at least 12,100. Using these results it is shown that there is, up to equivalence, only one four phase Barker sequence of length ≤ 31, the one of length 15 mentioned in the paper of Golomb and Scholz (1965), all the others being equivalent to the binary ones. Using similar techniques it is shown that any cubic Barker sequence (over the alphabet $\{1,\xi,\xi^2\}$ ξ a cubic root of unity) has a real periodic autocorrelation function and that there are no such sequences of length n where $9<n<16$. It is likely that there are no cubic Barker sequences of length greater than 9 nor any quaternary Barker sequences of length greater than 15 with the possible exception of length 16.

Chang (1967) and Moharir (1974) construct ternary sequences over the alphabet $\{0,\pm 1\}$ which is quite a different problem to the sequences above. Chang (1967) shows simply that any maximum length sequence over GF(3) has a periodic correlation function which is an impulse function. A few comments on the generation of uncorrelated sequences using the distinct maximal length sequences and a Hadamard matrix are also given.

Moharir (1974) also considered ternary codes over the alphabet $\{0,\pm1\}$ but using the aperiodic autocorrelation function. Sequences with an autocorrelation function of the form

$$c(k) = \begin{cases} n' \quad (< n) & , k=0 \\ 0,\pm1 & , k=1,2,\ldots,n-1 \end{cases}$$

were sought and those of length 6,8,9 and 10 displayed. It seems that such codes will exist for infintely many lengths.

Moharir (1977) defines a generalized pseudonoise sequence as one whose periodic autocorrelation function is zero for all nonzero shifts. Now consider two sequences $\underline{u} = (u_0,u_v\ldots,u_{\ell-1})$ and $\underline{v} = (v_0,v_1\ldots,v_{m-1})$, $(\ell,m) = 1$, $\ell m = n$. Then $\underline{x} = (x_0,x_1,\ldots,x_{n-1})$ is said to be the Chinese product of $\underline{u}$ and $\underline{v}$ if

$$x_i = u_g\, v_h$$

where

$$i = \begin{cases} g \pmod{\ell} \\ h \pmod{m}. \end{cases}$$

The periodic autocorrelation function of the sequence $\underline{x}$ is then the Chinese product of the autocorrelation functions $a_u(.)$ and $a_v(.)$. It follows immediately that the Chinese product of two generalized pseudonoise sequences with coprime lengths is again a generalized pseudonoise sequence. Such a construction can be applied to any generalized pseudonoise sequence over any real or complex alphabet and in particular to the sequences of Frank (1963) and Chu (1972). The relationship between asymmetrically binary sequences (binary sequences over an alphabet $\{\alpha,\beta\}$ $\alpha \neq -\beta$) which have an impulse function for a periodic correlation function and difference sets

is considered.

More recently Moharir (1977) examined ternary (0,±1) generalized pseudonoise sequences via combinatorial admissibility conditions to determine their existence or nonexistence. Once again the role of cyclic differences sets is examined.

Two other papers of marginal interest to the present report attempt to construct Barker sequences over the alphabet {0,1}, called optical Barker sequences due to their application to optical radar pulse compression. Certain techniques for the construction of such codes, largely ad hoc, are given in Moharir and Selvarajan (1974) and this work was continued in Moharir and Selvarajan (1974).

Delsarte (1968) introduced the notion of G-sequences which are of tangential interest to the present report and will not be considered. In terms of this report they discuss techniques, using group rings, of constructing ternary {0,±1} sequences with two level periodic autocorrelation functions.

Finally, we mention the impulse equivalent pulse trains of Huffman (1962). These are complex valued sequences, whose coordinates are not, necessarily, of magnitude unity, and whose correlation function (either periodic or aperiodic, depending on the author) are impulse-like; i.e. the ratio of the centre value to maximum off centre value of the correlation function is very large. We will not consider these sequences here, but simply refer the reader to the work of Golay (1975) and Caprio (1969).

We now consider some recent work of Scholz and Welch (1978) which uses group characters to define complex sequences over the complex mth roots of unity, for some m, with "good" aperiodic autocorrelation and cross-correlation functions. We consider this work in some detail since the

techniques appear to be promising for further work. Consider two sequences $\underline{a} = \{a_0, a_1, \ldots, a_{n-1}\}$ and $\underline{b} = \{b_0, b_1, \ldots, b_{n-1}\}$ and let, as usual, c(k) and a(k) be their aperiodic and periodic correlation functions respectively. Let ρ be a primitive n^{th} root of unity. The Fourier transform of the sequence $\underline{a}$ is then

$$\tilde{a}_k = \frac{1}{\sqrt{n}} \sum_{m=0}^{n-1} a_m \rho^{-km} \qquad a_m = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \tilde{a}_k \rho^{km}$$

and we write this as $\mathbb{F}\underline{a} = \tilde{\underline{a}}$. It is a simple matter to show that

$$a_{\underline{ab}}(k) = \sqrt{n} \{\frac{1}{\sqrt{n}} \sum_{\ell=0}^{n-1} \tilde{a}_\ell \tilde{\bar{b}}_\ell \rho^{\ell k}\}.$$

If we let $\underline{a} \, 0 \, \underline{b} = (a_0 b_0, a_1 b_1, \ldots, a_{n-1} b_{n-1})$ i.e. componentwise multiplication then the periodic crosscorrelation sequence between the two sequences $\underline{a}$ and $\underline{b}$ is

$$\underline{a}_{\underline{ab}} = (a_{\underline{ab}}(0), a_{\underline{ab}}(1), \ldots, a_{\underline{ab}}(n-1))$$
$$= \sqrt{n} \, \mathbb{F}^{-1} \{\mathbb{F}\underline{a} \, 0 \, \mathbb{F}\underline{b}\}.$$

Now if we could find a class of sequences which is closed under the operations i) $\mathbb{F}$ and $\mathbb{F}^{-1}$ ii) 0 iii) conjugation and such that each sequence is composed of elements of magnitude 1 then the crosscorrelation sequence will be n times a sequence in the set (since it is closed under these operations). Hence the magnitude of each crosscorrelation will be n. Similarly if $\underline{a} = \underline{b}$ then

$$\underline{a}_{\underline{ab}} = \sqrt{n} \, \mathbb{F}^{-1} (1, 1, \ldots, 1) = (n, 0, 0, \ldots, 0),$$

an ideal autocorrelation function for each sequence in the set.

Using the theory of group characters on M(n), the set of integers relatively prime to n as a multiplicative group with multiplication modulo n, we consider the possibility of constructing such a set of sequences. Much

of what follows is a tutorial on character theory.

The order of M(n) is $\varphi(n)$, Euler's Totient function and, as an Abelian group it can be expressed as a direct product of cyclic groups. Equivalently we can choose a set of generators in G = M(n), $g_1, g_2, \ldots, g_\alpha$, $g_i^{r_i} = e$, $i = 1, 2, \ldots, \alpha$ where e is the group identity and the r_i are not necessarily distinct. Of course we have

$$|G| = \varphi(n) = \prod_{i=1}^{\alpha} r_i$$

and G is isomorphic to the set $\{(i_1, i_2, \ldots, i_\alpha)\ 0 \le i_j \le r_i - 1\}$ under vector addition, where addition in the j^{th} coordinate position is modulo r_j.

A character of any group G is a homomorphism of G into the complex unit circle. For G Abelian there are precisely |G| distinct characters and each character is completely determined by its values on a set of generators of the group. Thus is

$$\chi(g_i) = \sigma_i^{\eta_i},\ 0 \le \eta_i \le r_i - 1,\ \sigma_i = e^{j(2\pi/r_i)} \qquad i = 1, 2, \ldots, \alpha$$

(note that $\chi(g_i)$ must be some r_i^{th} root of unity) then

$$\chi_{\underline{\eta}}(g) = \prod_{i=1}^{\alpha} \sigma_i^{\eta_i k_i(g)} \qquad g = \prod_{i=1}^{\alpha} g_i^{k_i}$$

and all |G| characters of the group are now clearly visible via the |G| choices for η. Distinct characters of the group are closed under conjugation ($\bar{\chi}_{\underline{\eta}}(g) = \chi_{-\underline{\eta}}(g)$) and multiplication ($\chi_{\underline{\eta}}(g)\chi_{\underline{\eta}'}(g) = \chi_{\underline{\eta}+\underline{\eta}'}(g)$). The identity of the character group is called the principal character $\chi_{\underline{0}}(\cdot)$. The following are useful properties of group characters:

i) $$\sum_{g \in G} \chi_{\underline{\eta}}(g) = \begin{cases} |G| & \text{if } \underline{\eta} = \underline{0} \\ 0 & \text{if } \underline{\eta} \neq \underline{0} \end{cases}$$

ii) $$\sum_{g \in G} \chi_{\underline{\eta}}(g)\, \bar{\chi}_{\underline{\eta}'}(g) = |G|\, \delta_{\underline{\eta}\underline{\eta}'}$$ (orthogonality property)

iii) $\sum_{\underline{\eta}} \chi_{\underline{\eta}}(g) = |G| \, \delta_{ge}$.

The characters of M(n) are defined only on M(n) and yet it will be convenient to define them for each integer. We extend the definition as follows:

$$\chi_{\underline{\eta}}^{(n)}(t) = \begin{cases} \chi_{\underline{\eta}} \ (t \bmod n) & (t,n) = 1 \\ 0 & (t,n) \neq 1 \end{cases}$$

The extended characters are closed under the operations of conjugation and multiplication and take on values of magnitude either 0 or 1. The Fourier transform of these characters will be of interest to us.

The first important theorem can be described as follows: Let p be a prime and consider the (p-2) non-principal characters, $\chi_\eta(\cdot)$, $\eta = 1,2,\ldots,$ p-2 extended by defining $\chi_\eta^{(p)}(0) = 0$. Then the periodic correlation function is given by

$$a_{\eta\gamma}(k) = \begin{cases} \sqrt{p} \ \tilde{\chi}_0^{(p)}(k), & \eta = \gamma \\ \sqrt{p} \ C_0 \ \chi_{\eta-\gamma}^{(p)}(k), & \eta \neq \gamma \end{cases}$$

where C_0 is a constant of unit magnitude and so

$$a_\eta(k) = \begin{cases} p-1, & k = 0 \\ -1, & k \neq 0 \end{cases}$$

and

$$|a_{\eta\gamma}(k)| = \begin{cases} \sqrt{p} & (k,p) = 1 \\ 0 & (k,p) = 1 \end{cases}$$

and thus the (p-2) characters come very close to achieving the bounds of Welch (1974). The result is based on the fact that the transform of a character is a scalar multiple of another character. These characters

are determined for n composite and once again applied to the construction of sequences with good correlation properties.

To conclude the section we briefly summarize the results contained in Turyn (1967) on the existence of multiphase periodic sequences. On the question of the existence of periodic sequences for which a(j) vanishes for $j \neq 0$, several observations have already been made. Turyn notes also the following theorem:

Theorem: If q is an odd prime power, there exists a sequence of length q, with terms which are q^{th} roots of 1, with $a(j) = 0$, $J \neq 0$. For any n there also exist sequences of length n^2 over n^{th} roots of 1 for which $a(j) = 0$, $J \neq 0$.

These latter sequences have, of course, already been encountered as the polyphase codes of Frank, Zadoff and Chu. Some special nonexistence results can also be achieved. For example, by rather laborious means it can be established that there is no sequence of length 12 over cube roots of unity for which $a(j) = 0$, $j \neq 0$. Similarly one can state the following:

Theorem: Let q be a power of a prime and $\underline{x}$ a sequence over the q^{th} roots of unity of length q^m with the property that $a(j) = 0$, $j \neq 0$. Then $m \leq 2$.

This theorem establishes the unique position of the sequences of the first theorem. It is also known that there are no sequences of lengths 11, 14, 17, 20, 23, 29, 38 or 41 over the cube roots of unity for which $a(j) = -1$, $j \neq 0$.

Let χ be a character of order e on GF(q)* ie. $e \mid q-1$ and $\chi^e(g) = 1$, $g \in GF(q)^*$, and define $\chi(0) = 0$. The following theorem constructs sequences over the e^{th} roots of unity.

Theorem: If q is a prime power, $e|(q-1)$, ξ a primitive e^{th} root of 1, then $\chi(-1) = 1$ if $e|\frac{(q-1)}{2}$, -1 otherwise, then there exist sequences $\underline{x}$ of length $n = q-2$ over the e^{th} roots of 1 which satisfy

$$x_i = \chi(-1)x_{n+1-i}\xi^{-i}$$

for which

$$c(j) + \bar{c}_{n-j} = -1-\xi^{-j}.$$

These sequences can be obtained as $x_i = \chi(g^i-1)$ where g is a primitive element of GF(q)*.

2.6 Multivalued Correlation Functions

In this section we consider constructions which have appeared in the literature which produce correlation functions with certain properties eg. two level correlation functions or correlation functions which vanish at certain points. In certain ways the distinction between this approach and the approach of the papers considered in the previous section is blurred and imprecise. It serves nonetheless to divide the papers.

We begin with the work of Boehmer (1967). Observing that $a(k) = c(k) + c(n-k)$ for binary ± 1 sequences a necessary but not sufficient condition for $|c(k)|$ to be small for all k is that $|a(k)|$ be small for all k. Thus good periodic sequences were first sought in the hope they would also make good aperiodic sequences. All sequences will be of prime length p and we assume g is a primitive element mod p. If $p = ns+1$ we say that the integer k, $1 \leq k \leq p-1$ belongs to residue class i if $k = g^{mn+i} \pmod{p}$ for some integer m, $0 \leq m \leq s-1$. Denote the cyclotomic constant (i,j) as the number of members of the residue class i which are

followed by a member of the residue class j ie. the number of solutions of the congruence

$$g^{\nu n+i} + 1 = g^{\mu n+j} \pmod{p}.$$

The sequences will then be constructed by assigning a_i to be +1 if i is in a chosen subset of residue classes and -1 otherwise. The correlation function can then be determined by a knowledge of the cyclotomic constants. Of the n residue classes choose q of them, $1 \leq q < n$ to assign +1, and denote these by $c_1, c_2, \ldots, c_q$. Define x_k by the equation $k = g^{\mu n+x_k}$ and recall that members of the residue class c_i are all expressible as $g^{\nu n+c_i} \pmod{p}$, $0 \leq \nu \leq s-1$. With these definitions it is not hard to show that

$$a(k) = p - 4sq + r \sum_{i=1}^{q} \sum_{j=1}^{q} (c_i - x_k, c_j - x_k).$$

The only remaining problem is to decide on the number q, the number of residue classes to assign +1 to, and to determine the cyclotomic constants. Determining the "best" q for a given prime is very much an ad hoc procedure. When q = 1 and the integers 1 through p-1 are split into 2 residue classes, the off centre values of the periodic correlation were either -3 or +1 when (p-1)/2 is even and were -1 when (p-1)/2 is odd. Similar types of results were obtained by splitting the integers into 4, 6 and 8 residue classes and choosing q in some manner. The periodic sequences obtained in this manner were tested for their aperiodic properties. The maximum off centre magnitude appears to follow the curve $0.6\sqrt{n}$ for a sequence of length n.

The approach of Boehmer was followed by Chakrabarti and Tomlinson (1976) in designing sequences with good aperiodic correlation properties and aperiodic crosscorrelation properties. In addition to her work

however they experimented using the technique to find multiphase sequences, assigning each of the phases to certain residue classes and examining the peak autocorrelation and crosscorrelation sidelobes. Applications of these sequences to the frequency-time coding of signals are considered.

Lempel, Cohn and Eastman (1977) were able to design binary ± 1 sequences with two valued autocorrelation functions which are optimal in a sense to be defined. This result was discovered independently by Sidelnikov (1969) (as noted by Sarwate) in an earlier paper but we will give the approach of Lempel et al (1977) first. Let α be a primitive element of $GF(p^m)$ for p an odd prime and m some positive integer and let $G = GF(p^m)^*$ the multiplicative group of $GF(p^m)$. For $k = (p^m-1)/2$ define $S \subset G$ as

$$S = \{\alpha^{2i+1}-1,\ i = 0,1,\ldots,k-1\}$$

and define the function f by

$$f(\alpha^t) = \begin{cases} 1 & \text{if } \alpha^t \in S \\ -1 & \text{if } \alpha^t \notin S. \end{cases}$$

Define the binary sequence $(a_0,a_1,\ldots,a_{2k-1})$ by $a_t = f(\alpha^t)$, $t = 0,1,\ldots,2k-1$. Then the periodic autocorrelation function of such a sequence satisfies $a(0) = 2k$ and

$$a(i) = \begin{cases} 2 \text{ or } -2 \text{ if } k \text{ is odd} \\ 0 \text{ or } -4 \text{ if } k \text{ is even.} \end{cases}$$

Furthermore this sequence is balanced in that $\sum_{i=0}^{n-1} a_i = 0$ and it can be shown that the periodic autocorrelation of any balanced binary sequence must have at least two off centre values which are at least as large as those obtained here. In this sense the sequences constructed are optimal.

Sidelnikov (1969) also constructed pseudorandom sequences over the k^{th} roots of unity and examines nearly equidistant codes obtainable from

them. The construction is a little more general than that of Lempel et al (1977). Let GF(q) be the finite field with q elements and assume that $q \equiv 1 \pmod{k}$. Let ψ be a character of GF(q)*. Since $q-1 \equiv 0 \pmod{k}$, $\psi(\cdot)$ is a k^{th} root of unity. For $k = 2$, $\psi(\cdot)$ is either +1 or -1 and is clearly +1 on the set S described by Lempel et al (1977). Notice that $\psi(-1) = -1$, assuming that q is not a power of 2, iff $(q-1)/k \equiv 1 \pmod{2}$. With this notation Sidelnikov constructed sequences of length $n = q-1$ where $n \equiv 0 \pmod{k}$, $(\beta_0,\beta_1,\ldots,\beta_{n-1})$ where $\beta_j = \psi(w^j+1)$ if $w^j + 1 \neq 0$ and $\beta_j = +1$ if $w^j + 1 = 0$. Then the periodic correlation function of this sequence is such that $|a(i)| \leq 4$ for $i \not\equiv 0 \pmod{n}$. If $k = 2$ and $\frac{n}{2} \equiv 1 \pmod{2}$ then $a(i) = 2$ or -2. The result for $\frac{n}{2} \equiv 0 \pmod{2}$ is not explicitly given in Sidelnikov.

Golay examined low autocorrelation sequences in a series of three papers (among many others) which we summarize. Consider the binary ± 1 sequence of odd length $(x_0,x_1,\ldots,x_{2n})$ such that x_i takes on the sign of $\sin(\pi\, x^2(i))$ where

$$x(i) = (\sqrt{n+1} - \sqrt{n})\ (i + \tfrac{1}{2}) \qquad i = 0,1,\ldots,2n$$

These sequences can be shown to be skewsymmetric (ie. $x_{n+i}\, x_{n-i} = -1$) and from this it follows immediately that the aperiodic autocorrelation c(k) vanishes for k odd.

To this point the quality of a low autocorrelation sequence has been, implicitly, the ratio of the maximum magnitude of its sidelobes to its centre value. Other criteria are sometimes employed and in Golay (1977) the figure of merit used in the investigation of binary sequences is

$$F = \frac{n^2}{2 \sum_{k=1}^{n-1} c(k)^2}$$

In some ways this measure has greater analytic tractability. Using random arguments Golay (1977) shows that asymptotically it seems reasonable to conjecture that for large n, the best sequences will achieve a value of F of approximately $2e^2$. By a similar argument it is shown that this is also approximately the value achievable by skew symmetric sequences. Thus one is sacrificing very little by searching for long skew symmetric sequences with its attendant savings in search time. A sequence of two other sieves and then a search algorithm is given to find long sequences with high figures of merit. The second sieve depends on the use and properties of complementary pairs of sequences. All skew symmetric sequences up to length 59 with optimal F-values were found to be determined by the search algorithms presented here. The results are inconclusive.

A slightly different figure of merit was used in Golay (1975) where real skew symmetric sequences $(a_0, a_1, \ldots, a_{2n})$ were sought for which

$$F_h = \frac{\left[\sum_{i=0}^{2n} |a_i|\right]^2}{2\sum_{k=1}^{2n} \left[\sum_{i=0}^{2n-k} \delta g_n(a_i).a_{i+k}\right]^2}$$

is high. The values $|a_i|$ are not constrained to be unity as was the case for so much of this work, and in this respect the study is similar to that of the impulse equivalent pulse trains of Huffman (1962). It turns out however that the sequence of signs of some of the sequences which had a high F_h is related to the Barker sequence of corresponding length.

There are two other works of significance to this study. They are however rather detailed and quite specialized and so we merely indicate the contents of these works here. The first is by Turyn (1974) whose main interest was the construction of Hadamard matrices using Baumert-Hall units

and quadruples of binary sequences whose nonperiodic correlations add up to zero (ie. a set of 4 complementary sequences in the sense of Tseng and Liu (1972)). Several such sets of sequences are constructed, including one infinite class. The other work referred to is the doctoral thesis of G. Seguin (1971). Once again there is too much information contained there to summarize it effectively. A few of its highlights will be mentioned however. Let $a(\cdot)$ and $b(\cdot)$ be the periodic and odd correlation function of a sequence, respectively. Let m_a and m_b denote the off centre maximum magnitudes of these two correlation functions and m_c be the corresponding quantity for the aperiodic correlation function. A set of sequences is constructed in which $b(k) = (-1)^k a(2k)$, where $2k$ is taken mod n and for this class

$$m = \max (m_a, m_b) = m_a = m_\theta .$$

The construction is essentially based on properties of the cyclotomic cosets of integers modulo n. Another construction yields sequences for which $b(k) = (-1)^k a(k)$, $0 < k < n$. For another class of sequences it is shown that $||a(k)| - |b(k)|| \leq 2$, $0 < k < n$.

Lindner (1975) lists the minimum possible maximum absolute value of offpeak aperiodic autocorrelations for all binary ±1 sequence lengths up to 40. The number of distinct sequences (up to inverse time and inverse amplitude) achieving this minimum is also given. In addition, four other quantities are tabulated:

i) $M_1 = \frac{1}{n-1} \sum_{i=1}^{n-1} c(i)$, mean of the sidelobes

ii) $M_2 = \left\{ \frac{1}{n-1} \sum_{i=1}^{n-1} c^2(i) \right\}^{1/2}$, rms value of the sidelobes

iii) M_3 = number of positive sidelobes with maximum absolute value

iv) M_4 = distance from mainlobe of first sidelobe with maximum absolute value.

and these quantities are generally not achieved by the same sequence. They are, of course, only given for those sequences achieving the minimum maximum off centre correlation.

Finally we mention two works of perceptual interest to the central problem. In Schroeder (1970) the problem of how to adjust the phases of the harmonics in a periodic signal in order to minimize the peak-to-peak amplitude was considered. One of the results obtained produced a construction method for sequences with low aperiodic autocorrelation, ie. if the sequence $(a_0,a_1,\ldots,a_{n-1})$ is chosen such that

$$a_i = 1 - 2\left\lfloor \frac{(i+1)^2}{n} \right\rfloor_{\text{mod } 2} \qquad i = 0,1,\ldots,n-1$$

the resulting sequence has reasonably good, but not optimal, autocorrelation properties. Lempel and Greenberger (1974) investigated the problem of finding sequences $\{x_0,x_1,\ldots,x_{q-1}\}$ and $\{y_0,y_1,\ldots,y_{q-1}\}$ over some alphabet A for which the quantity

$$H_{xy}(\ell) = \sum_{j=0}^{q-1} h[x(j),y(j+\ell)], \qquad j+\ell \text{ taken mod } q$$

where $h(x,y)$ is 0 if $x \neq y$ and 1 if $x=y$, is used as the basis for optimization criteria.

2.7 Error Correcting Codes and Sequences

Let $\underline{x}$ and $\underline{y}$ be two binary (0,1) n-tuples a Hamming distance d apart. Let $\eta(\underline{x})$ and $\eta(\underline{y})$ be the corresponding ± 1 n-tuples. Then the

correlation between $\eta(\underline{x})$ and $\eta(\underline{y})$ is n-2d. Consequently in a cyclic code with minimum distance d if one codeword is drawn from each cyclic equivalence class, the resulting set of codewords, tranformed to binary ±1 sequences, has the property that each off centre autocorrelation function and each crosscorrelation value is not greater than n-2d in absolute value.

From this observation a binary cyclic code with minimum distance d containing s nonzero weights, and assuming the all ones codeword is not in the code, corresponds to a set of sequences whose autocorrelations and crosscorrelations take on at most s distinct values, not greater than n-2d in absolute value. Similar types of observations can be made for codes over GF(p), p a prime, where the sequences are now over the primitive p^{th} roots of unity.

The cases s = 1, 2 and 3 have received some attention for s = 1, Semakov and Sinovev (1968) and Semakov, Zinovev and Zaitsev (1969) showed that every equidistant cyclic code has an irreducible parity check polynomial. The cases s = 2 and s = 3 were considered by Helleseth (1976) and Delsarte and Goethals (1969) respectively. Sidelnikov (1971) also contains interesting constructions from a coding theory point of view. The particular constructions of these codes will not be included here.

Massey and Uhran (1975) make the following observation. Let C be a binary cyclic code of length n with check polynomial $h(x) = (x+1)h_0(x)$, $(x+1) \nmid h_0(x)$ and distance d, and C_0 the code with check polynomial $h_0(x)$. Then a code with words chosen from different cyclic equivalent classes has the property that the maximum off peak value of the odd autocorrelation function and the maximum of the odd crosscorrelation function cannot exceed

n-d+2.

2.8 Complementary Sequences

Two binary ±1 sequences $\underline{x}^{\nu}$ and $\underline{x}^{\lambda}$ are called complementary sequences if the sum of the off peak aperiodic correlations is zero i.e. if

$$c_{\nu}(k) + c_{\lambda}(k) = 0 \qquad k = 1,2,\ldots,n-1.$$

Such sequences are of use for example in multislit spectroscopy (Golay, 1961) as well as communications. Clearly a pair of such sequences can be interchanged, reversed or multiplied by -1 and another pair of complementary sequences will result. It can also be shown that the length of these sequences must be both even and expressible as the sum of two squares.

If $\underline{x}^1 = \underline{a}\,\underline{b} = a_1,a_2,\ldots,a_n,\ b_1,b_2,\ldots,b_n$ and $\underline{x}^2 = a_1,a_2,\ldots,a_n,\ b_1',b_2',\ldots,b_n'$ where b_i' is $-b_i$, where $\underline{a}$ and $\underline{b}$ are complementary sequences then $\underline{x}^1$ and $\underline{x}^2$ are complementary sequences. Similarly the sequences $\underline{y}^1 = a_1b_1a_2b_2\ldots a_nb_n$ and $\underline{y}^2 = a_1b_1'a_2b_2'\ldots a_nb_n'$ are complementary. If $\underline{u} = u_1u_2\ldots u_m$ and $\underline{v} = v_1v_2\ldots v_m$ is another pair of complementary sequences then

$$\underline{z}^1 = \underline{a}^{u_1}\,\underline{a}^{u_2} \ldots \underline{a}^{u_m}\,\underline{b}^{v_1}\,\underline{b}^{v_2} \ldots \underline{b}^{v_m}$$

and

$$\underline{z}^2 \quad \underline{a}^{v_m}\,\underline{a}^{v_{m-1}} \ldots \underline{a}^{v_1}\,\underline{b}^{u_1'} \ldots \underline{b}^{u_m'}$$

are also complementary sequences. Thus given two pairs of complementary sequences of lengths n and m respectively then a pair of complementary sequences of length 2nm can be constructed. These comments are contained in the paper by Golay (1961). A construction is given in that paper of pairs of complementary sequences whose length is a power of 2. A pair of complementary sequences of length 18 exists. Using these facts and the

above constructions it is clear that complementary sequences of lengths $10.2^a.20^b$ can be derived.

The case of length 26 sequences was considered in the paper by Golay (1961) but was not settled. It was finally determined by Jauregi (1962) and Golay (1962a) that a pair of complementary sequences of length 26 exists. Andres and Stanton showed that there are no Golay sequence pairs of lengths 34, 36 and 50. The next unknown case is $n = 58 = 3^2 + 7^2$. The pair of sequences of length 26 can be used to construct pairs of sequences of length $2^a\ 10^b\ 26^c$.

We note in passing the following comments on the periodic analog to the notion of complementary sequences. It was conjectured in a paper by Levitt and Wolf that if $\underline{x}$ and $\underline{y}$ are binary ± 1 sequences of length n such that $\underline{b}$ is orthogonal to every cyclic permutation of $\underline{a}$ then $\underline{a}$ and $\underline{b}$ cannot both have least period n under cyclic permutation. MacWilliams (1967) disproves the conjecture by a construction and explicitly gives an example of length 18. Briggs and Godfrey (1976) showed however that it is impossible to design a pair of sequences with this property if each sequence is to have an autocorrelation function which is a delta function.

The existence of pairs of binary complementary sequences was shown by Turyn (1963) to be equivalent to the quaternary codes of Welti (1960) discussed in section 5. Differing slightly from the notation of Welti, Turyn considered quaternary codes over the symbols $\pm\alpha$ and $\pm\gamma$ with the multiplication rules given by $\alpha\gamma = \gamma\alpha = 0, \alpha^2 = \gamma^2 = 1$. He then commented that the following four notions are equivalent:

i) A pair of complementary binary sequences of length n

ii) A quaternary code of length 2n with correlation function a delta function whose elements with odd index are all of the form $\pm\alpha$ and whose elements with even index are all of the form $\pm\gamma$.

iii) A quaternary code of length 2n, with correlation function a delta function whose first n elements are all of the form $\pm\alpha$ and whose last n elements are all of the form $\pm\gamma$.

iv) A binary sequence of length 2n whose correlation function is zero for all even shifts.

The notion of a pair of complementary sequences was generalized in Tseng (1971), interested in the phase coding of surface acoustic wave devices for signal multiplexing. In this work it was shown that if $\underline{A} = (a_1, a_2, \ldots, a_n)$ and $\underline{A}' = (a_1', a_2', \ldots, a_n')$ is a pair of complementary sequences then the pair $\underline{M}_1 = (-a_n', -a_{n-1}', \ldots, -a_1')$ and $\underline{M}_1' = (a_n, a_{n-1}, \ldots, a_1)$ are also complementary sequences. Furthermore the sum of the aperiodic crosscorrelation functions of the sequences $\underline{A}$ and $\underline{M}_1$ and $\underline{A}'$ and $\underline{M}_1'$ are zero. Tseng and Liu (1972) extended these results. Specifically, let $\underline{A}_i$, $i = 1,2,\ldots,p$ be a set of finite sequences over ± 1. It is called a complementary sequence if

$$\sum_{i=1}^{p} c_{ii}(k) = 0 \qquad k \neq 0$$

A second set of sequences $\underline{B}_i$, $i = 1,2,\ldots,p$ is called a mate of the first set if i) the sequence $\underline{A}_i$ has the same length as the sequence $\underline{B}_i$ (it is not necessary that all sequences in a set have the same length). ii) The set $\underline{B}_i$, $i = 1,2,\ldots,p$ is a complementary set and iii)

$$\sum_{i=1}^{p} c_{A_i B_i}(k) = 0 \qquad \text{for any value of } k.$$

A collection of complementary sets of sequences $\{(\underline{A}_i), (\underline{B}_i), \ldots, (\underline{F}_i)\}$

is called mutually orthogonal if every two complementary sets are mates of each other. It can be shown that a complementary set must contain an even number of sequences. Furthermore, there is an even number of sequences of each length in such a set. If the length of each sequence in a complementary set is n, where n is odd, then the number of sequences in the set, p, is divisible by 4. A complementary set with only two sequences must have each sequence of even and identical length.

The problem of synthesizing a complementary set of sequences is also considered. For a given sequence $\underline{A}$ let $\tilde{\underline{A}}$ denote the reverse of the sequence, $-\underline{A}$ its negation and let

$$\underline{A}^h = \begin{cases} \underline{A} & \text{if } h = +1 \\ -\underline{A} & \text{if } h = -1 \end{cases} .$$

Denote by $\underline{AB}$ the concatenation of two sequences and $\underline{A} \otimes \underline{B}$ the interleaving of two sequences, assumed to be of the same length. Let $\underline{A}^*$ denote the subsequence of $\underline{A}$ consisting of the elements with odd subscripts and $\underline{A}^{**}$ the subsequence of elements with even subscripts.

If any number of sequences in a complementary set are reversed, the result is still a complementary set. Similarly negating any number of sequences or negating alternate elements in all sequences also results in complementary sets. If $\{A_i \; i = 1,2,\ldots,p\}$ is a complementary set then $\{\underline{A}_i^*, \underline{A}_i^{**}, i = 1,2,\ldots,p\}$ is a complementary set. If $\{\underline{A}_i, i = 1,2,\ldots p\}$ and $\{\underline{B}_i, i = 1,2,\ldots,p\}$ are each complementary sets and mates, then $\{A_i \otimes B_i, i = 1,2,\ldots,p\}$ is a complementary set. Other methods of constructing complementary sets are also given. Similarly methods of constructing orthogonal sets from a given complementary set are considered. For example if $\underline{A}_1, \underline{A}_2, \ldots, \underline{A}_p$ is a complementary set where $\underline{A}_1$ and $\underline{A}_2$,

$\underline{A}_3$ and $\underline{A}_4$, ..., $\underline{A}_{p-1}$ and $\underline{A}_p$ are pairs of sequences of the same length then

$$\{\tilde{\underline{A}}_2, -\tilde{\underline{A}}_1, \tilde{\underline{A}}_4, -\tilde{\underline{A}}_3, \ldots, \tilde{\underline{A}}_p, -\tilde{\underline{A}}_{p-1}\}$$

is one of its mates. Tseng and Liu (1972) give many other techniques of a recursive nature and note the lack of direct construction procedures for both complementary sets and their mates.

On a variation of the same theme Taki et al (1969) investigated E-sequences, defined as binary ±1 sequences whose aperiodic autocorrelation function vanishes for all even shifts except for the zero shift. Many properties of these sequences are established and in fact the D-sequences of Welti (1960) encountered in Section 2.5 form a subset of these. A mate of an E-sequence is again an E-sequence with the property that the cross-correlation function between the two is zero for all even shifts, including the zero shift. Constructions of E-sequences and their mates are given and it is shown that an E-sequence and one of its mates forms a complementary pair in the sense of Golay.

It is to be noticed that most of the work on constructing complementary sets or complex sequences is over a restricted alphabet eg. the complex m^{th} roots of unity for a given m. In the recent work of Swaswamy (1978) this condition is removed and more arbitrary phases are allowed. Specifically consider the sequence $\underline{S}_{N+1} = (S_0, S_1, \ldots, S_n)$ where

$$S_i = \exp\,(j(\phi_0 + \phi_1 + \ldots + \phi_i)).$$

The aperiodic autocorrelation function for such a sequence is

$$c_S(\ell) = \sum_{i=0}^{N-\ell} S_i\, \bar{S}_{i+\ell} = \sum_{i=0}^{N-\ell} \exp(-j(\phi_{i+1} + \ldots + \phi_{i+\ell})).$$

Similarly let $\underline{C}_{N+1} = (C_0, C_1, \ldots, C_N)$ be a second sequence where C_i has phase $(\theta_0 + \theta_1 + \ldots + \theta_i)$ and aperiodic autocorrelation function $c_C(\tau)$. As in the work of Golay (1961) the two sequences will be called complementary if

$$c_S(\ell) + c_C(\ell) = 0 \qquad \ell > 0$$

and this relationship establishes a connection between the phases θ_i and ϕ_i. For example, working through the equations shows that for N=2 (codes of length 3) the only conditions necessary for complementarity are:

$$\phi_2 = \phi_1 + \ell\Pi$$

$$\theta_1 = \phi_1 + (\ell - m + n)\Pi/2$$

$$\theta_2 = \phi_1 + (\ell + m + n)\Pi/2$$

and hence the two sequences are

$$\underline{S}_3 = (e^{j\phi_o}, e^{j(\phi_o+\phi_1)}, e^{j(\phi_o+2\phi_1+\ell\Pi)})$$

and

$$\underline{C}_3 = (e^{j\theta_o}, e^{j(\theta_o+\phi_1+(\ell-m+n)\Pi/2)}, e^{j(\theta_o+2\phi_1+(\ell+n)\Pi)})$$

where ℓ, m and n are odd integers and θ_o, ϕ_o and ϕ_1 are arbitrary. Unfortunately the relationship between the phases is not always so easy to determine.

A useful recursion technique follows from noting that if $\underline{S}_N$ and $\underline{C}_N$ are complementary then the concatenated sequences $(\underline{S}_N, e^{j\phi}\underline{C}_N)$ and $(\underline{S}_N, e^{j(\phi+\Pi)}\underline{C}_N)$ are also complementary of twice the length of the original. Some attention is also given to the construction of complementary sets of sequences and also to mutually orthogonal complementary sets of sequences.

References

Andres, T.H. and Stanton, R.G. (1977), Golay Sequences, Lecture Notes in Mathematics, Vol. 622, Springer Verlag, Berlin, pp. 44-54.

Boehmer, A.M. (1967), "Binary Pulse Compression Codes," IEEE Trans. Inform. Theory, Vol. IT-13, pp. 156-167.

Briggs, P.A.N. and Godfrey, K.R. (1976), "Design of Uncorrelated Signals," Electronics Letters, Vol. 12, pp. 555-556.

Caprio, J.R. (1969), "Strictly Complex Impulse-Equivalent Codes and Subsets with Very Uniform Amplitude Distributions," IEEE Trans. Inform. Theory, Vol. IT-15, pp. 695-706.

Chakrabarti, N.B. and Tomlinson, M (1976), "Design of Sequences with Specified Autocorrelation and Cross Correlation," IEEE Trans. Commun., Vol. COM-24, pp. 1246-1251.

Chang, J.A. (1967), "Ternary Sequences with Zero Correlation," Proc. IEEE, Vol. 55, pp. 1211-1213.

Chu, D.C. (1972), "Polyphase Codes with Good Periodic Correlation Properties," IEEE Trans. Inform. Theory, Vol. IT-18, pp. 531-532.

Delsarte, P.(1968), Orthogonal Matrices over a Group of Related Tactical Configurations," M.B.L.E. Laboratoire de Recherches, Brussels, Belgium, Report R90.

Delsarte, P. and Goethals, J.-M. (1969), "Tri-Weight Codes and Generalized Hadamard Matrices," Inform. and Control, Vol. 15, pp. 196-206.

_____ (1971), "On Quadratic Residue Like Sequences in Abelian Groups," Report R 168, M.B.L.E. Laboratoire de Recherches, Brussels, Belgium.

Everett, D. (1966), "Periodic Digital Sequences with Pseudonoise Properties," G.E.C. Jour. Science and Technol., Vol. 33, pp. 115-126.

Frank, R.L. (1963), "Polyphase Codes with Good Nonperiodic Correlation Properties," IEEE Trans. Inform. Theory, Vol. IT-9, pp. 43-45.

Frank, R.L. and Zadoff, S.A. (1962), "Phase Shift Pulse Codes with Good Periodic Correlation Properties," IRE Trans. Inform. Theory, Vol. IT-8, pp. 381-382.

Fredricsson, S.A. (1975), "Pseudo-Randomness Properties of Binary Shift Register Sequences," IEEE Trans. Inform. Theory, Vol. IT-21, pp. 115-120.

Goethals, J.-M. and Seidel, J.J. (1967), "Orthogonal Matrices with Zero Diagonal," Canad. J. Math, Vol. 19, pp. 1001-1010.

Golay, M.J.E. (1961), "Complementary Series," IEEE Trans. Inform. Theory, Vol. IT-7, pp. 82-87.

_____ (1972), "A Class of Finite Binary Sequences with Alternate Autocorrelation Values Equal to Zero," IEEE Trans. Inform. Theory, Vol. IT-18, pp. 449-450.

_____ (1975a), "Notes on Impulse Equivalent Pulse Trains," IEEE Trans. Inform. Theory, Vol. IT-21, pp. 718-720.

_____ (1975b), "Hybrid Low Autocorrelation Sequences," IEEE Trans. Inform. Theory, Vol. IT-21, pp.460-462.

_____ (1976), "Sieves for Low Autocorrelation Binary Sequences, IEEE Trans. Inform. Theory, Vol. IT-23, pp. 43-51.

Gold, R. (1966), "Characteristic Linear Sequences and Their Coset Functions," J. SIAM Appl. Math., Vol. 14, pp. 980-985.

_____ (1967), "Optimal Binary Sequences for Spread Spectrum Multiplexing," IEEE Trans. Inform. Theory, Vol. IT-13, pp. 619-621.

_____ (1968), "Maximum Recursive Sequences with 3-Valued Recursive Cross-Correlation Functions," IEEE Trans. Inform. Theory, Vol. IT-14, pp. 154-156.

Golomb, S.W. and Scholz, R.A. (1965), "Generalized Barker Sequences," IEEE Trans. Inform. Theory, Vol. IT-11, pp. 533-537.

Griffin, M. (1977), "There are no Golay Complementary Sequences of Length $2.q^t$," Aequationes Math., Vol. 15, pp. 73-77.

Huffman, D.A. (1962), "The Generation of Impulse-Equivalent Pulse Trains," IRE Trans. Inform. Theory, Vol. IT-8, pp. 510-516.

Helleseth, T. (1976a), "Some Two-Weight Codes with Composite Parity-Check Polynomials," IEEE Trans. Inform. Theory, Vol. IT-22, pp. 631-632.

_____ (1967b), "Some Results about the Cross Correlation Function Between Two Maximal Linear Sequences," Discrete Mathematics, Vol. 16, pp. 209-232.

Lempel, A., Cohn, M. and Eastman, W. (1977), "A Class of Balanced Binary Sequences with Optimal Autocorrelation Properties," IEEE Trans. Inform. Theory, Vol. IT-23, pp. 38-42.

Lempel, A. and Eastman, W. (1971), "High Speed Generation of Maximal Length Sequences," IEEE Trans. Computers, Vol. 20, pp. 227-229.

Lindholm, J.H. (1968), "An Analysis of the Pseudo-Randomness Properties of Subsequences of Long m-sequences," IEEE Trans. Inform. Theory, Vol. IT-14, pp. 569-576.

Lindner, J. (1975), "Binary Sequences Up to Length 40 with Best Possible Autocorrelation Function," Electronics Letters, Vol. 11, pp. 507.

Luenberger, D.G. (1963), "On Barker Codes of Even Length," Proc. IEEE, Vol. 51, pp. 230-231.

MacWilliams, F.J. (1967), "An Example of Two Cyclically Orthogonal Sequences with Maximum Period," IEEE Trans. Inform. Theory, Vol. IT-13, pp. 338-339.

MacWilliams, F.J. and Sloane, N.J.A. (1976), "Pseudo-Random Sequences and Arrays," Proc. IEEE, Vol. 64, pp. 1715-1729.

Massey, J.L. and Uhran, J.J. (1975), "Sub-baud Coding," Proceedings, 13th Annual Allerton Conf. on Circuit and System Theory, pp. 539-547.

Milstein, L.B. (1977), "Some Statistical Properties of Combination Sequences," IEEE Trans. Inform. Theory, Vol. IT-23, pp. 254-258.

Moharir, P.S. (1974), "Ternary Barker Codes," Electronics Letters, Vol. 10, pp. 460-461.

_____ (1977a), "Generalized PN Sequences," IEEE Trans. Inform. Theory, Vol. IT-23, pp. 782-784.

_____ (1977b), "Chinese Product Theorem for Generalized PN Sequences," Electronics Letters, Vol. 13, pp. 121-122.

Moharir, P.S. and Selvarajan, A. (1974a), "Optical Barker Codes," Electronics Letters, Vol. 10, pp. 154-155.

_____ (1974b), "Systematic Search for Optimal Barker Codes with Minimum Length," Electronics Letters, Vol. 10, pp. 245-246.

Moon, J.S. and Moser, L. (1968), "On the Correlation Function of Random Binary Sequences," SIAM J. Appl. Math., Vol. 16, pp. 340-343.

Pettit, R.J. (1967), "Pulse Sequences with Good Autocorrelation Properties," Microwave J., Vol. 10, pp. 63-67.

Pursley, M.B. and Sarwate, D.V. (1977a), "Evaluation of Correlation Parameters for Periodic Sequences," IEEE Trans. Inform. Theory, Vol. IT-23, pp. 508-513.

_____ (1977b), "Performance Evaluation for Phase-Coded Spread Spectrum Multiple Access Communication - Part II: Code Sequence Analysis," IEEE Trans. Communications, Vol. COM-25, pp. 800-803.

Roefs, H.F.A. and Pursley, M.B. (1977), "Correlation Parameters of Random Binary Sequences," Electronics Letters, Vol. 13, pp. 488-489.

Sarwate, D.V. (1978a), "Cross-Correlation Properties of Sequences with Applications to Spread-Spectrum Multiple-Access Communications," to appear.

_____ (1978b), "Bounds on Cross-Correlation and Autocorrelation Sequences," to appear.

Sarwate, D.V. and Pursley, M.B. (1977), "New Correlation Identities for Periodic Sequences," Electronics Letters, Vol. 13, pp. 48-49.

Schneider, K.S. and Orr, R.S. (1975), "Aperiodic Correlation Constraints on Large Binary Sequence Sets," IEEE Trans. Inform. Theory, Vol. IT-21, pp. 79-84.

Scholtz, R.A. and Welch, L.R. (1978), "Group Characters: Sequences with Good Correlation Properties," IEEE Trans. Inform. Theory, Vol. IT-24, pp. 537-545.

Schroeder, M.R. (1970), "Synthesis of Low Peak Factor Signals and Binary Sequences with Low Autocorrelation," IEEE Trans. Inform. Theory, Vol. IT-16, pp. 85-89.

Sequin, G. (1971), "Binary Sequences with Specified Correlation Properties," Technical Rept. No. 7103, Dept. of Electrical Engineering, University of Notre Dame, Notre Dame, Indiana.

_____ ( ), "Large Sets of Skew-Symmetric Sequences with Small Auto- and Cross-correlations," to appear.

Sidelnikov, V.M. (1969), "Some k-Valued Pseudo-Random Sequences and Nearly Equidistant Codes," Problems of Information Transmission, Vol. 5, pp. 12-16.

_____ (1971), "On Mutual Correlation of Sequences," Soviet Math. Dokl. Vol. 12, pp. 197-207.

Sivaswamy, R. (1978), "Multiphase Complementary Codes," IEEE Trans. Inform. Theory, Vol. IT-24, pp. 546-552.

Stiffler, J.J. (1968), "Rapid Acquisition Sequences," IEEE Trans. Inform. Theory, Vol. IT-14, pp. 221-225.

Surböck, F. and Weinrichter, H. (1978), "Interlacing Properties of Shift Register Sequences with Generator Polynomials Irreducible over GF(p)," IEEE Trans. Inform. Theory, Vol. IT-24, pp. 386-389.

Taki, Y. et al (1969), "Even-Shift Orthogonal Sequences," IEEE Trans. Inform. Theory, Vol. IT-15, pp. 295-300.

Tseng, C.C. (1971), "Signal Multiplexing in Surface Wave Delay Lines Using Orthogonal Pairs of Golay Complementary Sequences," IEEE Trans. Sonics and Ultrasonics, Vol. 18, pp. 103-107.

Tseng, C.-C. and Liu, C.L. (1972), "Complementary Sets of Sequences," IEEE Trans. Inform. Theory, Vol. IT-18, pp. 644-652.

Turyn, R. (1963a), "Ambiguity Functions of Complementary Sequences," IEEE Trans. Inform. Theory, Vol. IT-9, pp. 46-47.

_____ (1963b), "On Barker Codes of Even Length," Proc. IEEE, Vol. 51, pp. 1256.

_____ (1967), "The Correlation Function of a Sequence of Roots of 1," IEEE Trans. Inform. Theory, Vol. IT-13, pp. 524-525.

_____ (1968), "Sequences with Small Correlation," in Error Correcting Codes, H.B. Mann ed., John Wiley and Sons, Inc., New York, pp. 195-228.

_____ (1974a), "Hadamard Matrices, Baumert-Hall Units, Four Symbol Sequences and Surface Wave Encodings, "J. Comb. Theory, Vol. 16A, pp. 313-333.

_____ (1974b), "Four-Phase Barker Codes," IEEE Trans. Inform. Theory, Vol. IT-20, pp. 366-371.

Turyn, R.J. and Stores, J. (1961), "On Binary Sequences," Proc. Amer. Math. Soc., Vol. 12, pp. 394-399.

Wainberg, S. and Wolf, J.K. (1970), "Subsequences of Pseudo-Random Sequences," IEEE Trans. Commun. Technol. Vol. COM-18, pp. 606-612.

Welch, L.R. (1974), "Lower Bounds on the Maximum Cross Correlation of Signals," IEEE Trans. Inform. Theory, Vol. IT-20, pp. 397-399.

Welti, G.R. (1960), "Quarternary Codes for Pulsed Radar," IEEE Trans. Inform. Theory, Vol. IT-6, pp. 400-408.

3. SYNCHRONIZATION

3.1 Introduction

In all communication systems there are two basic modes of operation: that of acquisition and that of conveying information efficiently. In CDMA signaling synchronization of the reference code to the incoming signal is of critical importance for the removal of the code. If the reference code and the incoming signal are not in synchronism the wanted signal may appear to the receiver as a spread spectrum interferer. Thus, synchronization is a critical feature in maintaining the transparency of the code as mentioned in Section 1.

Code phase and carrier frequency uncertainties are the primary sources of synchronization uncertainties. Carrier frequency uncertainty is a manifestation of doppler frequency shift due to relative motions between transmitting and receiving stations. Let f_t be the transmitted carrier frequency, V be the relative velocity between transmitting and receiving stations, and C be the speed of light. Then the doppler shift frequency is $f_d = \pm f_t \frac{V}{C}$ and the received carrier frequency is $f_r = f_t (1 \pm V/C)$. Code phase uncertainty is due to changes in propagation path length. The arrival time is unknown and, in severe cases, the code symbol duration may be lengthened. Both code phase and carrier frequency uncertainties must be resolved before a spread spectrum (CDMA) receiver can operate satisfactorily. Specifically, the code phase must be resolved to better than one bit and the center frequency, as seen at the receiver, must be resolved to the degree that the despread signal is within the aperture of the postcorrelation filter.

Most synchronization coding studies have been concerned with ranging applications [Titsworth 1963], [Golomb et al 1964]. Because of its simplicity in generation and its pseudorandom properties, M-sequences or modifications of M-sequences [Gold 1967] have seen extensive use in ranging and spread spectrum applications. One of the more stringent requirements in spread spectrum is that the M-sequence must be long (perhaps of the order of $2^{20}-1$). For acquisition purposes it is desirable to combine many short shift register sequences to form one long composite sequence. Let ℓ_i, $i = 1, \ldots, P$, be the length of the ith component sequence. If the ℓ_i's are relatively prime the length of the resultant composite sequence is $\ell = \prod_{i=1}^{P} \ell_i$. Titsworth [1963] has shown that a total of $L = \sum_{i=1}^{P} \ell_i$ correlations are needed to determine the phase of each of the component sequences separately. Stiffler [1968] has devised a scheme in which only $\log_2 \ell$ binary decisions, or correlations, are needed for a given value of ℓ, primarily because the periods ℓ_i of the component sequences are constrained to be relatively prime. Rapid acquisition schemes such as that described by [Stiffler 1968] look promising for rapid acquisition in CDMA signaling. Also, the Gold sequences [Gold 1967] may offer rapid acquisition possibilities.

There are two stages of synchronization: initial acquisition and tracking, as depicted in Fig. 3.1. Initial synchronization requires rapid acquisition. Once the point of synchronization is located, the system enters the tracking mode. There are two principle ways of implementing a tracking loop for a pseudorandom (PN) code: the delay-lock loop [Spilker 1963] and the dithering loop [Hartmann 1974]. The principle of operation of these two types of loops is the same, i.e., the incoming

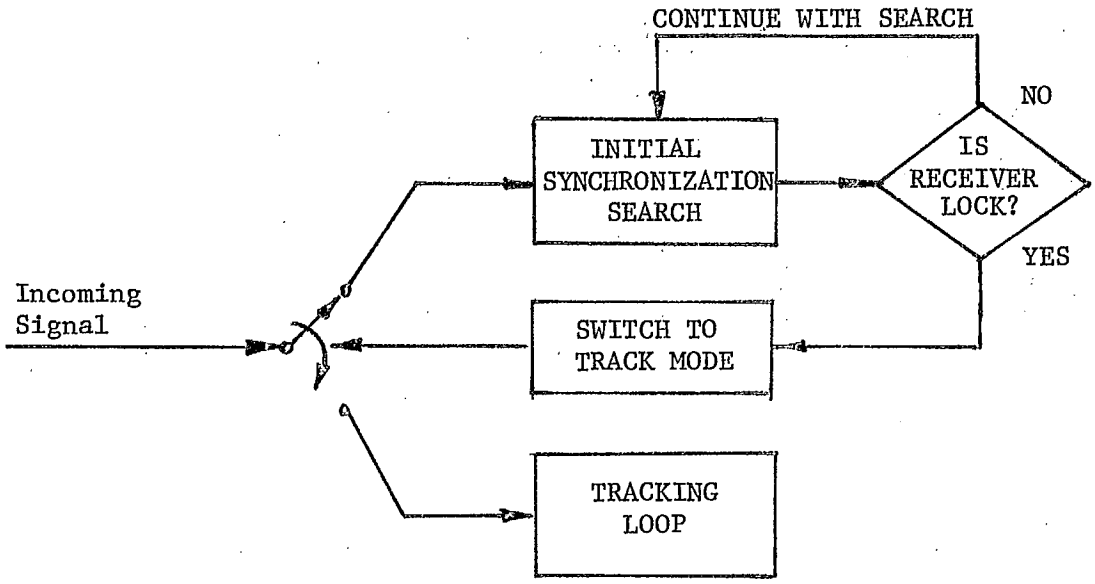


Fig. 3.1 Diagram Depicting Two-Stage Synchronization

code is correlated with an early and a late version of the locally generated replica of the code. The difference between the two loops lies in that the delay-lock loop requires two correlators while the dithering loop requires only a single correlator. In this section we are concerned with describing the available synchronization techniques rather than the mathematical analyses of such techniques. Specifically we shall concern ourselves with the initial acquisition and tracking operations.

3.2 Initial Synchronization

One of the simplest synchronization schemes is sliding correlation in which the incoming code is correlated with a variable rate code sequence as depicted in Fig. 3.2. Basically, the receiving system, in searching for synchronization, operates its code sequence generator at an

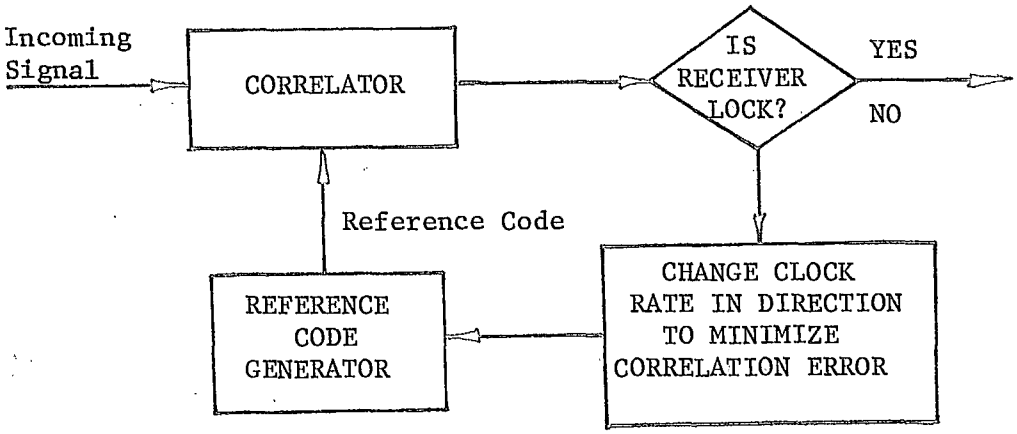


Fig. 3.2 Sliding Correlator

initial rate different from that of the transmitter's code generator. The two code sequences slip in phase (sliding past each other) with respect to each other, stopping only when the correlation produces a satisfactory decision. Since the receiver code generator must change its rate, some mechanism to shift the receiver code generator to different rates is needed. When the initial phase uncertainty is relatively small, the sliding correlator approach can yield relatively rapid synchronization. When a large degree of uncertainty is encountered, however, examination of all possible code phase positions would involve a very long search time. It is noted that recognization of synchronization, which must occur to stop the sliding or search process at or near the point of synchronization, is limited in response time by the bandwidth of the receiver system's post-correlation filter. When the search time is long, the synchronization scheme becomes impractical.

Another simple synchronization technique is the transmission of a synchronization preamble: a special code sequence which is short enough to

allow a search of all possible code positions. The preamble length must be such that its repetition rate does not fall within the information band. To allow rapid acquisition the preamble must be relatively short. On the other hand a short preamble tends to be more vulnerable to false correlations and to possible reproduction by a would be interferer. For direct sequence (DS) signaling the preamble lengths are of the order of several hundred bits to several thousand bits [Dixon 1976] . The minimum preamble length is bounded by crosscorrelation and interference rejection requirements, while the maximum preamble length is set by the maximum available acquisition time.

Synchronization in CDMA depends largely on the signaling method employed, eg., frequency-hopping (FH) or direct sequence (DS) signaling. The code rate associated with frequency-hopping signaling is substantially smaller than that for direct sequence signaling (say a ratio of 1: 1000). It is easier to synchronize the slower rate FH code than the high rate DS code. Let L be the number of DS code bits corresponding to one FH code bit in length. A good strategy may involve two stages of synchronization in which the CDMA signal employs a mixture of FH and DS coding such that the two code sequences are similarly generated. Then the receiver can first synchronize itself to the frequency hopper. The second stage in the search only needs to search L bits to attain synchronization with the DS subsystem. Let $L = R_{DS}/R_{FH}$, where R_{DS} and R_{FH} are respectively the code rate of the DS code and the FH code. If K bits are needed to synchronize the DS code, then only $N = K/L$ bits are sufficient for the synchronization of the FH code. An additional search of L bits will enable synchronization of the DS code. Thus, by employing two synch loops, only (N+L)

instead of K = NxL bits need to be processed in order to synchronize the high rate DS code. The employment of FH/DS as a two-layered synchronization coding scheme is but one example. It may be possible to superpose layers of codes to enhance signal acquisition.

Titsworth [1963] has suggested that a clock-component code, which employs Easterling's [Golomb et al 1964] double loop ranging receiver (Fig. 3.3), can be used for symbol rate synchronization. The inner loop,

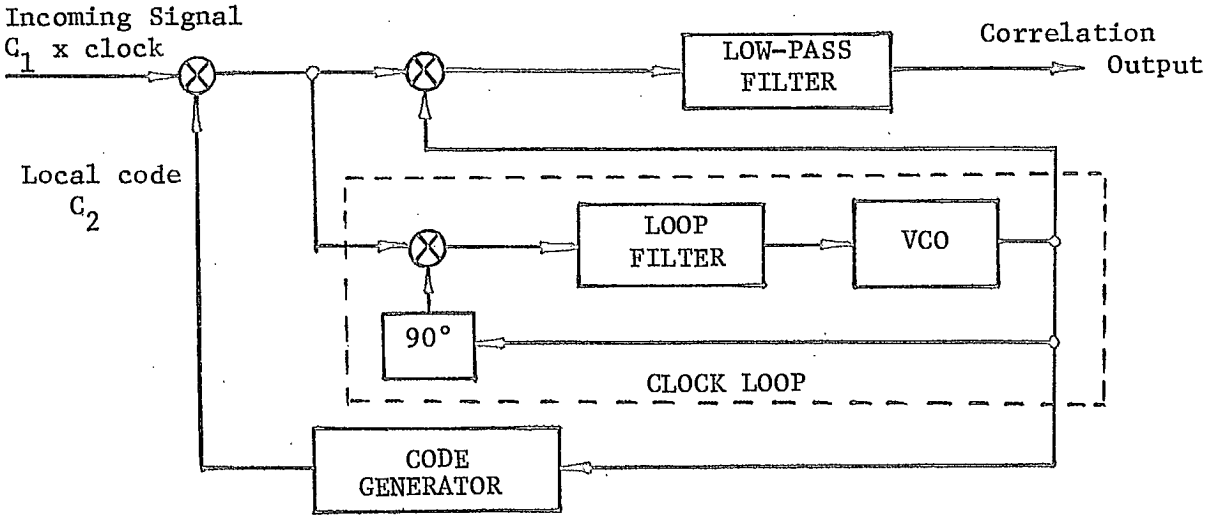


Fig. 3.3 Double Loop Synchronizer

or clock-loop, is synchronized to the symbol rate of the incoming code C_1 by the presence of a "clock component" in C_1, and the locally generated code C_2 is slaved to the output of this clock-loop. Whenever the clock-loop is locked to the clock component of C_1, the local code C_2 is stepwise synchronized to C_1. The status of synchronization can be monitored by observing the correlation output. The error signal that drives the VCO is given by

$$e(\tau) = \int_{\text{period}} C_1(t)\ \text{clock}\ (t)\ C_2(t+\tau)\ \text{clock}\ \left(t + \frac{P}{4} + \tau\right) dt$$

where P is the period of the clock, and integration is over the period of

the code x clock. The correlation output is given by

$$y(\tau) = \int_{\text{period}} C_1(t)\ \text{clock}\ (t)\ C_2(t+\tau)\ \text{clock}\ (t+\tau)dt$$

$$\simeq \left[\int_{\text{period}} C_1(t)\ C_2(t+\tau)dt\right] x \left[\int_{\text{period}} \text{clock}\ (t)\ \text{clock}\ (t+\tau)dt\right]$$

$$= R_{C_1C_2}(\tau).R_{C\ell}\left(\frac{P}{4} + \tau\right)$$

where $R_{C_1C_2}$ is the crosscorrelation of C_1 and C_2 and $R_{C\ell}$ is the auto-correlation of the clock.

As mentioned in Section 2, Stiffler [1968] has proposed a coding scheme whereby only $n = \log_2 N$ binary decisions or correlations need to be made in order to synchronize a code with length $N = 2^n$. The Stiffler code is constructed as follows: Let $b_j = \{\sigma_j^1, \sigma_j^2, \ldots, \sigma_j^n\}$ be the jth binary n-tuple with $\sigma_j^i \in \{1,-1\}$, $b_1 = \{1\ 1\ 1\ \ldots 1\}$, $b_2 = \{-1\ 1\ 1\ \ldots 1\}$ and $b_n = \{-1, -1, \ldots, -1\}$. The binary expansion satisfies the identity $\sum_{i=1}^{n} (1 - \sigma_j^i)2^{i-2} = j-1$. The components of the rapid acquisition binary sequence $C = \{\xi_1, \xi_2, \ldots, \xi_N\}$, $N = 2^n$, is generated by the following:

$$\xi_j = \begin{cases} 1 & \text{if } \sum_{i=1}^{n} \sigma_j^i \geq 0 \\ -1 & \text{if } \sum_{i=1}^{n} \sigma_j^i < 0 \end{cases}$$

$$= \text{sgn}\left(\sum_{i=1}^{n} \sigma_j^i\right).$$

Let $s_i = \{\sigma_1^i, \sigma_2^i, \ldots, \sigma_N^i\}$, $i = 1,2,\ldots,n = \log_2 N$. Stiffler has shown that synchronization of the code C can be attained after n serial correlations of the form

$$\rho_i = s_i \textcircled{\tau} C$$

$$= \frac{1}{N} \sum_{j=1}^{N} \xi_j\ \sigma_j^i$$

where the symbol Ⓣ denotes correlation. It is observed that s_i is a square wave with the period 2^i T/N, where T is the period of the code C. The correlation between s_i and C can have only one of two values, either ρ_i or $-\rho_i$. Stiffler [1968] shows that

$$\rho_i = \rho = \frac{1}{n} \sum_{i=1}^{n} \rho_i = \begin{cases} \frac{1}{2^{n-1}} \binom{n-1}{\frac{n-1}{2}} & n \text{ odd} \\ \frac{1}{2^n} \binom{n}{\frac{n}{2}} & n \text{ even.} \end{cases}$$

For large values of n, application of Stirling's formula yields

$$\rho \simeq (2/\pi)^{1/2} (\log_2 N)^{-1/2}$$

The correlator output, after τ seconds of integration, has mean value $\pm \rho A \tau$, where A is the amplitude of the received binary signal, and the + and - signs are the results of in-phase and out of phase conditions, respectively. In the presence of white Gaussian noise with two-sided spectral density $N_0/2$, the correlator output is Gaussian distributed with a variance $\sigma^2 = N_0 \tau/2$. The probability of a correct decision at the ith stage of the search is

$$P_C(i) = P_0 = (2\pi\sigma^2)^{1/2} \int_0^{\infty} \exp[-(\xi-\mu)^2/2\sigma^2] d\xi$$

$$= \frac{1}{2} [1 + \text{erf} (\frac{\mu}{\sqrt{2}\sigma})]$$

where $\mu = \rho A \tau$. Since $n = \log_2 N$ decisions are required, the probability of a correct acquisition is

$$P_C = \prod_{i=1}^{n} P_C(i) = P_o^n .$$

If the probability of error, $P_e = 1-P_C$, is small, the integration time τ is approximately given by:

$$\tau \simeq (\pi N_0/2A^2)\ \log_2 N\ \ell n\ (\log_2 N/P_e).$$

The total search time is therefore

$$T_S \simeq \tau x \log_2 N$$

$$= (\pi N_0/2A^2)\ (\log_2 N)^2\ \ell n\ (\log_2 N/P_e)$$

On the other hand, if N-cyclic permutations of the code C were to be correlated with the received signal, the total search time required would be approximately given by

$$T_S' \simeq (4N_0/A^2)\ (N/2)\ \ell n\ (N/P_e')$$

where P_e' is the probability of error associated with the N correlation strategy. In spread spectrum applications, N may have to be of the order 2^{20}. The difference between T_S and T_S' is therefore substantial.

Stiffler's code is not strictly applicable to spread spectrum since the local reference sequences $s_i = \{\sigma_1^i, \sigma_2^i, \ldots, \sigma_N^i\}$ do not themselves possess a wide spectrum to spread possible narrowband interferers. That is, the correlator output bandwidth is given by the sum of the bandwidths of the incoming signal and the local reference. If this sum bandwidth is comparable to the postcorrelation filter bandwidth, the interferer will penetrate through the receiving system.

Another drawback of the Stiffler code is that each binary decision requires an N bit correlation. In view of the fact that N is so large, the correlation time is still too long.

3.3 Tracking

There are two principle implementations of tracking loops: the delay-lock loop and the dithering loop. The principle involved with the operation of the delay-lock loop was first discussed by [Spilker 1963] and analyzed in detail by [Gill 1966]. All discussions concerning the operation of the delay-lock loop have been centered on the M-sequence, mainly because of the ease with which M-sequences can be generated and because the M-sequence possesses a reasonably good crosscorrelation property. The basic delay-lock loop is depicted in Fig. 3.4 in which the incoming code sequence is correlated with an early and a late version of the locally generated code. The difference signal between the two correlations is used to drive the VCO. Ward [1967] has considered the delay-lock loop tracking problem using sequence inversion modulation.

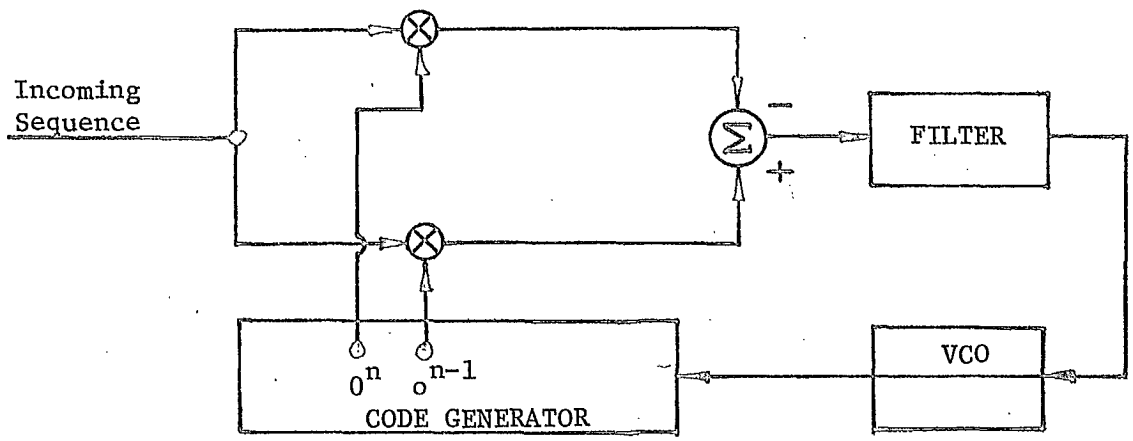


Fig. 3.4 Delay-Lock Loop

The dithering loop, depicted in Fig. 3.5, also operates on the principle of correlating the incoming signal with an early and late version of a locally generated code sequence, except that the correlation is done by a single correlator on an alternate basis. As a result the signal-to-noise performance of the dithering loop is about 3 db worse than the delay-lock loop [Hartmann 1974]. With reference to Fig. 3.5 the operation of the dithering loop is as follows:

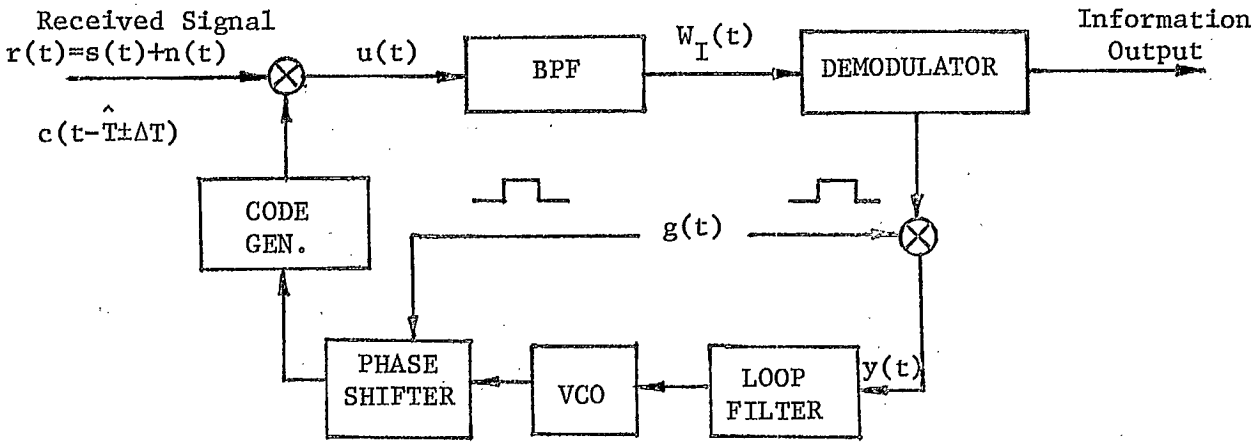


Fig. 3.5 Dithering Loop

Let the received signal be

$$r(t) = s(t) + n(t)$$

with $$s(t) = \sqrt{2P_s}\, m(t-T)\, c(t-T) \cos w_c t$$

where P_S = power of the incoming signal

$m(t)$ = information message sequence

$c(t)$ = code sequence

T = phase of received code clock

w_c = carrier frequency

$n(t)$ = white Gaussian noise with two-sided power spectral density $N_0/2$ watts/Hz.

The signal portion of the output from the BPF is alternately

$$w_+(t) = \sqrt{2P_s}\ \frac{T_C - |\tau - \Delta T|}{T_C} m(t-T) \cos w_o t$$

and

$$w_-(t) = \sqrt{2P}\ \frac{T_C - |\tau + \Delta T|}{T_C} m(t-T) \cos w_o t$$

where T_C is the chip duration, $\tau = T - \hat{T}$, $\hat{T}$ is the phase estimate of the reference code, and ΔT is the amount of dither. Let

$$x_+(t) = [w_+(t)]_{demod}$$

$$x_-(t) = [w_-(t)]_{demod}$$

Multiplication by the wave q(t) leaves the sign of $x_+(t)$ intact and inverts the sign of $x_-(t)$. In the track mode the clock phase error is close to zero. For $|\tau| \leq \Delta T$ the loop filter input is proportional to the phase error, i.e.,

$$y(t) = k_1\ \tau/T_C$$

where k_1 is a proportionality constant. The VCO d.c. control is prescribed by

$$z_{dc}(t) = y(t) \circledast h(t)$$

where $\circledast$ denotes convolution and h(t) is the impulse response of the loop filter. When the loop is tracking without error, $\tau = 0$ and $w_+(t) = w_-(t)$.

3.4 Summary

For spread spectrum applications, any coding strategy to enhance rapid acquisition must preserve the coding transparency. Since the code length for CDMA signaling is expected to be long (order of 2^{20}), composite codes as discussed by [Titsworth 1963], [Milstein 1976], which require $\sum_{i=1}^{P} \ell_i$ correlators, are unlikely to be fast enough for initial synchronization.

The Stiffler approach is intriguing and warrants further investigation. The two-layered FH/DS coding strategy coupled with good rapid acquisition codes may prove important.

References

Dixon, R.C. (1976), Spread Spectrum Systems, John Wiley, Chap. 6.

Gill, W.J. (May 1965), "Effect of Synchronization Error in the Cross-Correlation Reception of Binary Pseudo-Noise Carrier Communications," PHILCO (WOL) Palo Alto, Calif., Tech. Rept.

Gill, W.J. (July 1966), "A Comparison of Binary Delay-Lock Tracking-Loop Implementations," IEEE Trans. on Aerospace and Electronics Systems, Vol. AES-2, pp. 415-424.

Gold, R. (Oct. 1967), "Optimal Binary Sequences for Spread Spectrum Multiplexing," IEEE Trans. Inform Theory, Vol. IT-13, pp. 619-621.

Golomb, S.W. et al (1964), Digital Communications with Space Applications, Prentice-Hall.

Hartmann, H.P. (Jan. 1974), "Analysis of a Dithering Loop for PN Code Tracking," IEEE Trans. Aerosp. Electron. Syst., Vol. AES-10, pp. 2-9.

Holmes, J.K. and Chen, C.C. (Aug. 1977), "Acquisition Time Performance of PN Spread-Spectrum Systems," IEEE Trans. Commun., Vol. COM-25, pp. 778-783.

Kilgus, C.C. (June 1973), "Pseudonoise Code Acquisition Using Majority Logic Decoding," IEEE Trans. Commun., Vol. COM-21, pp. 772-773.

Milstein, L.B. (Mar. 1977), "Some Statistical Properties of Combination Sequences," IEEE Trans. Info. Theory, Vol. IT- , pp. 254-258.

Mohanty, N.C. (Aug. 1977), "Spread Spectrum and Time Division Multiple Access Satellite Communications," IEEE Trans. Commun., Vol. COM-25, pp. 810-815.

Sage, G.F. (Dec. 1964), "Serial Synchronization of Pseudonoise Systems," IEEE Trans. Commun. Technol., Vol. COM-12, pp. 123-127.

Sergo, J.R., Jr. and Hayes, J.F. (Oct. 1970), "Analysis and Simulation of a PN Synchronization System," IEEE Trans. Commun. Technol., Vol. COM-18, pp. 676-679.

Spilker, J.J. (Mar. 1963), "Delay-Lock Tracking of Binary Signals," IRE Trans. on Space Electron and Telemetry, Vol. SET-9, pp. 1-8.

Stiffler, J.J. (Mar. 1968), "Rapid Acquisition Sequences," IEEE Trans. on Info. Theory, Vol. IT-14, No. 2, pp. 221-225.

Titsworth, R.C. (Mar. 1963), "Optimal Ranging Codes," IEEE Trans. Space Elect. Telem. Vol. SET-10, pp. 19-30.

Toerper, K.E. (Mar. 1968), "Biphase Barker-Coded Data Transmission," IEEE Trans. Aerosp. Elect. Syst., pp. 278-289.

Ward, R.B. (Dec. 1965), "Acquisition of Pseudonoise Signals by Sequential Estimation," IEEE Trans. on Commun. Technol., Vol. COM-13, pp. 475-484.

Ward, R.B. (Feb. 1967), "Digital Communications on a Pseudonoise Tracking Link Using Sequence Inversion Modulation," IEEE Trans. Commun. Technol., Vol. COM-15, pp. 69-78.

Ward, R.B. and Yiu, K.P. (Aug. 1977), "Acquisition of Pseudonoise Signals by Recursion-Aided Sequential Estimation," IEEE Trans. Commun., Vol. COM-25, pp. 784-794.

ANNOTATED REFERENCES

T.H. Andres and R.G. Stanton, Gday Sequences, Lecture notes in Mathematics, volume 622, Springer Verlag, Berlin, (1977) 44-54.

It is shown that there are no Golay sequences of lengths 34, 36 and 50 hence the only occurrences up to length 50 are 2, 4, 8, 10, 16, 20, 26, 32 and 40. By recursive techniques sequences of lengths $2^{\alpha}\ 10^{\beta}\ 26^{\gamma}$, $\alpha,\ \beta,\ \gamma > 0$ can be constructed.

A.M. Boehmer, Binary Pulse Compression Codes, IEEE Trans. Information Theory, 13 (1967), 156-167.

An interesting construction technique for low autocorrelation sequences based on residue number classes and cyclotomic constants. There is some searching involved to find the subset of residue classes which lead to the best sequences.

P.A.N. Briggs and K.R. Godfrey, Design of Uncorrelated Signals, Electronics Letters, 12 (1976), 555-556.

It is shown that it is impossible to design uncorrelated signals with the same period with autocorrelation functions of the delta function form. The example of MacWilliams (1967) gave a pair of uncorrelated binary sequences of the same period, but not with impulse like autocorrelation functions.

J.R. Caprio, Strictly Complex Impulse - Equivalent Codes and Subsets with Very Uniform Amplitude Distributions, IEEE Trans. Information Theory, 15 (1969), 695-706.

The paper is concerned with constructing complex sequences $\{p_o, p_1, \ldots, p_N\}$ with very uniform amplitude distributions $\{|p_o|, |p_1|, \ldots, |p_N|\}$ and impulse like autocorrelation function ($|R_p(k)| << R_p(o)$).

N.B. Chakrabarti and M. Tomlinson, Design of Sequences with Specified Autocorrelation and Cross Correlation, IEEE Trans. Communications, 24 (1976), 1246-1251.

The method of designing sequences with good auto and cross correlation depends on first finding good periodic sequences using the method of Boehmer (1967). These sequences are then tested for their aperiodic correlation properties.

J.A. Chang, Ternary Sequences with Zero Correlation, Proc. IEEE, 55 (1967), 1211-1213.

It is shown that certain ternary m-sequences have a periodic correlation function which vanishes for values not a multiple of sequence length.

D.C. Chu, Polyphase Codes with Good Periodic Correlation Properties, IEEE Trans. Information Theory, 18 (1972), 531-532.

Sequences of any length over N^{th} roots of unity of length N with an autocorrelation function which is an impulse function are given. This is claimed to extend the work of Frank and Zadoff (1962) and Heimiller - whose lengths were N^2 over a primitive N^{th} root of 1.

P. Delsarte, Orthogonal Matrices over a Group and Related Tactical Configurations, M.B.L.E. Laboratoire de Recherches, Brussels, Belgium, 1968, Report R90.

A Class of matrices, whose non-zero elements are from a group is defined as well as a concept of orthogonality. Special cases of this class are generalized Hadamard matrices (the only case of interest here) and conference matrices (one zero per row). The relationship of these matrices to group divisible designs, balanced incomplete block designs, orthogonal arrays and finite geometries, is examined.

P. Delsarte and J. M. Goethals, Tri-Weight Codes and Generalized Hadamard Matrices, Information and Control, 15 (1969), 196-206.

A class of generalized Hadamard matrices over the complex pth. roots of unity is constructed and their connections with a class of tri-weight extended BCH codes of length p^{2m}, dimension $3m + 1$ and minimum weight $(p - 1)\, p^{2m-1} - p^{m-1}$ is given.

P. Delsarte and J.M. Goethals, On Quadratic Residue Like Sequences in Abelian Groups, Report R 168, MBLE Laboratoire de Recherches, Brussels, Belgium, July, 1971.

The construction of G-sequences in certain Abelian group algebras over the integers is considered. Such sequences are ternary over the alphabet 0, ±1, and are connected with periodic ternary sequences with impulse like periodic correlation functions.

D. Everett, Periodic Digital Sequences with Psendonoise Properties, G.E.C. Jour. Science and Technology, 33 (1966), 115-126.

A pseudonoise sequence here is defined as one for which the off centre periodic autocorrelation function is constant. It is shown that pseudonoise sequences, difference sets and cyclicBIBD'S are coexistent. The sampling of pseudonoise sequences is considered and the relationship of multipliers of different sets to this problem examined. Some known classes of pseudonoise sequences are displayed, including those derived from quadratic, biquadratic and octic residue sequences, twin prime sequences, Hall sequences maximum length sequences (including some interesting sampling properties of them) and finite projective planes.

R.L. Frank, Polyphase Codes with Good Nonperiodic Correlation Properties IEEE Trans. Information Theory, 9 (1963), 43-45.

A simple class of polyphase (N phases, N arbitrary) having good nonperiodic correlation properties is described, The procedure is somewhat arbitrary in that there is an element of search involved. The superiority of the polyphase codes. in the sense of higher centre peak to side peak ratio is established. Several conjectures on the behaviour of the correlation function for such sequences, are given. (see also Turyn (1967)).

R.L. Frank and S.A. Zadoff, Phase Shift Pulse Codes with Good Periodic Correlation Properties, IRE Trans. Information Theory, 8 (1962), 381-382.

It is pointed out that the code sequences described in an earlier paper by Heimiller were identical to those found by Frank nine years earlier (no reference given) and contained in a patent by Zabouff and Abourek - except those by Frank do not contain the restriction that code lengths be the square of the power of a prime. Heimiller comments on this note, immediately following it, agreeing with this observation and providing a proof of the only theorem in his paper which does not hold by removing this restriction.

S.A. Fredricsson, Pseudo-Randomness Properties of Binary Shift Register Sequences, IEEE Trans. Information Theory, 21 (1975), 115-120.

This paper is concerned with measuring the randomness of maximum length sequences over and above the original criterion given by Golomb. In particular the M-tuple weight distribution and high order correlations of these binary maximum length sequences are considered.

J.M. Goethals and J.J. Seidel, Orthogonal Matrices with Zero Diagonal, Canad. J. Math; 19 (1967), 1001-1010.

Symmetric and Skew-symmetric matrices C of order v with diagonal elements 0 and off diagonal elements ±1 with the property that $CC^T = (v-1)I_v$ are constructed.

M.J.E. Golay, Complementary Series, IEEE Trans. Information Theory, 7 (1961), 82-87.

A pair of binary sequences will be called complementary if the sum of their nonperiodic correlation functions is zero, except for the zero shift. General properties of such sequences are established and various constructions which double the length of a given complementary sequence given. It is shown that the length n of such series must be even and that $n = (n - p - q)^2 + (p - q)^2$ where p and q are the numbers of 1's in the two sequences. A construction method for such sequences when n is a power of two is given from which sequences of length $10.2^a.20^b$ can be constructed, since sequences of length 10 also exist. Sequences of length 18 are not possible while lengths 26 and 34 were left undecided (see Andres and Stanton (1977)).

M.J.E. Golay, A Class of Finite Binary Sequences with Alternate Auto-correlation Values Equal to Zero, IEEE Trans. Information Theory, 18 (1972), 449-450.

Binary (±1) sequences of odd length are constructed with the property that values of the correlation function at odd integers are zero. Comments on the ratio of peak sidelobe to centre values are also given.

M.J.E. Golay, Notes on Impulse Equivalent Pulse Trains, IEEE Trans. Information Theory, 21 (1975a), 718-720.

The impulse - equivalent pulse trains of Huffman are defined as finite, complex-valued sequences, having the property that

$\sum_{o}^{n-k} C_i\, C_{i+k} = 0$, $0 < k < N$. Only the case where the C_i are real is considered here and the figure of merit is E/C_i^2 max where $E = \sum_{o}^{N} C_i^2$.

Sequences are examined in the light of this restriction and criterion.

M.J.E. Golay, Hybrid Low Antocorrelation Sequences, IEEE Trans. Information Theory, 21 (1975b), 460-462.

Skew symmetric sequences of length (2n+1) $(a_o, a_1, \ldots, a_{2n})$ are described for which the figure of merit

$$\left(\sum_{o}^{2n} |a_i|\right)^2 / \left\{2 \sum_{1}^{2n} \left(\sum_{o}^{2n-k} \operatorname{sgn}(a_i) \cdot a_{i+k} \right)^2 \right\}$$

is high, where $a_{n-s} = (-1)^s\, a_{n+s}$. Many comments on the structure and

properties of such "good" sequences are discussed.

M.J.E. Golay, Sieves for Low Autocorrelation Binary Sequences, IEEE, Trans. Information Theory, 23 (1976), 43-51.

The ratio of central to sidelobe energies is taken as the figure of merit in the search for optimal sequences with low autocorrelation. Sieves are employed in the search, the first based on the conclusion that there exist long skew symmetric sequences with approximately the same figure of merit. A second sieve is based on the use of complementary sequences. Third and fourth sieves are based on certain properties of complementary sequences.

R. Gold, Characterisitc Linear Sequences and their Coset Functions, J. SIAM Appl. Math., 14 (1966), 980-985.

The vector space V(f), of all sequences satisfying the linear recursion $\sum_{k=0}^{n} f(k)\, h(i-k) = 0$ for all $i \geq n$, deg $f = n$, $f(0) \neq 0$, is n dimensional. A characteristic sequence of V(f) is a sequence $h \in V(f)$ such that $h(2k) = h(k)$ for all k. Some characterizations of the characteristic sequences of V(f) are given. In the final section the coset sequences of all maximal sequences of a given prime period are determined.

R. Gold, Optimal Binary Sequences for Spread Spectrum Multiplexing, IEEE Trans. Information Theory, 13 (1967), 619-621.

The construction of "preferred pairs" of polynomials which lead to two maximum length sequences with low cross correlation is given. It is shown that the product of these polynomials gives rise to 2^n+1 different (non maximum length) sequences of length 2^n-1 whose cross correlation is bounded.

R. Gold, Maximum Recursive Sequences with 3-Valued Recursive Cross-Correlation Functions, IEEE Trans. Information Theory, 14 (1968), 154-156.

A construction of a pair of maximal linear sequences is given for which the periodic cross correlation is two valued. The results have an interesting interpretation in terms of a class of tri-weight cyclic codes.

S.W. Golomb and R.A. Scholz, Generalized Barker Sequences, IEEE Trans. Information Theory, 11 (1965), 533-537.

Several transformations which preserve the properties of generalized Barker sequences are given and these are used to establish the existence of such sequences. Much of the work was established using a combination of computer search and these properties.

M. Griffin, There are no Golay Complementary Sequences of Length 2.9^t, Aequationes Math., 15 (1977), 73-77.

The possibility of the existence of complementary sequences with length of the form 2.9^t is eliminated.

D.A. Huffman, The Generation of Impulse-Equivalent Pulse Trains, IRE Trans. Information Theory, 8 (1962), 510-516.

An impulse equivalent pulse train is one that has an autocorrelation

function as close as is theoretically possible to that of a single pulse. Such sequences are pulse trains whose amplitudes are chosen from a continuum rather than from a finite set. It is shown that such sequences exist for all lengths and that the number of classes of these sequences is exponentially related to their length.

T. Helleseth, Some Two-Weight Codes with Composite Parity-Check Polynomials, IEEE Trans. Information Theory, 22 (1976a), 631-632.

A family of nonbinary cyclic codes, with composite parity check polynomials, which have only two nonzero weights is described.

T. Helleseth, Some Results about the Cross Correlation Function between Two Maximal Linear Sequences, Discrete Mathematics, 16 (1976b), 209-232.

The cross correlation function between two maximal length sequences is studied in considerable detail. A survey of known results is given. Many of the results are concerned with the values that the cross correlation function can have and the number of times in one period it takes on each possible value.

A. Lempel, M. Cohn and W. Eastman, A Class of Balanced Binary Sequences with Optimal Autocorrelation Properties, IEEE Trans. Information Theory, 23 (1977), 38-42.

For an odd prime p, a balanced (sum is zero) ±1 sequence of length p^m-1 is constructed with the property that $a_k = \pm 2$ for $(p^m-1)/2$ odd and $a_k = 0$ or -4 when (p^m-1) (2 is even). The optimality of such a correlation function is established in the sense that every balanced binary sequence has at least two distinct out of phase correlation values, and these must be at least as large as those constructed here. The construction given in this paper is actually a special case of one given by Sidelnikov (1969), as pointed out by Sarwate.

A Lempel and W.L. Eastman, High Speed Generation of Maximal Length Sequences, IEEE Trans. Computers, 20 (1971), 227-229.

A method for generating binary maximum length sequences of length $p = 2^k-1$ at a rate k times faster than the shift rate is given. The method is valid for any positive integer k which is not a multiple of p.

A Lempel and H. Greenberger, Families of Sequences with Optimal Hamming - Correlation Properties, IEEE Trans. Information Theory, 20 (1974), 90-94.

Let $X = \{x(j)\}$, $Y = \{y(j)\}$ be two sequences of length q over an alphabet A, $|A| = a$. Define

$H_{xy}(\tau) = \sum_{0}^{q-1} h\,[x(j), y(j+\tau)]$, $0 \le \tau < q$ where $h[x,y] = \delta_{xy}$ and let S be the set of all sequences over A. Let $H(x) = \max_{0<\tau<q} \{H_{xx}(\tau)\}$, $H(x,y) = \max_{0\le\tau<q} \{H_{xy}(\tau)\}$ and $M(x,y) = \max\{H(x), H(y), H(x,y)\}$. Then x is called an optimal sequence of $H(x) \le H(x')$ for all $x' \in S$. The pair x,y is called optimal if $M(x,y) \le M(x',y')$ for all $x',y' \in S$. A subset

F of S is an optimal family if every pair of distinct elements is an optimal pair. A method of constructing optimal sequences is given for $q = p^n - 1$ and $a = p^k$ for a given prime p and positive integers k,n, $1 \leq k \leq n$. Optimal families of size p^k are also constructed and each sequence in the family is optimal.

J.H. Lindholm, An Analysis of the Pseudo-Randomness Properties of Subsequences of Long m-Sequences, IEEE Trans. Information Theory, 14 (1968), 569-576.

Let A_w be the number of subsequences of length M, from an m-sequence, of weight w. The p^{th} moment of the weight distribution is $W^p = \frac{1}{N} \sum_{w=1}^{M} w^p A_w$. It is shown here that the first two moments of the weight distribution does not depend on the particular m-sequence or equivalently, its characterisitc polynomial. The third moment however depends on the quantity B_3, the number of trinomials of degree less than M divisible by f(x), and their degrees. Similar results hold for higher moments. For the third mement the notion is related to coset functions and characteristic sequences.

J. Lindner, Binary Sequences up to Length 40 with Best Possible Auto-correlation Function, Electronic Letters, 11 (1975), 507.

A special purpose minicomputer was used to find all optimal sequences of length 40 or less, where optimality is measured by minimum absolute sidelobe value. For each given length, the number of optimal sequences is given, as well as the mean of the sidelobes, rms value of the sidelobes, the number of sidelobes with maximum absolute value and the distance from the main lobe to the first sidelobe with maximum absolute value (although it is not clear for which optimal sequence these last four values are computed, or whether they are invariant over all optimal sequences).

D.G. Luenberger, On Barker Codes of Even Length, Proc. IEEE, 51 (1963), 230-231.

It is shown that the length N of a Barker sequence (in the sense of Turyn) of even length must be a perfect square. It is noted that there does not exist such a sequence of length 16 (Russian reference).

F.J. MacWilliams, An Example of Two Cyclically Orthogonal Sequences with Maximum Period, IEEE Trans. Information Theory, 13 (1967), 338-339.

In 1966 Levitt and Wolf made the conjecture: If a, b are two n place ±1 vectors such that b is orthogonal to every cyclic permutation of a, then a and b cannot both have least period n under cyclic permutation. This conjecture is disproved here by showing the existence of a family of such sequences using cyclotomic polynomials. The smallest case is for n = 18 and this case is worked out in detail.

F.J. MacWilliams and N.J.A. Sloane, Pseudo-Random Sequences and Arrays, Proc. IEEE, 64 (1976), 1715-1729.

An extensive and interesting survey of the properties and applications of pseudo-random sequences (binary, 0,1) is given. It is then

shown how such a sequence can be displayed as an $n_1 \times n_2$ array where $n = 2^{k_1 k_2} - 1$, $n_1 = 2^{k_1} - 1$, $n_2 = n/n_1$ and $(n_1, n_2) = 1$. Such arrays then have properties which are two dimensional analogs of properties enjoyed by the sequences. In particular, if $\underline{b}$ is the array and A is the number of positions in which $\underline{b}$ and $\underline{b}$ shifted i places down and j positions to the right agree, and D the number of positions in which they disagree, then the correlation function for arrays, in general, is defined as

$$\rho(i,j) = \frac{A-D}{n} \qquad i,j = 0, \pm 1, \pm 2, \ldots$$

For the arrays derived from the pseudo-random sequences, $\rho(0,0) = 1$ and $\rho(i,j) = -1/n$, $0 \leq i < n_1$, $0 \leq j < n_2$, $(i,j) \neq (0,0)$. Only the periodic correlation function is considered. Other sections consider non-binary sequences and arrays and transmission functions (a type of generalized autocorrelation function).

J.L. Massey and J.J. Uhran, Sub-baud Coding, Proceedings, 13th Annual Allerton Conference on Circuit and System Theory, (1975), 539-547.

The importance of both the even and odd correlation functions in sub-baud coding is demonstrated. While the even autocorrelation function is invariant to cyclic shifting while the odd function is strongly dependent on its phase. The auto and cross correlation functions of cyclically distinct maximum length sequences are considered. Expressions for the peak off centre autocorrelation and cross correlation for both the even and odd functions for codes derived from the cyclic equivalent classes of a cyclic code are given. The construction of a class of asymptotically good codes, for which the ratio of off centre value to length tends to zero with length, is given.

L.B. Milstein, Some Statistical Properties of Combination Sequences, IEEE Trans. Information Theory, 23 (1977), 254-258.

Combining sequences with a Boolean function has long been a technique used to derive long sequences with good autocorrelation properties. This paper also considers the cross correlation of the long sequence with its components for use as rapid acquisition sequences. It is assumed that the sequences involved are chosen at random and all arguments are probabilistic.

P.S. Moharir, Ternary Barker Codes, Electronics Letters, 10 (1974), 460-461.

Ternary $(0,\pm 1)$ sequences of length N with aperiodic correlation function $\rho(k) = N^1 < N$ if $k = 0$ and 0 or ± 1, $k \neq 0$ are discussed and a table of such sequences of length less than 11 given. Good binary sequences are obtained from the ternary.

P.S. Moharir, Generalized PN Sequences, IEEE Trans. Information Theory, 23 (1977a), 782-784.

A generalized PN sequence is defined as one whose off-centre periodic correlation function is identically zero. Attention is focussed on the ternary $(0,\pm 1)$ case where certain combinatorial admissibility conditions are derived which are satisfied by certain cyclic difference sets and lead to new generalized PN sequences.

P.S. Moharir, Chinese Product Theorem for Generalized PN Sequences, Electronics Letters, 13 (1977b), 121-122.

A product-type theorem, which relates the periodic correlation function of the product sequence to the correlation functions of the two component sequences, is given based on the chinese remainder theorem. Some relationships between different sets and asymmetrically binary gpn sequences are given.

P.S. Moharir and A. Selvarajan, Optical Barker Codes, Electronics Letters, 10 (1974), 154-155.

The notion of optical Barker codes is introduced. These sequences are (0,1), begin and end with 1 and have an off peak non-periodic correlation function of magnitude less than or equal to unity. A sufficient condition for the existence of such a sequence of length m with n units in it is given, a quasi-search technique.

P.S. Moharir and A. Selvarajan, Systematic Search for Optical Barker Codes with Minimum Length, Electronics Letters, 10 (1974), 245-246.

An earlier quasi-search technique of the authors for optical Barker codes is slightly extended.

J.W. Moon and L. Moser, On the Correlation Function of Random Binary Sequences, SIAM J. Appl. Math, 16 (1968), 340-343.

An upper and lower bound on $M(s_n)$, the maximum absolute value of the off peak nonperiodic correlation of a binary (±1) sequence of length n, valid for "almost all" such sequences is given.

R.J. Pettit, Pulse Sequences with Good Autocorrelation Properties, Microwave J., 10 (1967), 63-67.

An elementary survey article on the subject.

M.B. Pursley and D.V. Sarwate, Evaluation of Correlation Parameters for Periodic Sequences, IEEE Trans. Information Theory, 23 (1977a), 508-513.

Three types of correlation functions are considered; the auto-correlation, cross correlation and odd correlation function for both the periodic and aperiodic cases. Several properties of these functions useful in analyzing their application to CDMA and SS systems are given and the amount of computation required to determine them discussed.

M.B. Pursley and D.V. Sarwate, Performance Evaluation for Phase-Coded Spread-Spectrum Multiple-Access Communication - Part II: Code Sequence Analysis, IEEE Trans. Communications, 25 (1977b), 800-803.

Bounds on the important parameters of the code sequences for SSMA are given, including auto-cross- and odd correlation functions, are given, as well as some computational techniques to determine them.

H.F.A. Roefs and M.B. Pursley, Correlation Parameters of Random Binary Sequences, Electronics Letters, 13 (1977), 488-489.

The performance of random binary sequences in terms of their correlation parameters, is examined in multiple access systems.

D.V. Sarwate, Cross-Correlation Properties of Sequences with Applications to Spread-Spectrum Multiple-Access Communications, to appear (1978a).

The trade-off between autocorrelation and cross correlation properties of binary sequences is studied via an inequality on the sum of squares of the two functions. Both the periodic and aperiodic cases are considered.

D.V. Sarwate, Bounds on Cross-Correlation and Autocorrelation of Sequences, to appear (1978b)

If θ_a and θ_c are the maximum of the off-centre periodic autocorrelation and crosscorrelation values respectively of a set of complex-valued sequences, it is shown that $(\frac{\theta_c}{N})^2 + \frac{N-1}{N(K-1)} (\frac{\theta_a}{N})^2 \geq 1$. Thus by specifying one of the values this relationship gives a lower bound on the other. Similar results are obtained for the aperiodic correlation functions. Certain optimum or asymptotically optimum periodic sequence sets are constructed.

D.V. Sarwate and M.B. Pursley, New Correlation Identities for Periodic Sequences, Electronics Letters, 13 (1977), 48-49.

The main result of the paper is to show that

$$\mu_{x,y}(k) = \sum_{\ell=1-N}^{N-1} C_{x,y}(\ell)\, C_{x,y}(\ell+k) = \sum_{\ell=1-N}^{N-1} C_x(\ell)\, C_y(\ell+k)$$

This quantity was shown to be useful in determining the signal-to-noise ratio in spread spectrum multiple access systems and permits considerable computational simplification since only autocorrelations are involved.

K.S. Schneider and R.S. Orr, Aperiodic Correlation Constraints on large Binary Sequence Sets, IEEE Trans. Information Theory, 21 (1975), 79-84.

An existence type theorem, proved by random coding and expurgation techniques, is proven which allows an examination of the relationships between the length n, maximum off centre autocorrelation k and maximum crosscorrelation β. A new proof of the Gilbert bound of coding theory is also given.

R.A. Scholtz and L.R. Welch, Group Characters: Sequences with Good Correlation Properties, IEEE Trans. Information Theory, 24 (1978), 537-545.

The theory of group characters of Abelian groups and some transform theory is used to construct complex sequences with good periodic autocorrelation and crosscorrelation functions. A computer study of truncated versions of some of these sequences considers their aperiodic correlation functions.

M.R. Schroeder, Synthesis of Low Peak Factor Signals and Binary Sequences with Low Autocorrelation, IEEE Trans. Information Theory, 16 (1970), 85-89.

The problem of how to adjust the phase angles and amplitudes of harmonics of a periodic signal to minimize the difference between the maximum and minimum values is considered. A "generally good" technique is proposed, with little proof, and its application to the construction of binary sequences with low autocorrelation considered.

G. Sequin, Binary Sequences with Specified Correlation Properties, Technical Report No. 7103 (1971), Department of Electrical Engineering, University of Notre Dame, Notre Dame, Indiana.

The notion of a cyclotomic sequence is defined and their correlation properties examined. Similarily construction methods and correlation properties of self-dual sequences are given. A weakly Barker sequence is defined as one for which $|F_{n-k}| \leq 1$, $0 < k < (n+1)/2$, where F_k is the non-periodic correlation function with a shift of k. Some properties of sequences obtained from Arithmetic codes are examined.

G. Sequin, Large Sets of Skew-Symmetric Sequences with Small Auto-and Cross-Correlations, to appear.

It is shown that there exsits large sets of skew symmetric binary sequences with low auto- and cross-correlations. The proof technique is that of skew symmetric binary sequences chosen at random, whose maximum off peak auto-correlation is less than α and whose maximum cross-correlation is less than β, is found. This lower bound increases exponentially with n.

V.M. Sidelnikov, Some k-Valued Pseudo-Random Sequences and Nearly Equidistant Codes, Problems of Information Transmission, 5 (1969), 12-16.

Two classes of sequences over the kth roots of unity, depending on whether n, their length, is 0 or 1 mod k, are constructed which have autocorrelation functions with precisely two off peak values. These were later independently discovered by Lempel et al (1977). In a similar vein some nearly equidistant codes over the kth roots of unity, using Hamming distance, are constructed where the term nearly equidistant implies the minimum distance is within 1 or 2 of the Plotkin bound.

V.M. Sidelnikov, On Mutual Correlation of Sequences, Soviet Math. Dokl., 12 (1971), 197-201.

Lower bounds on the periodic autocorrelation and cross-correlation peaks of complex sequences over the kth roots of unity are established. Sets of sequences whose peaks come close to achieving these bounds are described using a coding-theoretic approach.

R. Sivaswamy, Multiphase Complementary Codes, IEEE Trans. Information Theory, 24 (1978), 546-552.

Let $[S_{N+1}] = [S_0, S_1, \ldots, S_N]$ be a sequence of complex numbers of magnitude 1 with aperiodic autocorrelation function $X(\tau)$ and $[C_{N+1}] = [C_0, C_1, \ldots, C_N]$ a second such sequence with autocorrelation function $\psi(\tau)$. The two sequences are termed complementary if the sum of their autocorrelation functions is an impulse function, as in the original work of Golay for binary sequences. The condition of complementarity can be used to establish a relationship between the phases of the elements of the two sequences. Several examples of solving the required matrix equations are given. It is shown that if $[S_N]$ and $[C_N]$ form a multiphase complementary (MPC) code then so do $[S_N C_N]$, $[S_N \bar{C}_N]$ where the bar indicates phase reversal. Thus if an MPC code pair of length N exists so does one of length $N \cdot 2^k$. Some comments on the generation of MPC code sets (of size larger than 2), whose autocorrelations add up to an impulse function are given.

J.J. Stiffler, Rapid Acquisition Sequences, IEEE Trans. Information Theory, 14 (1968), 221-225.

A class of binary sequences of length $N = 2^n$, for all integer values of n, is presented which permits the phase of any of these sequences to be determined in every case after only $n=\log_2 N$ binary decisions. This compares, for example, with $L = \sum_1^m p_i$ binary decisions required when using a maximum length sequence of length $N=p_1 p_2 \ldots p_m$, $(p_i, p_j) = 1$, $i \neq j$. An argument as to the optimality of these sequences is given.

F. Surbock and H. Weinrichter, Interlacing Properties of Shift-Register Sequences with Generator Polynomials Irreducible over GF(p), IEEE Trans. Information Theory, 24 (1978), 386-389.

The properties of elementary sequences generated by irreducible (but not primitive) polynomials are examined. It is shown that each such elementary sequence can be constructed by interlacing shorter elementary sequences generated by the same polynomial. Three applications of this characterization are given, the last concerning the cross-correlation properties of equal length m-sequences.

Taki, H. Miyakawa, M. Hatori and S. Namba, Even-Shift Orthogonal Sequences, IEEE Trans. Information Theory, 15 (1969), 295-300.

An E-sequence is a binary (±1) sequence whose autocorrelation function vanishes for all even shifts, except for the zero shift. The D-sequence of Welti 1969 form a subset of E-sequences. The length of an E-sequence is a multiple of 4 and is twice the sum of at most two squares, a consequence of the construction of an E-sequence from a pair of complementary sequences of Golay. If there exists two E-sequences of length m and n respectively then there exists an E-sequence of length mn. An E-sequence C is called the mate of the E-sequence S if the cross correlation function is zero for all even shifts. It is shown that if $S=(x;y)$ (x = all odd members of S and y all even members) then the only mates are $(y^R; -x^R)$ and $(-y^R; x^R)$. From an E-sequence and its mate, a complete function set can be defined. Finally it is shown that an E-sequence and one of its mates forms a complementary pair in the sense of Golay.

C.-C. Tseng, Signal Multiplexing in Surface Wave Delay Lines Using Orthogonal Pairs of Golay Complementary Sequences, IEEE Trans. Sonics and ultrasonics, 18 (1971), 103-107.

The notion of orthogonal pairs of Golay complementary sequences is defined and their use to improve the coding efficiency of surface wave delay lines examined.

C.-C. Tseng and C.L. Liu, Complementary Sets of Sequences IEEE Trans. Information Theory, 18 (1972), 644-652.

The concept of a complementary pair of sequences due to Golay (1961) is generalized to allow for more than two sequences not necessarily all of the same length. The mate to such a set is a second set whose corresponding sequences have the same length such that the sum $\Sigma \psi_{A_i B_i}(k)$ is zero for all k, A_i the ith sequence in the first set and B_i the ith sequence in its mate. A collection of complementary sets is called mutually orthogonal if any 2 distinct sets are mates. Numerous properties

complementary sets and mutually orthogonal sets are established and many recursive constructions given. Applications to the signal processing of one and two dimensional arrays of real numbers are discussed.

R. Turyn, Ambiguity Functions of Complementary Sequences, IEEE Trans. Information Theory, 9 (1963a), 46-47.

The ambiguity function of a (not necessarily binary) sequence of length n is defined by

$$A(x,k,w) = \sum_{i=1}^{n-k} x_i x_{i+k} w^i$$

The properties of this function, and the sum of such functions for two sequences, is studied.

R. Turyn, On Barker Codes of Even Length, Proc. IEEE, 51 (1963b), 1256.

This paper extends the results of Luenberger by showing that if a periodic sequence of length $n=4N^2$, $C_k+C_{n-k} = 0$ does not exist then a Barker sequence of length n cannot exist. It is shown that such sequences for N the power of a prime cannot exist and it is noted that the cases for N=6, 10, 12 and others have also been disposed of. The result for N = 2 (n = 16) was, in this manner, first observed by Hall (although not in this context).

R.J. Turyn, The Correlation Function of a Sequence of Roots of 1, IEEE Trans. Information Theory, 13 (1967), 524-525.

The conjecture of Frank (1963), that

$$|c_m| \leq b_n = \left| \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \xi^i \right|$$

is established, for the multiphase codes of Frank.

R.J. Turyn, Sequences with Small Correlation, in Error Correcting Codes, H.B. Mann ed., John Wiley and Sons Inc., New York, 1968, 195-228.

A detailed survey of the existence and properties of sequences, both binary and over higher roots of unity, with low periodic or aperiodic correlation. The paper is difficult to read but contains most of the important results on the subject to that date, as well as some new ones.

R.J. Turyn, Hadamard Matrices, Bammert-Hall Units, Four Symbol Sequences and Surface Wave Encodings, J. Comb. Theory, 16A (1974a), 313-333.

The construction of n-symbol δ-codes, a generalization of Golay's complementary sequences, using combinatorial structures called Baumert-Hall units, is given and many properties of such codes shown. In particular many results on ternary codes are established.

R.J. Turyn, Four-Phase Barker Codes, IEEE Trans. Information Theory, 20 (1974b), 366-371.

Three phase and four phase Barker sequences are investigated. Many details on the structure of four phase Barker sequences are given and it is shown that there is only one such sequence that is of length 15

(found by Carley and referred to in Golomb and Scholz (1965)) apart from those equivalent to the real sequences. It is also shown that the correlation function of a cubic Barker sequence must be real.

R.J. Turyn and J. Storer, On Binary Sequences, Proc. Amer. Math. Soc., 12 (1961), 394-399.

Properties of the aperiodic correlation coefficient are given. These are then used to show that sequences of odd length, for which $|c_k| \leq 1$, $k > 0$, must possess certain periodicities. From these it is concluded that $n \leq 13$ i.e. there are no Barker sequences of length greater than 13.

S. Wainberg and J.K. Wolf, Subsequences of Pseudo-Random Sequences, IEEE Trans. Communications Technology, 18 (1970), 606-612.

Lindholm (1968) noted that the first two moments of the weight distribution of subsequences of m-sequences did not depend on the particular m-sequence chosen. Here the third and fourth moments of subsequences of lengths $M < 100$ of 6 particular m-sequences are considered in detail. Algorithms for determining these moments are given.

L.R. Welch, Lower Bounds on the Maximum Cross Correlation of Signals, IEEE Trans. Information Theory, 20 (1974), 397-399.

By considering bounds on the cross correlation function of arbitrary sets of vectors in an L dimensional vector space over the complex numbers, lower bounds on the maximum value of either the cross correlations or the off centre autocorrelation, for both the periodic and aperiodic cases, are established.

G.R. Welti, Quaternary Codes for Pulsed Radar, IEEE Trans. Information Theory, 6 (1960), 400-408.

An algorithm for generating quaternary codes with an impulse autocorrelation function is described. Additionally each such code has a mate and the cross-correlation between a code and its mate is identically zero. The construction method is based on first constructing binary codes (and their "mates" and "neighbours" and then converting these by simple rules for quaternary codes. The generation of these waveforms for use in radar is considered.