TECHNICAL REPORT 400-125

CORRELATION PROPERTIES OF MULTI-LEVEL CYCLIC SEQUENCES

Karl N. Levitt

November 1965

PROJECT: FINITE MEMORY NONLINEAR FILTERING OF DIGITAL SEQUENCES

PRINCIPAL INVESTIGATOR: Jack K. Wolf

FINAL REPORT—PART II

Prepared for
U.S. ARMY RESEARCH OFFICE—DURHAM
BOX CM, DUKE STATION
DURHAM, NORTH CAROLINA 27706

CONTRACT NO. DA-31-124-ARO-D-253
ARO(D) PROJECT NO. 4949E

LABORATORY FOR ELECTROSCIENCE RESEARCH

DEPARTMENT OF ELECTRICAL ENGINEERING

SCHOOL OF ENGINEERING AND SCIENCE

NEW YORK UNIVERSITY bronx, new york 10453

TECHNICAL REPORT 400-125

CORRELATION PROPERTIES OF MULTI-LEVEL CYCLIC SEQUENCES

Karl M. Levitt

November 1965

Project: FINITE MEMORY NONLINEAR FILTERING OF DIGITAL SEQUENCES

Principal Investigator: Jack K. Wolf

NEW YORK UNIVERSITY
SCHOOL OF ENGINEERING AND SCIENCE
DEPARTMENT OF ELECTRICAL ENGINEERING
Laboratory for Electroscience Research

University Heights
Bronx, New York 10453

FINAL REPORT - PART II

Contract No. DA-31-124-ARO-D-253
ARO(D) Project No. 4949E

September 1, 1964 to August 31, 1965

Prepared
for
U.S. ARMY RESEARCH OFFICE - DURHAM
BOX CM, DUKE STATION
DURHAM, NORTH CAROLINA 27706

ACKNOWLEDGMENT

The author wishes to acknowledge the help of his advisors, Professor J.K. Wolf and Professor L. Kurz.

The support of the U.S. Army Research Office at Durham, North Carolina, under contract DA-31-124-ARO-D-253, is gratefully acknowledged.

ABSTRACT

This thesis considers the problem of synthesizing cyclic (or periodic) sequences, with binary and nonbinary (N-ary) symbols, for special communication applications. For the applications considered, the sequences are transmitted over channels with additive white Gaussian noise. For correlation detection the autocorrelation function of a sequence or the cross-correlation function between sequences are required for the evaluation of performance.

The first part of the thesis is concerned with the derivation of new classes of sequences. Some new theoretical developments are presented on the cyclic correlation properties of sequences containing the N^{th} complex roots of unity as symbols. These sequences are related to real sequences containing phase modulated sinusoids as symbols.

A class of sequences derived by the interleaving of two level binary sequences is presented. These interleaved sequences are shown to exhibit autocorrelation and cross-correlation functions with intermediate peaks. The locations of the peaks can be controlled to synthesize autocorrelation functions which are "almost" two level or autocorrelation functions with peaks of different magnitudes. The application of these sequences to synchronization is considered.

Classes of N-ary sequences (called cyclically orthogonal sequences), which exhibit cross-correlation functions which are zero for all cyclic shifts are derived.

The second part of the thesis is concerned with the application of the sequences derived in the first part, as well as other known classes of sequences, to two special communication problems.

The first application is a binary asynchronous linear multiplex system. There are k transmitter-receiver pairs, each using sequences (which are summed linearly) as carriers for binary information. Although a particular transmitter is synchronized with the corresponding receiver, the other transmitter-receiver pairs are asynchronous with this pair. The average probability of error with additive white Gaussian noise is evaluated when the carriers are the binary cyclically orthogonal sequences. The performance is also determined when the carriers are sinusoids of different periods, random binary sequences, and sequences associated with Bose-Chaudhuri Codes.

The second application is an N-ary synchronous "hard-limiting" multiplex system. For this application there are also k transmitter-receiver pairs, although the respective carrier sequences are not summed linearly, but "hard-limited" prior to transmission. It is shown that the optimum set of carriers are the cyclically orthogonal sequences. The system performance is determined for these sequences. This system might be useful for satellite repeaters which usually employ "hard-limiters."

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

CORRELATION PROPERTIES OF MULTI-LEVEL CYCLIC SEQUENCES

1. INTRODUCTION

Cyclic or periodic sequences are gaining increasing importance in such communications applications as synchronization, tracking and ranging, multiplex carrier systems, and signalling over a continuous channel.[1] This thesis is concerned with the derivation of some new classes of sequences, and the application of these sequences to two important multiplex problems.

An N-ary sequence S, of length L, is defined as an L-dimensional vector, $S = (a_0, a_1, \ldots, a_{L-1})$, with symbols a_i, $i = 0,1, \ldots, L-1$, taken from a finite alphabet, usually the ring of integers modulo N, where N is any integer greater than 1. For practical applications the symbols are mapped onto quantities $a_i^{(m)}$, for which the ordinary addition and multiplication operations are defined. A waveform or carrier, f(t) of time duration Lt_1, is then associated with the mapped sequence, of the form

$$f(t) = \begin{cases} a_0^{(m)} & 0 \le t \le t_1 \\ a_1^{(m)} & t_1 \le t \le 2t_1 \\ \vdots & \\ a_{L-1}^{(m)} & (L-1)t_1 \le t \le Lt_1 \end{cases}$$

If $f(t+nLt_1) = 0$, for $0 \le t \le Lt_1$, $n = \pm 1, \pm 2, \ldots$, then the original sequence is referred to as an aperiodic sequence. If $f(t+Lt_1) = f(t)$, for all t, then S is referred to as a periodic or cyclic sequence. Only cyclic sequences are considered in the thesis.

Generally the terms sequence, mapped sequence and carriers have been used interchangeably in the literature. This custom will be continued in this thesis when there is no possibility of ambiguity, as is the case with binary sequences. However, when several types of mappings are possible the correct term will be used.

1.1 Review of Pertinent Prior Work

Several types of periodic sequences have been studied previously, with the research divided into four phases: (a) theoretical derivation of classes of sequences exhibiting particular autocorrelation and cross-correlation functions, (b) proofs on the nonexistence of classes of sequences exhibiting certain correlation properties, (c) methods of generating particular sequences, and (d) applications of sequences to special communication problems. A sampling of prior work in each of these areas is now briefly described.

a. Theoretical Derivation of Classes of Sequences

Considerable effort has been devoted to the derivation of sequences exhibiting autocorrelation functions which are two-level, i.e. the autocorrelation function is constant (usually -1/L) for all nonzero integral shifts. The best known of the two-level sequences, the maximal length sequences with binary or nonbinary components, have been studied by Singer,[2] Zierler,[3] and Golomb.[4] Other two-level binary sequences which have been synthesized are the quadratic residue sequence,[5] twin prime sequence,[6] and Hall sequence.[7]

Perfect N-ary sequences with elements mapped onto the roots of unity (the autocorrelation function is zero for all nonzero shifts) have been studied by Heimiller[8] and Franck, et al.[9] Perfect ternary sequences with elements mapped onto +1, -1, 0 have been found by Tompkins[10] by a computer search. Titsworth[11] has derived a class of two-level sequences with the elements contained in the field of irrational numbers. Titsworth[12] has also derived a class of "almost" two-level binary sequences for some lengths not covered by the known two-level sequences.

Extensive searches have been conducted for classes of sequences which exhibit low cross-correlation. Classes of orthogonal binary sequences have been derived from the theory of Hadamard matrices.[1] The theory is presently being extended to roots of unity sequences.[13] For nonorthogonal sequences, bounds on the number of sequences with cross-correlation bounded by an arbitrary limit has been derived.[14] Bounds on the number of sequences, with the cyclic cross-correlation function, bounded by certain limits have been derived by Gilbert.[15]

b. Nonexistence Proofs

Turyn[16] has presented proofs on the nonexistence of perfect binary sequences beyond length 4. In addition, he has shown[13] that two-level N-ary sequences do not exist for many lengths.

c. Generation of Binary Sequences

The generation of many classes of binary sequences by linear feedback shift registers has been considered.[1,17,18] Some classes of sequences can be generated by the filtering[19] of maximal length sequences.

d. Applications of Sequences

An important application of sequence theory has been the use of the orthogonal binary sequences as a signalling alphabet for the continuous Gaussian Channel.[20] The theory has been extended to N-ary sequences.[21] Stiffler[22] has considered the use of sequences for the synchronization of error-correcting codes. Binary sequences have been considered as carriers for binary multiplex systems.[23]

1.2 Brief Review of New Developments Presented in the Thesis

In Chapter 2 the background for the succeeding chapters is presented. In addition, several properties of nonbinary sequences are discussed. A theorem on the shift and add property of nonbinary maximal length sequences is derived, from which the autocorrelation function of ternary (+1, -1, 0) maximal length sequences is derived. A method of signalling with N^{th} roots of unity sequences as carriers is outlined. Information is transmitted by sending a sequence or one of its N-1 complements.

In Chapter 3 a class of binary sequences with useful autocorrelation and cross-correlation properties is presented. These sequences are derived by the interleaving of two-level sequences, or two-level and complement two-level sequences. It is shown that if n two-level sequences are interleaved, the autocorrelation function of the resultant sequence has n(n-1) minor peaks of height $\frac{L - n + 1}{nL}$. Fewer peaks of larger amplitude are obtained if several peaks occur at the same location. Using this interleaving procedure, autocorrelation functions with (n-1)

peaks of different amplitude, and "almost" two-level autocorrelation functions are synthesized. Classes of sequences exhibiting low values of cross-correlation at all cyclic shifts are synthesized by interleaving. Autocorrelation and cross-correlation functions with positive and negative peaks are synthesized by interleaving the complement two-level sequence along with the uncomplemented sequence. Interleaved maximal length sequences can be generated by the nonlinear filtering of a single maximal length sequence. A number of examples illustrating this technique are presented. The application of the interleaved sequences for synchronization is considered.

In Chapter 4 methods are presented for the synthesis of N-ary sequences (called cyclically orthogonal sequences), which are orthogonal for all cyclic shifts. All of the binary sequences, derived by the techniques presented in this chapter are of different least period. It is conjectured that cyclically orthogonal binary sequences of the same least period do not exist.

In Chapter 5 the application of cyclically orthogonal sequences as carriers for an asynchronous linear multiplex system is considered. In this system there are k users on a channel, with each transmitter-receiver pair using a different sequence as a carrier. Although a particular transmitter is synchronized with its corresponding receiver, all of the other transmitter-receiver pairs can be asynchronous with this particular pair. The respective carriers are summed linearly on the channel. The density function of the interference is determined and the average probability of error is evaluated when the received signals are

corrupted by additive white Gaussian noise. Several other classes of functions are considered as carriers for this system.

A different type of multiplex system is considered in Chapter 6. In this system there are k users on the channel, all transmitting synchronously with N-ary sequences as carriers. Information is transmitted by sending a sequence or one of its N-1 complements. However, the carriers are summed and then passed through a hard-limiter prior to transmission. The set of cyclically orthogonal sequences are shown to minimize the average probability of error.

2. PRELIMINARY DERIVATIONS

In this chapter some basic definitions, mappings, and theorems, which will be required in the succeeding chapters, are established. Several types of sequences are described and the autocorrelation and cross-correlation functions of the mappings of these sequences are defined. The complements of sequences are defined and the application to signalling is noted. A theorem concerning the shift and add property of the maximal length sequence is derived, and is then used to derive the autocorrelation function of a mapped ternary (+1, -1, 0) maximal length sequence.

2.1 Basic Definitions and Mappings

An N-ary cyclic sequence, S_a, of length L, is defined in this thesis as a vector, $S_a = (a_0, a_1, \ldots, a_{L-1})$, where a_i, $i = 0, \ldots, L-1$, can assume the values $0, 1, \ldots, N-1$. S_a can also be represented as a polynomial $S_a(x)$,

$$S_a(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{L-1} x^{L-1} \qquad (2.1)$$

where x is an indeterminate and $x^L = 1$, mod L. For practical applications the symbols of S_a are mapped onto quantities for which the usual addition and multiplication operations are defined. Three useful mappings are described below.

a. Binary Mapping

For N = 2 the mapping of the a_i's is $0 \rightarrow +1$, $1 \rightarrow -1$.

b. N^{th} Complex Roots of Unity Mapping[+]

The N possible values of a_i are mapped onto the N^{th} complex roots of unity, $0 \rightarrow e^{j0}$, $1 \rightarrow e^{j(2\pi/N)}$, ..., $(N-1) \rightarrow e^{j(N-1)2\pi/n}$. In the determination of correlation functions this mapping will be shown to be equivalent to the mapping $0 \rightarrow \cos \omega t$, $1 \rightarrow \cos(\omega t + 2\pi/N)$, ..., $(N-1) \rightarrow \cos[\omega t + (N-1)2\pi/N]$.

c. Mapping Onto Positive and Negative Integers

As a generalization of the binary mapping the N values of a_i can be mapped onto positive and negative integers. For N odd $0 \rightarrow 0$, $1 \rightarrow 1$, ..., $(N-1)/2 \rightarrow (N-1)/2$, $(N+1)/2 \rightarrow -(N-1)/2$, ..., $(N-1) \rightarrow -1$. The only result obtained for this mapping is for $N = 3$.

The normalized cross-correlation, $\rho_{ab}(\lambda)$, between two mapped sequences, $(S_a)^{(m)}$ and $(S_b)^{(m)}$ delayed by λ digits, where

$$(S_a)^{(m)} = (a_o^{(m)}, \ldots, a_{L-1}^{(m)}) ,$$

$$(S_b)^{(m)} = (b_o^{(m)}, \ldots, b_{L-1}^{(m)}) ,$$

and

$$a_i^{(m)} \quad , \quad b_i^{(m)}$$

are the mappings of a_i and b_i, is defined as:[++]

[+]For N = 2 the N^{th} complex roots of unity mapping and the binary mapping are identical.

[++]The general time cross-correlation $\rho_{ab}(\tau)$, of two functions $S_a(t)$ and $S_b(t)$ of period T is defined as

$$\rho_{ab}(\tau) = \frac{1}{T} \int_0^T S_a(t) S_b^*(t-\tau)\, dt$$

For sequences the integral reduces to a summation.

$$\rho_{ab}(\lambda) = \frac{1}{L} \sum_{i=0}^{L-1} a_i^{(m)} \left(b_{i-\lambda}^{(m)}\right)^* \qquad (2.2)$$

where the subscripts of $b^{(m)}$ are taken mod L, and $\left(b_{i-\lambda}^{(m)}\right)^*$ indicates the complex conjugate of $b_{i-\lambda}^{(m)}$. If a = b, then (2.2) reduces to the autocorrelation function of S_a.

For the binary and roots of unity mappings, the cross-correlation can be determined from the polynomial representations of S_a and S_b. For the binary case form a polynomial $S_c(x) = S_a(x) \oplus x^{\lambda} S_b(x) \bmod (x^L-1)$ (where $\oplus$ indicates modulo 2 sum). Then $\rho_{ab}(\lambda)$ is seen to be:

$$\rho_{ab}(\lambda) = \frac{1}{L} \left[\text{No. of 0's in } S_c(x) - \text{No. of 1's in } S_c(x)\right] \qquad (2.3)$$

If S_a and S_b are N-ary sequences mapped onto the complex roots of unity, then form the polynomial $S_c(x) = S_a(x) - x^{\lambda} S_b(x)$, mod (x^L-1), (where the symbol subtraction is mod N). Then $\rho_{ab}(\lambda)$ is seen to be

$$\rho_{ab}(\lambda) = \frac{1}{L} \sum_{d=0}^{N-1} \left[\text{No. of d's in } S_c(x)\right] e^{j(2\pi d/N)} \qquad (2.4)$$

It can be shown that the mapping onto the phase modulated cosine functions is related to the mapping onto the complex roots of unity.

The cross-correlation function, $\rho_{ab}(\lambda)$, for the roots of unity mapping is

$$\frac{1}{L} \sum_{i=0}^{L-1} \exp\left[j \frac{2\pi}{N} (a_i - b_{i-\lambda})\right]$$

Under the mapping onto the phase modulated cosine functions the cross-correlation function becomes

$$\rho_{ab}(\lambda) = \frac{1}{Lt_1} \sum_{i=0}^{L-1} \int_{it_1}^{(i+1)t_1} \cos\left(\omega t + \frac{2\pi}{N} a_i\right) \cdot \cos\left(\omega t + \frac{2\pi b_{i-\lambda}}{N}\right) dt$$

$$= \frac{1}{2L} \sum_{i=0}^{L-1} \cos\left[\frac{2\pi}{N} (a_i - b_{i-\lambda})\right]$$

$$+ \frac{1}{L\omega t_1} \sum_{i=0}^{L-1} \left\{\sin\left[(i+1)\omega t_1 + \frac{2\pi}{N} a_{i+1}\right] \cdot \cos\left[(i+1)\omega t_1 + \frac{2\pi}{N} b_{i-\lambda+1}\right]\right.$$

$$\left. - \sin\left[i\omega t_1 + \frac{2\pi}{N} a_i\right] \cdot \cos\left[i\omega t_1 + \frac{2\pi}{N} b_{i-\lambda}\right]\right\}$$

where t_1 is the duration of one time slot. The second summation can be dropped if $\omega t_1 \gg 0$, and thus the correlation function under the cosine function mapping is proportional to the real part of the correlation function for the roots of unity mapping.*

*The analysis for the phase modulated cosine functions assumes that the phases of the carriers of the two functions which are cross-correlated are identical. However, if the phases are random, then the typical correlation term becomes

$$\frac{1}{2L} \cos\left[\varphi + \frac{2\pi}{N} (a_i - b_{i-\lambda})\right]$$

where φ is uniformly distributed between 0 and 2π. For the applications which will be considered, it will be assumed that φ is zero.

It can be shown that all correlation functions of mapped sequences (real and complex) are linear between integral cyclic shifts, indicating that the determination of the correlation function at integral cyclic shifts completely specifies the correlation function.*

A technique for binary signalling with binary sequences, (called coherent phase shift keying, PSK) is to transmit the mapping of a sequence or its complement (negative). If roots of unity (or phase modulated cosine) mapped sequences are used as carriers, then a generalization of the PSK case can be specified by defining complements of N-ary sequences. The r^{th} complement sequence, $S_a^{(q_r)}$ of S_a is defined as:

$$S_a^{(q_r)} = (a_0-r,\ a_1-r,\ \ldots,\ a_{L-1}-r) \bmod N \tag{2.5}$$

In polynomial representation the complement polynomial, $S^{(q_r)}(x)$, is seen to be:

$$S_a^{(q_r)}(x) = S_a(x) - r(x) \tag{2.6}$$

where $r(x) = r + rx + \ldots + rx^{L-1}$.

The cross-correlation function $\rho_{aa_r}(0)$ between a mapped root of unity sequence and its r^{th} complement is $\rho_{aa_r}(0) = e^{-j(2\pi r/N)}$. From a recent report by Reed and Scholtz,[21] integral expressions for the average probability of error for N^{th} roots of unity complement signalling can be derived.

*The proof for binary sequences is a special case of Theorem 5.1.

The complement sequence concept will be used in Chapter 4 for the synthesis of classes of N-ary sequences which are orthogonal for all cyclic shifts. The complement signalling concept will be discussed further in Chapter 6 when the N-ary "hard" limiting multiplex system is analyzed.

In the following section some new results are presented on the characteristics of maximal length p-nary (N = p where p is a prime number) sequences.

2.2 Maximal Length p-nary Sequences

The best known of the p-nary sequences is the maximal length p-nary sequence. Peterson[24] has shown that the polynomial representation $h_m(x)$ of a maximal length sequence can be derived from a primitive irreducible polynomial, $g_p(x)$, over GF(p). If $g_p(x)$ is of degree r, then the coefficients of $h_m(x)$, which is of degree p^r-1-r

$$h_m(x) = \frac{x^{p^r-1} - 1}{g_p(x)} \tag{2.7}$$

specify the first p^r-r digits of the maximal length sequences of length $L = p^r-1$, the last r-1 digits being zero. The sequence corresponding to $h_m(x)$ can be generated by an r stage p level shift register with feedback connections prescribed by $g_p(x)$. It has been shown[24] that in a maximal length sequence, the field elements, 1 through p-1, appear exactly p^{r-1} times and the field element 0 appears exactly $p^{r-1}-1$ times. It has also been established[24] that the p^r-1 r-tuples formed by taking r successive digits of a maximal length sequence, $a_0, a_1, \ldots, a_{r-1}$; $a_1, a_2, \ldots, a_r$;

...; $a_{p^r-1}, a_1, \ldots, a_{r-2}$; are the (p^r-1) distinct nonzero r-tuples over GF(p).

It is well known[4] that maximal length binary ($N = p = 2$) sequences exhibit the shift and modulo 2 add (or equivalently the shift and modulo 2 subtract) property. That is, if a maximal length binary sequence is delayed an integral number of digits and the delayed sequence is added (modulo 2) to the original sequence, the resultant sequence will itself be a delayed version of the original sequence.

The shift and add property may be written as:

$$h_m(x) \oplus x^{\lambda} h_m(x) \equiv \begin{cases} x^{I(\lambda)} h_m(x) & \lambda = 1, \ldots, L-1 \\ & \mod(x^L-1) \\ 0(x) & \lambda = 0 \end{cases} \tag{2.8}$$

It can be shown that $I(\lambda)$ is unique for given λ, and for $\lambda_i \neq \lambda_j \bmod L$, $I(\lambda_i) \neq I(\lambda_j) \bmod L$. These properties of $I(\lambda)$ will be used in Chapter 3 when the nonlinear filtering of maximal length sequences is discussed.

Wolf et al[25] using a set of tables computed by Elspas[26] described a method for determining $I(\lambda)$ as a function of the primitive polynomial $g_p(x)$, over GF(2).

The following theorem describes the shift and modulo p add property of p-nary maximal length sequences ($p > 2$).

THEOREM 2.1 If a p-nary maximal length sequence ($p > 2$) of length $L = p^r-1$ is delayed an integral number of digits, and the delayed sequence is added (mod p) to the original sequence, the resulting sequence will itself be a delayed version of the original sequence, except for a shift of $(p^r-1)/2 = L/2$ digits, in which case the resulting sequence is the all zero sequence.

Proof: Peterson[24] has shown that the p^r-1 nonzero terms in the ideal generated by $h_m(x)$ in the algebra of polynomials modulo x^L-1 correspond to the p^r-1 cyclic shifts of the maximal length sequence. Since the ideal is an additive subgroup, the addition (mod p) of $h_m(x)$ and a shifted version of $h_m(x)$ yields a unique shifted version of $h_m(x)$ except for the summation

$$h_m(x) + (p-1)h_m(x)$$

which will yield the polynomial 0(x) corresponding to the all zero sequence.

It will now be shown that the polynomial $(p-1)h_m(x)$ is congruent to $x^{L/2}h_m(x)$ modulo (x^L-1); the latter polynomial corresponding to a cyclic shift of L/2 digits. We know:

$$g_p(x)h_m(x) \equiv 0 \quad \text{mod}(x^L-1) \tag{2.9}$$

Thus in order to show that

$$(p-1)h_m(x) \equiv x^{L/2}h_m(x) \quad \text{mod}(x^L-1) \tag{2.10}$$

it is sufficient to demonstrate that

$$(x^{L/2}-p+1) \equiv (x^{L/2}+1) \equiv 0 \quad \text{mod } g_p(x) \tag{2.11}$$

However, for (2.11) to be true, it is necessary to show that

$$g_p(x) \mid (x^{L/2}+1) \tag{2.12}$$

We know that $g_p(x)$ divides $(x^\ell-1)$, for no value of ℓ less than $p^r-1 = L$ since $g_p(x)$ is primitive. Thus

$$g_p(x) \mid (x^{L/2}+1)(x^{L/2}-1) \tag{2.13}$$

Since $g_p(x)$ cannot divide $x^{L/2}-1$,

$$g_p(x) \mid (x^{L/2}+1)$$

establishing the theorem.

The following corollary to Theorem 2.1 pertains to the shift and subtract of p-nary maximal length sequences.

> COROLLARY 2.1 If a p-nary maximal length sequence is delayed an integral number of digits and the delayed sequence is subtracted (mod p) from the original sequence, the resultant sequence will itself be a delayed version of the original maximal length sequence for all nonzero shifts.

Proof: Since the subtraction from $h_m(x)$ of any term in the ideal generated by $h_m(x)$, yields a unique nonzero term, except for the operation $h_m(x) - h_m(x)$, the shift and subtract property is evident.

From Theorem 2.1, Corollary 2.1, and the properties of maximal length sequences, the autocorrelation functions of these sequences, transformed by two mappings, are now presented.

THEOREM 2.2 The autocorrelation function, $\rho_A(\lambda)$, of a ternary ($p = 3$) maximal length sequence transformed by the mapping $0 \rightarrow 0$, $1 \rightarrow 1$, $2 \rightarrow -1$ is:

$$\rho_A(\lambda) = \begin{cases} (2\cdot 3^{r-1})/(3^r-1) & \lambda = 0 \\ -(2\cdot 3^{r-1})/(3^r-1) & \lambda = L/2 \\ 0 & \lambda \neq 0,\ L/2 \end{cases} \tag{2.14}$$

The proof of Theorem 2.2 is presented in Appendix A. A plot of $\rho_A(\lambda)$ as given by Theorem 2.2 is shown in Figure 2.1.

The autocorrelation function of a maximal length p-nary sequence (all p) transformed by the roots of unity mapping is

$$\rho_A(\lambda) = \begin{cases} 1 & \lambda = 0 \\ -1/L & \lambda \neq 0 \end{cases} \tag{2.15}$$

The result is derived using Corollary 2.1 and Equation (2.4). A plot of the autocorrelation is shown in Figure 2.2. This type of autocorrelation function is known as a <u>two-level autocorrelation</u> function and the maximal length sequence is known as a <u>two-level sequence</u>.

Two-level <u>binary</u> sequences, besides the maximal length sequence, have been derived for the following values of L.

a. $L = 4$ (Perfect Sequence)

b. $L = 4n-1$ is prime $n = 1,2, \ldots$ (Quadratic Residue Sequence)[5]

c. $L = p(p+2)$ where p and $p+2$ are prime (Twin Prime Sequence)[6]

d. $L = 4n^2+27$ is prime (Hall Sequence)[7]

The out-of-phase autocorrelation of the first sequence is 0, and it is the only known binary sequence to exhibit this property. The out-of-phase autocorrelation function of the remaining sequences is $-1/L$. The two-level binary sequences with out-of-phase autocorrelation equal to $-1/L$ will be used in Chapter 3 to derive, by interleaving, larger classes of binary sequences with various autocorrelation and cross-correlation properties.

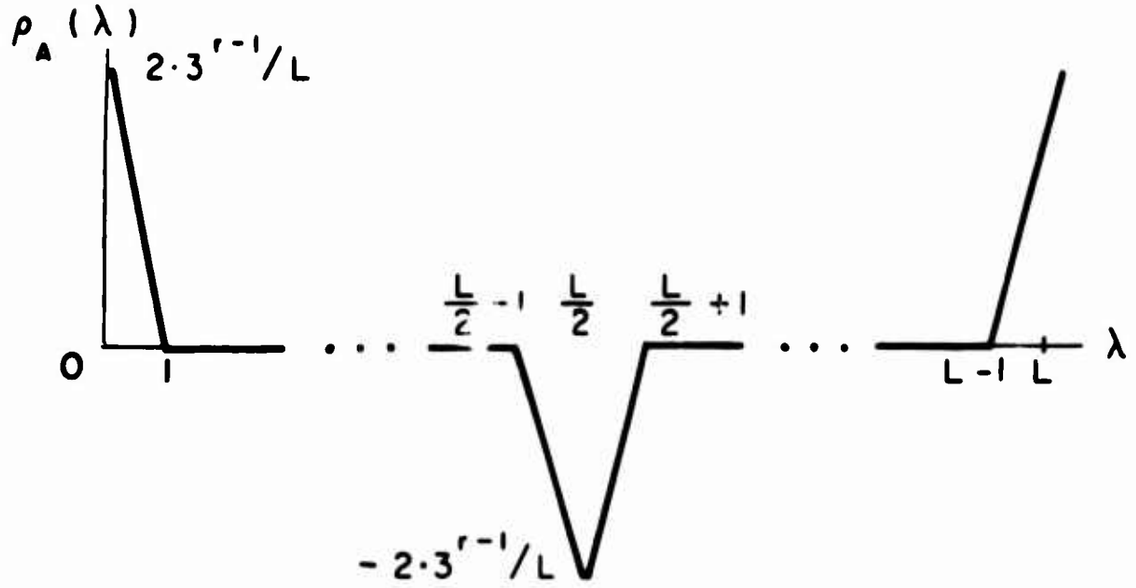


FIG. 2.1.

AUTOCORRELATION FUNCTION OF TERNARY MAXIMAL LENGTH SEQUENCE TRANSFORMED BY MAPPING $0 \rightarrow 0, 1 \rightarrow 1, 2 \rightarrow -1$

FIG. 2.2.

AUTOCORRELATION FUNCTION OF P-NARY MAXIMAL LENGTH SEQUENCE TRANSFORMED BY ROOTS OF UNITY MAPPING

Two-level perfect N-ary sequences, mapped onto the roots of unity, are known[8,9] for $L = N^2$. However, except for the maximal length sequences, the general theory of two-level sequences has not been satisfactorily generalized to N-ary sequences. For $N = 3$ a two-level root of unity mapped sequence (01221) has been found by the author and it has been indicated[27] that no two-level ternary roots of unity mapped sequences exist for lengths other than 5, 8, 9 up to 25.

3. SEQUENCES DERIVED BY THE INTERLEAVING OF TWO-LEVEL BINARY* SEQUENCES

3.1 Introduction

In Chapters 1 and 2 the prior research in the derivation of two-level binary sequences was summarized. Titsworth[12] has derived limited classes of "almost" two-level sequences (the autocorrelation function is close to zero for nonzero shifts), by forming either the tensor or term-by-term products of the known two-level sequences. From the theory of cyclic codes, in particular, Bose-Chaudhuri Codes,[28] bounds on the autocorrelation functions of some additional sequences can be found. Emphasis has been placed on the derivation of two-level sequences because they provide simple and accurate methods for tracking, ranging and synchronization.[1]

With the major emphasis placed on the derivation of two-level and "almost" two-level sequences, the general problem of synthesizing sequences exhibiting arbitrary realizable autocorrelation functions has remained unsolved.

In this chapter a large class of previously unknown sequences are synthesized by the arbitrary n-fold interleaving** of the same two-level sequence. It will be shown that the autocorrelation function of the interleaved sequence is similar to that of the original sequence

---

* The discussion to follow is limited to the interleaving of binary sequences since many more binary two-level sequences are known than general N-ary two-level sequences. However, the theory presented is applicable to the interleaving of N-ary sequences.

**The interleaving method has been used previously[29] to derive error-correcting codes with multiple burst error correction capability.

except for the addition of n(n-1) intermediate minor peaks of height (L-n+1)/nL. A number of these peaks can occur at the same location to produce fewer peaks of larger amplitude. A formula for calculating the location of the minor peaks is derived. Using the interleaving technique, a new set of "almost" two-level sequences are synthesized. Also autocorrelation functions with (n-1) peaks of different amplitudes are presented. The cross-correlation function between pairs of sequences, with these autocorrelation properties, is considered. The theory is extended to sequences formed by the interleaving of two-level and complement two-level sequences.

An n fold interleaved sequence can be generated by the gating of sequences from n separate shift registers. However, it is shown that a class of sequences formed by the interleaving of maximal length sequences can be generated by a relatively simple nonlinear filtering technique. Several examples of sequences derived by nonlinear filtering are presented.

The application of interleaved sequences for synchronization is discussed.

3.2 Derivation of Peak Locations

It was shown in Chapter 2 that the cross-correlation function of two transformed binary sequences or the autocorrelation function of a transformed binary sequence could be determined from the polynomial representations of the sequences. Throughout the remainder of this chapter $h(x)$ and $x^{\alpha}h(x)$ will be the polynomial representations of a

two-level binary sequence, with out-of-phase autocorrelation of -1/L, and a two-level binary sequence delayed by α digits, respectively. Hence, the polynomial h'(x), $h'(x) \equiv h(x) \oplus x^{\alpha} h(x) \equiv h(x)[1 \oplus x^{\alpha}]$, mod $x^{L}-1$, has L zeros if $\alpha = 0$, or (L-1)/2 zeros and (L+1)/2 ones if $\alpha \neq 0$.

Two definitions concerned with general interleaved sequences are now presented.

Definition: If the polynomial $S_a(x)$ corresponds to the sequence $(a_0, \ldots, a_{L-1})$ then the polynomial $x^{n\alpha+v} S_a(x^n)$, where n is a positive integer, $\alpha = 0, 1, \ldots, L-1$, $v = 0, 1, \ldots, n-1$, corresponds to the sequence

$$(\underbrace{0,0, \ldots, 0}_{v}, a_{L-\alpha}, \underbrace{0,0, \ldots, 0}_{n-1}, a_{L-\alpha+1}, \ldots,$$

$$\underbrace{0,0, \ldots, 0}_{n-1}, a_{L-\alpha-1}, \underbrace{0,0, \ldots, 0}_{n-1-v})$$

Polynomials must now be taken mod $(x^{nL}-1)$.

Definition: The sequence S_c resulting from the (2-fold) interleaving of sequence S_a, and sequence S_b delayed by α digits is:

$$S_c = (a_0, b_{-\alpha}, a_1, b_{1-\alpha}, \ldots, a_{L-1}, b_{L-1-\alpha}).$$

The polynomial $S_c(x)$ can then be written as

$$S_c(x) \equiv S_a(x^2) + x^{2\alpha+1} S_b(x^2) \bmod (x^{2L}-1).$$

The synthesis procedure presented is to interleave a two-level sequence with (n-1) shifted versions of the same two-level sequence.

The resultant sequence, (in polynomial representation), denoted as $S_r(x)$ is:

$$S_r(x) \equiv h(x^n) \sum_{v=0}^{n-1} x^{n\alpha_v+v} \text{ , mod } (x^{nL}-1) \tag{3.1}$$

where the α_v's, called the interleaving constants, can assume the values* 0,1, ..., L-1, and $\alpha_0 = 0$.

The procedure for deriving the autocorrelation function $\rho_r(n\delta+w)$, of the transformed binary sequence corresponding to $S_r(x)$, for an arbitrary integral delay $(n\delta+w)$, $\delta = 0,1, \ldots, L-1$, $w = 0,1, \ldots, n-1$ is:

a. Form the polynomial $S_p(x) \equiv S_r(x) \oplus x^{n\delta+w} S_r(x)$, mod $(x^{nL}-1)$

b. Apply Equation (2.3) to $S_p(x)$ [count the number of 0's and 1's in $S_p(x)$] replacing 1/L by 1/nL.

It is seen that:

$$x^{n\delta+w} S_r(x) \equiv h(x^n) \sum_{v=0}^{n-1} x^{n(\alpha_v+\delta)+v+w} \text{ , mod } (x^{nL}-1) \tag{3.2}$$

Thus the polynomial $S_p(x)$ is:

$$S_p(x) = h(x^n) \sum_{v=0}^{n-1} x^{(n\alpha_v+v)} \left[1 \oplus x^{n(\delta+\alpha_{n-w+v}-\alpha_v+\mu_{wv})}\right] \text{ mod } (x^{nL}-1) \tag{3.3}$$

where

$$\mu_{wv} = \begin{cases} 1 & v < w \\ 0 & v \geq w \end{cases}$$

and subscripts are taken mod n.

*For the most general type of interleaved sequence $\alpha_0 \neq 0$. However, assuming $\alpha_0 = 0$ does not reduce the generality of the autocorrelation functions.

The exponents of the terms $x^{n(\delta+\alpha_{n-w+v}-\alpha_v+\mu_{wv})}$ determine the value of the autocorrelation function for a particular delay $(n\delta+w)$. If no exponent is equal to zero (for a particular δ and w) then the sequence S_p consists of n interleaved sequences each containing $(L-1)/2$ zeros and $(L+1)/2$ ones providing an autocorrelation value of $\rho_r(n\delta+w) = -1/L$. However, if σ exponents are equal to zero (for a particular set of δ and w) then S_p consists of σ all zero sequences plus $n-\sigma$ sequences, each containing $(L-1)/2$ zeros and $(L+1)/2$ ones, providing an autocorrelation value of $\rho_r(n\delta+w) = (\sigma L-n+\sigma)/nL$. For this condition the autocorrelation function is said to have a "σ" order minor peak, $\sigma = 0,1, \ldots, n$.

From (3.3) it can be seen that an "n" order peak occurs at a delay of 0, (corresponding to unity autocorrelation), and no peaks occur for delays of $n,2n, \ldots, (L-1)n$.

From (3.3) it is determined that peaks occur for

$$\delta_{w,v} \equiv \alpha_v - \alpha_{n-w+v} - \mu_{wv} \text{ , mod } L \qquad (3.4)$$

where

$$w = 1,2, \ldots, n-1$$

$$v = 0,1, \ldots, n-1$$

and

$$\alpha_o = 0$$

In order to identify each peak, subscripts have been placed on the parameter δ. For a given value of w there are n peaks providing a total of $n(n-1)$ single order peaks. However, a number of single peaks can occur at the same point to produce multiple order peaks.

The $n(n-1)$ peak locations cannot be arbitrarily chosen. Since there are $(n-1)$ independent parameters - the interleaving constants

$\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ - only (n-1) peak locations are computable.

It will be useful also to know the cross-correlation function between two interleaved sequences. For two interleaved sequences,

$$S_r^{(1)}(x) \equiv h(x^n) \sum_{v=0}^{n-1} x^{n\alpha_v^{(1)}+v}$$

and

$$S_r^{(2)}(x) \equiv h(x^n) \sum_{v=0}^{n-1} x^{n\alpha_v^{(2)}+v} \text{ , mod } (x^{nL}-1) \tag{3.5}$$

cross-correlation peaks, $\delta'_{w,v}$, occur for:

$$\delta'_{w,v} \equiv \alpha_v^{(1)} - \alpha_{n-w+v}^{(2)} - \mu_{wv} \text{ , mod } L \tag{3.6}$$

where $w,v = 0,1, \ldots, n-1$ and $\alpha^{(1)}$, $\alpha^{(2)}$ are the interleaving constants of the respective sequences. There are n^2 single order cross-correlation peaks (some of which can occur at the same point to yield multiple order peaks).

In the following section a number of constraint equations on the autocorrelation peak locations are derived and a synthesis technique is indicated.

3.3 Constraints on Autocorrelation Peak Locations

The following constraint equations are derived from (3.4).

a. If all of the peak locations for a given value of w are summed, mod L, it is noted that:

$$\sum_{v=0}^{n-1} \delta_{w,v} = -w \equiv L - w \text{ , mod } L \tag{3.7}$$

b. There is a symmetry relationship which the peak locations satisfy which ensures that $\rho_r(n\delta+w) = \rho_r(-n\delta-w)$. The resulting constraint equation is:

$$\delta_{w,v} \equiv -\delta_{n-w,v-w} - 1 \text{ , mod } L \tag{3.8}$$

c. The peak locations $\delta_{w,v}$, $w = 2,3, \ldots, n-1$, can be easily calculated from the peak locations for $w = 1$ from the equation:

$$\delta_{w,v} \equiv \sum_{b=v-w+1}^{v} \delta_{1,b} \text{ , mod } L \tag{3.9}$$

Equations (3.7) and (3.9) can be used to synthesize sequences with various autocorrelation functions. The procedure used in the examples to follow is to prescribe values for $\delta_{1,0}, \delta_{1,1}, \ldots, \delta_{1,n-2}$; utilize (3.7) to calculate $\delta_{1,n-1}$, and utilize (3.9) to calculate the remaining peak locations. Equation (3.4) is then used to determine the interleaving constants from $\delta_{1,0}, \ldots, \delta_{1,n-2}$.

It is interesting to note that although there are L^{n-1} possible combinations of interleaving constants (i.e., L^{n-1} different interleaved sequences), there are fewer distinct autocorrelation structures. If the peak locations for $w = 1$ are written as a linear array, $(\delta_{1,0}, \delta_{1,1}, \ldots, \delta_{1,n-1})$, then from (3.9), any cyclic shift of the array or any cyclic shift of the reciprocal array (backwards array), will yield identical autocorrelation functions although the interleaved sequences will in general be different. The exact number of distinct autocorrelation structures is the number of unequivalent n-tuples in the ring of integers mod L, with the constraint that the sum of the elements of the n-tuple is

-1 mod L. Two n-tuples are defined as unequivalent if and only if one n-tuple cannot be derived from the other by a cyclic shift or a cyclic shift of the reciprocal. The number of such unequivalent n-tuples has not been determined.

In the following two sections examples will be presented of two types of autocorrelation functions which can be derived by interleaving two-level sequences. In the first example the interleaving constants are chosen so that the highest autocorrelation peak is "2" order, providing an almost two-level autocorrelation function. In the second example, the interleaving constants are chosen so that all autocorrelation peaks are of different heights.

3.4 "Almost" Two-Level Autocorrelation Function

The synthesis procedure will be to choose $\delta_{1,0}, \ldots, \delta_{1,n-2}$ and derive the remaining peaks from these values. Let L be a prime* and let n = L+1. Thus the length of the interleaved sequence will be L(L+1). Choose the peak locations for w = 1 as:

$$\delta_{1,0} \equiv L-1,\ \delta_{1,1} \equiv 0,\ \delta_{1,2} \equiv d,\ \delta_{1,3} \equiv 2d,\ \ldots,\ \delta_{1,L} \equiv (L-1)d \pmod{L} \tag{3.10}$$

where $d \equiv 1,2, \ldots, L-1 \pmod{L}$.

Since L is prime, the numbers 0,d, ..., (L-1)d are all of the distinct numbers mod L. It is easily verified that the peak locations given by (3.10) satisfy the constraint (3.7) since

*Most of the two-level binary sequences are of prime length. The quadratic residue and Hall sequences are always of prime length and the maximal length sequences of length 2^r-1 are of prime length if r is a Mersenne prime.

$$\sum_{v=0}^{L} \delta_{1,v} = \sum_{\nu=0}^{L-1} \nu + (L-1) \equiv -1 \ , \ \mathrm{mod}\ L$$

There are then (L-1) single order peaks and one double order peak for $w = 1$.

The remaining peak locations are calculated using (3.9). In applying (3.9) consider the (L+1) peak locations for a given value of w divided into two groups. The first group contains those values of $\delta_{w,v}$, which are not explicit functions of $\delta_{1,o}$. The peak locations for this group will assume the value

$$\delta_{w,v} \equiv \sum_{b=v-w+1}^{v} \delta_{1,b} \equiv \sum_{\nu=v-w}^{v-1} \nu d \equiv v(wd) - \frac{wd}{2}(w+1) \ , \qquad (3.11)$$
$$\mathrm{mod}\ L \ .$$

From the above equation it is noted that all of the peak locations in the first group are unequal since

$$v(wd) - \frac{wd}{2}(w+1) \not\equiv v'(wd) - \frac{wd}{2}(w+1) \quad \mathrm{mod}\ L$$

for $v \not\equiv v'$, mod L.

The second group of peak locations contains those values of $\delta_{w,v}$ which are functions of $\delta_{1,o}$. For these values of v a typical peak location is

$$\delta_{w,v} \equiv v(wd) - \frac{wd}{2}(w+1) + (L-1) \ , \ \mathrm{mod}\ L \ .$$

The peak locations in this second group also are all distinct. However, a peak location in the first group can be equal to a peak location in the second group. Hence, the autocorrelation function will contain zero,

first and second order peaks. The magnitudes of first and second order peaks are 0 and +1/L respectively. The autocorrelation function of the sequence derived by the (L+1) fold interleaving of the length L = 7 maximal length sequence, with d = 1, is shown in Figure 3.1.

L sequences instead of (L+1) can be interleaved to provide autocorrelation functions bounded by double order peaks by choosing the peak locations for w = 1 as $\delta_{1,0} = L-1$, $\delta_{1,1} = d$, $\delta_{1,2} = 2d$, ..., $\delta_{1,L-1} = (L-1)d$.

Fewer than L sequences can be interleaved to provide sequences with autocorrelation functions bounded by double order peaks. If a sequence of length nL, $n < L$, is to be synthesized, a synthesis procedure would be to find a set of n numbers, $\nu, \nu+d, \ldots, \nu+(n-1)d$, which sum to -1 mod L. There is always a unique number ν for any d and n such that this congruence can be satisfied. These numbers (in order) are then the peak locations $\delta_{1,0}, \delta_{1,1}, \ldots, \delta_{1,n-1}$, and it can be shown that the resultant autocorrelation function is bounded by double order peaks. It has been found that for certain values of n the autocorrelation function derived in this manner is bounded by single order peaks, although no general result to this effect was found.

It can be shown that the cross-correlation function, for all cyclic shifts, between two "almost" two-level interleaved sequences, for $n \leq L$ and n prime, is bounded by fourth order peaks. The proof for $n = L$ has been presented elsewhere;[30] the proof for $n < L$ is given below.

Consider an "almost" two-level interleaved sequence with the peak locations $\delta^{(1)}_{w,v}$ for w = 1 chosen as

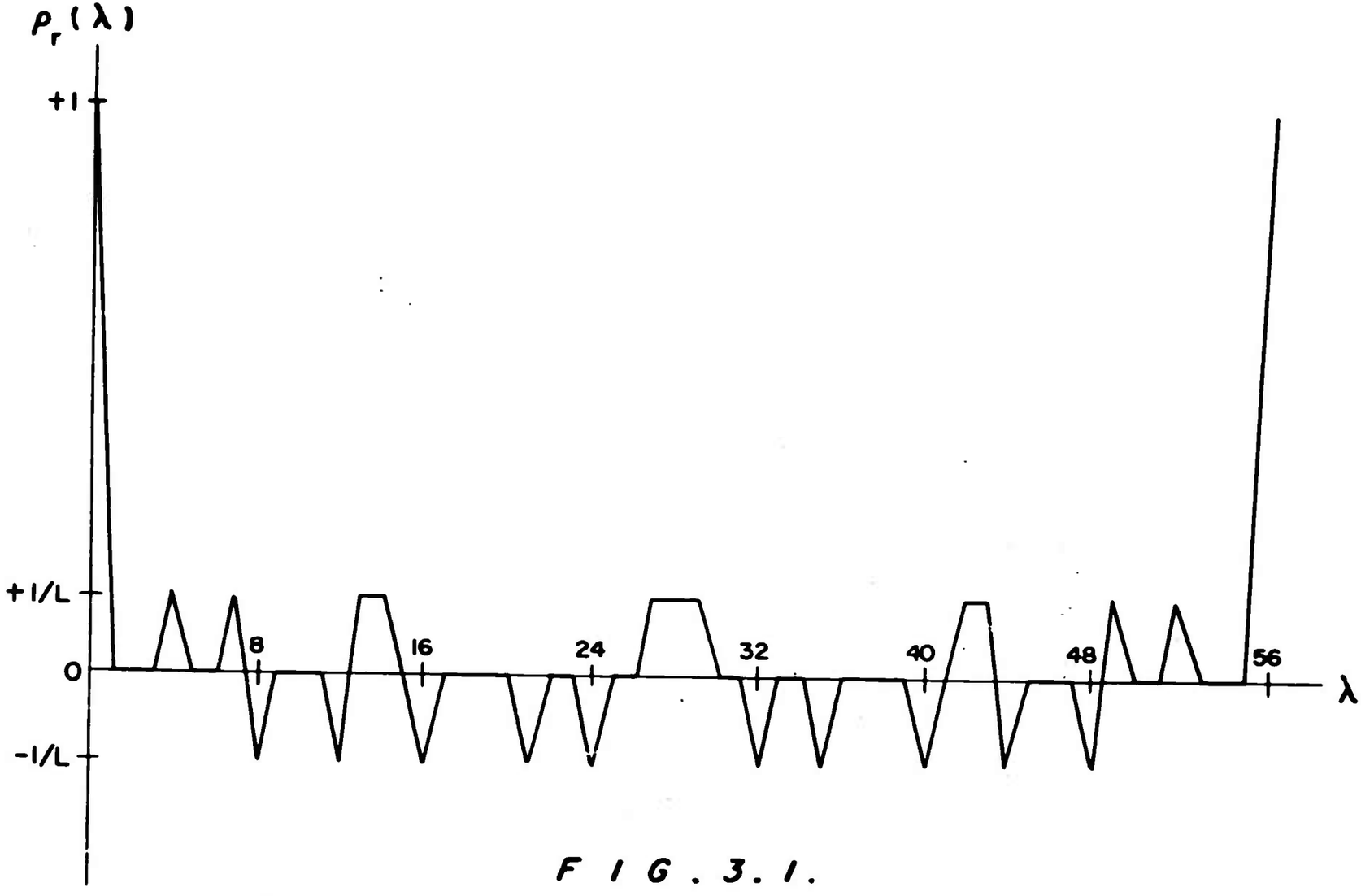


FIG. 3.1.

"ALMOST" TWO-LEVEL AUTOCORRELATION SYNTHESIZED BY 8 FOLD INTERLEAVING OF LENGTH 7 MAXIMAL LENGTH SEQUENCE WITH d = 1

$$\delta_{1,0}^{(1)} = \nu^{(1)},\ \delta_{1,1}^{(1)} = \nu^{(1)} + d^{(1)},\ \ldots,\ \delta_{1,n-1}^{(1)} = \nu^{(1)} + (n-1)d^{(1)} .$$

Similarly a different "almost" two-level sequence will have peak locations $\delta_{w,v}^{(2)}$ for w = 1 chosen as

$$\delta_{1,0}^{(2)} = \nu^{(2)},\ \delta_{1,1}^{(2)} = \nu^{(2)} + d^{(2)},\ \ldots,\ \delta_{1,n-1}^{(2)} = \nu^{(2)} + (n-1)d^{(2)} ,$$

where $d^{(1)}, d^{(2)} = 1,2, \ldots, L-1$ with $d^{(1)} \neq d^{(2)}$, mod L, $\nu^{(1)}$ and $\nu^{(2)}$ are determined from (3.7) setting w = 1.

The cross-correlation peak locations, $\delta'_{w,v}$, are given by (3.6)

$$\delta'_{w,v} \equiv \alpha_v^{(1)} - \alpha_{n-w+v}^{(2)} - \mu_{wv} , \quad \text{mod L}$$

where the $\alpha^{(1)}$'s and $\alpha^{(2)}$'s are the interleaving constants of the two sequences.

From (3.4) it is determined that

$$\alpha_v^{(1)} \equiv v\nu^{(1)} + \frac{v(v+1)d^{(1)}}{2} , \text{ mod L} ,$$

and

$$\alpha_{n-w+v}^{(2)} \equiv (n-w+v)\nu^{(2)} + \frac{(n-w+v)(n-w+v+1)d^{(2)}}{2} , \text{ mod L}$$

Define a variable $g'_{w,v}$ as $g'_{w,v} = \delta'_{w,v} + \mu_{wv}$. Thus $g'_{w,v}$ is the cross-correlation peak location for $v \geq w$, and the peak location increased by one for $w < v$. Thus $g'_{w,v}$ is

$$g'_{w,v} = v\nu^{(1)} + \frac{v(v+1)d^{(1)}}{2} - (n-w+v)\nu^{(2)} - \frac{(n-w+v)(n-w+v+1)d^{(2)}}{2} ,$$

mod L

In order to determine the maximum multiplicity of peaks, it is necessary to determine the values of $v' \neq v$ mod n for which $g'_{w,v} \equiv g_{w,v'}$,

mod L. The procedure is to set $g'_{w,v} \equiv g'_{w,v'}$, mod L and solve for the values of v' mod n which satisfy the congruence. It is apparent that a quadratic equation in v' results, and if r is prime then only two solutions exist, one of which is evidently $v' \equiv v \bmod n$. Thus any value of $\delta'_{w,v}$ can occur with maximum multiplicity of two for a given value of w. However, if the effect of μ_{wv} is considered, it is seen that the first w values of $g'_{w,v}$ are reduced by 1 to yield the cross-correlation peak locations $\delta'_{w,v}$. It is then possible that four values of $\delta'_{w,v}$ will be identical (for a given w), providing a cross-correlation function bounded by fourth order peaks.

The class of sequences just described has "good" autocorrelation and cross-correlation properties. Thus these sequences can be used as a set of code words for a communication system with the transmitter asynchronous with the receiver. The "almost" two-level autocorrelation property can provide a means for synchronization, and the "good" cross-correlation property for all cyclic shifts provides a low probability of deciding on the wrong code word.

As a final remark on these "almost" two-level interleaved sequence it should be noted that the class of sequences of length L^2 forms a set of good error-correcting codes, if the code consists of all cyclic shifts of all of the (L-1) interleaved sequences. A total of $L^2(L-1)$ code words are formed with minimum distance,* $d_{min} = \frac{1}{2}(L^2-3L+4)$. Thus for large L the code consists of (approximately) L^3 code words of length

*The minimum distance is easily evaluated by relating the maximum value of cyclic cross-correlation (equivalent to fourth order peak) to the Hamming distance.

L^2 with an error-correction capability of $L^2/4$. A Bose-Chaudhuri code,[28] (the best of the known linear codes) containing L^3 code words of length L^2 provides a guaranteed error-correction capability of only $L^2/2 \log_2 L$. Thus the code formed from the interleaved sequences provides protection greater than a Bose-Chaudhuri code of equal length with an equal number of words.

In the following section a class of sequences with autocorrelation functions containing intermediate peaks all of different amplitude will be synthesized.

3.5 Autocorrelation Function with All Peaks of Different Amplitude

The synthesis procedure is to choose the peak locations $\delta_{w,v}$ for $w = 1$. Choose $\delta_{1,0} = \delta_{1,1} = \ldots = \delta_{1,n-2} = \nu$, where ν can assume any value, mod L, except values for which the congruence $\nu n \equiv L-1$, mod L, is satisfied,* where n is any positive integer. The choice of allowable values of ν provides an "(n-1)" order peak in the autocorrelation function at $(n\nu+1)$. There is then a single order peak at $(n\delta_{1,n-1}+1)$ where $\delta_{1,n-1} \equiv (L-1) - (n-1)\nu$, mod L.

The remaining peak locations are calculated from (3.9). It is determined that $\delta_{w,w-1} = \delta_{w,w'} = \ldots = \delta_{w,n-2} \equiv w\nu$, mod L, and $\delta_{w,n-1} = \delta_{w,0} = \ldots = \delta_{w,w-2} \equiv (L-1) - (n-w)\nu$, mod L. Hence there is an "(n-w)" order peak of $(nw\nu+w)$ and a "w" order peak at $[n(L-1) - n(n-1)\nu + w]$, mod L. The autocorrelation function thus contains (n-1) peaks, (excluding the symmetric peaks), all of different order. If $n < L$ and $n\nu$ and L

*Interleaved sequences for which ν satisfies the congruence $\nu n \equiv L-1$, mod L, reduce to n repeated versions of a cyclic shift of the original two-level sequence.

are relatively prime, the different order peaks correspond to distinct values of δ. This condition ensures that the (n-1) peaks are not "bunched" together.

The autocorrelation function of the interleaved sequence derived from the length 15 maximal length sequence by choosing $n = 7$, $\nu = 1$ is shown in Figure 3.2.

It will now be shown that the cross-correlation function, at all cyclic shifts, between two "different" peak sequences, derived from different values of ν for L a prime and $n \leq L$, is bounded by double order peaks.

It can be seen that two different "different" peak autocorrelation functions result for interleaving constants $\alpha_v^{(1)}$, $\alpha_v^{(2)}$,

$$\alpha_0^{(1)} \equiv 0,\ \alpha_1^{(1)} \equiv \nu^{(1)},\ \alpha_2^{(1)} \equiv 2\nu^{(1)},\ \ldots,\ \alpha_{n-1}^{(1)} \equiv (n-1)\nu^{(1)} \ , \text{ mod L} \ ,$$

and

$$\alpha_0^{(2)} \equiv 0,\ \alpha_1^{(2)} \equiv \nu^{(2)},\ \ldots,\ \alpha_{n-1}^{(2)} \equiv (n-1)\nu^{(2)} \ , \text{ mod L} \ ,$$

where

$$n \leq L \ ,\ \nu^{(1)},\ \nu^{(2)} = 1,\ \ldots,\ L-1 \ ,\ \nu^{(1)} \neq \nu^{(2)} \text{ mod L} \ .$$

Cross-correlation peaks, $\delta'_{w,v}$, then occur for

$$\delta'_{w,v} \equiv \alpha_v^{(1)} - \alpha_{n-w+v}^{(2)} - \mu_{wv} \ \text{ mod L}$$

Defining again the variable $g'_{w,v} = \delta'_{w,v} + \mu_{wv}$, it is seen that

$$g'_{w,v} \equiv v\nu^{(1)} - (n-w+v)\nu^{(2)} \equiv (w-n)\nu^{(2)} + v(\nu^{(1)} - \nu^{(2)}) \text{ mod L}$$

Hence, for a given value of w, $g'_{w,v} \neq g'_{w,v'}$, mod L for $v \neq v'$ mod L.

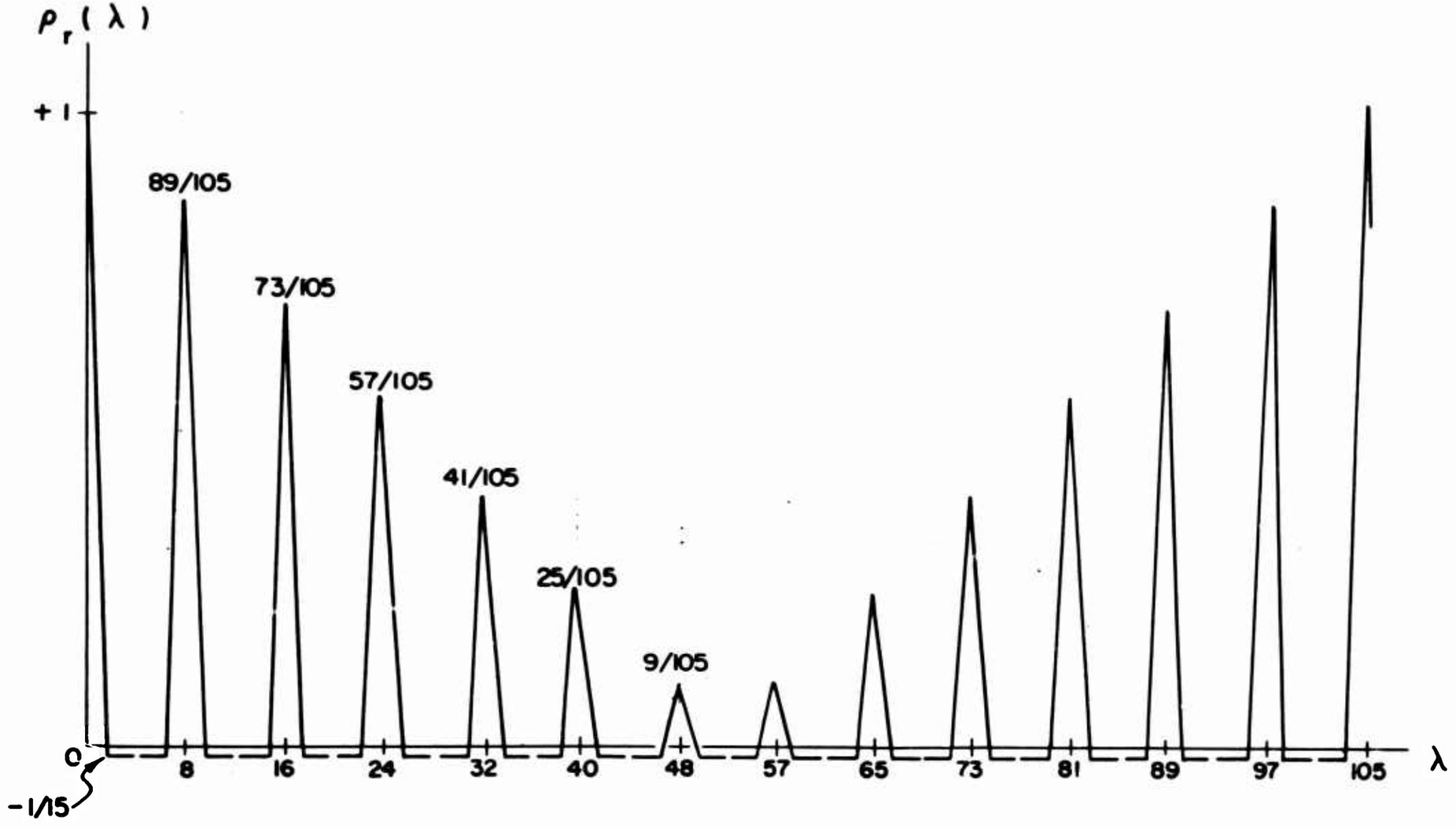


FIG. 3.2.

"DIFFERENT" PEAK AUTOCORRELATION FUNCTION SYNTHESIZED FROM 7 FOLD INTERLEAVING OF LENGTH 15 MAXIMAL LENGTH SEQUENCE WITH $\nu = 1$

Thus the values of $g'_{w,v}$ are all distinct for a given w, indicating, after considering the $\mu_{v'v}$ function, the maximum multiplicity of cross-correlation peaks is 2.

The application of a simple "different" peak sequence for synchronization is considered in Section 3.8.

3.6 Complement Sequence Interleaving

A method of synthesizing sequences with useful autocorrelation properties by the n-fold interleaving of the same two-level sequence was presented in the previous sections. Additional sequences can be synthesized by proper interleaving of a two-level sequence along with the complement of that sequence uch sequences will exhibit autocorrelation functions with positive and negative peaks.

It is recalled that the complement sequence, $h^{(q_1)}(x)$, of a two-level sequence, h(x) is, $h^{(q_1)}(x) = h(x) \oplus 1(x)$. The polynomial, h"(x), $h"(x) \equiv h(x) \oplus x^{\alpha} h^{(q_1)}(x) \equiv h^{(q_1)}(x) \oplus x^{\alpha} h(x)$, mod (x^L-1), has L ones if $\alpha = 0$, or $(L+1)/2$ zeros and $(L-1)/2$ ones if $\alpha \neq 0$. The polynomial h'"(x), $h'"(x) \equiv h^{(q_1)}(x) \oplus x^{\alpha} h^{(q_1)}(x)$, mod (x^L-1) is identical to the polynomial h'(x) defined previously.

The synthesis procedure used is the n-fold interleaving, with arbitrary shifts, of a two-level sequence of length L and its complement. The resultant sequence (in polynomial representation), denoted as $S_{r'}(x)$ is:

$$S_{r'}(x) \equiv \sum_{v=0}^{n-1} x^{n\alpha_v+v} h_v(x^n) \ , \text{ mod } (x^{nL}-1) \ , \qquad (3.11)$$

where $h_v(x)$ is either h(x) or $h^{(q_1)}(x)$.

In order to find the autocorrelation function, it is necessary to form the polynomial, $S_{p'}(x)$,

$$S_{p'}(x) \equiv S_{r'}(x) \oplus x^{n\delta+w} S_{r'}(x) \ , \ \mathrm{mod}\ (x^{nL}-1) \ .$$

Thus

$$S_{p'}(x) \equiv \sum_{v=0}^{n-1} x^{n\alpha_v+v} \left[h_v(x^n) \oplus x^{n(\delta+\alpha_{n-w+v}-\alpha_v+\mu_{wv})} h_{n-w+v}(x^n) \right] , \quad \mathrm{mod}\ (x^{nL}-1) \qquad (3.12)$$

Peaks will occur in the autocorrelation function for

$$\delta + \alpha_{n-w+v} - \alpha_v + \mu_{wv} \equiv 0 \ , \ \mathrm{mod}\ L \ .$$

However, the peak can be either positive or negative. A positive peak occurs if $h_v(x)$ and $h_{n-w+v}(x)$ are both uncomplemented or both complemented polynomials. A negative peak occurs if one of the polynomials is uncomplemented and the other complemented. The peak locations satisfy (3.7), (3.8) and (3.9). No peaks occur for w = 0, (excluding of course v = 0), and the autocorrelation function for these delays is -1/L.

It can be shown if a weight of +1 is assigned to a positive peak and a weight of -1 to a negative peak, then the total weight of the peaks of a sequence interleaved from n_1 two-level sequences and n_2 complement sequences ($n_1+n_2 = n$) is $(n_1-n_2)^2 - n$.

In Figure 3.2 an autocorrelation function with (n-1) peaks of different amplitude was presented. By interleaving complement sequences, autocorrelation functions with positive and negative peaks, all of different amplitude, can be synthesized. The procedure is to choose $h_v(x)$ = h(x) for v = 0,2,4, ..., and $h_v(x) = h^{(q_1)}(x)$ for v = 1,3, ... The

peak locations for $w = 1$ are again chosen as $\delta_{1,0} = \ldots = \delta_{1,n-2} = \nu$. Negative peaks occur for $w = 1,3, \ldots$, and positive peaks for $w = 2,4, \ldots$. A positive and negative "different" peak autocorrelation function for $n = 7$, $L = 15$, $\nu = 1$ is shown in Figure 3.3.

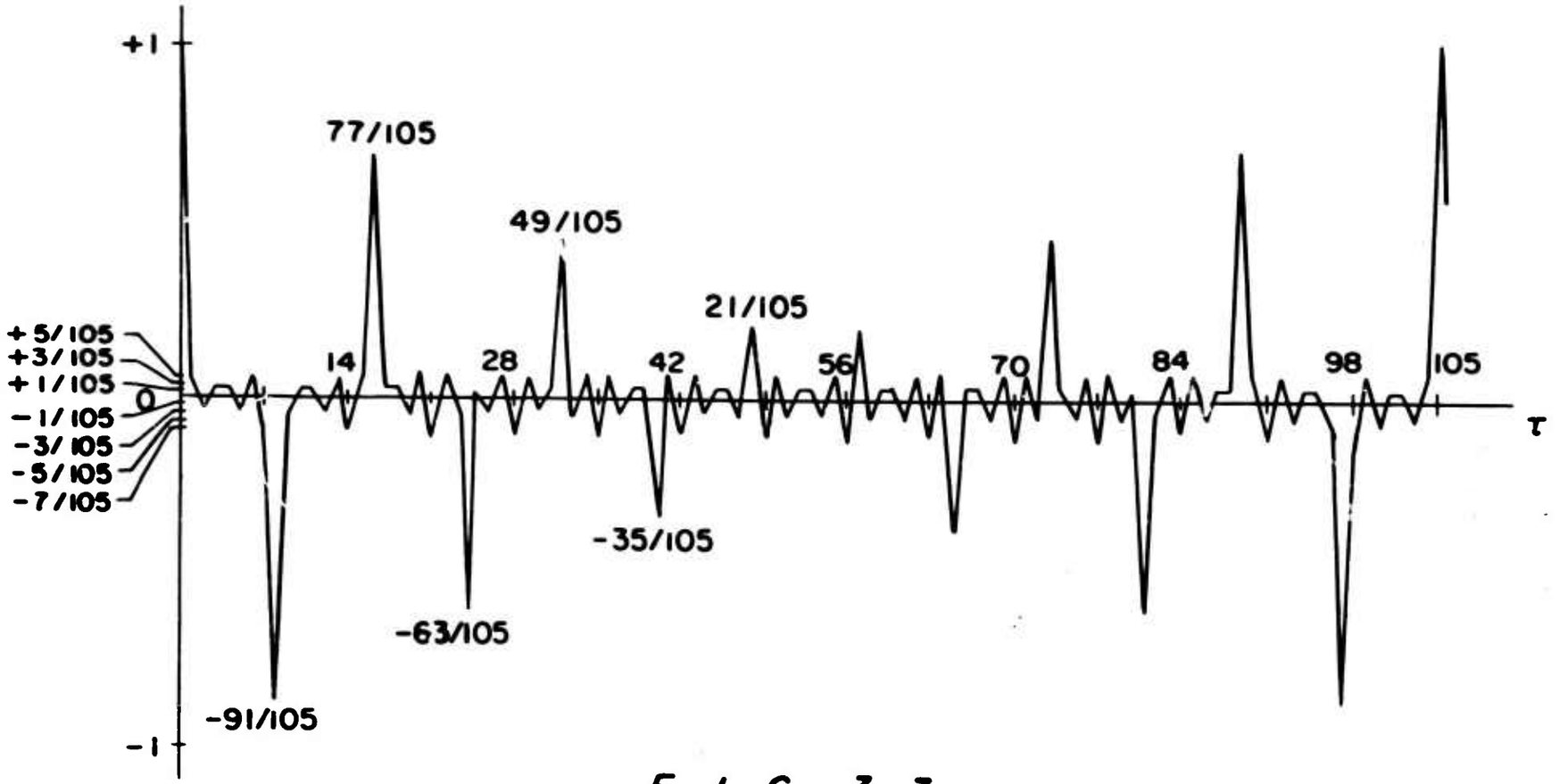
In the following section it is shown that sequences generated by the interleaving of maximal length sequences can be generated by the simple nonlinear filtering of a maximal length sequence.

3.7 Generation of Interleaved Sequences by Nonlinear Filtering

Raphael[19] has described a technique for synthesizing binary sequences (which are recognized as interleaved maximal length sequences), with autocorrelation functions containing minor peaks, by the nonlinear filtering of a maximal length sequence. The filter* (shown in Figure 3.4) forms the mod 2 sum of a maximal length sequence, of length L, (with each symbol repeated n times, $n = 2,3, \ldots$), and this sequence delayed by $n\gamma+y$ digits, $\gamma = 1,2, \ldots, L-1$, $y = 1,2, \ldots, n-1$. Raphael found the autocorrelation function of the output sequence for a few values of L, n, γ and y, by computer simulation. The generalization of these results are presented as an example at the end of this section.

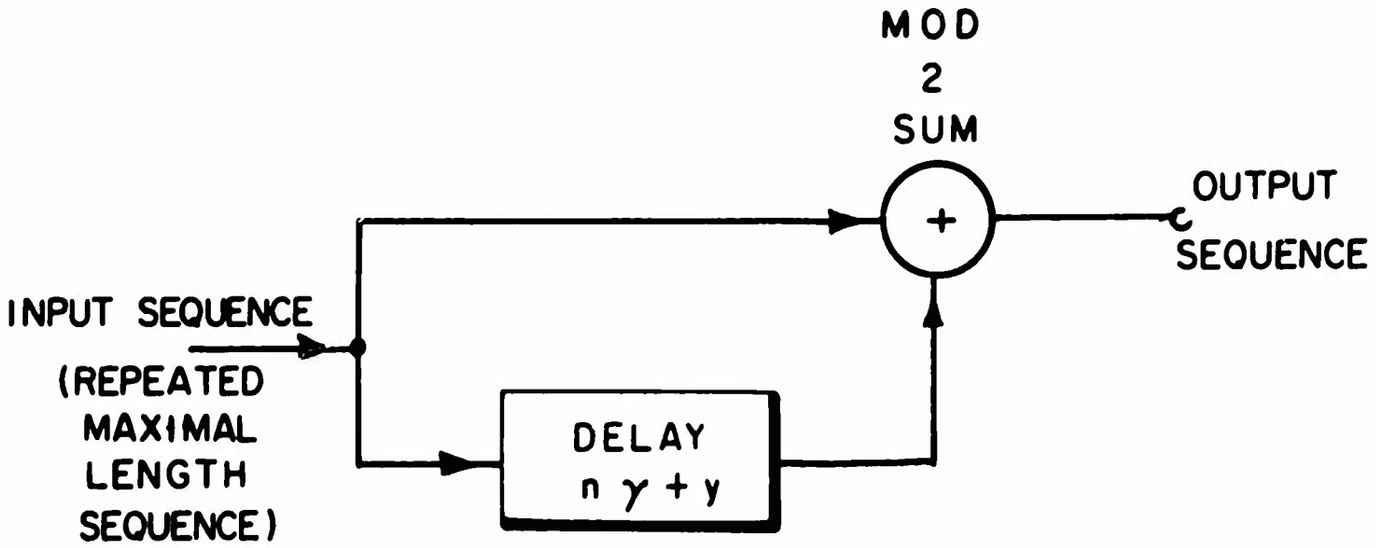
First a multiple nonlinear filter which can be used to generate a wider class of interleaved maximal length sequences is presented. The filter, as shown in Figure 3.5, consists of n delay elements, delaying the input repeated maximal length sequence $n\gamma_0$, $n\gamma_1+1$, ..., $n\gamma_{n-1}+n-1$

*The filter operation is nonlinear because the mod 2 sum of binary sequences is isomorphic to the product of mapped binary sequences.



F I G . 3.3.

POSITIVE AND NEGATIVE "DIFFERENT" PEAK AUTOCORRELATION FUNCTION OF 7-FOLD INTERLEAVING OF LENGTH 15 MAXIMAL LENGTH SEQUENCE AND COMPLEMENTS



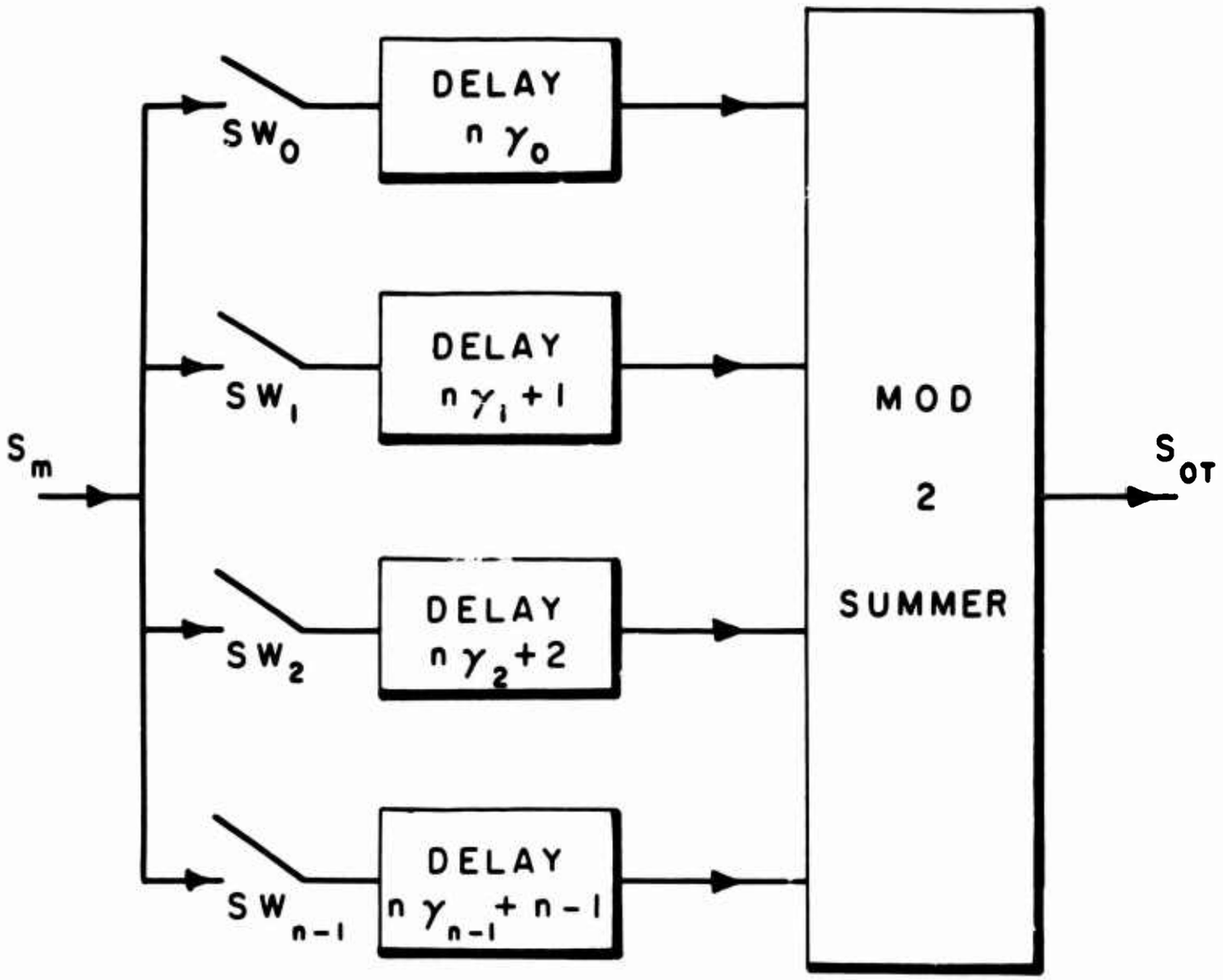
$n = 2, 3, \ldots$

$\gamma = 1, 2, \ldots, L-1$

$y = 1, 2, \ldots, n-1$

FIG. 3.4.

NONLINEAR FILTER



$\gamma_i = 0, 1, \ldots, L-1$

FIG. 3.5.

MULTIPLE NONLINEAR FILTER

digits respectively, (γ_y = 0,1, ..., L-1, y = 0,1, ..., n-1), and a mod 2 summer. There is also the provision that particular delay elements can be switched out of the circuit by the operation of switches $SW_0, SW_1, \ldots, SW_{n-1}$. The opening of switch SW_y is equivalent to adding, (mod 2), an all zero sequence in place of the input sequence delayed $n\gamma_y+y$ digits. The analysis of the multiple nonlinear filter is as follows.

The input maximal length sequence, with each symbol repeated n times, is represented as the polynomial $S_m(x)$,

$$S_m(x) = h_m(x^n) \sum_{\sigma=0}^{n-1} x^{\sigma} , \tag{3.13}$$

where $h_m(x)$ is the polynomial representation of a maximal length sequence of length L.

The output of the y^{th} delay element, $S_y(x)$, in polynomial representation, is

$$S_y(x) \equiv x^{n\gamma_y+y} a_y(x^n) \sum_{\sigma=0}^{n-1} x^{\sigma} , \text{ mod } (x^{nL}-1)$$

$$\equiv a_y(x^n) \sum_{\nu=0}^{n-1} x^{n(\gamma_y+\mu_{y\nu})+\nu} , \text{ mod } (x^{nL}-1) \tag{3.14}$$

where

$$\mu_{y\nu} = \begin{cases} 1 & \nu < y \\ 0 & \nu \geq y \end{cases}$$

and

$$a_y(x) = \begin{cases} h_m(x) & \text{if } SW_y \text{ is closed} \\ 0(x) & \text{if } SW_y \text{ is open} \end{cases}$$

Then the polynomial representation of the output of the mod 2 summer, $S_{oT}(x)$, is

$$S_{oT}(x) = S_0(x) \oplus S_1(x) \oplus \ldots \oplus S_{n-1}(x) ,$$

$$\equiv \sum_{\nu=0}^{n-1} x^{\nu} \sum_{y=0}^{n-1} \oplus x^{n(\gamma_y+\mu_{y\nu})} a_y(x^n) , \text{ mod } (x^{nL}-1) , \quad (3.15)$$

where $\Sigma_{\oplus}$ indicates mod 2 summation.

Since the mod 2 summation of n arbitrarily shifted maximal length sequences yields either a shifted maximal length sequence or an all zero sequence, $S_{oT}(x)$ can be represented as

$$S_{oT}(x) = \sum_{v=0}^{n-1} x^{n\alpha_v+v} a_v(x^n) , \text{ (mod } x^{nL}-1) , \quad (3.16)$$

where the α_v's and $a_v(x)$'s are functions* of γ_y and $a_y(x)$, y = 0, ..., n-1. Hence the output sequence is an interleaving of shifted maximal length sequences and all zero sequences.** There are L possible states of the delay element $(n\gamma_y+y)$, corresponding to the L values of γ_y with SW_y closed, and one extra state corresponding to SW_y open, providing a total of (L+1) states. Hence there are $(L+1)^n$ states of the nonlinear filter. However, there are also $(L+1)^n$ possible n-fold interleaved

*$a_v(x)$ is either $h_m(x)$ or $0(x)$

**The autocorrelation functions of sequences interleaved from binary two-level sequences and all zero sequences were not considered in the previous sections. However, it can be shown that these autocorrelation functions have similar minor peak structures as those sequences considered previously except for the occurrence of an "ℓ" order peak at delays of n,2n, ..., (L-1)n, where ℓ is the number of all zero sequences interleaved.

sequences, suggesting the possibility that every interleaved sequence can be generated by the multiple nonlinear filter. It is proved, in Appendix B, that this is indeed the case for n = 2, by demonstrating that each filter state yields a different interleaved sequence as an output. It is conjectured that the result is true for all n, although the method of proof appears involved for n > 2.

Two examples of sequences derived by nonlinear filtering are now given. In the first example the general solution to the filter (Figure 3.4), consisting of a single arbitrary delay, $n\gamma+y$, is given. In the second example the synthesis of a certain type of "different" peak sequence is presented.

Example 3.1 With a single delay element, $n\gamma+y$, the output sequence, $S_{oT}(x)$, in polynomial form is

$$S_{oT}(x) \equiv S_m(x) \oplus x^{n\gamma+y} S_m(x) \ , \ \mathrm{mod}\ (x^{nL}-1) \ , \tag{3.17}$$

or

$$S_{oT}(x) \equiv h(x^n) \left\{ x^{nI(\gamma+1)} \sum_{b=o}^{y-1} x^b + x^{nI(\gamma)} \sum_{c=y}^{n-1} x^y \right\} \quad \mathrm{mod}\ (x^{nL}-1) \ . \tag{3.18}$$

Thus the interleaving constants, α_v, are

$$\alpha_o = \alpha_1 = \ldots = \alpha_{y-1} = I(\gamma+1)$$
$$\alpha_y = \alpha_{y+1} = \ldots = \alpha_{n-1} = I(\gamma)$$

Applying the theory of Section 3.2, it is found that autocorrelation peaks occur at shifts of $n\delta+w$, with the following peak orders.

a. For $w \leq \min[y, n-y]$ the peak orders are:

"w" order peak at $\delta = I(\gamma+1) - 1 - I(\gamma)$
"w" order peak at $\delta = I(\gamma) - I(\gamma+1)$
"(n-2w)" order peak at $\delta = 0$

b. For $y \leq w \leq n-y$, with $y \leq n/2$,* the peak orders are:

"y" order peak at $\delta = I(\gamma+1) - 1 - I(\gamma)$
"y" order peak at $\delta = I(\gamma) - I(\gamma+1)$
"(n-y-w)" order peak at $\delta = 0$
"(y-w)" order peak at $\delta = L - 1$

c. For $w \geq \max[n-y, y]$ the peak orders are:

"(n-w)" order peak at $\delta = I(\gamma+1) - 1 - I(\gamma)$
"(n-w)" order peak at $\delta = I(\gamma) - I(\gamma+1)$
"(2w-n)" order peak at $\delta = L - 1$

It is noted that the peak locations $I(\gamma) - I(\gamma+1)$ and $I(\gamma+1) - 1 - I(\gamma)$ correspond to symmetrical peaks. A plot of the autocorrelation function of S_{oT} is shown in Figure 3.6 for arbitrary values of n, (n even), and L, and three values of y, $y_1 = 1 < y_2 < y_3 = n/2$. The case $y = 2n$ is the situation investigated by Raphael.[19]

Example 3.2 Consider the multiple nonlinear filtering network, Figure 3.5, with all switches closed and $\gamma_o = \gamma_1 = \ldots = \gamma_{n-1} = 0$. For n odd, S_{oT} becomes

$$S_{oT}(x) = h(x^n) \left\{ \sum_{\substack{b=0 \\ b \text{ even}}}^{n-1} x^b + x^n \sum_{\substack{b=1 \\ b \text{ odd}}}^{n-2} x^b \right\} \tag{3.19}$$

*For $y \geq n/2$, then y is replaced by n-y in all relationships in case (b).

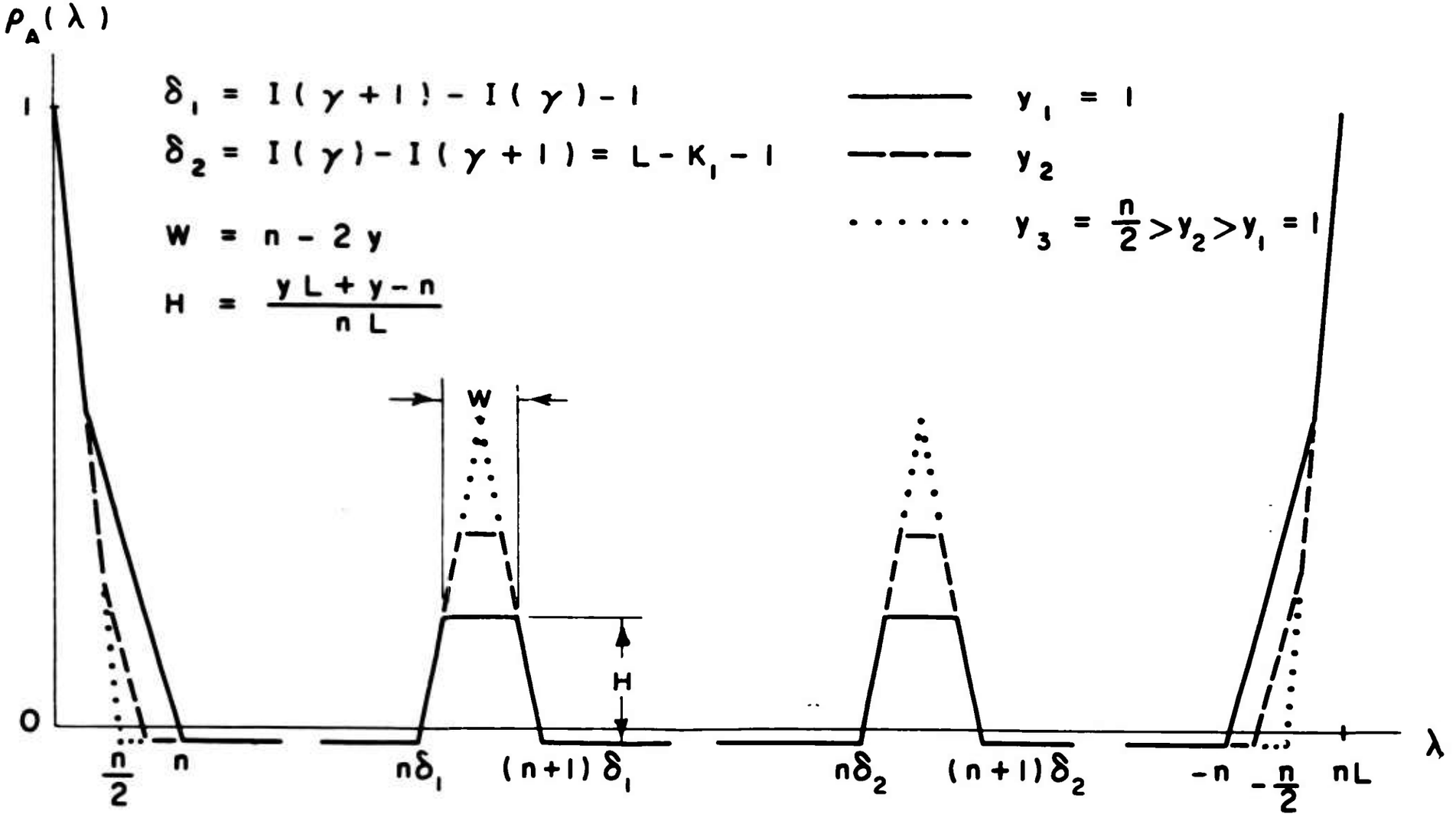


FIG. 3.6.

AUTOCORRELATION FUNCTION OF NONLINEAR FILTERED REPEATED MAXIMAL LENGTH SEQUENCE WITH SINGLE DELAY ELEMENT $n\gamma + y$

Thus the interleaving constants, α_v, are

$$\alpha_0 = \alpha_2 = \ldots = \alpha_{n-1} = 0$$
$$\alpha_1 = \alpha_3 = \ldots = \alpha_{n-2} = 1 \quad .$$

The peak locations, $\delta_{w,v}$, for w = 1 are then

$$\delta_{1,0} = \delta_{1,2} = \ldots = \delta_{1,n-1} = L-1$$
$$\delta_{1,1} = \delta_{1,3} = \ldots = \delta_{1,n-2} = 1 \quad .$$

There is a "[(n+1)/2]" order peak at a delay of n(L-1)+1 and a "[(n-1)/2]" order peak at (n+1). Then applying (3.9), the peak locations $\delta_{w,v}$ for arbitrary $w \leq n/2$ are:

w odd:
$$\delta_{w,0} = \delta_{w,1} = \delta_{w,2} = \ldots = \delta_{w,w-1} = L-1$$
$$\delta_{w,w} = \delta_{w,w+2} = \ldots = \delta_{w,n-2} = 1$$
$$\delta_{w,w+1} = \delta_{w,w+3} = \ldots = \delta_{w,n-1} = L-1$$

There is then a "[(n+w)/2]" order peak at n(L-1)+w and a "[(n-w)/2]" order peak at (n+w)

w even:
$$\delta_{w,0} = \delta_{w,2} = \ldots = \delta_{w,w-2} = L-2$$
$$\delta_{w,1} = \delta_{w,3} = \ldots = \delta_{w,w-3} = 0$$
$$\delta_{w,w-1} = \delta_{w,w} = \delta_{w,w+1} = \ldots = \delta_{w,n-1} = 0$$

There is then a "(w/2)" order peak at n(L-2)+w, and a "[n-w/2]" order peak at w. This is a "different" peak autocorrelation, although the peaks are "bunched" together. The plot, for n = 7, L = 7 is shown in Figure 3.7.

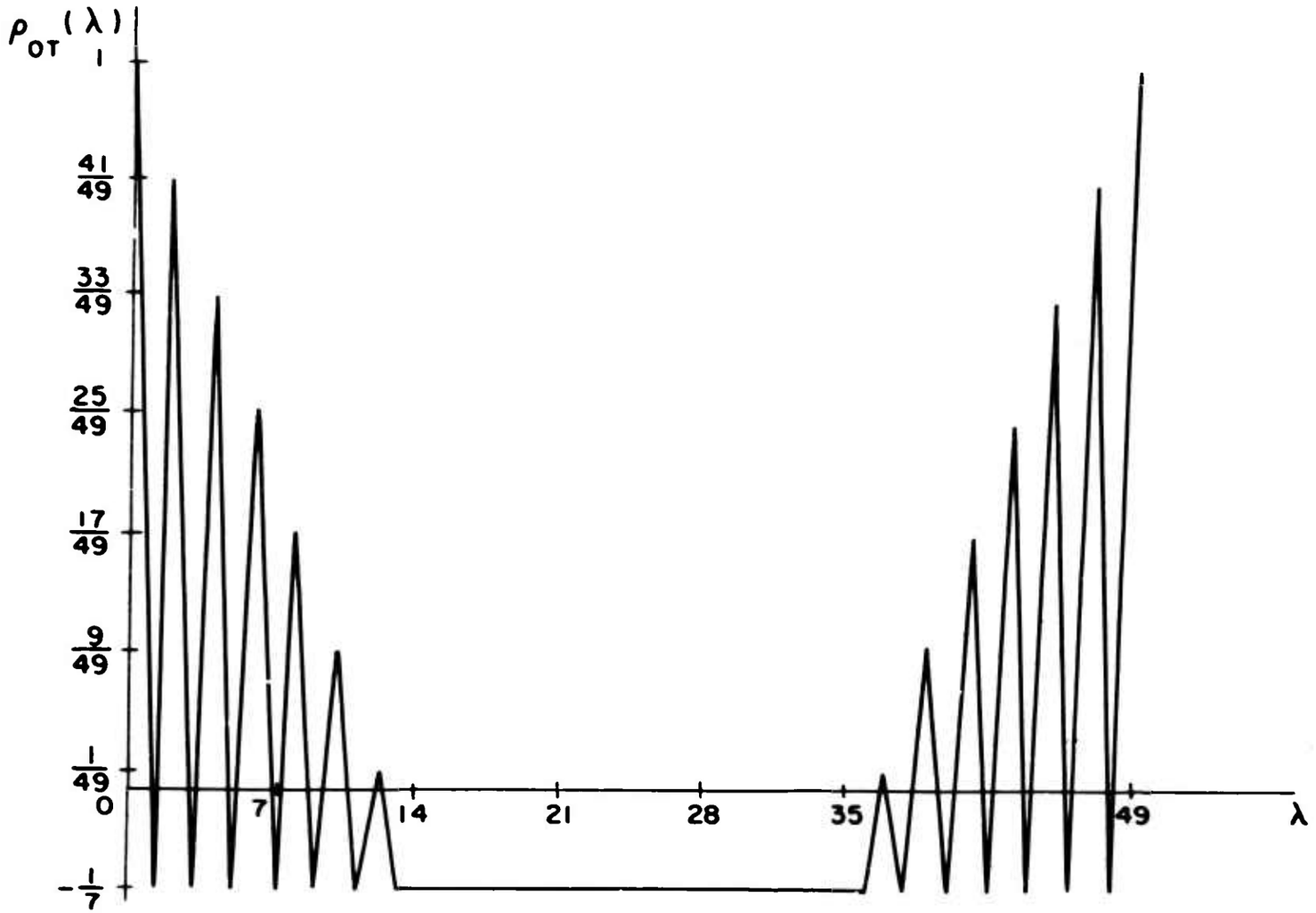


FIG. 3.7.

AUTOCORRELATION FUNCTION OF SEQUENCE SYNTHESIZED BY NONLINEAR FILTERING, $n = 7$, $L = 7$, $\gamma_0 = \gamma_1 = \cdots = \gamma_6 = 0$

3.8 Synchronization with Sequences

In order to detect, by correlation techniques, the information carried by most signals, the correlator receiver and transmitter must be synchronized. Synchronization information can be transmitted on the channel carrying the signal or on a separate channel.[22] For separate channel synchronization a two-level sequence (or "almost" two-level sequence), whose period is equal to the duration of the information signal, can be transmitted on the separate channel. The two-level property of the sequence provides unique synchronization with a low probability of error.

A two-level sequence can also be used for synchronization when the synchronization information is carried on the channel with the signal. In this case the two-level sequence, used as a subcarrier, is phase modulated by the signal.

Several techniques for utilizing the two-level sequence (for either the separate channel or same channel method) are possible, assuming that symbol synchronization is known for the sequence.

a. The transmitted sequence, with unknown delay, is cross-correlated with all cyclic shifts of itself, and all of the correlator outputs are stored. The shift which provides the largest output determines the synchronization decision. The probability of correct synchronization is determined by noting that the set of L sequences resulting from L cyclic shifts of two-level sequence, form a set of simplex codes. The error probability for these codes has been derived.[20]

b. The transmitted sequence is cross-correlated with successive cyclic shifts of itself. The shift which provides a correlator output exceeding a predetermined threshold specifies the synchronization decision.

Fewer correlation operations, on the average, are required for case (b). The number of operations can be reduced further by using interleaved sequences as synchronization carriers, and "locking-onto" a minor peak or the peak at zero delay. The average probability of correct synchronization is now derived, when a two-level sequence is used with the technique specified in (b), and when two classes of interleaved sequences are used.

Consider the application of the two-level sequence, of length L, with the autocorrelation function shown in Figure 3.8, for synchronization. Assume the transmitted sequence is initially delayed by b digits, b = 0,1, ..., L-1, with respect to a reference sequence. The first shift which yields a correlator output above the threshold M_1 determines the synchronization. If the average sequence power is S, the time duration of the sequence T, and additive white Gaussian noise with zero mean and two-sided power spectral density $N_o/2$ is assumed, then the average probability of correct decision, $\bar{P}_{c_1}$, is:

$$\bar{P}_{c_1} = \frac{1}{L} \sum_{b=0}^{L-1} \left(\frac{1}{2}\right)^{b+1} \left[1 + \operatorname{erf}\left(M_1 \sqrt{\frac{ST}{N_o}}\right)\right]^b \left[1 - \operatorname{erf}\left((M_1-1) \sqrt{\frac{ST}{N_o}}\right)\right] \tag{3.20}$$

where

$$\operatorname{erf}(y) = \frac{2}{\sqrt{\pi}} \int_0^y e^{-t^2}\, dt \quad . \tag{3.21}$$

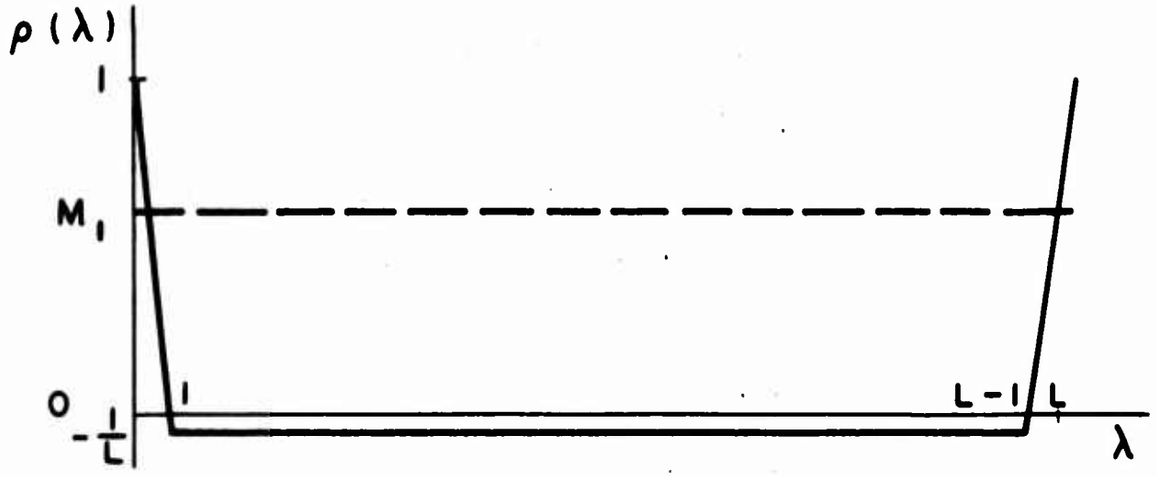


FIG. 3.8.

TWO-LEVEL AUTOCORRELATION FUNCTION

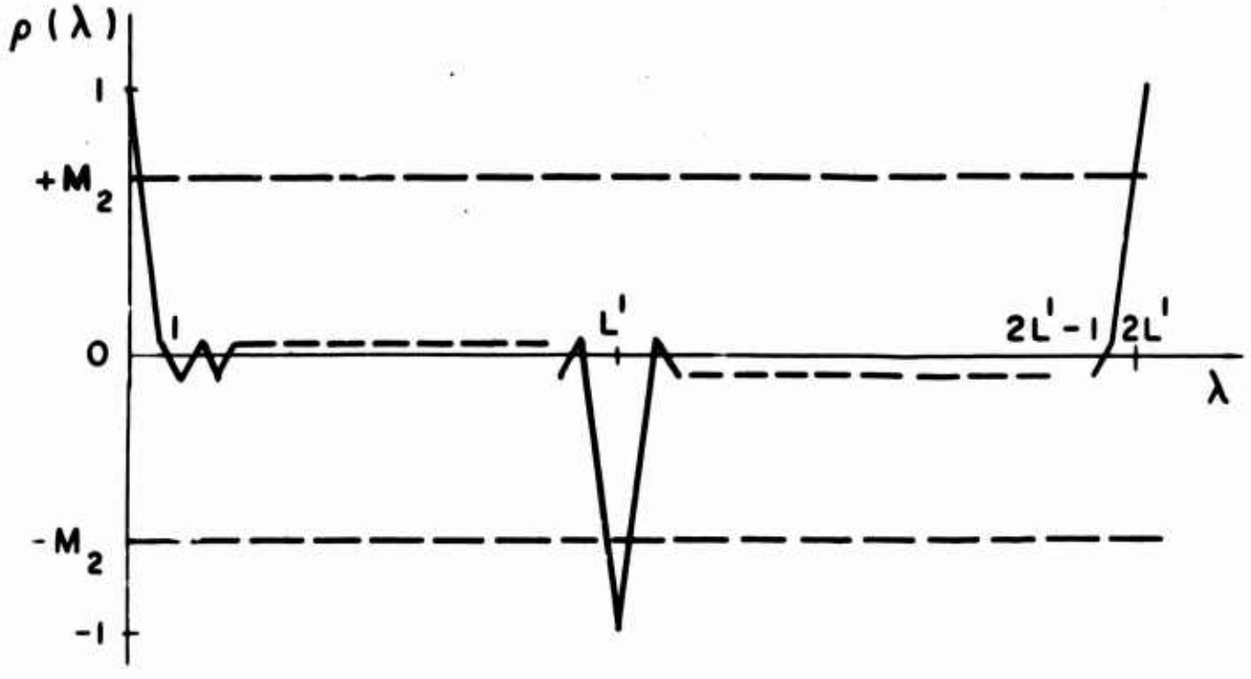


FIG. 3.9.

AUTOCORRELATION FUNCTION OF
$h(x^2) + x^{L'} h(x^2)$

It is necessary to find the threshold value, M_1, which maximizes $\bar{P}_{c_1}$. For high values of ST/N_o, the quantity $[1 + \text{erf}\,(M_1\sqrt{ST/N_o})]$, can be approximated by

$$1 + \text{erf}\left(M_1\sqrt{\frac{ST}{N_o}}\right) \approx 2 - \frac{1}{M_1\sqrt{\frac{\pi ST}{N_o}}} \exp\left[-M_1^2\,\frac{ST}{N_o}\right] \tag{3.22}$$

Then retaining only the first two terms in the expansion of

$$2 - \frac{1}{M_1\sqrt{\frac{\pi ST}{N_o}}} \exp\left(-M_1^2\,\frac{ST}{N_o}\right)^b$$

the expression for $\bar{P}_{c_1}$ becomes

$$\bar{P}_{c_1} \approx \frac{1}{2L}\left[1 - \text{erf}\left((M_1-1)\sqrt{\frac{ST}{N_o}}\right)\right]\left[L - \frac{L(L-1)}{4M_1\sqrt{\frac{ST}{N_o}}} \exp\left(-M_1^2\,\frac{ST}{N_o}\right)\right] \tag{3.23}$$

For given values of L and ST/N_o, (3.23) can be maximized by a trial and error procedure.

Now consider the application of two-fold interleaved sequences for synchronization. The sequence with polynomial representation, $R(x) \equiv h(x^2) + x^{L'}h^{(q_1)}(x^2)$ exhibits the autocorrelation function shown in Figure 3.9. If the delay of the transmitted sequence, b, is , $b \geq L'$, then synchronization can be achieved by "locking-onto" the negative peak at a delay of L'. If $b < L'$, then synchronization is achieved by "locking-onto" the positive peak at zero delay. For thresholds $\pm M_2$, the average probability of correct synchronization, $\bar{P}_{c_2}$ is derived

$$\bar{P}_{c_2} = \frac{1}{2L'}\sum_{b=0}^{L'-1}\left[\text{erf}\left(M_2\sqrt{\frac{ST}{N_o}}\right)\right]^b\left[1 - \text{erf}\left((M_2-1)\sqrt{\frac{ST}{N_o}}\right)\right] \tag{3.24}$$

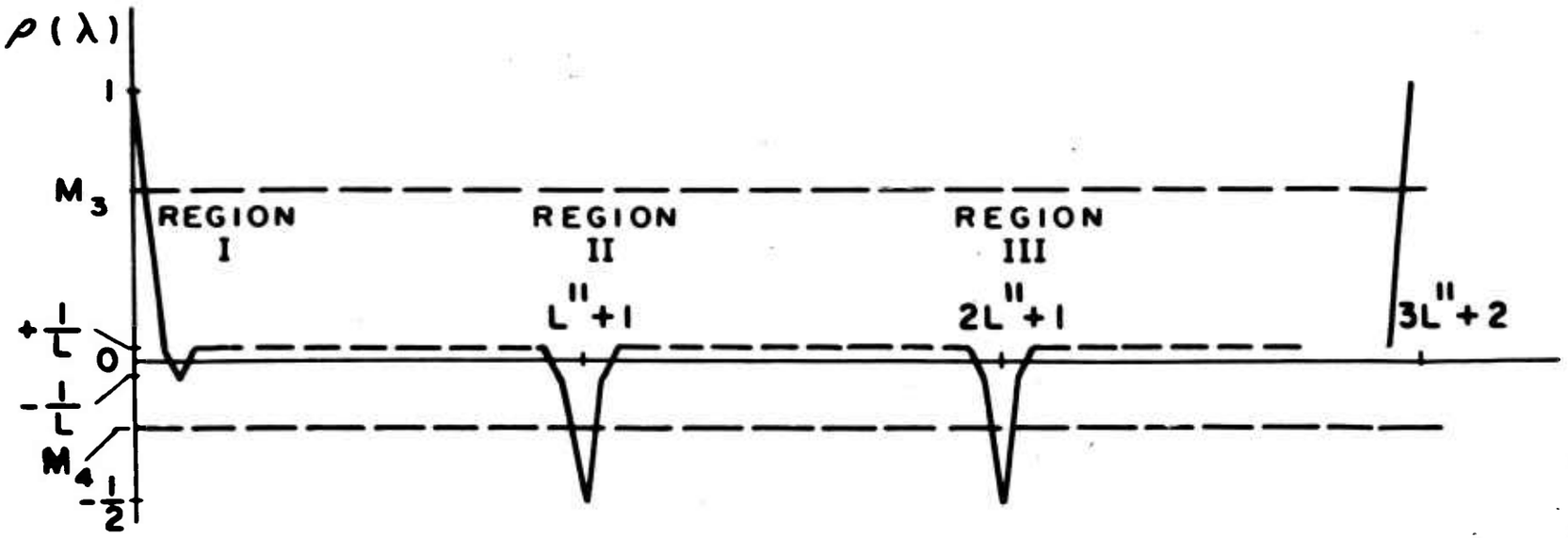
Then $\bar{P}_{c_2}$ can be approximated as, for large signal-to-noise ratios,

$$\bar{P}_{c_2} \approx \frac{1}{2L'}\left[1 - \operatorname{erf}\left((M_2-1)\sqrt{\frac{ST}{N_o}}\right)\right]\left[L' - \frac{L'(L'-1)}{2M_2\sqrt{\frac{\pi ST}{N_o}}}\exp\left(-M_2^2\frac{ST}{N_o}\right)\right] \tag{3.25}$$

If $L' \approx L/2$, then the expression for $\bar{P}_{c_1}$ and $\bar{P}_{c_2}$ are identical, although the use of the interleaved sequence requires only half the number of delays (on the average) for synchronization.

As a final example consider the interleaved sequence $R(x) = h(x^2) + x^{2a+1}h^{(q_1)}(x^2)$. If a is properly chosen, the autocorrelation function shown in Figure 3.10 can be realized. For this sequence synchronization can be achieved by "locking-onto" either of the negative minor peaks. However, when a particular minor peak is "locked-onto", it is necessary to perform one additional operation to achieve synchronization.

The synchronization procedure, referring to Figure 3.10, is as follows. If the initial delay corresponds to region III, the reference sequence is shifted until a minor negative peak is detected. Then the reference sequence is shifted L"+1 digits, and the correlator output should indicate no peak. If the initial delay corresponds to region II, the reference sequence is shifted until a minor peak is detected. Then the reference sequence is shifted L"+1 digits, and the correlator output should indicate a large positive peak. For region I the reference sequence is shifted until a large positive peak is detected. With thresholds M_3 and $-M_4$ the average probability of correct synchronization $\bar{P}_{c_3}$ for large signal-to-noise ratios is approximated by:



$$R(x) = h(x^2) + x^{2a+1} h(x^2)$$

$$a = -\frac{L''-2}{2}$$

FIG. 3.10.

AUTOCORRELATION FUNCTION WITH TWO NEGATIVE MINOR PEAKS

$$\bar{P}_{c3} \approx \frac{1}{3}\left\{ L'' - \frac{L''(L''-1)}{2\sqrt{\frac{\pi ST}{N_o}}}\left[\frac{e^{-M_3^2\, ST/N_o}}{M_3} + \frac{e^{-M_4^2\, ST/N_o}}{M_4}\right]\right\}$$

$$\cdot \left\{\frac{1}{2L''}\left[1 - \operatorname{erf}(M_3-1)\sqrt{\frac{ST}{N_o}}\right] + \frac{1}{4L''}\left[1 - \operatorname{erf}(M_4-\tfrac{1}{2})\sqrt{\frac{ST}{N_o}}\right]\right.$$

$$\left.\cdot \left[1 - \operatorname{erf}(M_3-1)\sqrt{\frac{ST}{N_o}}\right] + \frac{1}{2L''}\left[1 - \operatorname{erf}(M_4-\tfrac{1}{2})\sqrt{\frac{ST}{N_o}}\right]\right\} \qquad (3.26)$$

The number of operations required to synchronize with this sequence is approximately one-third the number required with a two-level sequence, or two-thirds the number required with the single negative peak sequence. However, a significant decrease in average probability of correct synchronization is observed with the reduction in synchronization time. For $ST/N_o = 100$, $L = 63$, $L' = 31$, $L'' = 20$, the values of $\bar{P}_{c1}$ and $\bar{P}_{c2}$, maximized over M_1 and M_2 are each $1 - 6 \cdot 10^{-11}$. The value of $\bar{P}_{c3}$, maximized over M_3 and M_4 is only 0.999.

The general "different" peak sequence, analyzed in Section 3.5 can be used to further reduce synchronization time by "locking-onto" a minor peak, although there will be a corresponding decrease in the probability of correct synchronization.

4. N-ORTHOGONAL AND CYCLICALLY N-ORTHOGONAL SEQUENCES

4.1 Introduction

In this chapter sequences with symbols mapped onto the N^{th} complex roots of unity, which are N-orthogonal and cyclically N-orthogonal will be derived.

Definition: A class of N-ary sequences is N-orthogonal if given any two sequences in the set, the cross-correlation function at zero delay, between the mappings of

a. the sequences

b. one of the sequences and any complement of another sequence

c. any complement of one sequence and any complement of another sequence

is zero.

For the roots of unity mapping sequences S_a and S_b,

$$S_a = (a_0, a_1, \ldots, a_{L-1}) \quad , \quad S_b = (b_0, b_1, \ldots, b_{L-1})$$

are N-orthogonal if

$$\rho_{ab}(0) = \frac{1}{L} \sum_{i=0}^{L-1} e^{j\frac{2\pi}{N}[(a_i - r) - (b_i - t)]} = 0 \quad , \qquad (4.1)$$

where r, t = 0, 1,..., N-1 to yield the r^{th} and t^{th} complements of S_a and S_b respectively.

Definition: A class of N-ary sequences is cyclically N-orthogonal if the class is N-orthogonal for all cyclic shifts of all sequences.

Then S_a and S_b are cyclically N-orthogonal, for the roots of unity mapping, if

$$\rho_{ab}(\lambda) = \frac{1}{L} \sum_{i=0}^{L-1} e^{j(2\pi/N)[(a_i - r) - (b_{i-\lambda} - t)]} = 0 \quad , \quad (4.2)$$

for all λ, r and t.

In this chapter techniques will be presented for the derivation of sets of cyclically N-orthogonal sequences. A subset of the set of cyclically N-orthogonal sequences form a basis for a set of N-orthogonal sequences. The relationship between N-orthogonal sequences and the generalization of Hadamard matrices is indicated.

All of the techniques for the synthesis of binary cyclically orthogonal sequences produced a class of sequences all of different least period. It is conjectured that cyclically orthogonal binary sequences of the same least period do not exist. This conjecture, along with the Fourier analysis of binary sequences, is discussed.

4.2 Derivation of Cyclically N-orthogonal Sequences

In this section some theorems will be derived on the construction of cyclically N-orthogonal sequences, with symbols mapped onto the roots of unity. Most of the proofs will be established by noting the symbol structures of a sequence which is the mod N difference between the two sequences which are to be shown cyclically orthogonal. Modulo N arithmetic is used for all arithmetic operations with the symbols of sequences.

A lemma is now presented on the symbol structure of N-ary sequences.

Lemma 4.1 Given any N-ary sequence, S_a of length L, then the sequence, S_a' of length NL which consists of a complement of S_a followed by all other distinct complements of S_a, and the sequence S_a itself (in any order) has each symbol appearing exactly L times.

Proof: The sequence S_a' can be denoted as

$$S_a' = \left[S_a^{(q_{i_0})}, S_a^{(q_{i_1})}, \ldots, S_a^{(q_{i_{N-1}})}\right],$$

where $S_a^{(q_{i_j})}$ is the i_j complement of S_a and $i_j \neq i_{j'}$ for $j \neq j'$. If the i^{th} symbol of S_a is a_i, then the i, L+i, 2L+i, ..., (N-1)L+i, symbols of S_a are $a_i - i_0$, $a_i - i_1$, ..., $a_i - i_{N-1}$, which are all distinct modulo N. Hence each symbol appears exactly L times in S_a' and the lemma is true.

A method of constructing two cyclically N-orthogonal sequences is given by the following theorem.

THEOREM 4.1 Given any two N-ary sequences S_a and S_b, of length L, then the sequences S_a' and S_b', of length NL,

$$S_a' = \left[S_a^{(q_{i_0})}, S_a^{(q_{i_1})}, \ldots, S_a^{(q_{i_{N-1}})}\right]$$

$$S_b' = \left[S_b, S_b, \ldots, S_b\right],$$

are cyclically N-orthogonal.

Proof: Form the sequence $S_c' = (S_a')^{(q_r)} \cdot x^{nL+\ell}(S_b')^{(q_t)}$, where $x^{nL+\ell}(S_b')^{(q_t)}$ represents the t^{th} complement of S_b' shifted by $nL+\ell$ digits. Noting that $x^{nL+\ell}(S_b')^{(q_t)}$ is just the sequence $x^{\ell}(S_b)^{(q_t)}$ repeated N times, S_c' reduces to

$$S_c' = \left[(S_a - x^{\ell} S_b)^{(q_{i_0}+r-t)}, (S_a - x^{\ell} S_b)^{(q_{i_1}+r-t)}, \ldots, (S_a - x^{\ell} S_b)^{(q_{i_{N-1}}+r-t)}\right]$$

Thus from Lemma 4.1 each symbol in S_c' appears exactly L times indicating that S_a' and S_b' are cyclically N-orthogonal.

It is noted that the sequences S_a' and S_b' defined in Theorem 4.1 are of different least period. Theorem 4.2 gives a procedure for constructing non-binary sequences of the same least period which are cyclically N-orthogonal.

THEOREM 4.2 Given the sequence S_a'',

$$S_a'' = \left[S_a, S_a^{(q_1)}, S_a^{(q_2)}, \ldots, S_a^{(q_{N-1})}\right],$$

noting that the complements of S_a are taken in a specific order - not the arbitrary order of S_a'. Then the sequences $\beta S_a''$ and $\beta' S_a''$, $\beta, \beta' = 0, 1, \ldots, N-1, \beta \neq \beta'$, are cyclically N-orthogonal.

Proof: Form the sequence S_c'',

$$S_c'' = \beta(S_a'')^{(q_r)} - x^{nL+\ell}\beta'(S_a'')^{(q_t)} .$$

Then the $i, L+i, \ldots, (N-1)L+i$, $(i < \ell)$ symbols of S_c'' are

$$\beta(a_i - r) - \beta'\left[a_{i-\ell-(N-n-1)-t}\right], \beta(a_i - r - 1) - \beta'\left[a_{i-L-(N-n-1)-t-1}\right],$$

$$\ldots, \beta(a_i - r + 1) - \beta'\left[a_{i-\ell-(N-n-1)-t+1}\right],$$

respectively. These terms, using ring of integer mod N operations, reduce

to $\lambda+0(\beta'-\beta)$, $\lambda+1(\beta'-\beta)$, ..., $\lambda+(N-1)(\beta'-\beta)$, where $\lambda=\beta(a_i-r) - \beta'[a_{i-\ell}-(N-n-1)-t]$. In order to complete the proof it is necessary to show that

$$e^{j\frac{2\pi\lambda}{N}}\sum_{\ell=0}^{N-1}\left[e^{j\frac{2\pi(\beta'-\beta)}{N}}\right]^{\ell} = 0 \quad .$$

However, Van der Waerdan[31] shows that the sum of all powers of any root of unity (except 1), is zero, thus establishing the theorem for $i < \ell$. The proof for $i \geq \ell$ is similar and hence is omitted.

It is of interest to note which of the sequences $\beta S_a"$, all β, are of the same least period. Two sequences $\beta S_a"$ and $\beta' S_a"$ are of the same least period if the roots of unity $e^{j\frac{2\pi\beta}{N}}$ and $e^{j\frac{2\pi\beta'}{N}}$ are of the same order. If $N=p$ is prime all of the non-real roots are of the same order and thus all of the sequences $\beta S_a"$, $\beta=1, \ldots, p-1$ are of the same least period, NL. If N≠ prime then only the values of β corresponding to primitive roots, yield sequences of least period NL.

From Theorems 4.1 and 4.2 a general class of $(N-1)k+1$ cyclically N-orthogonal sequences* of length N^kL can be derived from an arbitrary sequence S_a of length L. The set of sequences are: the all zero sequence plus $\beta_i S_{a_i}$, $\beta_i=1, \ldots, N-1$, $i=0, \ldots, k-1$ where S_{a_i} is

$$S_{a_i} = \Big[\underbrace{S_a, \ldots, S_a}_{N^i}, \underbrace{S_a(q_1), \ldots, S_a(q_1)}_{N^i}, \ldots, \underbrace{S_a(q_{N-1}), \ldots, S_a(q_{N-1})}_{N^i}\Big],$$

repeated N^{k-i-1} times.

*The least period of all of the sequences is not N^kL.

An important special set of (N-1)k+1 cyclically N-orthogonal sequences of length N^k is derived by letting $S_a=(0)$. Then the sequence S_{a_i} reduces to

$$S_{a_i} = \Big[\underbrace{0, \ldots, 0}_{N^i}, \underbrace{N-1, \ldots, N-1}_{N^i}, \ldots, \underbrace{1, \ldots, 1}_{N^i}\Big],$$

repeated N^{k-i-1} times.

It is easily shown that the set of reciprocal sequences, are also cyclically N-orthogonal. Examples of cyclically N-orthogonal sequences are presented below.

Example: N=3, k=2, $S_a=(0)$

$$\begin{aligned} S_{a_0} &= (021021021) \\ 2S_{a_0} &= (012012012) \\ S_{a_1} &= (000222111) \\ 2S_{a_1} &= (000111222) \end{aligned}$$

Example: N=4, k=1, $S_a=(0)$

$$\begin{aligned} S_{a_0} &= (0321) \\ 2S_{a_0} &= (0202) \\ 3S_{a_0} &= (0123) \end{aligned}$$

It can be proven that the set of sequences, S_{a_i}, i=0, 1, ..., k-1 are a basis for a set of N-orthogonal sequences. For the special case of $S_a=(0)$, the set of N^k N-orthogonal sequences of length N^k result.[21] For N=2 this set reduces to the set of 2^k bi-orthogonal sequences known as the Walsh functions.[41] The set of binary sequences S_{a_i} will hereafter

be denoted as the Basic Walsh functions.

The set of sequences S_{a_i}, [with $S_a=(0)$], are not the only set of cyclically N-orthogonal sequences in the set of N^k N-orthogonal sequences. The set of sequences $\beta_i' S_{a_i}'$, i=1, ..., k-1,

$$S_{a_i}' = \sum_{j=0}^{i} \beta_j'' S_{a_j} \quad , \quad \beta_{j\neq i}'' = 0, 1, \ldots, N-1,$$

$$\beta_{j=i}'' = 1, 2, \ldots, N-1 \qquad (4.3)$$

are also cyclically N-orthogonal.* It can be shown that the set of sequences S_{a_i}' form a basis for the set of N^k N-orthogonal sequences.

It is shown in the following theorem that there are no additional sequences in the set of N^k N-orthogonal sequences which are cyclically orthogonal with each of the sequences $\beta_i' S_{a_i}'$.

THEOREM 4.3 There is no set of cyclically N-orthogonal sequences in the set of N^k N-orthogonal sequences which contains more than (N-1)k+1 sequences.

Proof: The proof will demonstrate that there are no sequences, (except the all zero sequence), in the set of N^k N-orthogonal sequences, which are cyclically N-orthogonal to $\beta_i S_{a_i}$, [with $S_a=(0)$]. The more general proof which demonstrates that there are no sequences which are cyclically orthogonal to each of the sequences $\beta_i S_{a_i}'$ is similar to the proof which follows, except for a more complicated notation. Hence, this more general

*For $\beta_j''=0$, j=0, 1, ..., i-1 and $\beta_i''=1$, the set S_{a_i}' reduces to S_{a_i}.

proof is not given.

Consider the sequence S_d generated by linear combinations of the basis elements S_{a_i}. Then S_d is

$$S_d = \sum_{j=1}^{\ell} \beta_{i_j} S_{a_{i_j}} \quad , \quad i_j < i_{j+1} \quad , \quad i_\ell \leq k-1$$

The sequence S_d, which has the same least period as $\beta_{i_\ell} S_{a_{i_\ell}}$, is of the form

$$S_d = \left[\underbrace{S_\alpha}_{N^{i_\ell}}, (S_\alpha)^{(q\beta_{i_\ell})}, (S_\alpha)^{(q_2\beta_{i_\ell})}, \ldots, (S_\alpha)^{(q_{(N-1)}\beta_{i_\ell})} \right]$$

repeated $N^{k-i_{\ell-1}}$ times, where S_α is a sequence which has the property that the sum of the sequence symbols (mapped onto the N^{th} complex roots of unity) is zero, and the first symbol of S_α is zero also.

Consider the cross correlation function between S_d and $\beta_{i_\ell} S_{a_{i_\ell}}$ shifted by one place. This is done by considering the structure of the sequence $S_e = S_d - x^1\left[\beta_{i_\ell} S_{a_{i_\ell}}\right]$, which is found to be:

$$S_e = \left[\underbrace{S_\alpha}_{N^{i_\ell}}, S_\alpha, \ldots, S_\alpha \right] + \left[\beta_{i_\ell}(N-1), 0, \ldots, 0, \beta_{i_\ell}(N-1), 0, \ldots, \right.$$

$$\left. 0, \beta_{i_\ell}(N-1), 0, \ldots, 0 \right]$$

with the $\beta_{i_\ell}(N-1)$ term occurring in the 1, $N^{i_{\ell+1}}, \ldots, N^k - N^{i_{\ell+1}}$ places.

Thus the structure of S_e is identical to the structure of S_α repeated N^{k-i_ℓ} times except that the first term of S_α is changed from 0 to $\beta_{i_\ell}(N-1)\neq 0$. Thus the sum of the symbols of S_e mapped out the roots of unity, is not zero and S_d is not cyclically orthogonal to $B_i\ S_{a_{i_\ell}}$, indicating that there are no sequences cyclically orthogonal to every sequences in the set $\beta_i S_{a_i}$.

In Section 4.3 the relationship between N-orthogonal sequences and generalized Hadamard matrices is discussed.

4.3 N-orthogonal Sequences and Generalized Hadamard Matrices

It has been shown[1] that the theory of bi-orthogonal sequences (N=2) is closely related to the theory of Hadamard matrices. A Hadamard matrix is a square mxm matrix whose elements are ones and minus ones, and whose row vectors are mutually orthogonal and whose column vectors are also mutually orthogonal. The dimension of a Hadamard matrix must be* m=1, 2, 4r, r=1, 2, ... For every known Hadamard matrix of dimension m there is a set of m binary bi-orthogonal sequences of length m. Many techniques for the construction of Hadamard matrices exist.[32]

The concept of Hadamard matrices can be logically generalized to square matrices whose elements are the N^{th} roots of unity. The theory of these generalized Hadamard matrices is at this point practically nonexistent, although some theorems have been suggested by related work.[13] Throughout the remainder of this section the elements of the generalized Hadamard matrice will be indicated to be the ring of integers mod N,

*Although the dimension of a Hadamard matrix must be 1, 2, 4r, Hadamard matrices are not known for every value of r.

although it is understood that the elements should be the mapping of these integers onto the complex roots of unity.

Generalized Hadamard matrices of dimension N^k exist since it has been shown that a set of N^k N-orthogonal sequences of length N^k exist. As an example consider two possible matrices $[H_1]$, $[H_2]$, for N=p=3, k=1.

$$[H_1] = \begin{bmatrix} 000 \\ 012 \\ 021 \end{bmatrix} \qquad [H_2] = \begin{bmatrix} 000 \\ 021 \\ 012 \end{bmatrix}$$

If generalized Hadamard matrices $[H_1]$ of dimension m_1, and $[H_2]$ of dimension m_2, are known then a generalized Hadamard matrix $[H_3]$ of dimension $m_3=m_1 \cdot m_2$ is derived by forming the Kronecker product written $[H_3]=[H_1]x[H_2]$, of $[H_1]$ and $[H_2]$. The Kronecker product matrix is formed by substituting* $[H_2]$ for each zero in $[H_1]$, the first complement of $[H_2]$ for each one in $[H_1]$, ..., the (N-1) complement of $[H_2]$ for each N-1 in $[H_1]$. As an example consider the Kronecker product of the two three by three matrices indicated above. Then

$$[H_3] = \left[\begin{array}{c|c|c} 000 & 000 & 000 \\ 021 & 021 & 021 \\ 012 & 012 & 012 \\ \hline 000 & 222 & 111 \\ 021 & 210 & 102 \\ 012 & 201 & 120 \\ \hline 000 & 111 & 222 \\ 021 & 102 & 210 \\ 012 & 120 & 201 \end{array}\right] ,$$

*The proof of this result follows immediately from the proof for the ordinary Hadamard matrices[32] and hence is omitted.

where the Kronecker product formation is indicated by the dotted partition lines. It is noted that the Kronecker product of matrices of dimension N^{k_1} and N^{k_2} to yield a matrix of dimenstion $N^{k_1+k_2}$ does not yield a new class of N-orthogonal sequences since a class of N-orthogonal sequences is known for N^k, all k.

However, new classes of N-orthogonal sequences can be generated from generalized Hadamard matrices derived from certain two-level N-ary sequences. From a two-level N ry sequence of length L, (for the roots of unity mapping) with out of phase autocorrelation $-1/L$, a generalized Hadamard matrix of dimension L+1 is derived whose rows are the all zero row, plus all cyclic shift of the sequence with an extra zero at the beginning. For example consider the matrix $[H_4]$, derived from the two level sequence (01221),

$$[H_4] = \begin{bmatrix} 000000 \\ 001221 \\ 010122 \\ 021012 \\ 022101 \\ 012210 \end{bmatrix} .$$

The set of sequences derived by forming the Kronecker product of the above matrix with the matrices of dimension $N^{k'}$ will not be of length $N^{k'}$.

All of the Kronecker products considered previously were between two matrices each with elements in the same ring (same value of N). However, some additional classes of N-orthogonal sequences can be derived by forming the Kronecker product of generalized Hadamard matrices with elements contained in the ring of integers mod N_1, N_2 respectively. The resultant matrix will contain elements in the ring of integers mod

[L.C.M. (N_1,N_2)]. For example the generalized Hadamard matrix $[H_6]$, shown below, with elements in the ring of integers mod 6, is derived by forming the Kronecker product of $[H_4]$, (shown previously) and $[H_6]$ with elements in GF(2),

$$[H_6] = \begin{bmatrix} 00 \\ 01 \end{bmatrix}.$$

Thus $[H_6]$ is

$$[H_6] = \begin{bmatrix} 000000000000 \\ 030303030303 \\ 000442222244 \\ 030341252541 \\ 004400442222 \\ 034103412525 \\ 002244004422 \\ 032541034125 \\ 002222440044 \\ 032525410341 \\ 004422224400 \\ 034125254103 \end{bmatrix}$$

4.4 Cyclically Orthogonal Binary Sequences of the Same Least Period

In Section 2 of this chapter some techniques were presented for the synthesis of sets of cyclically orthogonal sequences. The sets of binary cyclically orthogonal sequences, synthesized by these techniques, contained sequences all of different least period. For example the periods of the three Basic Walsh functions of length 8,

$$\begin{aligned} S_{a_0} &= 01010101 \\ S_{a_1} &= 00110011 \\ S_{a_2} &= 00001111 \quad , \end{aligned}$$

are 2, 4, and 8 respectively. The all zero sequence, which is cyclically

orthogonal to each of the Basic Walsh functions, is of period 1.

It is conjectured that cyclically orthogonal binary sequences of the same period do not exist. This conjecture is discussed by noting the Fourier series of mapped binary sequences. The following theorem gives necessary and sufficient conditions that two periodic functions must satisfy if they are to be cyclically orthogonal.

THEOREM 4.4 Two periodic functions are cyclically orthogonal if and only if th respective Fourier series of the two functions have no terms in common.

Proof: Let $f^{(1)}(t)$, of period (not necessarily least period) T, be represented in the complex Fourier series

$$f^{(1)}(t) = \sum_{v=-\infty}^{v=+\infty} C_v^{(1)} e^{j\frac{v2\pi t}{T}}, \qquad (4.4)$$

with Fourier coefficients C_v. Similarly $f^{(2)}(t)$ is represented in the series

$$f^{(2)}(t) = \sum_{v=-\infty}^{\infty} C_v^{(2)} e^{j\frac{v2\pi t}{T}} \qquad (4.5)$$

The cross-correlation function, $\rho_{12}(\tau_2)$ between these two periodic functions, at a delay of τ_2 is then

$$\rho_{12}(\tau_2) = \frac{1}{T}\int_0^T f^{(1)}(t)\left[f^{(2)}(t-\tau_2)\right]^* dt$$

$$= \frac{1}{T}\sum_{v=-\infty}^{\infty}\sum_{w=-\infty}^{\infty} C_v^{(1)}\left[C_w^{(2)}\right]^* e^{j\frac{w2\pi\tau_2}{T}}\int_0^T \exp\left[j\frac{2\pi t}{T}(v-w)\right]dt$$

$$= \sum_{w=-\infty}^{w=\infty} C_w^{(1)}\left[C_w^{(2)}\right]^* e^{j\frac{w2\pi\tau_2}{T}} \qquad (4.6)$$

However, Equation (4.6) is equal to zero for all τ_2 if and only if either $C_w^{(1)}$ or $\left[C_w^{(2)}\right]^*$ is zero for every w. Since $\left[C_w^{(2)}\right]^* = 0$ if and only if $C_w^{(2)} = 0$, the theorem is established.

From Theorem 4.4 it is immediately established that if two binary sequences are cyclically orthogonal then at least one of the sequences must have an equal number of 1's and 0's since otherwise both sequences would possess D.C. (w=0) components.

It is clear that the theorem, as presented, does <u>not</u> prove that cyclically orthogonal functions of the same least period do not exist. The least period T_L of a function with a Fourier series gives by 4.4, with non-zero Fourier coefficients $C_{v_1}, C_{v_2}, \ldots, C_{v_K}$, is

$$T_L = T/[G.C.D\ (v_1, v_2, \ldots, v_K)] \qquad (4.7)$$

Thus for example the functions $f^{(1)}(t) = \sin t$, $f^{(2)}(t) = \sin 2t + \sin 3t$ of the same least period are cyclically orthogonal.

Consider the binary sequence S_σ of length $L=2\sigma$ which is σ ones followed by σ zeros. If we set $T=2\sigma t_1$ (where t_1 is the duration of one time slot), then it is easily verified that the non-zero Fourier coefficients of the mapping of S_σ are $C_{\pm 1}$, $C_{\pm 3}$, ... Then any sequence cyclically orthogonal to S_σ can only have even Fourier coefficients indicating that its period is an even fraction ($\frac{1}{2}$, $\frac{1}{4}$, $\frac{1}{6}$, ...) of the period of S_σ. Thus there is no sequence cyclically orthogonal to S_σ with least period $2\sigma t_1$

In order to consider more general sequences it is necessary to derive the Fourier coefficient of an arbitrary mapped binary sequence. Consider the mapped binary sequence S,

$$S = [a_0, a_1, \ldots, a_{L-1}] \quad , \quad a_i = \pm 1 \quad .$$

Then the Fourier coefficient C_v is

$$C_v = \frac{1}{Lt_1} \int_0^{Lt_1} f^{(1)}(t) e^{-j\frac{v2\pi t}{Lt_1}} dt$$

$$= \frac{1}{Lt_1} \left[\sum_{b=0}^{L-1} a_b \int_{bt_1}^{(b+1)t_1} \exp\left[-j\frac{v2\pi t}{Lt_1}\right] dt \right]$$

$$= \frac{1}{2\pi jv} \left[\sum_{b=0}^{L-1} a_b e^{-j\frac{bv2\pi}{L}} - \sum_{b=1}^{L} a_{b-1} e^{-j\frac{bv2\pi}{L}} \right] \qquad (4.8)$$

Equation (4.8) can be simplified to

$$C_v = \frac{1}{2\pi jv}\left[1-e^{-jv\frac{2\pi}{L}}\right]\sum_{b=0}^{L-1} a_b e^{-jbv\frac{2\pi}{L}} \qquad (4.9)$$

In attempting to prove the existence or non-existence of cyclically orthogonal sequences it is necessary to establish only whether a particular Fourier coefficient exists. The following remarks on the existence of Fourier coefficients are noted.

a. A particular coefficient, C_v is zero if and only if

$$\sum_{b=0}^{L-1} a_b e^{-j\frac{bv2\pi}{L}} = 0$$

b. If $C_v=0$, then $C_{v+mL}=0$, m=0, 1, ...
Thus it is only necessary to consider the values of V, mod L.

c. Assume $C_v=0$. Then from (4.9) it is noted that

$$\sum_{\substack{\text{all b mod L}\\ \text{such that}\\ a_b=+1}} a_b e^{-jbv\frac{2\pi}{L}} + \sum_{\substack{\text{all b mod L}\\ \text{such that}\\ a_b=-1}} a_b e^{-jbv\frac{2\pi}{L}} = 0 \qquad (4.10)$$

Substituting the indicated values of a_b in (4.10),

$$\sum_{\substack{\text{a particular}\\ \text{subset Q of}\\ \text{the integers}\\ \text{mod L}}} e^{-jbv\frac{2\pi}{L}} = \sum_{\substack{\text{the subset, R,}\\ \text{of integers}\\ \text{mod L disjoint}\\ \text{with Q}}} e^{-jbv\frac{2\pi}{L}} \qquad (4.11)$$

However, from the property of the sum of all powers of any root of unity (see proof of Theorem 4.2) it is noted that

$$\sum_{\text{all } b\epsilon Q} e^{-jbv\frac{2\pi}{L}} + \sum_{\text{all } b\epsilon R} e^{-jbv\frac{2\pi}{L}} = 0 \qquad (4.12)$$

But (4.11) and (4.12) contradict each other unless <u>each</u> of the summations of (4.10) are zero. Thus C_v is zero if and only if

$$\sum_{\substack{\text{all } b \\ \text{such that} \\ a_b=+1}} a_b e^{-jbv\frac{2\pi}{L}} ,$$

indicating that only the components of a mapped sequence which are +1 need be considered in determining the existence of a particular Fourier coefficient.

Clearly if two sequences, S_1 and S_2 of length L are to be cyclically orthogonal, then for at least one of the sequences the fundamental, C_1 (or C_{-1}), must be zero. However, if C_{-1} is zero then

$$\sum_{\text{all } b\epsilon Q} e^{jb\frac{2\pi}{L}} = 0 \qquad (4.13)$$

If Equation (4.13) is to be satisfied a sum of a subset, Q, of the L complex roots of unity must be zero. For the following situations Equation (4.13) is satisfied.

a. Q contains all of the integers mod L. Then the components of mapped sequence associated with the subset Q are all +1.

b. Let $L=p_1 \cdot p_2$ where p_1 and p_2 are different prime numbers. Then (4.13) is satisfied if Q contains b, $b+p_1$, $b+2p_1$, ..., $b+(p_2-1)p_1$.

The least period of the sequence derived from (a) is 1. The least period of the sequence derived from (b) is p_1. In case (c), below, a technique for synthesizing sequences with least period L for which $C_{-1}=C_1=0$ is presented

c. Let $L=\prod_{i=1}^{M} p_i$, where the p_i's i=1, ..., M, are primes not all the same. Then if p_ℓ and p_m are different prime factors of L, let Q contain the integers of the following 2 subsets $(b, b+L/p_\ell, b+2L/p_\ell, \ldots, b-L/p_\ell)$; $(b', b'+L/p_m, b'+2L/p_m, \ldots, b'-L/p_m)$; with $b \neq b'$, and $b+\ell p_\ell \neq b'+mp_m$, mod L for all integers ℓ and m.

As an example of the procedure outlined in (c), let $L=2 \cdot 2 \cdot 3=12$, indicating $p_\ell=3$, $p_m=2$. Then let b=0 and b'=1; the integers contained in Q are 0, 4, 8; 1, 7. The corresponding sequence (unmapped) is 001101100111. It is easily shown that the above sequence is of least period L, and $C_{-1}=C_1=0$.

It appears that the synthesis techniques outlined in (a), (b) and (c) are the only techniques* which will yield (mapped) binary sequences which do not possess fundamentals. The technique outlined in (c) cannot be used if $L=2p_1$ since the two subsets are not disjoint. The subset $(b, b+\frac{L}{2})$ and $(b', b'+\frac{L}{p_1}, b'+\frac{L}{2p_1}, \ldots, b'-\frac{L}{p_1})$ respectively contain one even integer and one odd integer, and all of the even integers or all of the odd integers mod L. Hence, it appears that cyclically orthogonal binary sequences of the same least period of length $L=2p_1$ do not exist.

If $L=2\prod_{i=1}^{M} p_i$, where M > 1 (eg. L=12) then the synthesis tech-

*Additional subsets of integers, $b^{(r)}$, $b^{(r)}+L/p_r$, ..., $b^{(r)}-L/p_r$, can be added to the two subsets already in Q (case c) provided all of the subsets remain disjoint.

nique outlined in (c) will yield a sequence, S_1, of least period L, for which $C_1=0$. However, for S_1 it can be shown that the Fourier coefficients $C_v^{(1)}$ ($v=mp_m$ $m=1, 2, \ldots,$ and $v=\ell p_\ell$, $\ell=1, 2, \ldots$) will not be zero. Hence if a sequence S_2 is to be cyclically orthogonal to S_1 then $C_{p_\ell}^{(2)}$ must be zero. It was found that if the components of S_2 were chosen such that $C_{p_\ell}^{(2)}=0$ and the sequence was of least period L, then the Fourier coefficients of S_2, $C_v^{(2)}$, $v=rp_r$ (where p_r is a prime which could be equal to p_m) were not zero. Thus the Fourier coefficients $C_{p_\ell p_r}^{(1)}$, $C_{p_\ell p_r}^{(2)}$ are not zero indicating that S_1 and S_2 are not cyclically orthogonal.

As a final remark it should be noted that classes of sequences, all of the same least period, with "good" cyclic cross-correlation properties can be derived by choosing the sequence components such that the mapped sequences have few Fourier coefficients in common. Utilizing this technique a set of 3 sequences of length 24 were derived which exhibited a cyclic cross-correlation, (between any pair of sequences) bounded by $\pm 1/4$.

These sequences are

(111111111111000000000000)
(111101001010011111000000)
(101100101101001010101100) .

5 BINARY ASYNCHRONOUS SIGNALLING

5.1 Introduction

Significant attention is presently being directed towards the derivation of techniques for the simultaneous transmission of many binary messages on the same channel Most of these multiple-access systems under consideration operate as follows There are k users on the channel with each transmitter-receiver pair assigned a different carrier * Information is transmitted by sending the carrier or its negative. Correlation detection is usually specified, with the polarity of the correlator output determining the decision on whether the carrier or its negative was transmitted The only external noise is assumed to be additive white Gaussian noise with mean zero and two-sided power spectral density $N_o/2$. Several types of systems with different constraints can be specified.

a. Linear Summation of Carriers, All Carriers Synchronous

The carriers from the different transmitters are summed on the channel, and the transmitters are all synchronized with each other, and with the corresponding receivers. The optimum set of binary carriers for this system are the bi-orthogonal carriers specified by rows of Hadamard matrices The performance is specified by the usual binary PSK probability of error relationship since there is no interference between carriers.

---

*In this chapter a carrier will be the unmodulated signal emanating from the transmitter. The carrier can be the mapping of a binary sequence.

b. Hard Limiting of Carriers, All Carriers Synchronous

For satellite repeater applications the linear summation of carriers is inefficient because of the nonlinear characteristic of travelling wave tubes - the usual satellite transmitter. The linear sum of the carriers, for this application, is usually hard limited prior to transmission over the channel. This problem with the carriers synchronized has been studied[33] in great detail.*

c. Linear Summation of Carriers, All Carriers Asynchronous

Each transmitter is synchronized with the corresponding receiver but the set of k transmitter-receiver pairs are asynchronous with each other. The carriers are summed linearly on the channels. Interference among carriers then arise from two sources:

1. if the carriers are not mutually bi-orthogonal for all cyclic shifts,
2. the complementing or "flipping" of an asynchronous carrier.

d. Hard Limiting of Carriers, All Carriers Asynchronous

This is a combination of cases (b) and (c).

In this chapter the communications system described under case (c) will be analyzed. First, some preliminary derivations are presented and then the system performance is analyzed for four different choices of carriers - mapped cyclically bi-orthogonal Basic Walsh functions, sinusoids of different periods, mapped randomly

---

* In Chapter 6 some aspects of the problem of the hard limiting of mapped N-ary sequences are considered.

chosen binary sequence and mapped cyclic error-correcting codes.

Consider the asynchronous linear multiplexing of k carriers, $S_o(t)$, $S_1(t)$, ..., $S_{k-1}(t)$, of period T. The receiver synchronously correlates with $S_i(t)$ and the phase of the other carriers with respect to $S_i(t)$ is random. (As previously stated a carrier or its negative is sent by each transmitter.) A block diagram of the system is shown in Figure 5.1. Then the received signal, $r_i(t)$ at the input to the i^{th} receiver is

$$r_i(t) = d_i\, S_i(t) + \sum_{\substack{\ell=0 \\ \ell \neq i}}^{k-1} [d_\ell^{(1)} S_\ell(t-\tau_\ell) + d_\ell^{(2)} S_\ell(t-\tau_\ell)] + n(t) \qquad (5.1)$$

where: n(t) is white Gaussian noise with zero mean and two-sided power spectral density $N_o/2$, τ_ℓ is a uniformly distributed random variable over the interval $0 \leq \tau_\ell \leq T$, and zero elsewhere; τ_ℓ and $\tau_{\ell'}$ are statistically independent for $\ell \neq \ell'$ (τ_i is by definition zero),

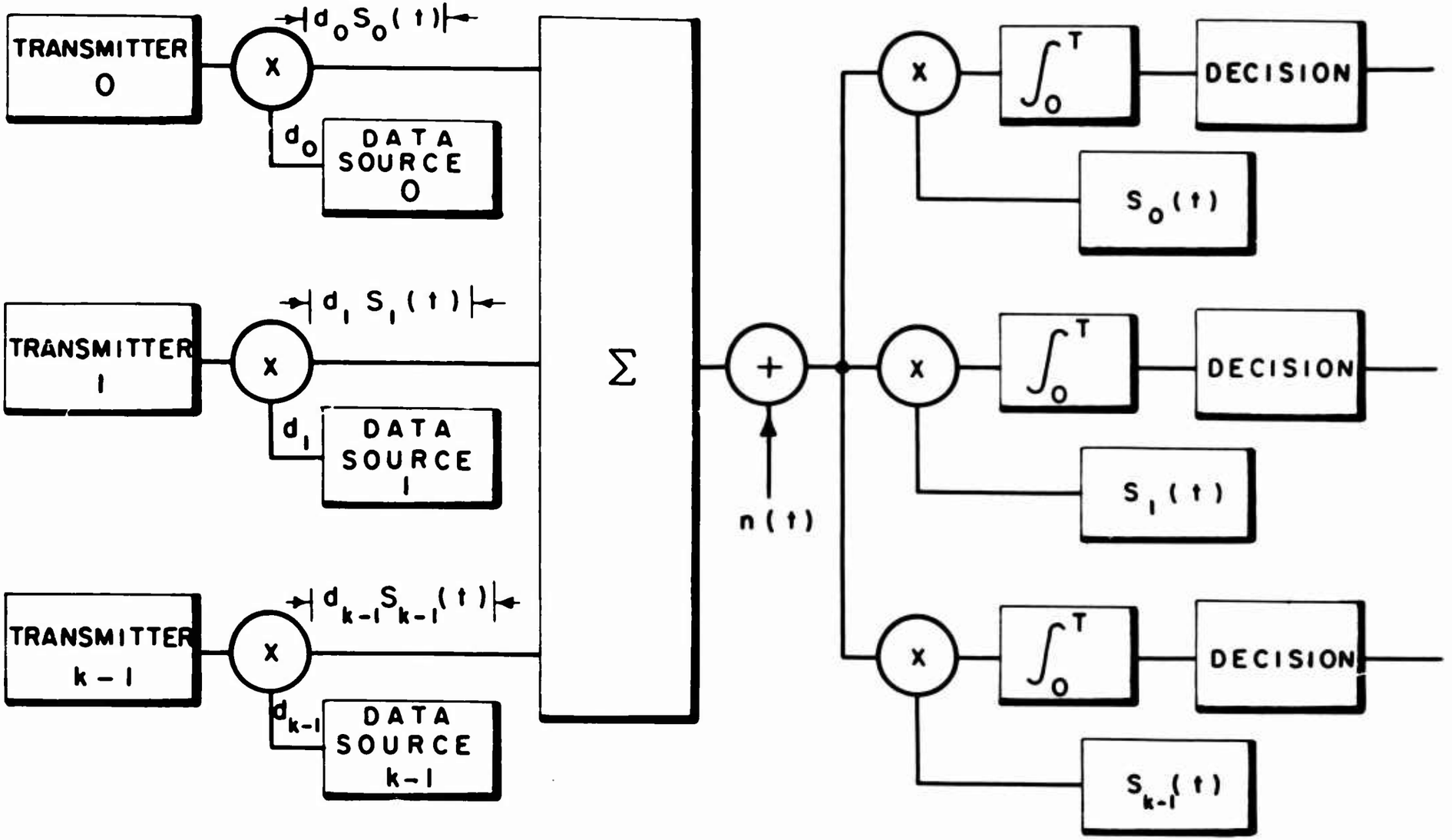
and

$$d_\ell^{(1)} = \begin{cases} \pm 1 \text{ with equal probability over the interval} & 0 \leq t \leq \tau_\ell \\ 0 \text{ elsewhere} & \end{cases},$$

$$d_\ell^{(2)} = \begin{cases} \pm 1 \text{ with equal probability over the interval} & \tau_\ell \leq t \leq T \\ 0 \text{ elsewhere,} & \end{cases}$$

$d_\ell^{(\sigma)}$ and $d_{\ell'}^{(\sigma')}$ are statistically independent for $\ell \neq \ell'$ or $\sigma \neq \sigma'$,

$d_i = \pm 1$ with equal probability.



F I G . 5. 1.

ASYNCHRONOUS COMMUNICATION SYSTEM MODEL

If $d_\ell^{(1)} \neq d_\ell^{(2)}$, then it will be said that carrier $S_\ell(t)$ has been complemented or "flipped". The detection procedure is to cross-correlate $r_i(t)$ with $S_i(t)$ with the polarity of the correlator output determining the decision on d_i. The output of the i^{th} correlator is then

$$Z_i = \frac{1}{T} \int_0^T S_i(t)\, r_i(t)\, dt$$

$$= \frac{1}{T} \int_0^T S_i(t)\, n(t)\, dt + \frac{1}{T} \int_0^T d_i\, S_i^2(t)\, dt$$

$$+ \frac{1}{T} \sum_{\substack{\ell=0 \\ \ell \neq i}}^{k-1} \left\{ \int_0^{\tau_\ell} d_\ell^{(1)}\, S_i(t)\, S_\ell(t-\tau_\ell)\, dt \right.$$

$$\left. + \int_{\tau_\ell}^T d_\ell^{(2)}\, S_i(t)\, S_\ell(t-\tau_\ell)\, dt \right\} . \qquad (5.2)$$

Equation (5.2) can be written in a more simplified notation as follows:

$$Z_i = \rho_{in} + S \sum_{\substack{\ell=0 \\ \ell \neq i}}^{k-1} d_\ell\, \rho_{i\ell} \qquad (5.3)$$

where

$$\rho_{in} = \frac{1}{T} \int_0^T S_i(t)\, n(t)\, dt + \frac{1}{T} \int_0^T d_i\, S_i^2(t)\, dt$$

is Gaussian distributed with means $\pm S$ and variance $N_o S/2T$, where S,

the average signal power (assumed equal) for all carriers, is

$$S = \frac{1}{T} \int_0^T S_i^2(t)\, dt \tag{5.4}$$

and*

$$\rho_{i\ell} = \begin{cases} \rho_{i\ell}^{(u)}(\tau_\ell) = \frac{1}{T} \int_0^T S_i(t)\, S_\ell(t-\tau_\ell)\, dt, \\ \qquad\qquad \text{with probability } 1/2, \\ \rho_{i\ell}^{(f)}(\tau_\ell) = \frac{1}{T} \int_0^{\tau_\ell} S_i(t)\, S_\ell(t-\tau_\ell)\, dt \\ \qquad - \frac{1}{T} \int_{\tau_\ell}^T S_i(t)\, S_\ell(t-\tau_\ell)\, dt \quad , \\ \qquad\qquad \text{with probability } 1/2 \, . \end{cases} \tag{5.5}$$

The cross-correlation functions $\rho_{i\ell}^{(u)}(\tau_\ell)$ and $\rho_{i\ell}^{(f)}(\tau_\ell)$ are the "unflipped" and "flipped" cross-correlation functions between $S_i(t)$ and $S_\ell(t)$ delayed by τ_ℓ seconds, respectively, and $d_\ell = \pm 1$ with equal probability.

The probability density function of $\rho_{i\ell}(\tau_\ell)$ is dependent upon the characteristics of the carriers.

---

* If carriers $S_i(t)$ and $S_\ell(t)$ are cyclically orthogonal, then

$$\rho_{i\ell}^{(u)} = 0$$

and

$$\rho_{i\ell}^{(f)}(\tau_\ell) = \frac{2}{T} \int_0^{\tau_\ell} S_i(t)\, S_\ell(t-\tau_\ell)\, dt \tag{5.5a}$$

Assuming a zero threshold, the average probability of binary error in the i^{th} channel, $P(e_i)$, is

$$P(e_i) = \frac{1}{2} \int_{-\infty}^{0} p(z_i|d_i=+1)\, dz + \frac{1}{2} \int_{0}^{\infty} p(z_i|d_i=-1)\, dz_i \qquad (5.6)$$

where $p(z_i|d_i=+1)$ and $p(z_i|d_i=-1)$ are the conditional pdf's of the output of i^{th} correlator given that $d_i = +1$ and -1 respectively. These conditional density functions are given by the convolution of the pdf's of the k terms of (5.3).

Most of the carriers to be considered in the following sections are mapped binary sequences. It was stated in Chapter 2 that the cross-correlation function of mapped binary sequences between integral delays is linear. It is now shown that the "flipped" cross-correlation function between integral delays is also linear.

THEOREM 5.1 Consider the mapping of two binary sequences, A and B, of length L, where, $A = (a_0, a_1, \ldots, a_{L-1})$ and $B = (b_0, b_1, \ldots, b_{L-1})$ and $a_i, b_i = 0,1$. (The mapped elements are $a_i^{(m)}$ and $b_i^{(m)}$.) The "flipped" cross-correlation function, $\rho_{ab}^{(f)}(\lambda+\epsilon)$, $(\lambda=0,1, \ldots, L-1,\ 0 \le \epsilon \le 1)$ is linear between integer values of $\lambda + \epsilon$.

Proof: The "flipped cross-correlation function at a delay of $(\lambda+\epsilon)$ is

$$\rho_{ab}^{(f)}(\lambda+\epsilon) = \frac{\epsilon}{L} \sum_{j=0}^{\lambda} a_j^{(m)}\, b_{L-\lambda+j}^{(m)} + \frac{(1-\epsilon)}{L} \sum_{j=0}^{\lambda-1} a_j^{(m)}\, b_{L-\lambda+j+1}^{(m)}$$

$$- \frac{\epsilon}{L} \sum_{j=\lambda+1}^{L-1} a_j^{(m)}\, b_{L-\lambda+j}^{(m)} - \frac{(1-\epsilon)}{L} \sum_{j=\lambda}^{L-1} a_j^{(m)}\, b_{L-\lambda+j+1}^{(m)} .$$

$$= \frac{\epsilon}{L} \rho_{ab}^{(f)}(\lambda) + \frac{1 - \epsilon}{L} \rho_{ab}^{(f)}(\lambda+1)$$

Thus the "flipped' cross-correlation function is linear between integral values of $\lambda + \epsilon$.

The noise or interference (in the determination of d_i) due to the presence of the other carriers on the channel is related to the values of $\rho_{i\ell}^{(u)}(\lambda_\ell)$ and $\rho_{i\ell}^{(f)}(\lambda_\ell)$. In the selection of binary sequences for the binary asynchronous signalling application the goal is to find sequences for which the "unflipped" and "flipped" cross-correlation functions are low for all cyclic shifts. Since it is difficult to deterministically derive sequences for which both types of cross-correlation functions are low, the basis for choosing the sequences analyzed in the following sections was that the value of $\rho_{i\ell}^{(u)}(\lambda_\ell)$ be low for all i, ℓ, and λ_ℓ.

5.2 Signalling With Basic Walsh Functions

In this section the performance of the mapped cyclically bi-orthogonal Basic Walsh functions, as carriers for the asynchronous signalling system, is determined. The "flipped" cross-correlation function is determined from which an integral expression for the probability of binary error, $P(e_i)$, is derived. By application of the Central Limit Theorem $P(e_i)$ is determined for $k \to \infty$, and all i. The probability of error for finite k is found by asymptotic series approximation and computer evaluation of the probability of error integral.

It was shown in Chapter 4 that the set of k sequences, S_{a_i}, $i = 0,1, \ldots, k-1$ of length 2^k, where S_{a_i} is

$$S_{a_i} = \underbrace{0\,0\,\ldots\,0}_{2^i}\ \underbrace{1\,1\,\ldots\,1}_{2^i} \quad \text{repeated } 2^{k-i-1} \text{ times,}$$

are cyclically bi-orthogonal. Hence for the mapping of these sequences $\rho_{i\ell}^{(u)}(\lambda_\ell) = 0$, $i \neq \ell$, for all λ_ℓ.

It is now necessary to derive an expression for the "flipped" cross-correlation, $\rho_{i\ell}^{(f)}(\lambda_\ell)$. The procedure is

a. form the sequence $S_g = S_{a_i} \oplus x^{\lambda_\ell} S_{a_\ell}^{(f)}$, mod $(x^L - 1)$, where $x^{\lambda_\ell} S_{a_\ell}^{(f)}$ is a sequence which is the last λ_ℓ digits of S_{a_ℓ} followed by the first $L - \lambda_\ell$ digits of S_{a_ℓ} complemented.

b. count the number of zeros and ones in the first in the first λ_ℓ digits of S_g.

Then from Equation (5.5a), the "flipped" cross-correlation is

$$\rho_{i\ell}^{(f)}(\lambda_\ell) = \frac{2}{L}\,[\text{No. of zeros in first } \lambda_\ell \text{ digits of } S_g - \text{No. of ones in first } \lambda_\ell \text{ digits of } S_g] \qquad (5.7)$$

The derivation of $\rho_{i\ell}^{(f)}(\lambda_\ell)$ for the Basic Walsh Functions is outlined in Appendix C. A general plot of $\rho_{i\ell}^{(f)}(\lambda_\ell)$ for* $\ell > i$ is shown in Figure 5.2. It is thus seen that the maximum value of the "flipped" cross-correlation for $\ell > i$ is 2^{i+1-k}. Thus, the interference a particular user can expect, due to the presence of the

* For $i > \ell$ the plot is similar except the roles of i and ℓ are interchanged.

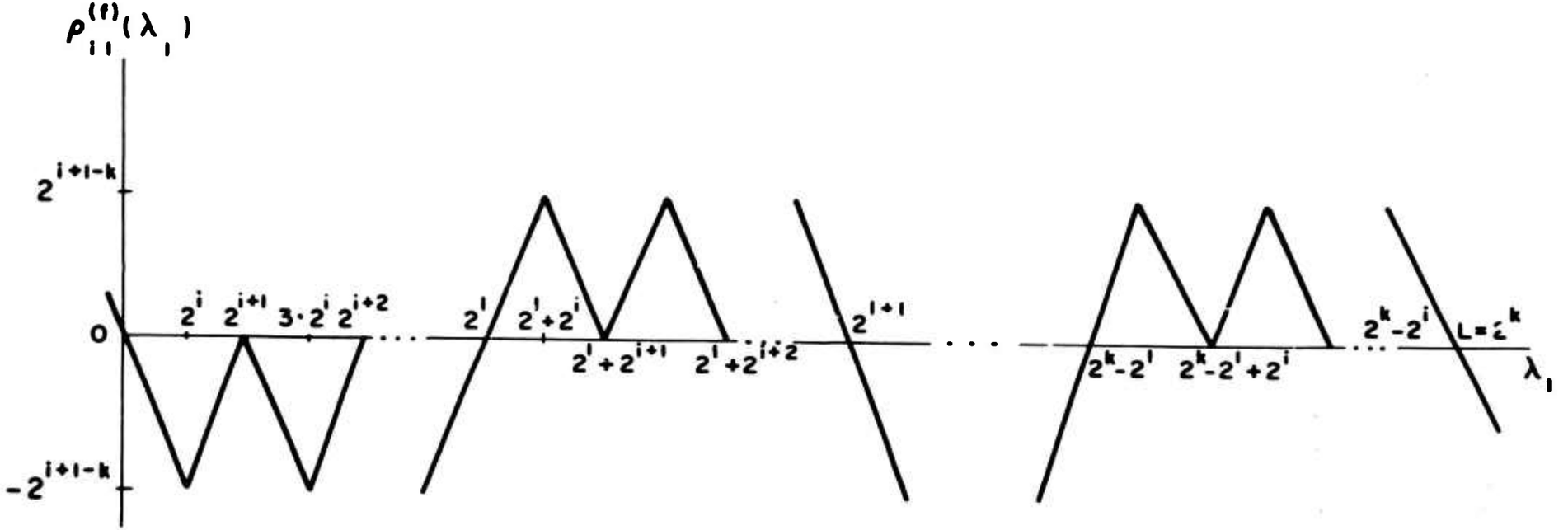


FIG. 5.2.

PLOT OF $\rho_{il}^{(f)}(\lambda_l)$ FOR $l>i$

"flipping" of other carriers is dependent upon the sequence he is using. The longer the period of the sequence (i.e. the higher the value of i), the larger is the interference.

Before determining the average probability of error in the presence of white Gaussian noise, it will be useful to determine the noiseless channel performance of these carriers.

Without the external additive Gaussian noise, the output of the i^{th} correlator z_i is

$$z_i = d_i S + S \sum_{\substack{\ell=0 \\ \ell \neq i}}^{k-1} d_\ell \, \rho_{i\ell}^{(f)}(\lambda_\ell) \, . \tag{5.8}$$

It is assumed that $d_i = +1$ and the minimum value of z_i, $(z_i)_{min}$, under the "worst" flipping conditions is found. An error will occur if $(z_i)_{min} < 0$. From the maximum value of $\rho_{i\ell}^{(f)}(\lambda_\ell)$ indicated in Figure 5.2, $(z_i)_{min}$ is

$$(z_i)_{min} = S - 2^{1-k} S \sum_{\ell=0}^{i-1} 2^\ell - (k-1-i)2^{1-k+i} S \, . \tag{5.9}$$

The interference term, $2^{1-k} S \sum_{\ell=0}^{i-1} 2^\ell + (k-1-i)2^{1-k+i} S$, is maximized for $i = k-1$ or $k-2$. Substituting $i = k-1$ in (5.9), $(z_{k-1})_{min}$ is

$$(z_{k-1})_{min} = S - 2^{1-k} S \sum_{\ell=0}^{k-2} 2^\ell = S - S(1-2^{1-k}) > 0 \tag{5.10}$$

Hence, an error cannot occur, even under the "worst flipping" conditions for a noiseless channel.

Now the average probability of error in the presence of white Gaussian noise will be determined. In Section 1 of this chapter, it was shown that the average probability of error, $P(e_i)$ when correlating synchronously with the carrier associated with S_{a_i} is given by Equation (5.6). However, since all of the noise phenomena are clearly symmetric, and the apriori probabilities that $d_\ell = +1$ and $d_\ell = -1$ (all ℓ) are the same, the expression for $P(e_i)$ is simplified to

$$P(\mathcal{E}_i) = \int_{-\infty}^{0} p(z_i \,|\, d_i=+1)\, dz_i \tag{5.11}$$

where $p(z_i \,|\, d_i=+1)$ is given by the k fold convolution of the probability density functions, $p(\rho_{in})$ and $p[S\cdot\rho_{i\ell}]$, $\ell = 0, 1, \ldots, k-1$, $\ell \neq i$. But,

$$p(\rho_{in}) = \frac{1}{\sqrt{\frac{\pi N_o S}{T}}} \exp - \left[\frac{(\rho_{in}-S)^2}{N_o S/T}\right], \tag{5.12}$$

$p[S\rho_{i\ell}]$ is the probability density function of $S\cdot\rho_{i\ell}$ assuming τ_ℓ is uniformly distributed between 0 and T, and Prob ["flip" in S_{a_ℓ}] = Prob [no "flip" in S_{a_ℓ}] = $\frac{1}{2}$. We can then represent $p[S\cdot\rho_{i\ell}]$ as the sum of the two density functions

$$p[S\cdot\rho_{i\ell}] = \tfrac{1}{2}p[S\cdot\rho_{i\ell}^{(u)}(\tau_\ell)] + \tfrac{1}{2}p[S\cdot\rho_{i\ell}^{(f)}(\tau_\ell)] \tag{5.13}$$

Since $\rho_{i\ell}^{(u)}(\tau_\ell) = 0$, all τ_ℓ, then

$$p[S\rho_{i\ell}^{(u)}(\tau_\ell)] = \delta[\rho_{i\ell}] \quad . \tag{5.14}$$

The density function of the "flipped" cross-correlation function for τ_ℓ uniformly distributed, is uniformly distributed between $+2^{i+1-k}$ and -2^{i+1-k}. Thus

$$p[S\cdot\rho_{i\ell}^{(f)}(\tau_\ell)] = \begin{cases} \left.\begin{array}{ll} \frac{1}{S}\,2^{-i-2+k} & -2^{i+1-k}\,S \le \rho_{i\ell} \le 2^{i+1-k}\,S \\ 0 & \text{elsewhere} \end{array}\right\} & i < \ell \\ \left.\begin{array}{ll} \frac{1}{S}\,2^{-\ell-2+k} & -2^{\ell+1-k}\,S \le \rho_{i\ell} \le 2^{\ell+1-k}\,S \\ 0 & \text{elsewhere} \end{array}\right\} & i > \ell \end{cases} \tag{5.15}$$

Substituting (5.15) and (5.14) into (5.13) the expression for $p[S\cdot\rho_{i\ell}]$ becomes

$$p(S\cdot\rho_{i\ell}) = \begin{cases} \frac{1}{2}\delta(\rho_{i\ell}) + \frac{1}{S}\,2^{-i-3+k} & -2^{i+1-k}\,S \le \rho_{i\ell} \le 2^{i+1-k}\,S \\ 0 & \text{elsewhere} \end{cases} \qquad i < \ell \tag{5.16}$$

or

$$p(S\cdot\rho_{i\ell}) = \begin{cases} \frac{1}{2}\delta(\rho_{i\ell}) + \frac{1}{S}\,2^{-\ell-3+k} & -2^{\ell+1-k}\,S \le \rho_{i\ell} \le 2^{\ell+1-k}\,S \\ 0 & \text{elsewhere} \end{cases} \qquad i > \ell \tag{5.17}$$

The result of convolving the k density functions, ρ_{in}, $\rho_{i\ell}$, $\ell = 0, 1, \ldots, k-1$, $\ell \neq i$, to form $p(z|d_i=+1)$ and then performing the integration of $p(z|d_i=+1)$ to derive $P(e_i)$ is not easily derived in closed form for $k > 2$. The derivation of $P(e_o) = P(e_1)$

for k = 2 by the convolution method is presented in Appendix D. It is shown that

$$P(e_o) = P(e_1) = \frac{1}{2} - \frac{1}{4}\,\mathrm{erf}\sqrt{\frac{ST}{N_o}} - \frac{3}{8}\,\mathrm{erf}\left(\frac{3}{2}\sqrt{\frac{ST}{N_o}}\right)$$

$$+ \frac{1}{8}\,\mathrm{erf}\left(\frac{1}{2}\sqrt{\frac{ST}{N_o}}\right) - \frac{1}{\sqrt{\pi}}\sqrt{\frac{N_o}{ST}}\,e^{-ST/4N_o} + \frac{1}{\sqrt{\pi}}\sqrt{\frac{N_o}{ST}}\,e^{-9ST/4N_o} . \tag{5.18}$$

A convenient integral expression for $P(e_i)$ with $k > 2$ is obtained using the characteristic functions of the cross-correlation functions. The characteristic function $M_x(jv)$ of a variable x with pdf p(x) is defined as

$$M_x(jv) = \int_{-\infty}^{\infty} \exp(jvx)\, p(x)\, dx \tag{5.19}$$

The characteristic function $M_{\rho_{in}}(jv)$ of the Gaussian distributed variable, ρ_{in} is

$$M_{\rho_{in}}(jv) = \exp\left[jvS - \frac{v^2 N_o^2 S^2}{2T^2}\right] . \tag{5.20}$$

Similarly the characteristic function $M_{\rho_{i\ell}}(jv)$ of the random variable $S\cdot\rho_{i\ell}$ is for $i < \ell$,

$$M_{\rho_{i\ell}}(jv) = \frac{1}{2} + \frac{2^{-i-2+k}}{jv}\left[\exp\left(jvS2^{i+1-k}\right) - \exp\left(-jvS2^{i+1-k}\right)\right] . \tag{5.21}$$

For $i > \ell$, $M_{\rho_{i\ell}}(jv)$ is obtained from (5.21) by replacing i with ℓ.

The characteristic function $M_{z_i}(jv)$ of the correlator output, z_i given that $d_i = +1$, is given by the product

$$M_{z_i}(jv) = M_{\rho_{in}}(jv)\left[\prod_{\substack{\ell=0 \\ \ell<i}}^{i-1} M_{\rho_{i\ell}}(jv)\right]\left[M_{\rho_{i\ell}}(jv)\right]^{k-1-i} \qquad (5.22)$$

Then the conditional pdf $p(z_i|d_i=+1)$ is derived from $M_{z_i}(jv)$ by the integral

$$p(z_i|d_i=+1) = \frac{1}{2\pi}\int_{-\infty}^{\infty} M_{z_i}(jv)\exp(-jvz_i)\,dv\,. \qquad (5.23)$$

Thus, the expression for the probability of error, when correlating with the i^{th} carrier becomes

$$P(e_i) = \int_{-\infty}^{0} dz_i \frac{1}{2\pi}\int_{-\infty}^{\infty}(dv)\exp\left[jvS - \frac{v^2 N_0^2 S^2}{2T^2}\right]\cdot\exp(-jvz_i)$$

$$\cdot\prod_{\ell=0}^{i-1}\left\{\frac{1}{2} + \frac{2^{-\ell+2+k}}{jv}\left[\exp(jvS2^{\ell+1-k}) - \exp(-jvS2^{\ell+1-k})\right]\right\}$$

$$\cdot\left\{\frac{1}{2} + \frac{2^{-i-2+k}}{jv}\left[\exp(jvS2^{i+1-k}) - \exp(-jvS2^{i+1-k})\right]\right\}\,. \qquad (5.24)$$

This integral can be transformed by noting some simplifications and substitutions. First it should be noted that

$$\int_{-\infty}^{0} dz_i \exp(-jvz_i) = -\frac{1}{jv} + \pi\delta(v) \quad . \tag{5.25}$$

Then the exponentials with complex arguments can be replaced by sine and cosine functions, the odd function terms of the integrand deleted. Then, $P(e_i)$ reduces to

$$P(e_i) = \frac{1}{2} - \frac{1}{\pi 2^{k-1}} \int_{0}^{\infty} \left[\frac{\sin Gv}{v}\right] \left[\exp\left(-\frac{v^2}{4}\right)\right] \prod_{\ell=0}^{i-1} \left[\frac{\sin 2^{\ell+1} - k_{Gv}}{2^{\ell+1} - k_{Gv}} + 1\right]$$

$$\cdot \left[\frac{\sin 2^{i+1} - k_{Cv}}{2^{i+1} - k_{Gv}} + 1\right]^{k-i-1} dv \quad , \tag{5.26}$$

where $G = \sqrt{\frac{ST}{N_o}}$.

It is clear from the above integral that $P(e_i)$ is a function of (a) the carrier in question, i, (b) the number of carriers on the channel, k, and (c) the signal-to-noise ratio $G^2 = ST/N_o$. It is also noted that $P(e_{k-1}) = P(e_{k-2})$.

No technique was found for evaluating (5.26) in closed form. Some computer derived curves which give the probability of error as a function of the parameters G, i, and k, will be presented later. However, first some indications of the performance can be noted by evaluating the asymptotic behavior of $P(e_i)$.

a. For large signal-to-noise ratio ($G \to \infty$)

First evaluate, $\lim_{G \to \infty} \sin \frac{Gv}{v}$ considered as a generalized function. Thus

$$\lim_{G\to\infty} \frac{\sin Gv}{v} = \frac{d}{dv} \lim_{G\to\infty} \int_0^v \frac{\sin Gv}{Gv}\, d(Gv)$$

$$= \frac{d}{dv} \lim_{n\to\infty} \int_0^{nv} \frac{\sin x}{x}\, dx = \frac{\pi}{2} \frac{d}{dv} \operatorname{Sgn} v$$

$$= \frac{\pi}{2}\, \delta(v)$$

Substituting this result into (5.26) it is found that

$$\lim_{G\to\infty} P(e_i) = \frac{1}{2} - \int_0^{\infty} \frac{1}{2^{k-1}} \cdot \delta(v) \cdot 2^{k-1}\, dv = 0$$

b. For small signal-to-noise ratio ($G\to o$)

It is seen that

$$\lim_{G\to o} \frac{\sin Gv}{v} = 0$$

Thus

$$\lim_{G\to o} P(e_i) = \frac{1}{2}$$

c. For an unbounded number of carriers on the channel ($k \to \infty$), when we are correlating with carrier associated with S_{a_i}, i finite it is seen that

$$\lim_{k\to\infty} \frac{\sin 2^{1+\ell-k} Gv}{2^{1+\ell-k} Gv} = 1.$$

Thus

$$\lim_{k\to\infty} P(e_i) = \frac{1}{2} - \frac{1}{\pi} \int_0^{\infty} \frac{\sin Gv}{v} \exp(-v^2/4)\, dv \qquad (5.27)$$

The integral in Equation (5.27) is noted to be $\frac{1}{2}$ erf (G).[34]

Thus

$$\lim_{k\to\infty} P(e_i) = \frac{1}{2} - \frac{1}{2} \text{ erf } (G) \tag{5.28}$$

Summarizing the results derived in (a), (b) and (c), it is seen that the limiting values of $P(e_i)$ for high and low values of signal-to-noise ratio (any k, i) are 0 and $\frac{1}{2}$, respectively. As the number of carriers on the channel becomes unbounded, then $P(e_i)$, (i finite), approaches the probability of error value that would be realized if there were no interfering signals on the channel.*

For large values of k and relatively small values of i, an asymptotic series approximation to the integral expression (5.26) can be derived. In Appendix E an asymptotic series approximation to $P(e_o)$ which yields accurate results for $k \geq 4$ is derived.

It was shown that the probability of error when correlating with the i^{th} carrier (i finite) approaches the PSK error probability as $k \to \infty$. Using the Central Limit Theorem, the limiting probability of error curves for $i = k - E$, $k \to \infty$ and $E = 1, 2, \ldots$, can be derived.

As $k \to \infty$, the correlator output $z_i = z_{k-E}$ becomes Gaussian distributed with mean m_{z_i} and variance $\sigma^2_{z_i}$,

$$m_{z_i} = m_{\rho_{in}} + \sum_{\substack{\ell=0 \\ \ell\neq i}}^{k-1} m_{S\cdot\rho_{i\ell}} \tag{5.29}$$

---

* This is referred to as the coherent binary PSK error probability.

where $m_{\rho_{in}}$, the mean of ρ_{in}, is + S

and $m_{S\cdot\rho_{i\ell}}$, the mean of $S\cdot\rho_{i\ell}$ is 0

Thus

$$m_{z_i} = S,$$

$$\sigma^2_{z_i} = \sigma^2_{\rho_{in}} + \sum_{\substack{\ell=0 \\ \ell\neq i}}^{k-1} \sigma^2_{S\cdot\rho_{i\ell}} \qquad (5.30)$$

where

$$\sigma^2_{\rho_{in}} = N_o S/2T$$

and

$$\sigma^2_{S\cdot\rho_{i\ell}} = \begin{cases} \frac{S^2}{3} 2^{2i-2k+1} & i < \ell \\ \frac{S^2}{3} 2^{2\ell-2k+1} & \ell < i \end{cases}$$

Performing the summation indicated by (5.30), $\sigma^2_{z_i} = \sigma^2_{z_{k-E}}$ is found to be for E = 1, 2

$$\sigma^2_{z_{k-E}} = \frac{N_o S}{2T} + \frac{S^2}{3} \sum_{c=2}^{\infty} 2^{2(k-c)-2k+1} = \frac{2S^2}{3} \left(\frac{1}{16}\right) \sum_{d=0}^{\infty} 2^{-2d} + \frac{N_o S}{2T}$$

$$\sigma^2_{z_{k-E}} = \frac{S^2}{18} + \frac{N_o S}{2T} \quad , \qquad (5.31)$$

and for E = 3, 4, ...

$$\sigma^2_{z_{k-E}} = \frac{N_o S}{2T} + \frac{S^2}{3}\left[(E-1)\ 2^{2(k-E)-2k+1} + \sum_{c=E+1}^{\infty} 2^{2(k-c)-2k+1}\right]$$

$$\sigma^2_{z_{k-E}} = \frac{N_o S}{2T} + \frac{S^2}{3}\left[(E-1)\ 2^{-2E+1} + (\tfrac{4}{3})(2^{-2E-1})\right] \quad . \tag{5.32}$$

The conditional pdf, $p(z_i|d_i=+1)$, for unbounded k becomes

$$\lim_{k\to\infty} p(z_i|d_i=+1) = \frac{1}{\sqrt{2\pi\ \sigma^2_{z_i}}} \exp - \left[\frac{(z_i-S)^2}{2\sigma^2_{z_i}}\right] \quad . \tag{5.33}$$

Hence the error probability, $P(e_i) = P(e_{k-E})$, for $k \to \infty$ is

$$\lim_{k\to\infty} P(e_{k-E}) = \int_{-\infty}^{o} p(z_{k-E}|d_{k-E}=+1)\ dz_{k-E} = \frac{1}{2} - \frac{1}{2}\ \mathrm{erf}\left[\frac{S}{\sqrt{2}\ \sigma_{z_{k-E}}}\right]$$

$$= \frac{1}{2} - \frac{1}{2}\ \mathrm{erf}\left[\frac{1}{\sqrt{G^2 + \frac{2}{S^2}\left(\sigma^2_{z_{k-E}} - \frac{N_o S}{2T}\right)}}\right] \tag{5.34}$$

Plots of $\lim_{k\to\infty} P(e_{k-E})$, as a function of $G = \sqrt{\frac{ST}{N_o}}$, for E = 1 (or 2), 3, 4, 5, and ∞, are shown in Figure 5.3 for ranges of probability of error down to 10^{-5}.

The curves shown in Figure 5.3 indicate the maximum probability of error, $P(e_{k-E})$, maximized over k for given values of E and G. The minimum of $P(e_{k-E})$, (also for a given E and G) occurs for k = E. Plots of $P(e_o)$, as a function of G, for E = k = 2, 3, 4, 5, ∞,

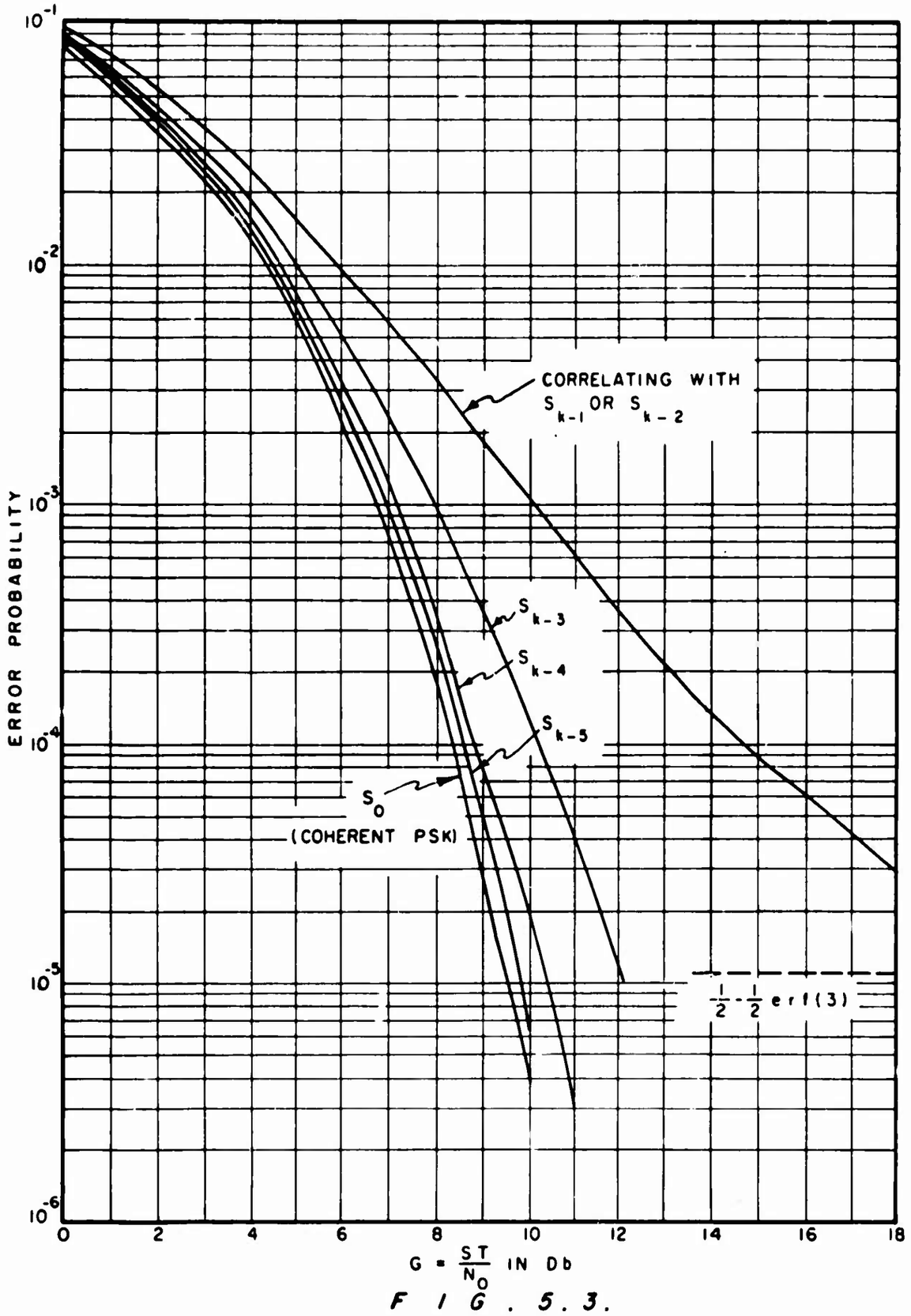


FIG. 5.3.

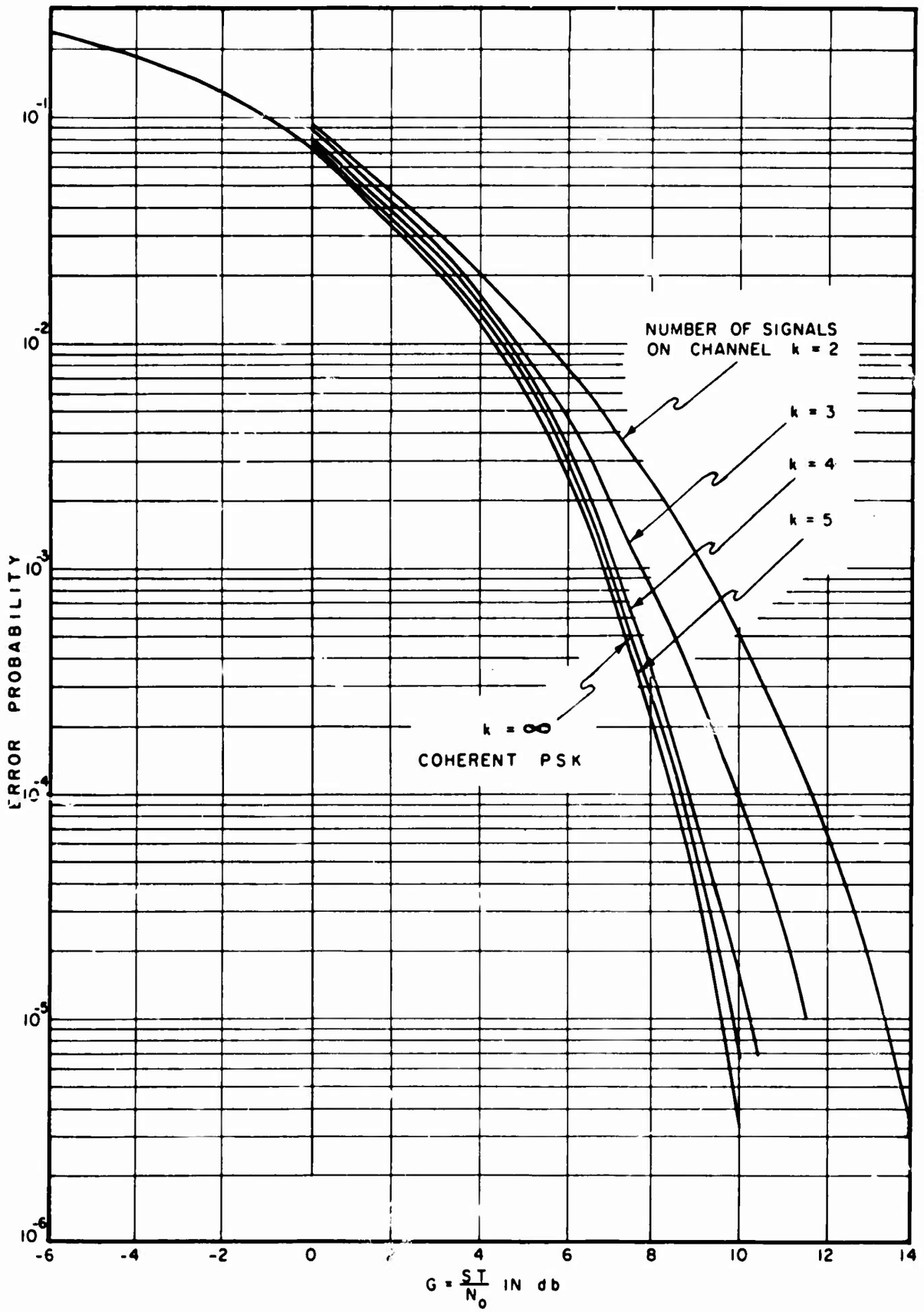
PROBABILITY OF ERROR VS SIGNAL TO NOISE RATIO (PER BIT) / NOISE POWER DENSITY WHEN CORRELATING WITH S_{k-1}, S_{k-2}, S_{k-3}, S_{k-4}, S_{k-5}, ..., S_0, WHEN ALL SEQUENCES ARE OF LENGTH 2^k AS $K \to \infty$ (ALL CURVES THEORETICALLY DERIVED)

are shown in Figure 5.4. The values of $P(e_o)$ for k = 2 are calculated from Equation (5.18). The values for k = 4, 5 are calculated from the asymptotic series approximation derived in Appendix E. The values for k = 3 were obtained by numerical evaluation of the integral expression (5.26) on the PDP5 and IBM 7094 computers.

The curves shown in Figures (5.3) and (5.4) are the limiting curves of $P(e_{k-E})$. In Figure (5.5), $P(e_{k-1}) = P(e_{k-2})$ is plotted for k = 2, 3, 4, 5, 6, ∞. The curves for k = 2, ∞ were taken from Figures (5.4) and (5.3). The probability of error values for the remaining curves were obtained by numerical evaluation of (5.26). In Figure (5.6), $P(e_{k-3})$ is plotted for k = 3, 4, 5, ∞. In Figure (5.7), $P(e_{k-4})$ is plotted for k = 4, ∞.

The error probability curves not included in these plots, $P(e_{k-E})$, E = 5, 6, ..., were omitted because the curves (for a given E) for k = E and k = ∞ (and hence the curves for all k between E and ∞) were indistinguishable. From the given plots, it is possible to determine the error probability curves for any carrier (S_{a_i}) with any number of interfering carriers on the channel.

It was noted in the previous analysis that the highest error probability occurs when we are correlating synchronously with carriers associated with $S_{a_{k-1}}$ or $S_{a_{k-2}}$ as k $\rightarrow \infty$. If the carrier associated with $S_{a_{k-1}}$ is removed from the channel (providing k-1 carriers on the channel), then the maximum error probability occuring for $S_{a_{k-2}}$ or $S_{a_{k-3}}$ will be significantly lower. Similarly, if $S_{a_{k-1}}$ and $S_{a_{k-2}}$ are removed (providing k-2 carriers on the channel), then the highest



F I G. 5. 4.

PROBABILITY OF ERROR VS SIGNAL ENERGY (PER BIT) / NOISE POWER DENSITY WHEN CORRELATING WITH SIGNAL S_0 = (10101010....)
CURVE FOR k = 2 DERIVED FROM CLOSED FORM SOLUTION
CURVE FOR k = 3 DERIVED BY COMPUTER
CURVES FOR k = 4,5 DERIVED BY ASYMPTOTIC METHOD

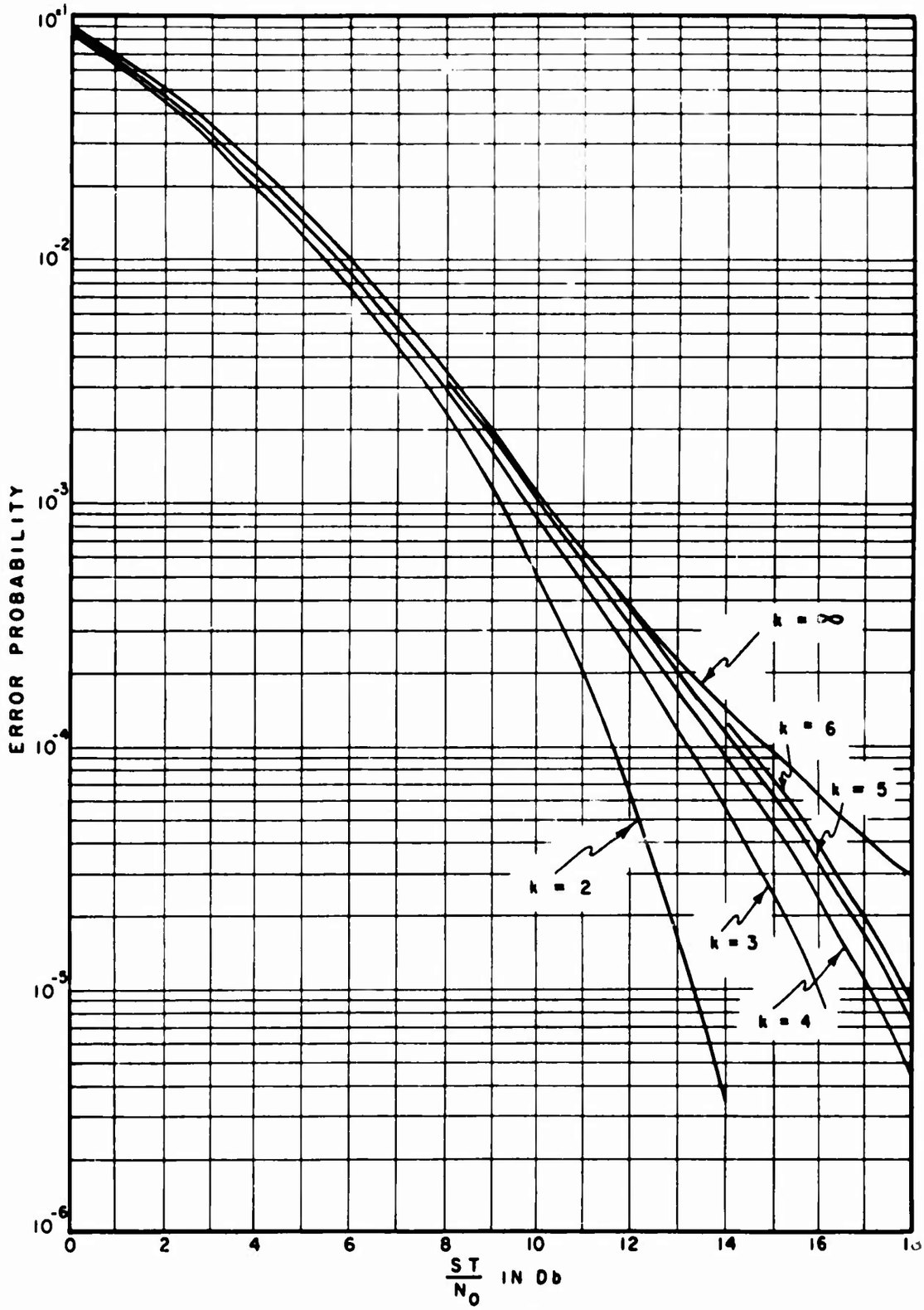
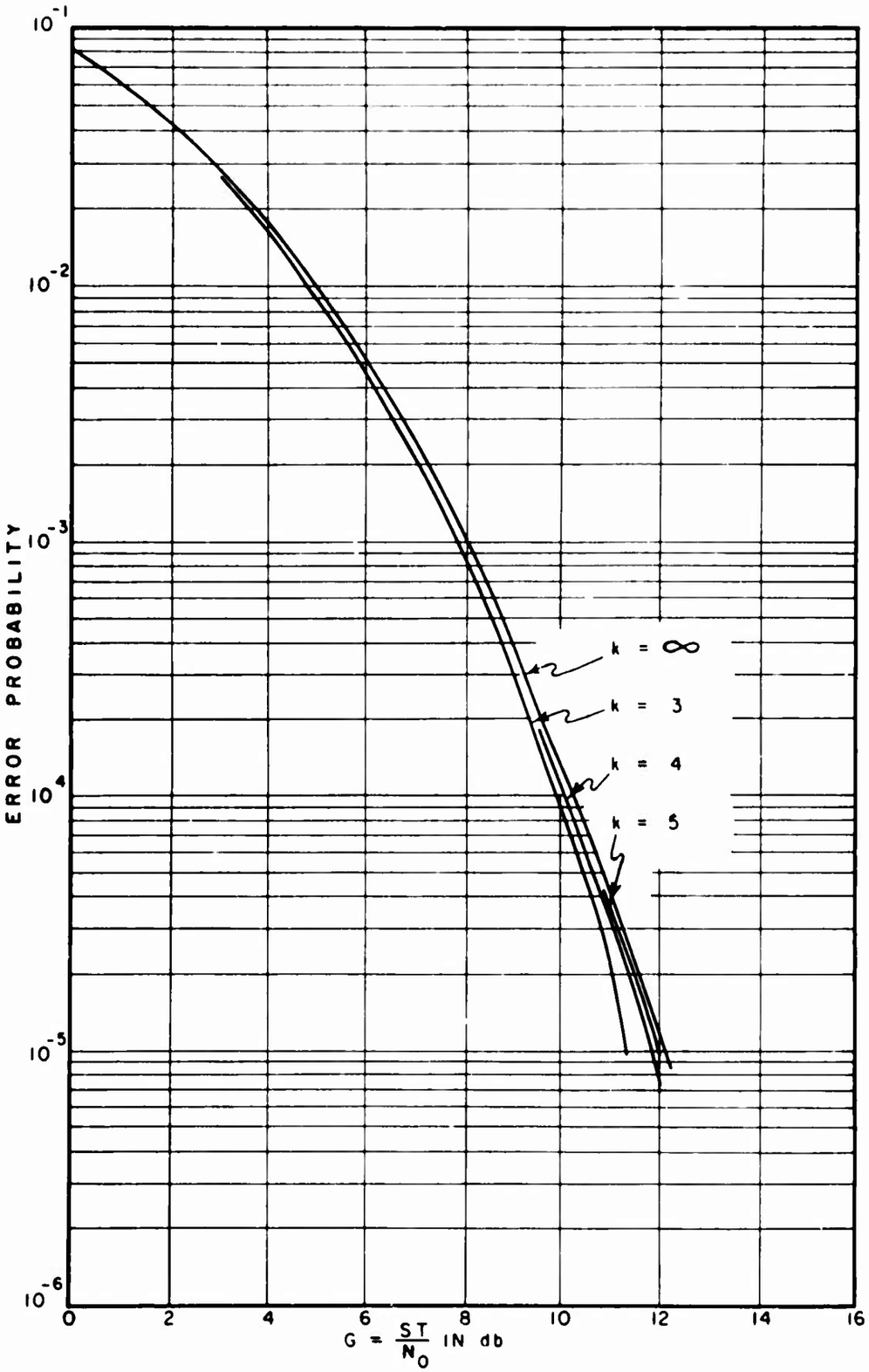


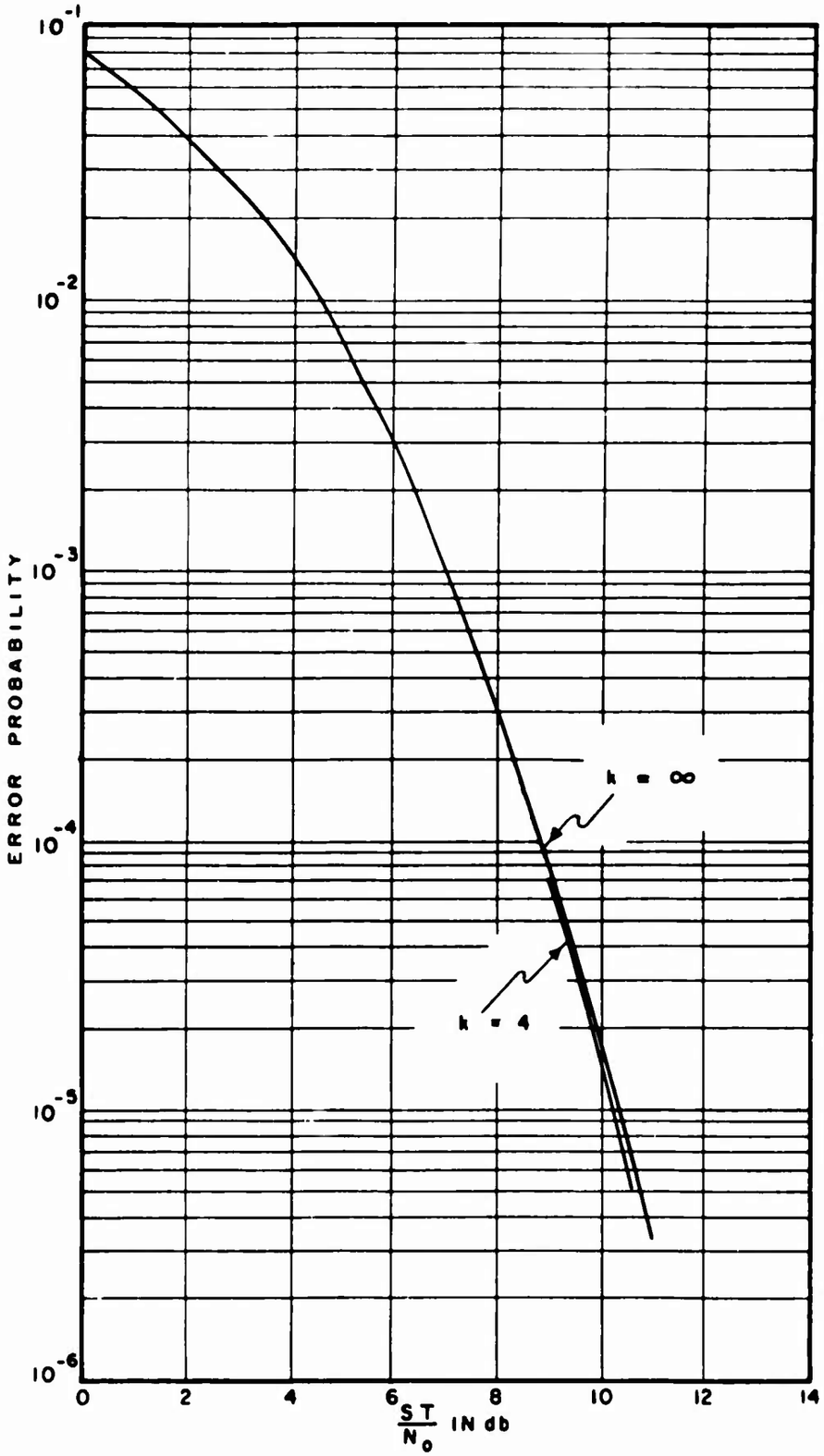
FIG. 5.5.

PROBABILITY OF ERROR VS SIGNAL ENERGY
(PER BIT) / NOISE POWER DENSITY WHEN
CORRELATING WITH SIGNAL S_{k-1} OR S_{k-2}
CURVES FOR k = 2 DERIVED FROM CLOSED FORM SOL.
CURVE FOR k = ∞ DERIVED FROM THEORETICAL FORMULA
CURVES FOR k = 3,4,5,6 COMPUTER DERIVED
LENGTH OF SEQUENCES = 2^k



F I G. 5.6.

PROBABILITY OF ERROR VS SIGNAL ENERGY (PER BIT) / NOISE POWER DENSITY WHEN CORRELATING WITH SIGNAL S_{k-3}
CURVES FOR k = 3, 4, 5 COMPUTER DERIVED
CURVE FOR k = ∞ DERIVED FROM THEORETICAL FORMULA



F I G . 5.7.

PROBABILITY OF ERROR VS SIGNAL ENERGY (PER BIT) / NOISE POWER DENSITY WHEN CORRELATING WITH S_{k-4}
CURVE FOR k = 4 ASYMPTOTICALLY DERIVED FROM SERIES
CURVE FOR k = ∞ THEORETICALLY DERIVED

error probability occurs for $S_{a_{k-3}}$ or $S_{a_{k-4}}$. The maximum error probability curves when there are k, k-1, k-2 carriers of length 2^k, with $k \to \infty$ on the channel are shown in Figure 5.8.

For future comparison of the performance of the k Basic Walsh function carriers with randomly derived mapped binary sequences for asynchronous signalling, the probability of error, $\overline{P_w}$, averaged over all k carriers will be determined. It is shown in Appendix F that

$$\overline{P_w} = \frac{1}{2} - \frac{1}{2} \operatorname{erf}(G) \quad , \tag{5.34}$$

for all values of $G^2 < 9$.

5.3 Asynchronous Binary Signalling With Sinusoids

In the previous section the performance of the k Basic Walsh functions of length 2^k, as the carriers for the binary asynchronous communications system, was analyzed. In this section another set of cyclically orthogonal signals - the set of sine functions whose frequencies are all different and all multiples of some fundamental frequency - will be analyzed for this application, and the asymptotic performance will be compared with the asymptotic performance of the Basic Walsh functions.

Consider the set of sinusoids $S_i(t)$ of period T,

$$S_i(t) = \sqrt{2S} \sin i \omega t \quad , \qquad 0 \leq t \leq T \tag{5.35}$$

where

$\omega = 2\pi/T$

$i = 1, 2, \ldots ,$

S is the average signal power assumed equal for all i.

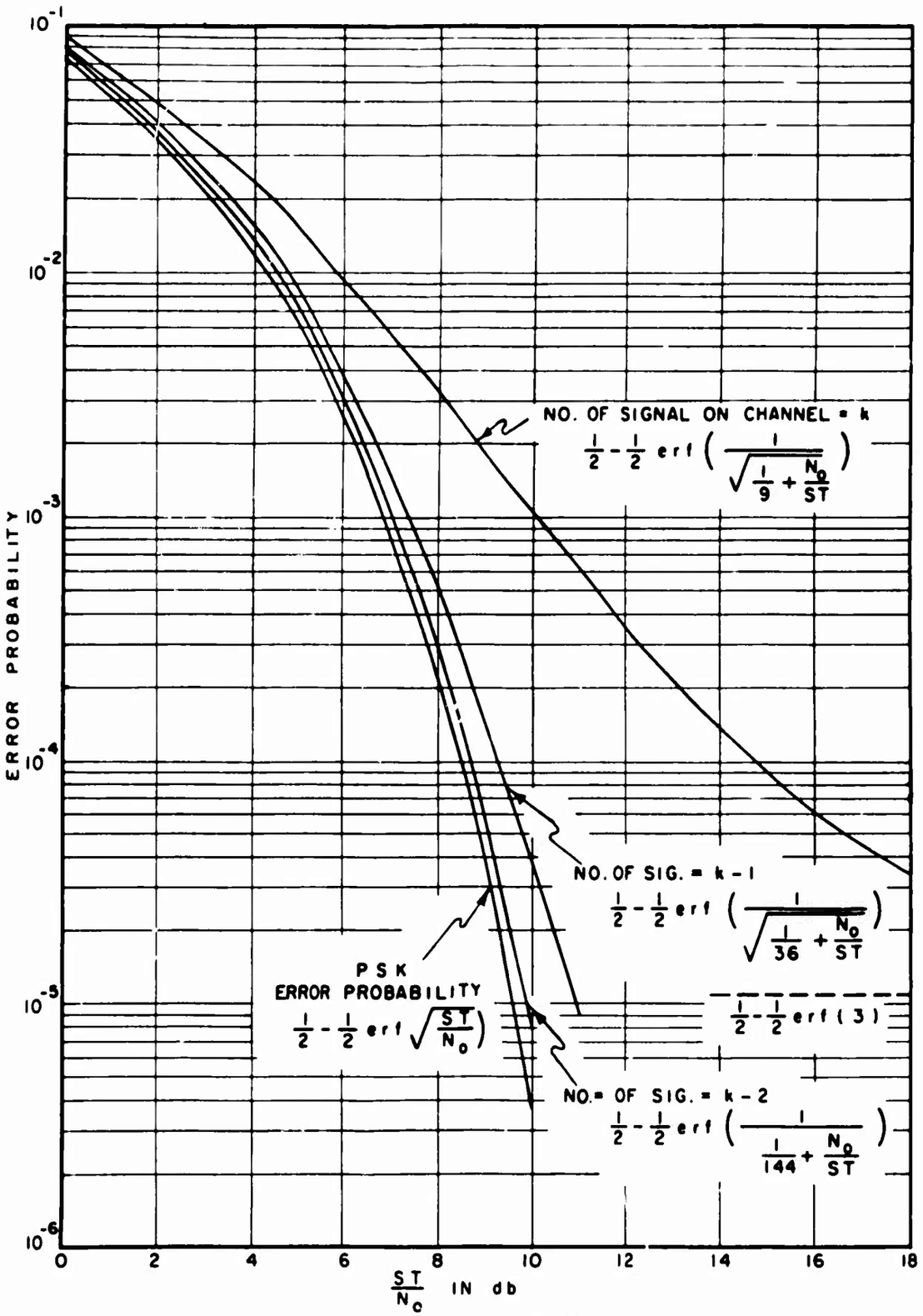


FIG. 5.8.

PROBABILITY OF ERROR VS SIGNAL TO NOISE RATIO (PER BIT) / NOISE POWER, MAXIMUM PROBABILITY OF ERROR CURVES FOR k, k - 1, k - 2 SEQUENCES ON CHANNEL ALL OF LENGTH 2^k, $k \to \infty$ (ALL CURVES THEORETICALLY DERIVED)

A set of these sinusoids are considered as carriers. It is clear that $S_i(t)$ and $S_\ell(t)$, $i \neq \ell$ are cyclically bi-orthogonal. The "flipped" cross-correlation function, $\rho_{i\ell}^{(f)}(\tau_\ell)$ between $S_i(t)$ and $S_\ell(t)$ at a delay of τ_ℓ, $0 \leq \tau_\ell \leq T$, is derived as follows. Since $S_i(t)$ and $S_\ell(t)$ are cyclically orthogonal the "flipped" cross- correlation is, from (5.5a),

$$\rho_{i\ell}^{(f)}(\tau_\ell) = \frac{2}{T} \int_0^{\tau_\ell} S_i(t)\, S_\ell(t-\tau_\ell)\, dt$$

$$= \frac{4S}{T} \int_0^{\tau_\ell} [\sin i\,\omega t][\sin \ell\,\omega(t-\tau_\ell)]\, dt \,. \qquad (5.36)$$

Performing the indicated integration, it is seen

$$\rho_{i\ell}^{(f)}(\tau_\ell) = \frac{4S}{T} \left\{ \frac{\sin[(i-\ell)\omega t + \ell\,\omega\,\tau_\ell]}{2\omega(i-\ell)} - \frac{\sin[(i+\ell)\omega t - \ell\,\omega\,\tau_\ell]}{2\omega(i+\ell)} \right\}_0^{\tau_\ell},$$

or

$$\rho_{i\ell}^{(f)}(\tau_\ell) = \frac{2S}{\pi(i^3-\ell^2)} [i \sin \ell\,\omega\,\tau_\ell - \ell \sin i\,\omega\,\tau_\ell] \qquad (5.37)$$

For noiseless channel consideration, we are interested in the maximum interference resulting from the presence of other carriers on the channel, when correlating synchronously with $S_i(t)$. It is thus

necessary to find the maximum value of the flipped cross-correlation, maximized over τ_ℓ. Differentiating (5.37), the following expression is obtained:

$$\frac{d\,\rho_{i\ell}^{(f)}(\tau_\ell)}{d\,\tau_\ell} = \frac{2S\,\omega\,i\,\ell}{\pi(i^2-\ell^2)}\left[\cos\,\ell\,\omega\,\tau_\ell - \cos\,i\,\omega\,\tau_\ell\right] \qquad (5.38)$$

Thus local extremum points are found for

$$\cos\,\ell\,\omega\,\tau_\ell - \cos\,i\,\omega\,\tau_\ell = 0 \quad ,$$

or equivalently,

$$-\,2\,\sin\tfrac{1}{2}(i+\ell)\omega\,\tau_\ell \cdot \sin\tfrac{1}{2}(\ell-i)\omega\,\tau_\ell = 0 \quad . \qquad (5.39)$$

Equation (5.39) is satisfied for

$$\omega\,\tau_\ell = \frac{2m\pi}{i+\ell} \qquad \text{or} \qquad \omega\,\tau_\ell = \frac{2m\pi}{\ell-i} \quad , \qquad (5.40)$$

$$m = 0,\ 1,\ \ldots \quad .$$

It is still necessary to determine which value of τ_ℓ, or equivalently $\omega\,\tau_\ell$, given by (5.40), absolutely maximizes $\rho_{i\ell}^{(f)}(\tau_\ell)$. This can be derived by substituting the values indicated by (5.40) into (5.37).

Case a. $\omega\,\tau_\ell = \frac{2m\pi}{i+\ell}$

The local extremum values of $\rho_{i\ell}^{(f)}(\tau_\ell)$ written as $\rho_{i\ell}^{(f)}(\tau_\ell)\Big|_{ext}$ are then

$$\rho_{i\ell}^{(f)}(\tau_\ell)\Big|_{ext} = \frac{2S}{\pi(i^2-\ell^2)}\left[i\,\sin\left(\frac{\ell 2m\pi}{i+\ell}\right) - \ell\,\sin\left(\frac{i2m\pi}{i+\ell}\right)\right]$$

$$= \frac{2S(i+\ell)}{\pi(i^2-\ell^2)}\,\sin\left(\frac{\ell 2m\pi}{i+\ell}\right) = \frac{2S}{\pi(i-\ell)}\,\sin\left(\frac{\ell 2m\pi}{i+\ell}\right) \quad . \qquad (5.41)$$

From (5.41), it is seen that the maximum absolute value of "flipped" cross-correlation, $|\rho_{i\ell}^{(f)}(\tau_\ell)|_{max}$, is achieved for the value of m, for a given i and ℓ, for which the angle $\frac{\ell 2m\pi}{i+\ell}$ is "closest" to $\pi/2$ or $3\pi/2$. For $(i+\ell) \geq 10$ the maximum "flipped" cross-correlation for $\omega \tau_\ell = \frac{2m\pi}{i+\ell}$ is

$$|\rho_{i\ell}^{(f)}(\tau_\ell)|_{max} = \frac{2S}{\pi|i-\ell|} \qquad (5.42)$$

$$i + \ell \geq 10$$

Case b. $$\omega \tau_\ell = \frac{2m\pi}{\ell-i}$$

For this case the local extremum values of $\rho_{i\ell}^{(f)}(\tau_\ell)$ are

$$\rho_{i\ell}^{(f)}(\tau_\ell)\Big|_{ext} = \frac{2S}{\pi(i^2-\ell^2)}\left[i \sin\left(\frac{\ell 2m\pi}{\ell-i}\right) - \ell \sin\left(\frac{i2m\pi}{\ell-i}\right)\right]$$

$$= \frac{2S(i-\ell)}{\pi(i^2-\ell^2)} \sin\left(\frac{\ell 2m\pi}{\ell-i}\right) = \frac{2S}{\pi(i+\ell)} \sin\left(\frac{\ell 2m\pi}{\ell-i}\right) \qquad (5.43)$$

As in Case (a) the maximum absolute "flipped" cross-correlation is achieved for $\frac{\ell 2m\pi}{\ell-i}$ "closest" to $\pi/2$ or $3\pi/2$. For $i + \ell \geq 10$, the maximum absolute value for $\omega \tau_\ell = \frac{2m\pi}{\ell-i}$ is

$$|\rho_{i\ell}^{(f)}(\tau_\ell)|_{max} = \frac{2S}{\pi(i+\ell)} \qquad (5.44)$$

$$i + \ell \geq 10$$

Clearly for $i + \ell \geq 10$, the absolute maximum value indicated by (5.42) is greater than the value indicated by (5.44). However, it can be

verified that for all i, ℓ, the maximum value achieved by Case (a) is always greater than that achieved by (b).

It is now of interest to compare the noiseless channel performance of k Basic Walsh functions, $k \to \infty$ with a similarly chosen set of sinusoids. The frequencies of the Basic Walsh functions, $S_{a_{k-1}}, S_{a_{k-2}}, \ldots, S_{a_{k-E}}$, are proportional to 1, 2, ... , 2^{E-1}, respectively. Thus, a similarly chosen set of sinusoids would be $S_1(t)$, $S_2(t)$, ... , $S_{2F}(t)$ ($F = 0, 1, \ldots, k-1, k \to \infty$) where $S_1(t)$ is given by (5.35).

Without any external noise, the output of the i^{th} correlator z_i, given by (5.8), can be represented as

$$z_i = z_{2F} = d_{2F} \cdot S + I_{2F} \quad , \tag{5.45}$$

where I_{2F} is the interference term due to the presence of the other sinusoidal carriers.

The maximum value of the interference $|I_{2F}|_{max}$ for the sinusoid carriers is

$$\left|I_{2F}\right|_{max} = \sum_{\substack{F'=0 \\ F' \neq F}}^{k-1} \left|\rho^{(f)}_{2F,2F'}(\tau_\ell)\right|_{max} \tag{5.46}$$

For $F \geq 4$, the value of $\left|\rho^{(f)}_{2F,2F'}(\tau_\ell)\right|_{max}$ specified by (5.42) can be used. Thus, for $F \geq 4$ and $F << k$, $k \to \infty$,

$$\left|I_{2^F}\right|_{max} = \frac{2S}{\pi}\left[\sum_{d=1}^{F}\frac{1}{2^F - 2^{F-d}} + \sum_{c=1}^{\infty}\frac{1}{2^{F+c} - 2^F}\right] \tag{5.47}$$

A lower bound on $\left|I_{2^F}\right|_{max}$, denoted as $I_{2^F}^{(L)}$, which is an accurate representation for $F \geq 6$ is found as

$$I_{2^F}^{(L)} = \frac{2S}{\pi}\left[\sum_{d=1}^{F}\frac{1}{2^F} + \frac{1}{2^{F+1}}\sum_{c=o}^{\infty}2^{-c}\right] = \frac{2S}{\pi}\frac{F+1}{2^F} \tag{5.48}$$

An upper bound for $\left|I_{2^F}\right|_{max}$, denoted as $I_{2^F}^{(u)}$, is found as

$$I_{2^F}^{(u)} = \frac{2S}{\pi}\left[\sum_{d=1}^{F}\frac{1}{2^{F-1}} + \frac{1}{2^F}\sum_{c=o}^{\infty}2^{-c}\right] = \frac{2S}{\pi}\frac{F+1}{2^{F-1}} \quad . \tag{5.49}$$

For the Basic Walsh function carriers the maximum interference has been determined (as a modification of 5.9) as $\frac{S\,E}{2^{E-1}}$, when we are correlating with the carrier associated with sequence $S_{a_{k-E}}$, E = 1, 2, ... , k, $k \to \infty$. A comparison of maximum interference of the two types of carriers, for several small values of E, and for large E, where E = F + 1, is presented in Table 5.1.

TABLE 5.1

Maximum Interference For Basic Walsh Function and Sinusoidal Carriers

E	$\lvert I_{2E}\rvert_{max}$-Walsh	$\lvert I_{2E}\rvert_{max}$-sinusoids
1	S	$0.92 \cdot S$
2	S	$1.04 \cdot S$
3	$0.75 \cdot S$	$0.73 \cdot S$
$>> 0$	$\frac{SE}{2^{E-1}}$	$\frac{2SE}{\pi\, 2^{E-1}}$

It is concluded then that the sinusoid carriers provide slightly less maximum interference for large E. However, the interference for the sinusoid carriers can introduce an error in the absence of additive noise, when the received asynchronous signal is correlated synchronously with $S_2(t)$.

In order to determine the average probability of error, when correlating with sinusoid $S_i(t)$ in the presence of white Gaussian noise, it is necessary to determine $p(z_i|d_i=+1)$ and then apply (5.11). However, the determination of $p(z_i|d_i=+1)$, for a finite number of carriers, requires the derivation of the pdf of the cross-correlation function between two sinusoids. This derivation appears difficult.

However, as the number of carriers increase without limit, then $p(z_i|d_i=+1)$ approaches a Gaussian distribution with mean S, and variance $\sigma^2_{z_i}$ as derived below.

The variance, $\sigma^2_{\rho^{(f)}_{i\ell}}$ of the "flipped" cross-correlation function between sinusoids $S_i(t)$ and $S_\ell(t)$, is*

$$\sigma^2_{\rho^{(f)}_{i\ell}} = \frac{1}{T} \int_0^T \left[\rho^{(f)}_{i\ell}(\tau_\ell)\right]^2 d\tau_\ell \quad . \tag{5.50}$$

Substituting for $\rho^{(f)}_{i\ell}(\tau_\ell)$, it is seen that

$$\sigma^2_{\rho^{(f)}_{i\ell}} = \frac{4S^2}{\pi^2 T^2 (i^2-\ell^2)} \int_0^T \left[i^2 \sin^2 \ell\,\omega\,\tau_\ell + \ell^2 \sin^2 \ell\,\omega\,\tau_\ell - 2i\ell \sin i\,\omega\,\tau_\ell \cdot \sin \ell\,\omega\,\tau_\ell\right] d\tau_\ell$$

$$= \frac{2S^2}{\pi^2} \cdot \frac{(i^2+\ell^2)}{(i^2-\ell^2)^2} \quad . \tag{5.51}$$

If it is considered that the probability of a "flip" in $S_\ell(t)$ is 1/2, then the variance of the correlation function, $\sigma^2_{i\ell}$, between $S_i(t)$ and $S_\ell(t)$ (considering both "flipped" and "unflipped" cross-correlation) is then

$$\sigma^2_{i\ell} = \frac{1}{2}\,\sigma^2_{\rho^{(f)}_{i\ell}} = \frac{S^2}{\pi^2} \frac{(i^2+\ell^2)}{(i^2-\ell^2)^2} \tag{5.52}$$

Then the variance $\sigma^2_{z_i}$ is

$$\sigma^2_{z_i} = \frac{N_o S}{2T} + \sum_{\text{all } \ell \neq i} \sigma^2_{i\ell} \tag{5.53}$$

---

*Note that τ_ℓ is uniformly distributed over the interval 0-T and the mean of the flipped cross-correlation function is zero.

If we set $i, \ell = 2^F$, $F = 0, 1, \ldots, k-1$, $k \to \infty$, then for $F << k - 1$,

$$\sigma^2_{z_i} = \sigma^2_{z_{2^F}} = \frac{N_o S}{2T} + \frac{S^2}{\pi^2}\left[\sum_{c=1}^{F} \frac{2^{2F} + 2^{2F-2c}}{2^{4F} + 2^{4F-4c} - 2^{4F-2c+1}}\right.$$

$$\left. + \sum_{d=1}^{\infty} \frac{2^{2F+2d} + 2^{2F}}{2^{4F+4d} + 2^{4F} - 2^{4F+2d+1}}\right] . \qquad (5.54)$$

A comparison of the corresponding variances of the Basic Walsh Function Carriers (see 5.32) and the sinusoid carriers (see 5.54) for $E = F + 1 = 1, 2, 3$ and 4, is presented in Table 5.2.

Table 5.2

Values of Corresponding Variances for Basic Walsh Functions and Sinusoids

E	Variance-Walsh	Variance-Sinusoid
1	$0.055 \cdot S^2 + N_o S/2T$	$0.066 \cdot S^2 + N_o S/2T$
2	$0.055 \cdot S^2 + N_o S/2T$	$0.073 \cdot S^2 + N_o S/2T$
3	$0.024 \cdot S^2 + N_o S/2T$	$0.026 \cdot S^2 + N_o S/2T$
4	$0.0087 \cdot S^2 + N_o S/2T$	$0.0081 \cdot S^2 + N_o S/2T$

The average probability of error, given by (5.34) is plotted for sinusoids $S_1(t)$, $S_2(t)$, $S_4(t)$ and $S_8(t)$ in Figure (5.9). Comparing these curves with the corresponding curves of Figure (5.3) it is seen that for $k \to \infty$ the Basic Walsh functions provide a lower probability

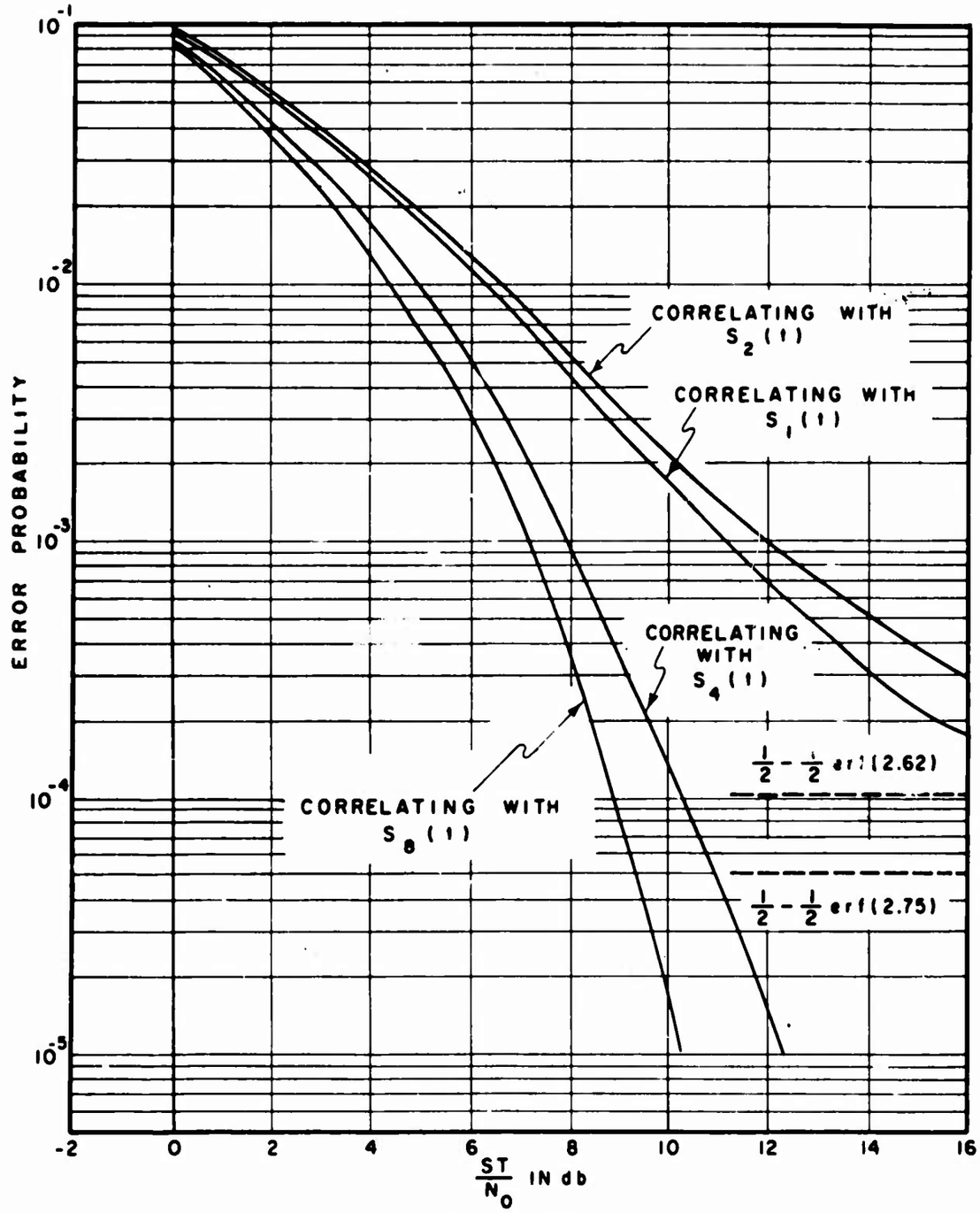


FIG. 5.9.

PROBABILITY OF ERROR (PER BIT) / NOISE POWER DENSITY
CORRELATING WITH SINUSOIDS
$S_1(t)$, $S_2(t)$, $S_4(t)$, $S_8(t)$

of error than the sinusoids for the carrier of longest period, although the error probabilities are approximately equal for the remaining cases.

5.4 Asynchronous Binary Signalling With Random Binary Sequences

In this section the average performance of the binary asynchronous signalling system will be determined, when the carriers are mapped randomly chosen binary sequences. The results will be compared with the results derived in Section 5.2 for the Basic Walsh functions.

The cross-correlation function $\rho_{i\ell}(\lambda_\ell)$ between the mappings of randomly chosen binary sequences S_i and S_ℓ of length L (considering the possibility that S_ℓ is "flipped") will now be determined.

Let $S_i^{(m)}$ and $S_\ell^{(m)}$ be random chosen mapped binary sequences,

$$S_i = \left[a_o^{(i)}, a_1^{(i)}, \ldots, a_{L-1}^{(i)}\right] \quad , \quad S_\ell = \left[a_o^{(\ell)}, a_1^{(\ell)}, \ldots, a_{L-1}^{(\ell)}\right] ,$$

where $a_\sigma^{(i)}, a_\sigma^{(\ell)} = \pm 1, \quad \sigma = 0, 1, \ldots, L-1$, with equal probability and $a_\sigma^{(i)}$ and $a_{\sigma'}^{(\ell)}$ are statistically independent, for $\sigma = \sigma'$, $i \neq \ell$ and for $\sigma \neq \sigma'$, all i and ℓ. Then the cross-correlation function between $S_i^{(m)}$ and $S_\ell^{(m)}$ at a delay of λ_ℓ is

$$\rho_{i\ell}(\lambda_\ell) = \frac{d_\ell^{(1)} S}{L} \sum_{b=o}^{\lambda_\ell - 1} a_b^{(i)} \, a_{L-\lambda_\ell+b}^{(\ell)}$$

$$+ \frac{d_\ell^{(2)} S}{L} \sum_{b=\lambda_\ell}^{L-1} a_b^{(i)} \, a_{L-\lambda_\ell+b}^{(\ell)} \quad , \qquad (5.55)$$

where S is the signal power, $d_\ell^{(1)}$, $d_\ell^{(2)}$ = ±1 with equal probability and $d_\ell^{(1)}$ and $d_\ell^{(2)}$ are statistically independent.*

The mean value of $\rho_{i\ell}(\lambda_\ell)$ is zero. Hence the variance, $\sigma^2_{\rho_{i\ell}}$ is

$$\sigma^2_{\rho_{i\ell}} = \frac{S^2}{L^2} \sum_{b=0}^{\lambda_\ell-1} \sum_{c=0}^{\lambda_\ell-1} \overline{\left[a_b^{(i)}\ a_c^{(i)}\ a_{L-\lambda_\ell+b}^{(\ell)}\ a_{L-\lambda_\ell+c}^{(\ell)}\right]}$$

$$+ \frac{S^2}{L^2} \sum_{b=\lambda_\ell}^{L-1} \sum_{c=\lambda_\ell}^{L-1} \overline{\left[a_b^{(i)}\ a_c^{(i)}\ a_{L-\lambda_\ell+b}^{(\ell)}\ a_{L-\lambda_\ell+c}^{(\ell)}\right]}$$

$$+ \frac{d_\ell^{(1)}\ d_\ell^{(2)}\ S^2}{L^2} \sum_{b=0}^{\lambda_\ell-1} \sum_{c=\lambda_\ell}^{L-1} \overline{\left[a_b^{(i)}\ a_c^{(i)}\ a_{L-\lambda_\ell+b}^{(\ell)}\ a_{L-\lambda_\ell+c}^{(\ell)}\right]} \qquad (5.56)$$

Since the symbols of the carriers were chosen randomly, each of the expectations taken over the ensemble of carrirers, is non-zero only if b = c. Thus $\sigma^2_{\rho_{i\ell}}$ reduces to

$$\sigma^2_{\rho_{i\ell}} = \frac{S^2}{L^2} \sum_{b=0}^{\lambda_\ell-1} \sum_{c=0}^{\lambda_\ell-1} \delta_{bc} + \frac{S^2}{L^2} \sum_{b=\lambda_\ell}^{L-1} \sum_{c=\lambda_\ell}^{L-1} \delta_{bc}$$

$$+ \frac{d_\ell^{(1)}\ d_\ell^{(2)}\ S^2}{L^2} \sum_{b=0}^{\lambda_\ell-1} \sum_{c=\lambda_\ell}^{L-1} \delta_{bc}\ , \qquad (5.57)$$

*It is recalled that if $d_\ell^{(1)}$ and $d_\ell^{(2)}$ are of opposite sign then S_ℓ has "flipped" at a delay of λ_ℓ digits.

where δ_{bc} is the Kronecker delta function. Thus

$$\sigma^2_{\rho_{i\ell}} = \frac{S^2}{L^2}\left[\lambda_\ell + L - \lambda_\ell + o\right] = \frac{S^2}{L} \quad . \tag{5.58}$$

It can be shown that $\rho_{i\ell}(\lambda_\ell)$ is in general binomially distributed, but for large L the binomial distribution approaches Gaussian. The output, z_i of the i^{th} correlator for $L \to \infty$, is then Gaussian distributed with mean $\pm S$, and variance $\sigma^2_{z_i}$,

$$\sigma^2_{z_i} = \frac{N_o S}{2T} + \sum_{\substack{\ell=o \\ \ell \neq i}}^{k-1} \sigma^2_{\rho_{i\ell}} = \frac{N_o S}{2T} + \frac{(k-1)S^2}{L} \quad . \tag{5.59}$$

The average probability of error, $P(e_i)$ is then

$$P(e_i) = \frac{1}{2} - \frac{1}{2}\,\mathrm{erf}\left[\frac{1}{\sqrt{\frac{2(k-1)}{L} + \frac{1}{G}}}\right] \quad . \tag{5.60}$$

Thus, if the ratio of the number of sequences on the channel (k) to sequence length (L) approaches zero as $L \to \infty$, then the average probability of error approaches the binary PSK error probability. Although the Basic Walsh functions provide an average probability of error (averaged over all k carriers) approaching the binary PSK result (for $G = \sqrt{\frac{ST}{N_o}} \leq 3$), only $\log_2 L$ carriers, $L \to \infty$, are used. Equation (5.60) indicates an "average" set of randomly derived mapped binary sequences will provide this error probability although permitting

many more than $\log_2 L$ carriers on the channel.

Some questions have been raised by Wolf and Elspas[37] on the validity of determining the performance of random carriers in the manner specified in this section. The analysis appears to indicate that z_i is Gaussian distributed with known variance $\sigma_{z_i}^2 = \frac{N_o S}{2T} + \frac{(k-1)S^2}{L}$. However, the variance of the interference σ_i^2 due to the presence of the other carriers is not a known factor but a random variable with mean, $\overline{\sigma_i^2} = \frac{(k-1)S^2}{L}$, and variance $\overline{(\sigma_L^2 - \sigma_i^2)^2} = \frac{2(k-1)S^4}{L^2}$. For a large number of carriers on the channel, the fluctuations around the mean of σ_i^2 are small since the ratio of $\left[\overline{(\sigma_i^2 - \overline{\sigma_i^2})^2}\right]^{\frac{1}{2}}$ to $\overline{\sigma_i^2}$ is $[2/(k-1)]^{\frac{1}{2}}$. Thus, we can approximate σ_i^2 by its mean and then the output of the i^{th} correlator is approximately Gaussian.

5.5 Asynchronous Signalling with Linear Error-Correcting Codes

In this section the noiseless channel performance of the asynchronous signalling system with mapped cyclic error-correcting codes as carriers will be determined. The "unflipped" cross-correlation function will be shown to be related to the minimum distance of the code. A bound on the "flipped" cross-correlation function will be related to the solid burst error-correction capability of the code. The theory will then be used to derive the performance of several Bose-Chaudhuri codes, the largest known class of cyclic codes, for the asynchronous application. A brief description of binary cyclic

codes is first given.

A linear code C is called a cyclic code, if for each code word $C_1 = (a_0, a_1, \ldots, a_{L-1})$ in C, the code word $C_2 = (a_{L-1}, a_0, \ldots, a_{L-2})$ is also in C.

Every cyclic code can be generated by a monic polynomial, g(x), in the algebra of polynomials modulo x^L-1, where L is the length of each code word. If g(x) of degree r, divides x^L-1, then g(x) generates a cyclic code of dimension $k' = L - r$. Each of the $2^{k'}$ code words is expressible in the form $g(x)[b_0 \oplus b_1 x \oplus \ldots \oplus b_{k'-1} x^{k'-1}]$ where b_i, $i = 0, 1, \ldots, k'-1$, is either 0 or 1.

It has been shown[24] that each code word can be generated by a k' stage shift register with feedback connections corresponding to the polynomial $h(x) = (x^L-1)/g(x)$, with the proper initial loading. For the asynchronous signalling application we are only interested in code words which are inequivalent under any cyclic permutation. The number of "inequivalent" code words (hereafter designated as root words) in a cyclic code, is related to the cycle set[18] structure of h(x).

A cycle of the polynomial, h(x), is the set of polynomials $x^d h_1(x)$, mod h(x) where $d = 0, 1, \ldots$, and $h_1(x)$ is any polynomial of degree less than the degree of h(x). The length of a cycle is the smallest integer ν, (ν always divides $2^{k'}-1$), such that $x^\nu h_1(x) \equiv h_1(x)$, mod h(x). [The root code word, considered as a periodic sequence, generated by the k' shift register with feedback connections prescribed by h(x) and initial loading corresponding to $x^d h_1(x)$, will have a minimum period or length ν.]

As an example, consider the cycles of the polynomial $h(x) = x^4 + x^3 + x^2 + x + 1$, over GF(2), shown in Table 5.3.

Table 5.3

Cycles of $h(x) = x^4 + x^3 + x^2 + x + 1$

$h_1(x)$	0	1	$x + 1$	$x^3 + 1$
$x\,h_1(x)$	0	x	$x^2 + x$	$x^3 + x^2 + 1$
$x^2h_1(x)$		x^2	$x^3 + x^2$	$x^2 + 1$
$x^3h_1(x)$		x^3	$x^2 + x + 1$	$x^3 + x$
$x^4h_1(x)$		$x^3 + x^2 + x + 1$	$x^3 + x^2 + x$	$x^3 + x + 1$
$x^5h_1(x)$		1	$x + 1$	$x^3 + 1$

From Table 5.3 it is seen that $x^4 + x^3 + x^2 + x + 1$ has 4 cycles (1 of length 1 and 3 of length 5). The cycle set structure is denoted as $1(1) + 3(5)$. From this cycle set analysis it can be determined that the cyclic code of length 15 with generating polynomial $g(x) = (x^{15}-1)/(x^4 + x^3 + x^2 + x + 1) = (x+1)(x^2 + x + 1)(x^4 + x + 1)$ $(x^4 + x^3 + 1)$ has 4 root words, one of which is the all zero code word.

In general, an irreducible polynomial of degree k' will have 1 cycle of length 1 and μ' of length ν', denoted as $1(1) + \mu'(\nu')$, where μ' and ν' are in general difficult to determine. However, if $h(x)$ is a primitive irreducible polynomial of degree k', then $\mu' = 1$ and $\nu' = 2^{k'}-1$. Elspas[18] has shown that a polynomial $h(x)$ which is the product of two different irreducible polynomials, $h_1(x)$ and $h_2(x)$,

with cycle set structures $1(1) + \mu_1(\nu_1)$ and $1(1) + \mu_2(\nu_2)$ respectively, will have a cycle set structure of $1(1) + \mu_1(\nu_1) + \mu_2(\nu_2) + \mu(\nu)$, where

$$\mu = \mu_1 \mu_2 \text{ [G.C.D. } (\nu_1, \nu_2)]$$

$$\nu = \text{L.C.M. } (\nu_1, \nu_2)$$

This technique is easily extended to derive the cycle set structure of a polynomial which is the product of an arbitrary number of different irreducible polynomials.

If the minimum distance of a cyclic code is known then the minimum distance between cyclic shifts of root words is known. However, for binary signalling a root word or its complement is transmitted, and only if the complement of each code word is in the code will the minimum distance between cyclic shifts of any root word and the complement of another root word be known. The following theorem gives the condition for a cyclic code to contain the complement of every code word.

THEOREM 5.2 The complement of every code word of a binary cyclic code, is a code word if the generating polynomial, $g(x)$ does not contain $1 + x$ as a factor.

Proof: Since the code is a linear code the theorem can be established by proving that the all zero and all one code words are in the code. If $1 + x$ is not a factor of $g(x)$, then $1 + x$ is a factor of $h(x) = (x^L-1)/g(x)$. The polynomial $1 + x$ has two cycles of length 1. Hence, by the product rule of cycle sets, $h(x)$ contains two cycles of length 1. However, the lengths of distinct cycles are the lengths of distinct root words, and the only two root words of length 1 are the all zero and all one code words.

It will be shown in the succeeding analysis that the magnitude of the "flipped" cross-correlation between mapped root words can be reduced by using repeated mapped code words[38] as carriers. The following theorem relates to the structure of a repeated cyclic code.

THEOREM 5.3 The code formed by repeating m times each code word of a cyclic code of length L with generating polynomial g(x) is also a cyclic code, but of length m L with generating polynomial

$$g'(x) = \sum_{b=0}^{m-1} x^{bL}\, g(x) \quad .$$

The number of root words in the repeated code is identical to the number in the original code. If the original code had minimum distance d, then the resultant code has minimum distance md.

It will now be shown that the "flipped" cross-correlation function is related to the solid burst error-correction capability of the cyclic code. Consider the "flipped" cross-correlation function $\rho_{i\ell}^{(f)}(\lambda_\ell)$ between the mappings of code words (in polynomial representation) $C_i(x)$ and $C_\ell(x)$ at a shift of λ_ℓ digits. Then $\rho_{i\ell}^{(f)}(\lambda_\ell)$ is determined as

$$\rho_{i\ell}^{(f)}(\lambda_\ell) = \frac{1}{L}[\text{no. of 0's in } A(x) - \text{no. of 1's in } A(x)] \qquad (5.61$$

where

$$A(x) \equiv C_i(x) \oplus x^{\lambda_\ell}\, C_\ell(x) \oplus x^{\lambda_\ell}[1 + x + \ldots + x^{L-1-\lambda_\ell}], \bmod (x^L - 1) \qquad (5.62)$$

Since $C_i(x)$ and $C_\ell(x)$ are the polynomial representations of code words from a cyclic code, A(x) can be reduced to

$$A(x) \equiv C_q(x) \oplus x^{\lambda_\ell}[1 + \ldots + x^{L-1-\lambda_\ell}], \bmod (x^L - 1) \quad , \qquad (5.63)$$

where $C_q(x)$ corresponds to a code word of minimum weight d and maximum weight L - d, provided 1 + x is not a factor of g(x).

It is thus seen that A(x) is formed by adding the polynomial representation of a solid error burst* of length L - λ_1. A theorem on the correction of solid bursts follows.

THEOREM 5.4 A double error correcting cyclic code ($d \geq 5$) can correct all solid bursts that do not "wrap" around the end of the code, provided the generating polynomial g(x) does not contain 1 + x as a factor.

The above theorem is generalized to multiple solid burst error correction by the following theorem.

THEOREM 5.5 A t error correcting cyclic code (t even) can correct all error patterns that consist of t or fewer solid bursts, each starting at the beginning of the code word, provided g(x) does not contain 1 + x as a factor.

Proof: Since the code can correct t or fewer errors, then the error pattern E(x),

$$E(x) = \sum_{f=0}^{t'} \oplus (x + x^{\lambda_f + 1}) \quad , \tag{5.64}$$

where $t' \leq t$

$\lambda_f \leq L - 1$,

is correctable by reducing the received vector E(x) + $C_m(x)$ (in polynomial form), modulo g(x). However, E(x) can be represented as

*A solid error burst[39] is defined as an error burst where every digit in the burst is in error.

$$E(x) = \sum_{f=0}^{t'} \oplus (1 + x)(1 + x + \ldots + x^{\lambda_f}) \qquad (5.65)$$

Since $1 + x$ and $g(x)$ are relatively prime, the error pattern $E'(x)$,

$$E'(x) = \frac{E(x)}{1 + x} = \sum_{f=0}^{t'} \oplus (1 + x + \ldots + x^{\lambda_f}) \qquad (5.66)$$

is correctable, indicating that t or fewer solid bursts starting at the beginning of the code word are correctable.

From the preceding theorem, upper and lower bounds on the weight of a vector formed by adding (mod 2) a solid burst, starting at the beginning of the code word,* to a code word (except the all zero or all one code words) is now derived.

THEOREM 5.6 Consider the vector which is formed by the mod 2 addition of a code word [from a t error-correcting(t even) cyclic code for which $1 + x$ is not a factor of $g(x)$] and a solid burst starting at the beginning of the code word. The minimum and maximum weights of the resultant vector are $\frac{t}{2} + 1$ and $L - \frac{t}{2} - 1$ respectively.

Proof: For t even, it has been shown that t or fewer "beginning" solid bursts are correctable. Hence, the vector, A, corresponding to a code word (which is not the all zero or all one code words)plus t "beginning" solid bursts must be different from the vector corresponding to the all zero code word plus t or less "beginning" solid bursts. However, any

*The bound when a solid burst starts in the middle of a code word and proceeds to the end will be identical to the bound which is derived for the "beginning" solid burst.

vector of weight t/2 can be formed by the proper mod 2 summation of t "beginning" solid bursts. Hence, for A to be different from the all zero code word plus any t or few "beginning" solid bursts, A must have weight at least $\frac{t}{2} + 1$. If the comparison is made with the all one code word, then the maximum weight of A is derived as $L - \frac{t}{2} - 1$.

From the preceding analysis it is now possible to specify the bounds on the "unflipped" and "flipped" cross-correlations for a cyclic code of length L, for which $1 + x$ is not a factor of $g(x)$, with a minimum distance $d = 2t + 1$, t even.

The "unflipped" cross-correlation function is bounded by $\pm \frac{L - 2d}{L}$. From Theorem 5.6 it can be shown that the "flipped" cross-correlation is bounded by $\pm \frac{L - t - 2}{L}$.

For the repeated cyclic code, Theorem 5.3, the "unflipped" cross-correlation is still bounded by $\pm \frac{L - 2d}{L}$. However, the bounds on the "flipped" cross-correlation are lowered when the cyclic code is repeated m times. The maximum absolute value of "flipped" cross-correlation occurs when the relative delay of the code words, λ_ℓ is either $0 \leq \lambda_\ell \leq L$, or $(m - 1)L \leq \lambda_\ell \leq m\,L$. It is then determined that the "flipped" cross-correlation is bounded by

$$\pm \left\{ \frac{(m-1)[L-2d]}{mL} + \frac{1}{mL}[L - t - 2] \right\} .$$

For large values of m, the "flipped" cross-correlation approaches the "unflipped" value.

From the bounds on the "flipped" cross-correlation, the maximum number of carriers which can be asynchronously multiplexed, on a

noiseless channel with zero probability of binary error can be derived. It should be noted if t is odd then t is replaced by t - 1 in all of the cross-correlation bounds.

As an illustrative example consider the (31,11) Bose-Chaudhuri code for which t = 5 and d = 11. The generating polynomial for this code is[40]

$$g(x) = (1+x^2+x^5)(1+x^2+x^3+x^4+x^5)(1+x+x^2+x^4+x^5)(1+x+x^2+x^3+x^5) \quad (5.67)$$

The shift register polynomial is then

$$h(x) = \frac{(x^{31}-1)}{g(x)} = (1+x)(1+x+x^3+x^4+x^5)(1+x^3+x^5) \quad (5.68)$$

The number of root words (not including complements) are the number of cycles of the polynomial h'(x),

$$h'(x) = (1+x+x^3+x^4+x^5)(1+x^3+x^5)$$

Since each of the factors of h'(x) are primitive polynomials, it is immediately apparent that the cycle set structure of h'(x) is

$$1(1) + 1(31) + 1(31) + 31(31)$$

Hence, there are 34 root words in the code.

Under the no "flipping" condition, the bound on the maximum number of carriers is 4. Under the "flipping" condition, the maximum number which can appear is 2. If the repeated code is used with m = 3 (code length = 93) then 3 code words can appear. The code length must be increased to (11)(31) = 341 to enable 4 code words to appear with zero probability of error. In Table 5.4 the bounded asynchronous

performance of several other Bose-Chaudhuri codes, which give the "optimum" performance for the given length, are tabulated.

Table 5.4

Asynchronous Performance of Root Words of Bose-Chaudhuri Codes

Code	t	No. of Root Words	Max. No. for "unflipped" Case	Max. No. for "flipped" Case	Length for 3 Words	Length for 4 Words
(15,7)	2	6	4	2	$3 \cdot 15 = 45$	∞
(31,11)	5	34	4	2	$3 \cdot 31 = 93$	$11 \cdot 31 = 341$
(63,10)	13	10	8	2	$2 \cdot 63 = 126$	$4 \cdot 63 = 252$

The performance characteristics listed in Table 5.4 indicate that the noiseless channel performance of the mapped Bose-Chaudhuri codes is inferior to the performance of the Basic Walsh functions, under the "flipping" condition, in that fewer carriers can appear on the channel with the assurance that the probability of error is zero. However, an advantage of using Bose-Chaudhuri codes is that root words can be chosen which have least period equal to the length of the code. (The Basic Walsh functions do not exhibit this property.) Since the autocorrelation function of the mapped root words is low for non-zero delays (it is bounded by $\pm \frac{L - 2d}{L}$), synchronization of a particular transmitter-receiver pair can be gained.

It should be noted that the bound on the "flipped" cross-correlation is a pessimistic bound. By proper choice of the root words,

the absolute maximum value of "flipped" cross-correlation will be significantly reduced. It was found that by choosing a preferred set of root wrods of the (15,7) code, it was possible to place 3 code words on the channel when the word length was 30, instead of the value of 45 indicated in Table 5.4.

6. HARD LIMITING MULTIPLEXING OF N-ARY SEQUENCES

6.1 Introduction

Titsworth[12,23] has described a binary synchronous multiplex system which is applicable for

a. the transmission of several signals from several different transmitters over the same channel.

b. the simultaneous transmission of messages to several receivers in a single sequence stream.

There are k users on the channel, each using a different binary mapped Basic Walsh function of length 2^k as a carrier. Information is sent by transmitting either the mapping of the sequence itself, or the mapping of the complement sequence. (Hence, 1 bit of information is sent by each carrier in 2^k time slots.) The multiplexing operation is performed by operating on the sum of the k mapped sequences (with the provision that some may be complemented) with a Boolean logic device. The output of the logic device is

a. plus one if there is a majority of plus ones in the k mapped sequences during a particular time slot,

or

b. minus one if there is a majority of minus ones in the k mapped sequences during a particular time slot.

For an equal number of plus ones and minus ones, the output is arbitrary. For k odd, the logic operation can be performed by a hard limiter. (The use of a hard limiter is particularly desirable for multiple access to a satellite[33] because of the nonlinear characteristic of the travelling wave tube usually used for economical transmission.)

The single sequence binary stream is then transmitted to k receivers, which are k filters (or correlators) matched to the k mapped

basis sequence used as initial carriers. The output of a particular correlator is a positive or negative value, depending upon whether a mapped basis sequence or its complement was initially transmitted, independent of the information state of the other carriers.

It will be shown in this chapter that a hard limiting synchronous multiplex system can be designed with N-ary sequences with symbols mapped onto the roots of unity or phase modulated cosine functions. The k (mapped) cyclically N-orthogonal basis sequences, S_{a_o}, S_{a_1}, ... , $S_{a_{k-1}}$, of length N^k are the carriers* to be multiplexed. A mapped sequence or one of its N-1 complements is transmitted. (Hence $\log_2 N$ bits of information are transmitted with each carrier in N^k time slots.) As in the Boolean system, the optimum multiplexing is achieved by a logic device operating on the sum of the components of the carriers.

The output of the logic device, $f(\zeta^{(g)})$ during time slot g, $g = 0, \ldots, N^k-1$, is

a. a unit amplitude vector with a phase angle equal to the angle of the vector which is the linear sum of the components of k carriers (arbitrarily complemented) during the particular time slot, for the roots of unit mapping,

or

b. a unit amplitude cosine function phase modulated by the angle defined in (a) above.

It can be seen that the logic device for the roots of unit mapping acts as a "hard-limiter", provided G.C.D.[N,k] = 1.** The interpretation of the optimum logic for the phase modulated cosine mapping will be discussed

---

* Throughout the remainder of the chapter, the word carrier will be used to indicate a mapped sequence and complement carrier will be used to indicate a mapped complement sequence.

** This provision ensures that the linear sum of the components of the carriers is not zero. The output of the logic device is arbitrary if the sum of the components is zero.

in the succeeding sections.

The receiver which is to decide on the information contained in the i^{th} carrier is

a. A cross-correlator between $f(S_q)$ and S_i mapped onto the roots of unity. The phase of the correlator output determines the decision on which complement of S_i was sent,

or

b. A set of N cross-correlators between $f(S_q)$ and S_i and its N-1 complements all mapped onto phase modulated cosine functions. The correlator which yields the largest output determines the decision on the information contained in the particular carrier.

The complete multiplexed system is shown in Figure 6.1 for roots of unity mapped sequences. In the following sections, the results summarized in this introduction are derived and the system performance is analyzed. For the development of the theory it will be assumed that the N-ary sequences are mapped onto the roots of unity. When allusion is made to real sequences the theory will be appropriately qualified to the phase modulated cosine mapping.

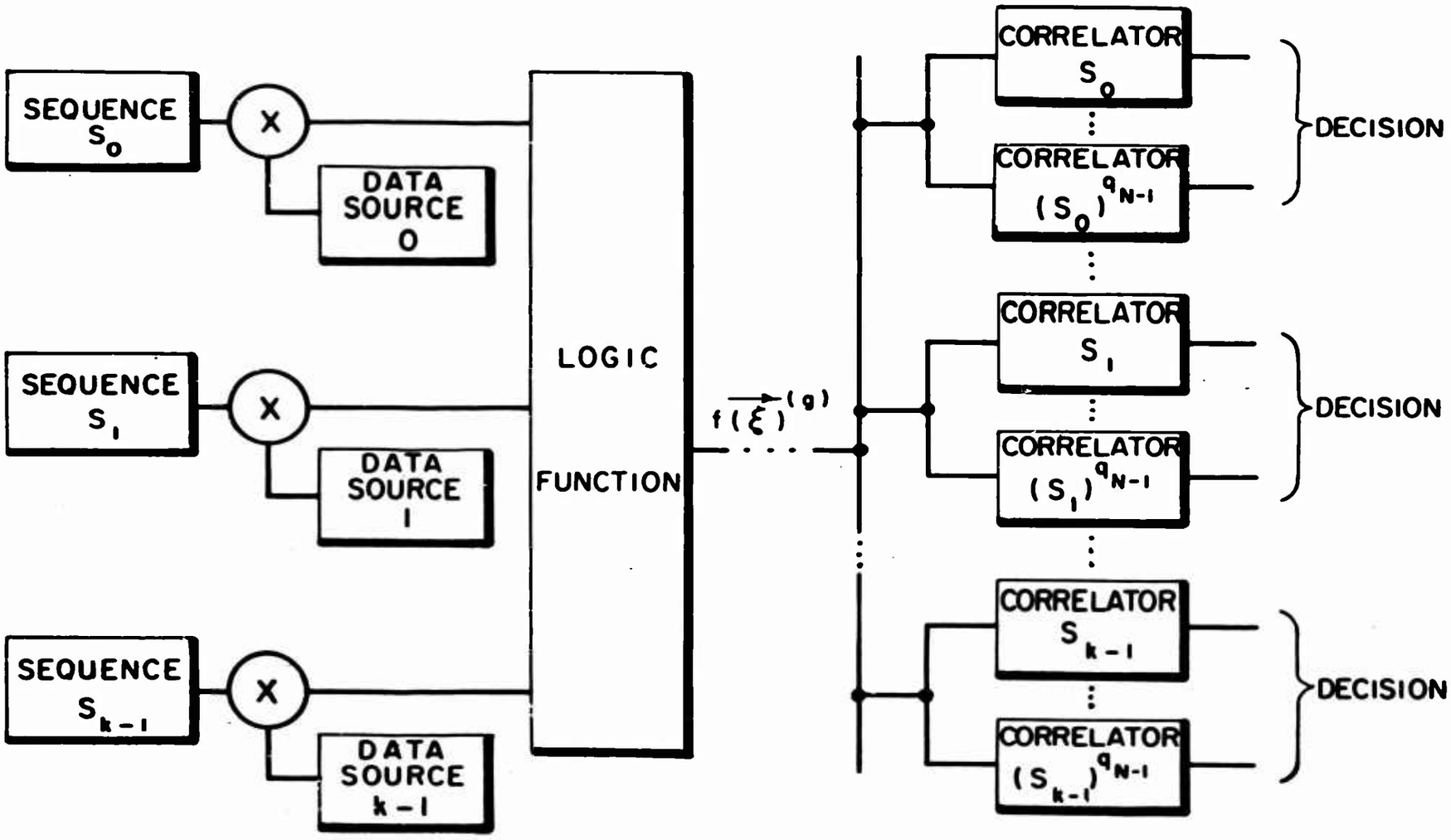
6.2 Transform Analysis of N-ary Sequences

A transform pair will be derived which will be used to evaluate the performance of the multiplexed N-ary system. The transform pair will be shown to relate to the optimum logic function and the magnitude of the correlator output.

Define a function, $\Phi(\vec{s},\vec{x})$ of the vectors

$$\vec{s} = (s_0, s_1, \ldots, s_{k-1}) \ , \ s_i = 0,1, \ldots, N-1 \ ,$$

$$\vec{x} = (x_0, x_1, \ldots, x_{k-1}) \ , \ x_i = 0,1, \ldots, N-1 \ ,$$



F I G . 6 . 1 .

N - ARY MULTIPLEXING SYSTEM

$$\varphi(\vec{s},\vec{x}) = N^{-k/2} \exp[j \frac{2\pi}{N} (s_o x_o + \ldots + s_{k-1} x_{k-1})] \tag{6.1}$$

It is apparent that there are N^k functions $\varphi(\vec{s}_c,\vec{x})$ of $\vec{x}$ for a given vector $\vec{s}_c$. It is easily verified that $\varphi(\vec{s}_c,\vec{x})$ and $\varphi(\vec{s}_d,\vec{x})$ are orthonormal, that is:

$$\sum_{\substack{\text{all} \\ N^k \vec{x}}} \varphi(\vec{s}_c,\vec{x})\ \varphi^*(\vec{s}_d,\vec{x}) = \begin{cases} 0 & c \neq d \\ 1 & c = d \end{cases}, \tag{6.2}$$

where $c,d = 0,1, \ldots, N^k-1$, and $\varphi^*(\vec{s}_d,\vec{x})$ is the complex conjugate of $\varphi(\vec{s}_d,\vec{x})$.

Similarly

$$\sum_{\substack{\text{all} \\ N^k \vec{s}}} \varphi(\vec{s},\vec{x}_e)\ \varphi^*(\vec{s},\vec{x}_f) = \begin{cases} 0 & e \neq f \\ 1 & e = f \end{cases}, \tag{6.3}$$

where $e,f = 0,1, \ldots, N^k-1$.

An interesting transform pair can be derived with function $\varphi(\vec{s},\vec{x})$ as the kernel. Define a function $F(\vec{s})$ by:

$$F(\vec{s}) = N^{-k/2} \sum_{\substack{\text{all} \\ N^k \vec{x}}} f(\vec{x})\ \varphi(\vec{s},\vec{x}) \tag{6.4}$$

where $f(\vec{x})$ is a unit amplitude vector which is a function of the k components of $\vec{x}$.

The inverse transform $f(\vec{x})$ is derived as follows. Consider

$$\sum_{\substack{\text{all} \\ N^k \vec{s}}} F(\vec{s})\, \varphi^*(\vec{s},\vec{x}_f) = N^{-k/2} \sum_{\substack{\text{all} \\ \vec{x}_e}} \sum_{\substack{\text{all} \\ \vec{s}}} f(\vec{x}_e)\, \varphi(\vec{s},\vec{x}_e)\, \varphi^*(\vec{s},\vec{x}_f)$$

$$= N^{-k/2} \sum_{\substack{\text{all} \\ \vec{x}_e}} f(\vec{x}_e) \sum_{\substack{\text{all} \\ \vec{s}}} \varphi(\vec{s},\vec{x}_e)\, \varphi^*(\vec{s},\vec{x}_f) \quad .$$

Applying the orthonormal property (6.3) it is seen that

$$\sum_{\substack{\text{all} \\ N^k \vec{s}}} F(\vec{s})\, \varphi^*(\vec{s},\vec{x}_f) = N^{-k/2}\, f(\vec{x}_f) \quad ,$$

or

$$f(\vec{x}) = N^{k/2} \sum_{\substack{\text{all} \\ \vec{s}}} F(\vec{s})\, \varphi^*(\vec{s},\vec{x}) \quad . \tag{6.5}$$

The equivalent to Parseval's formula is derived as

$$\sum_{\substack{\text{all} \\ \vec{s}}} F(\vec{s})\, F^*(\vec{s}) = \sum_{\substack{\text{all} \\ \vec{x}}} f(\vec{x})\, f^*(\vec{x}) = 1 \tag{6.6}$$

6.3 Derivation of the Optimum Logic and Correlator Output

Consider the multiplexing of k N-ary sequences, S_0, S_1, ... , S_{k-1} (at present arbitrary) of length N^k, mapped onto the N^{th} complex roots of unity. Then if the N-ary sequence S_i has components,+

+Note the change in notation from the definition of a sequence given in Chapter 2.

$S_i = \left(\xi_i^{(0)}, \xi_i^{(1)}, \ldots, \xi_i^{(N^k-1)}\right)$ then the component of the mapping of S_i during time slot g, $g = 0,1, \ldots, N^k-1$, is $S_i^{(g)} = \exp [j2\pi \xi_i^{(g)}/N]$. The output of the logic network during time slot g will be denoted as $f(\vec{\xi}^{(g)})$. It is clear that $f(\vec{\xi}^{(g)})$ is strictly a function of $\left(\xi_0^{(g)}, \ldots, \xi_{k-1}^{(g)}\right)$, the symbols of each of the k sequences during time slot g.

A set of sequences, S_i, will now be specified and the result of cross-correlating $f(\vec{\xi}^{(g)})$ (for all g) with the mapping of a particular sequence will be determined. Choose the k sequences to be the set of k cyclically N-orthogonal basis sequences of the N^k N-orthogonal sequences of length N^k. Thus, in the notation of Chapter 4, we have $S_0 = S_{a_0}, \ldots, S_{k-1} = S_{a_{k-1}}$, with a typical sequence

$$S_i = S_{a_i} = (\underbrace{0,0, \ldots, 0}_{N^i}, \underbrace{N-1, \ldots, N-1}_{N^i}, \ldots, \underbrace{1, \ldots 1}_{N^i},) ,$$

repeated N^{k-i-1} times. (6.7)

At the receiver, let ρ_{fa_i} be the cross-correlation of $f(\vec{\xi}^{(g)})$ and the mapping of S_{a_i}. Thus, ρ_{fa_i} becomes

$$\rho_{fa_i} = \frac{1}{N^k} \sum_{g=0}^{N^k-1} f(\vec{\xi}^{(g)}) \exp [-j2\pi \xi_i^{(g)}/N] . \quad (6.8)$$

Noting that $f(\vec{\xi}_i^{(g)})$ is given by

$$f(\vec{\xi}_i^{(g)}) = N^{k/2} \sum_{\text{all } \vec{s}} F(\vec{s}) \varphi^*(\vec{s}, \vec{\xi}_i^{(g)})$$

$$= \sum_{\substack{\text{all} \\ \vec{s}}} F(\vec{s}) \exp\left[-j\frac{2\pi}{N}(s_o\, \xi_o^{(g)} + s_1\, \xi_1^{(g)} + \ldots + s_{k-1}\, \xi_{k-1}^{(g)})\right], \qquad (6.9)$$

ρ_{fa_i} is found to be

$$\rho_{fa_i} = \frac{1}{N^k} \sum_{\substack{\text{all} \\ \vec{s}}} F(\vec{s}) \sum_{g=o}^{N^k-1} \exp\left[-j\frac{2\pi}{N}(s_o\, \xi_o^{(g)} + \ldots + (s_i+1)\, \xi_i^{(g)} + \ldots + s_{k-1}\, \xi_{k-1}^{(g)})\right] \qquad (6.10)$$

Now define a vector, $\vec{v}_i$, in the $\vec{s}$ space as

$$\vec{v}_i = (0, \ldots, N-1, \ldots, 0)$$

where the only non-zero term occurs in the i^{th} place. Hence, the expression for ρ_{fa_i} can be reduced to

$$\rho_{fa_i} = F(\vec{v}_i) + \frac{1}{N^k} \sum_{\substack{\text{all} \\ \vec{s} \neq \vec{v}_i}} F(\vec{s}) \sum_{g=o}^{N^k-1} \exp\left[-j\,\frac{2\pi}{N}(s_o \xi_o^{(g)} + \right.$$

$$\left. \ldots + (s_i+1)\, \xi_i^{(g)} + \ldots + s_{k-1}\, \xi_{k-1}^{(g)})\right], \qquad (6.11)$$

where

$$F(\vec{v}_i) = N^{-k/2} \sum_{\substack{\text{all} \\ N^k \vec{x}}} f(\vec{x})\, \varphi(\vec{v}_i, \vec{x})$$

However, if the sequences are chosen as the k cyclically N-orthogonal

basis sequences with components given by (6.7) then

$$\sum_{g=0}^{N^k-1} \exp\left[-j \frac{2\pi}{N}(s_o\, \xi_o^{(g)} + \ldots + (s_i+1)\, \xi_i^{(g)} + \ldots + \xi_{k-1}^{(g)})\right] = 0$$

since for all $\vec{s} \neq \vec{v}_i$, the symbols

$$s_o\, \xi_o^{(g)} + \ldots + (s_i+1)\, \xi_i^{(g)} + \ldots + s_{k-1}\, \xi_{k-1}^{(g)}, \text{ mod } N,$$

for $g = 0, \ldots, N^k-1$ are the N^k symbols of one of the N^k N-orthogonal sequences.

Thus, the value of the correlator output for the k cyclically N-orthogonal sequences is

$$\rho_{fa_i} = F(\vec{v}_i) \tag{6.12}$$

The value of the correlator output will now be derived if the mapping of the r^{th} ($r=1, \ldots, N-1$) complement of S_{a_i} is multiplexed instead of S_{a_i}. Then, $\xi_i^{(g)}$ is replaced by $\xi_i^{(g)}-r$ in Equation (6.7). Also under the condition, the r^{th} complement is transmitted the expression for $f(\vec{\xi}^{(g)})$, Equation (6.9) is changed to $[f(\vec{\xi}^{(g)})]_r$,

$$[f(\vec{\xi}^{(g)})]_r = \sum_{\substack{\text{all} \\ \vec{s}}} F(\vec{s}) \exp\left[-j \frac{2\pi}{N}(s_o\, \xi_o^{(g)} + \ldots + s_i\, \xi_i^{(g)} - s_i r\, \xi_i^{(g)} + \right.$$

$$\left. \ldots + s_{k-1}\, \xi_{k-1}^{(g)})\right] . \tag{6.13}$$

Then repeating the operations defined by Equations (6.10) and (6.11) with the substitution $[f(\vec{\xi}^{(g)})]_r$ in place of $f(\vec{\xi}^{(g)})$, the output of the

i^{th} correlator, $[\rho_{fa_i}]_r$, under the condition that the r^{th} complement was transmitted is

$$[\rho_{fa_i}]_r = \rho_{fa_i} \exp[-j\, 2\pi\, r/N] \,. \tag{6.14}$$

It is noted then that the information carried by the i^{th} carrier is determined uniquely by the phase of the correlator output, independent of the information content of the other k-1 carriers. The contribution of the i^{th} sequence to the total output is then maximized by maximizing the value of $F(\vec{v}_i)$ over all possible logic functions, $f(\vec{x})$, under the condition that the k cyclically N-orthogonal sequences are used. However, it can be shown that for any set of input sequences, $F(\vec{v}_i)$ should be maximized to maximize the contribution of the i^{th} input independent of the condition of the other inputs.*

Now it is necessary to determine the logic function $f(\vec{x})$ which maximizes $F(\vec{v}_i)$, where $f(\vec{x})$ is specified as a unit amplitude complex vector. If we assume that the magnitude of the outputs from all correlators is to be identical, then $F(\vec{v}_i) = F(\vec{v}_{i'})$, for all i, i'. We can then set

$$F(\vec{v}_i) = \frac{1}{k} \sum_{i=o}^{k-1} F(\vec{v}_i) = \frac{N^{-k}}{k} \sum_{i=o}^{k-1} \sum_{\substack{\text{all} \\ \vec{x}}} f(\vec{x}) \exp[-j\, \frac{2\pi}{N}\, x_i]$$

or

$$F(\vec{v}_i) = \frac{N^{-k}}{k} \sum_{\substack{\text{all} \\ \vec{x}}} f(\vec{x}) \sum_{i=o}^{k-1} \exp[-j\, \frac{2\pi}{N}\, x_i] \tag{6.15}$$

*The proof is similar to the proof for the Boolean multiplexed system[23] and hence is omitted.

Now the x_i's, i = o, ... , k-1 are the symbols of each of the k multiplexed sequences during a particular time slot. Hence $\sum_{i=o}^{k-1} \exp[-j \frac{2\pi}{N} x_i]$ is a complex vector which is the sum of the mapped symbols of the k sequences during the time slot. Thus, $F(\vec{v}_i)$ is maximized if for all N^k values of $\vec{x}$ the complex vectors $f(\vec{x}) \sum_{i=o}^{k-1} \exp[-j \frac{2\pi}{N} x_i]$ all have the same phase angle. If the phase angle of $F(\vec{v}_i)$ is to be zero (this is an arbitrary, but practical choice), then $F(\vec{v}_i)$ is maximized if $f(\vec{x})$ is a vector (unit amplitude) with a phase angle equal to the negative of the phase angle of $\sum_{i=o}^{k-1} \exp[-j \frac{2\pi}{N} x_i]$. Thus, the optimum logic can be interpreted as a hard limiter on the sum of the complex components of the input mapped sequences, so that the output vectors of the logic network during each time slot are all of unit amplitude. If $\sum_{i=o}^{k-1} \exp(j \frac{2\pi}{N} x_i) = 0$, which can only result if G.C.D. [N,k] $\neq$ 1, then $f(\vec{x})$ can be chosen to be any unit amplitude vector since there is no contribution to the maximality of $F(\vec{v}_i)$.

It is of interest to note the nature of the optimum logic network under the condition that phase modulated cosine functions are used as a mapping instead of the N^{th} roots of unity. From the discussion in Chapter 2 on the relationship between the correlation function with cosine function and roots of unity signalling, it can be seen that the output of the logic network $[f(\vec{x})]_{cos}$ which maximizes the correlator outputs for cosine function signalling is

$$[f(\vec{x})]_{cos} = \cos(\omega t + \theta_L) \quad , \tag{6.16}$$

where θ_L is the phase angle of $\sum_{i=o}^{k-1} \exp(j \frac{2\pi}{N} x_i)$. However, θ_L can be

written as

$$\theta_L = \tan^{-1} \frac{\sum_{i=o}^{k-1} \sin\left(\frac{2\pi}{N} x_i\right)}{\sum_{i=o}^{k-1} \cos\left(\frac{2\pi}{N} x_i\right)} \quad . \tag{6.17}$$

Substituting (6.17) in (6.16), and expanding $\cos(\omega t + \theta_L)$, $[f(\vec{x})]_{\cos}$ becomes

$$[f(\vec{x})]_{\cos} = \frac{1}{\sqrt{\left[\sum_{i=o}^{k-1} \cos \frac{2\pi}{N} x_i\right]^2 + \left[\sum_{i=o}^{k-1} \sin \frac{2\pi}{N} x_i\right]^2}} \sum_{i=o}^{k-1} \cos \frac{2\pi}{N} x_i \cos \omega t$$

$$+ \sum_{i=o}^{k-1} \sin \frac{2\pi}{N} x_i \sin \omega t$$

$$= \frac{1}{\sqrt{\left[\sum_{i=o}^{k-1} \cos \frac{2\pi}{N} x_i\right]^2 + \left[\sum_{i=o}^{k-1} \sin \frac{2\pi}{N} x_i\right]^2}} \sum_{i=o}^{k-1} \cos\left(\omega t + \frac{2\pi}{N} x_i\right) \tag{6.18}$$

Thus the optimum output of the logic network, under the cosine function mapping, is proportional to the linear sum of the mapped components of the sequences during a particular time slot. Then the optimum logic for this condition can also be interpreted as a hard limiter. The instrumentation of the logic can either be an "infinitely" fast acting AGC,

or a bandpass limiter.

For either mapping it has been shown that the value of $F(\vec{v}_i)$ (which is the correlator output when the cyclically N-orthogonal sequences are used), specifies the system performance. It is seen from (6.15) that $F(\vec{v}_i)$ is a function of N and k. Values of $F(\vec{v}_i)$ for N = 2,3,4 and several values of k are given in Table 6.1. The values for N = 2 are taken from Titsworth's papers.

Table 6.1

Values of $F(\vec{v}_i)$

k	N = 2	N = 3	N = 4
1	1	1	1
2	0.5	0.667	0.604
3	0.5	0.496	0.684
4	0.375	0.455	0.439
5	0.375	0.405	0.404
6	0.312	0.358	0.362
7	0.312	0.340	

It has been noted previously that there is no crosstalk in the reception of the information in the i^{th} carrier due to the complementing of the other signals on the channel. However, from Table 6.1 it is noted that the correlator output (normalized) decreases as the number of users increases, resulting in an effective

decrease in the signal to noise ratio. The loss in signal to noise ratio due to the hard limiting appears to be lower for non-binary signalling. An interesting comparison can be made between the performance for N = 2 and N = 4. It has been shown[21] that the probability of error per bit of information is lower for N = 4 than for N = 2 when the symbols for N = 4 are mapped onto phase modulated cosine functions. Since the signal to noise ratio loss due to hard limiting is lower for N = 4, it is apparent that significant improvement in multiplexed performance is obtainable by using quaternary encoding instead of binary encoding.

7. SUMMARY AND CONCLUSIONS

7.1 Summary of Major Results

The major objectives of the thesis were

a. The synthesis of new classes of periodic sequences, with binary and non-binary symbols, which exhibit useful autocorrelation and cross-correlation properties, when the symbols are appropriately mapped.

b. The analysis of two types of multiple-access systems using, as carriers, these sequences along with some known classes of sequences.

In Chapter 3 the method of interleaving two level binary sequences was analyzed as a method for synthesizing large classes of sequences with prescribed correlation properties. A large class of almost two-level sequences with low cyclic cross-correlation function was synthesized. These sequences are applicable for synchronization, some asynchronous carrier systems or as a set of non-linear error-correcting codes with good data rates. A class of sequences exhibiting autocorrelation functions with intermediate minor peaks all of different amplitude and cyclic cross-correlation functions which are uniformly low was synthesized. These sequences are applicable for synchronization under high signal to noise conditions and also as carriers for the asynchronous multiplexing system. It was shown that some classes of interleaved sequences are easily generated by a non-linear filtering technique.

In Chapter 4 classes of binary and N-ary sequences which are cyclically orthogonal (orthogonal for all cyclic shifts) were derived. A set of binary cyclically orthogonal sequences are the k basis sequences, (re-

ferred to as the Basic Walsh functions) for the set of 2^k Walsh functions. All of the classes of binary cyclically orthogonal sequences derived, contained sequences all of different least period. It is conjectured that binary cyclically orthogonal sequences of the same least period do not exist. This conjecture was discussed by noting the Fourier components of mapped binary sequences.

In Chapter 5 the problem of multiplexing, on a linear channel with additive white Gaussian noise, the carriers from k different transmitter-receiver pairs, when each transmitter is synchronous with its corresponding receiver, although the various transmitter-receiver pairs are asynchronous with each other, was analyzed. Information is transmitted by sending a carrier or its negative. It was shown that the average binary error probability when the k carriers are a set of mapped randomly chosen binary sequences, reduces to the binary PSK formula when the ratio of number of sequences to sequence length is zero as the sequence length becomes unbounded. The average probability of error when the carriers are mapped Basic Walsh functions was derived, and it was shown that the result is a function of the particular sequence assigned to a user, and the number of users sharing the channel. The average probability of error, averaged over all of the cariers, approaches the PSK formula as the number of users (and of course the sequence length) becomes unbounded. However, only $\log_2 L$ (with $L \to \infty$) users, can be present when the carriers are mapped Basic Walsh functions, while a greater number can be present if mapped random binary sequences are used. The average probability of error was computed when the carriers are a set of sinusoids of periods comparable to the

periods of the Basic Walsh functions. The average probability of error was higher for the sinusoid carriers.

A set of mapped Bose-Chaudhuri error-correcting codes was considered as carriers. The noiseless channel performance of these carriers appeared to be significantly worse than the performance of the Basic Walsh functions.

Chapter 6 dealt with the "hard-limiting" multiplexing, prior to transmission, of a set of mapped N-ary sequences, with all carriers synchronous. Information is transmitted by sending the mapping of a sequence or one of the N-1 complements. The optimum set of sequences were the k cyclically N-orthogonal sequences of length N^k derived in Chapter 4. It was shown that the signal to noise ratio degradation due to "hard-limiting" multiplexing was lower for N=3 and 4 than for the binary case.

7.2 Problems Yet to Be Solved

In this section a number of unsolved problems suggested by the research described in this thesis are listed.

a. The synthesis of two-level N-ary sequences for both mappings presented in Chapter 2.

b. A listing of all of the autocorrelation functions which arbitrarily interleaved two-level sequences can exhibit.

c. A search for large classes of sequences (binary and N-ary) which exhibit good cyclic cross-correlation properties, besides the Bose-Chaudhuri codes, interleaved sequences and cyclically orthogonal sequences considered in the thesis. It appears that the technique of choosing

sequences with distinct Fourier components will be useful for the synthesis of binary sequences.

d. Investigation of cyclically orthogonal binary sequences of the same least period.

e. Additional searching for sequences for the asynchronous linear multiplexing system which provide performance comparable to the set of "average" randomly chosen sequences. The computer derivation of the "flipped" cross-correlation function of mapped Bose-Chaudhuri codes, and the interleaved sequences considered in Chapter 3, might indicate that these carriers are applicable for this system.

f. An analysis of the asynchronous linear multiplexing of mapped non-binary sequences, with a mapped sequence or complement sequence sent as information.

g. Derivation of sequences for an asynchronous "hard-limiting" multiplexing system.

7.3 Relationship Between Thesis Problems and Prior Work

In this section the problems, results and proofs presented in this thesis are related to the prior work which has appeared in the literature.

In Chapter 2 the concept of the N-1 complement sequences of an N-ary sequence was introduced. Although the existence of complement sequences has been "hinted" at in the literature,[21] the technique of signalling with mapped complement sequences has not been analyzed to the extent that binary signalling has. The proof of the shift and add property

of p-nary maximal length sequences and the derivation of the autocorrelation function of the maximal length sequences with symbols mapped to -1, 0, +1 has not appeared previously. The shift and subtract property is probably known.

The analysis of the correlation functions of mapped interleaved two-level sequences, presented in Chapter 4, appears to be a problem which has not been previoulsy solved. Interleaving has been used previously for the derivation of large classes of error-correcting codes[29] and the product "almost" two-level sequences which Titsworth has derived are recognized as interleaved complement sequences. The large class of "almost" two-level sequences and "different" peak sequences derived in Chapter 4 were not previously known. The non-linear filtering technique as a method for generating certain classes of interleaved sequences is an extension of the work of Raphael.[19]

It is probable that the cyclically-orthogonal property of the Basic Walsh functions is known. However, the general techniques for the synthesis of cyclically N-orthogonal sequences, presented in Chapter 4, have not appeared previously in the literature. No work has appeared on the Fourier analysis of binary sequences or on the existence of cyclically orthogonal binary sequences of the same least period. The results presented on the generalized Hadamard matrices are probably known.

Although a significant effort has been directed towards the solution of the multiple access problem,[33] the problem of the binary asynchronous linear multiplexing of carriers has not been previously considered.

The technique used for the asymptotic series approximation to the probability of error integral for the Basic Walsh functions was suggested by the work on a similar integral.[35,36] The derivation of the asynchronous performance of the random sequences is similar to a derivation of the performance for a synchronous system.[37]

The transform analysis of N-ary sequences, presented in Chapter 6, utilized in the derivation of the "hard-limiting" performance of N-ary sequences mapped onto the roots of unity is an extension of the work of Titsworth.[12,23]

APPENDIX A: Proof of Theorem 2.2

The normalized autocorrelation, $\rho_A(\lambda)$ was defined in Section 2 as

$$\rho_A(\lambda) = \frac{1}{L} \sum_{i=0}^{L} a_i^{(m)} (b_{i-\lambda}^{m})^* \quad . \tag{A.1}$$

For the mapping, $0 \rightarrow 0$, $1 \rightarrow 1$, $2 \rightarrow -1$ of the ternary maximal length sequence, Equation (A.1) is formed by the sum of products of the form, $0 \cdot 0$, $1 \cdot 1$, $(-1) \cdot (-1)$. However, since there are 3^{r-1} 2's and 3^{r-1} 1's in a ternary maximal length sequence it is seen that

$$\rho_A(0) = \frac{2 \cdot 3^{r-1}}{L} = \frac{2 \cdot 3^{r-1}}{(3^r-1)} \quad .$$

From Theorem 2.1 it is noted that the mod 3 sum of the maximal length sequence and the maximal length sequence shifted by L/2 digits, yields the all zero sequence. Hence, for $\lambda = L/2$, Equation (A.1) is formed by the sum of products of a mapped symbol and its mapped additive inverse. The products appearing are $1 \cdot (-1)$, $(-1) \cdot 1$, $0 \cdot 0$ resulting in

$$\rho_A\left(\frac{L}{2}\right) = \frac{-2 \cdot 3^{r-1}}{L} \quad .$$

The result for the remaining integral shifts will now be proven. It is noted if any two ternary sequences are summed, (mod 3), there are three sub-sums which generate each of the three symbols in the resultant sequence. These sub-sums are

$$\left.\begin{matrix} 0+1 \\ 1+0 \\ 2+2 \end{matrix}\right\} = 1 \qquad \left.\begin{matrix} 1+1 \\ 0+2 \\ 2+0 \end{matrix}\right\} = 2 \qquad \left.\begin{matrix} 2+1 \\ 1+2 \\ 0+0 \end{matrix}\right\} = 0 \quad .$$

It will now be established that if a ternary maximal length sequence is summed with a shifted version of itself (except for shifts of 0, L/2), each of these sub-sums will occur 3^{r-2} times, except the last sum, (0+0) which will occur $3^{r-2} - 1$ times. Once this is established, it will be clear that $\rho_A(\lambda) = 0$, $\lambda \neq 0, L/2$.

Write the original maximal length sequence, and its first (r-1) cyclic shifts as the row vectors of an r x L matrix M.

$$M = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{L-1} \\ a_{L-1} & a_0 & a_1 & \cdots & a_{L-2} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{L-r+1} & a_{L-r+2} & a_{L-r+3} & \cdots & a_{L-r} \end{bmatrix}$$

The row space of M is a basis for the L cyclic shifts of the original sequence, where the vector generated by twice the first row is the sequence shifted by L/2 digits.

From the characteristic of the maximal length sequence, the $L = 3^r - 1$ columns of M are the $3^r - 1$ nonzero r-tuples over GF(3). Hence, if we consider the corresponding elements of row 1 and any other row as forming L 2-tuples, it is clear that in this set of L 2-tuples, each of the 9 possible 2-tuples over GF(3) will occur 3^{r-2} times except (0,0) which will occur $3^{r-2} - 1$ times. Thus the result is established for $\lambda = 1, \ldots, r-1$.

Next, form a new matrix M', of the form

$$M' = \begin{bmatrix} \overbrace{0\ 0 \quad \ldots \quad 0}^{(L+1)/3} & \overbrace{1\ 1 \quad \ldots \quad 1}^{(L+1)/3} & \overbrace{2\ 2 \quad \ldots \quad 2}^{(L+1)/3} \\ \underbrace{0\ 0\ 0}_{(L+1)/9}\ \underbrace{1\ \ldots\ 1}_{(L+1)/9}\ 2\ \ldots\ 2 & 0\ 0 \quad \ldots \quad 2\ 2 & 0\ 0 \quad \ldots \quad 2\ 2 \\ 0\ 1\ 2 \quad \ldots \quad 2 & 0\ 1\ 2\ \ldots\ 2 & 0\ 1\ 2\ \ldots\ 2 \end{bmatrix}$$

by permutation of the rows and columns of M, and the addition of a column containing all zeros. It is apparent that M' can be formed from the characteristic of the maximal length sequence. Replace any row of M', except the first row, by a vector, V, which is any linear combination of the r rows except twice the first row. If the vector is viewed as divided into 3 segments - the first (L+1)/3 symbols, the second (L+1)/3 symbols and the last (L+1)/3 symbols - then each of these segments will contain (L+1)/9 ones, (L+1)/9 twos, and (L+1)/9 zeros. Thus in the set of (L+1) 2-tuples which are formed by taking corresponding elements of row 1 and V, each of the 9 possible 2-tuples over GF(3) occurs 3^{r-2} times. Discarding one of the (0,0) 2-tuples, which results from the addition of the all zero column in M', it is seen that the 9 possible sub-sums, resulting from the summing of a maximal length ternary with any shifted version of the sequence, (except L/2), occur 3^{r-2} times except the 0 + 0 sub-sum which occurs $3^{r-2} - 1$ times. Hence Equation (A.1), for the mapped sequence, reduces to

$$\rho_A(\lambda)_{\lambda \neq 0, L/2} = \frac{3^{r-2}}{L}\left[1 \cdot 1 + (-1)\cdot(-1) + (-1)\cdot 1 + 1\cdot(-1)\right] = 0 \quad .$$

APPENDIX B: Proof that Every 2-Fold Interleaved Sequence Can Be Generated by Multiple Nonlinear Filtering

For n = 2, the output sequence of the multiple nonlinear filter, in polynomial representation, reduces to

$$S_{oT}(x) \equiv x^{2\gamma_o}[a_o(x^2) \oplus x^{2(\gamma_1+1-\gamma_o)}a_1(x^2)] + x^{2\gamma_o+1}[a_o(x^2) \oplus x^{2(\gamma_1-\gamma_o)}a_1(x^2)] \text{ , mod } (x^{2L}-1) \text{ .} \tag{B.1}$$

In order to simplify (B.1), let $\gamma_1' = \gamma_1 - \gamma_o$. Then $S_{oT}(x)$ becomes

$$S_{oT}(x) \equiv x^{2\gamma_o}[a_o(x^2) \oplus x^{2(\gamma_1'+1)}a_1(x^2)] + x^{2\gamma_o+1}[a_o(x^2) \oplus x^{2(\gamma_1')}a_1(x^2)] \text{ , mod } (x^{2L}-1) \text{ .} \tag{B.2}$$

It will now be shown that each of the states of the filter generates a different output interleaved sequence. Since there are as many filter states as interleaved sequences, the proof will be complete. The following cases will be considered for γ_o, γ_1', $a_o(x)$, $a_1(x)$.

Case a. $a_o(x) = 0(x)$, $a_1(x) = 0(x)$. Then $S_{oT}(x) = 0(x^2) + x0(x^2)$, indicating that the output sequence is the all zero sequence.

Case b. $a_o(x) = 0(x)$, $a_1(x) = h_m(x)$. Then $S_{oT}(x) \equiv x^{2b}h(x^2) + x^{2(b-1)}h_m(x^2)$, mod $(x^{2L}-1)$, where $b = \gamma_o + \gamma_1' + 1$, where $b = 0,1, \ldots, L-1$. The interleaved sequences for different values of γ_1 are all different,* and for no value of γ_1 can the all zero sequence of Case (a) result.

*The result is independent of γ_o since sw_o is open ($b = \gamma_o+\gamma_1'+1 = \gamma_1+1$).

Case c. $a_0(x) = h_m(x)$, $a_1(x) = 0(x)$. Then

$$S_{oT}(x) \equiv x^{2c}h_m(x^2) + x^{2c+1}h_m(x^2) \ , \ \mathrm{mod}\ (x^{2L}-1) \ ,$$

where $c = \gamma_o$, $c = 0,1, \ldots, L-1$. The interleaved sequences for different values of γ_o are all different, and for no values of γ_o can the sequences of Cases (a) or (b) result.

Case d. $a_0(x) = h_m(x)$, $a_1(x) = h_m(x)$. Then

$$\begin{aligned} S_{oT}(x) \equiv\ & x^{2[\gamma_o+I(\gamma_1'+1)]}h_m(x^2) \\ & + x^{2[\gamma_o+I(\gamma_1')]+1}h_m(x^2) \ , \ \mathrm{mod}\ (x^{2L}-1) \end{aligned} \tag{B.3}$$

It is clear that this polynomial cannot reduce to the polynomial represented in Case (a). In order to establish that Case (b) cannot result, it is necessary to demonstrate that

$$\gamma_o + I(\gamma_1'+1) \neq \gamma_o + I(\gamma_1') + 1 \ ,$$

or equivalently that,

$$I(\gamma_1'+1) \neq I(\gamma_1') + 1$$

The properties of the function $I(\lambda)$ defined by (2.8) will now be used. From (2.8) we know that

$$x^{I(\gamma_1'+1)}h_m(x) \equiv h_m(x) \oplus x^{\gamma_1+1}h_m(x) \ , \ \mathrm{mod}\ (x^L-1) \ ,$$

and

$$x^{I(\gamma_1')+1}h_m(x) \equiv xh_m(x) \oplus x^{\gamma_1+1}h_m(x) \ , \ \mathrm{mod}\ (x^L-1) \ .$$

However, from the uniqueness of the shift and add property it is clear

that $x^{I(\gamma_1'+1)}h_m(x) \not\equiv x^{I(\gamma_1')+1}h_m(x)$, mod (x^L-1) indicating that $I(\gamma_1'+1) \neq I(\gamma_1'+1)$.

In order to show that Case (c) cannot result from Equation (B.3) it is only necessary to indicate, because of uniqueness, that $I(\gamma_1'+1) \neq I(\gamma_1')$.

As a final step it will be shown that the L^2 different combinations of γ_0 and γ_1, in (B.3) each generate different interleaved sequences.

For $\gamma_1' = L-1$, $S_{oT}(x)$ reduces to

$$S_{oT}(x) \equiv 0(x^2) + x^{2[\gamma_0+I(L-1)]+1}\, h_m(x^2) \ , \text{ mod } (x^{2L}-1) \ ,$$

which, for the L values of γ_0, represents all cyclic shifts of the maximal length sequence in the "second" position and the all zero sequence in the "first" position.

For $\gamma_1' = 0$, $S_{oT}(x)$ reduces to

$$S_{oT}(x) \equiv x^{2[\gamma_0+I(1)]}h_m(x^2) + x0(x^2) \ , \text{ mod } (x^{2L}-1) \ ,$$

which represents, for the L values of γ_0, all cyclic shifts of the maximal length sequence in the "first" position and the all zero sequence in the "second position.

For $\gamma_1' \neq 0$, L-1 the output sequence S_{oT} is an interleaving of shifted maximal length sequences. In order to show that these interleaved sequences are all different, it is necessary to establish that, if $\gamma_0 \neq \delta_0$, and $\gamma_1' \neq \delta_1'$, then both of the following equalities cannot be satisfied simultaneously.

$$\left.\begin{aligned} \gamma_o + I(\gamma_1'+1) &= \delta_o + I(\delta_1'+1) \\ \gamma_o + I(\gamma_1') &= \delta_o + I(\delta_1') \end{aligned}\right\} \qquad (B.4)$$

This is accomplished by showing that only d = 0 satisfies the equality

$$I(\gamma_1'+1) - I(\gamma_1') = I(\gamma_1'+1+d) - I(\gamma_1'+d) \qquad (B.5)$$

Equation (B.5) can be transformed to

$$I(\gamma_1'+1) + I(\gamma_1'+d) = I(\gamma_1'+1+d) + I(\gamma_1') \ . \qquad (B.6)$$

From the definition of $I(\lambda)$, (B.6) implies

$$x^{I(\gamma_1'+1)}[h_m(x) \oplus x^{\gamma_1'+d}h_m(x)] \equiv x^{I(\gamma_1')}[h_m(x) \oplus x^{\gamma_1'+1+d}h_m(x)] \ , \ \text{mod } (x^L-1) \ ,$$

or

$$x^{I(\gamma_1'+1)+\gamma_1'+d}h_m(x) \oplus x^{I(\gamma_1')+\gamma_1'+1+d}h_m(x) \equiv x^{I(\gamma_1'+1)}h_m(x) + x^{I(\gamma_1')}h_m(x), \text{mod } (x^L-1),$$

or

$$x^d\left[x^{I(\gamma_1'+1)+\gamma_1'}h_m(x) \oplus x^{I(\gamma_1')+\gamma_1'+1}h_m(x)\right] \equiv x^{I(\gamma_1'+1)}h_m(x) \oplus x^{I(\gamma_1')}h_m(x), \text{ mod } (x^L-1) \qquad (B.7)$$

However, (B.7) can be transformed to

$$x^d\left\{x^{\gamma_1'}\left[h_m(x) \oplus x^{\gamma_1'+1}h_m(x)\right] \oplus x^{\gamma_1'+1}\left[h_m(x) \oplus x^{\gamma_1'}h_m(x)\right]\right\}$$

$$\equiv \left[h_m(x) \oplus x^{\gamma_1'+1}h_m(x) \oplus h_m(x) \oplus x^{\gamma_1'}h_m(x)\right] \ , \quad \text{mod } (x^L-1)$$

or

$$x^d\left[x^{\gamma_1'}h_m(x) \oplus x^{\gamma_1'+1}h_m(x)\right] \equiv \left[x^{\gamma_1'}h_m(x) \oplus x^{\gamma_1'+1}h_m(x)\right] \ , \quad \text{mod } (x^L-1) \qquad (B.8)$$

From (B.8) it is seen that only d = 0 satisfies (B.5), establishing the proof.

APPENDIX C: Derivation of "Flipped" Cross-correlation Function for Basic Walsh Functions

In this appendix, $\rho_{i\ell}^{(f)}(\lambda_\ell)$ will be derived for $\ell > i$ and $\lambda_\ell = n\,2^{i+1} + w$ where $n = 0,1, \ldots, 2^{\ell-i-1}-1$, and $w = 0,1, \ldots, 2^i$. The derivation for the values of λ_ℓ not included above is quite similar and only the final result will be indicated.

Let $S_{a_i} = [(a_i)_0, \ldots, (a_i)_b, \ldots, (a_i)_{L-1}]$, $S_{a_\ell} = [(a_\ell)_0, \ldots, (a_\ell)_c, \ldots, (a_\ell)_{L-1}]$ and $S_g = [g_0, \ldots, g_d, \ldots, g_{L-1}]$. Then the first λ_ℓ symbols of S_{a_i}, $[(a_i)_b,\ b = 0, \ldots, \lambda_\ell - 1]$, are

$$(a_i)_b = \begin{cases} 0 & b = 0,1, \ldots, 2^i-1;\ 2^{i+1}, \ldots, 3\cdot 2^i-1;\ \ldots; \\ & \quad n2^{i+1}, n2^{i+1}+1, \ldots, n2^{i+1}+w-1 \\ 1 & b = 2^i, 2^i+1, \ldots, 2^{i+1}-1;\ 3\cdot 2^i, \ldots, 4\cdot 2^i-1;\ \ldots; \\ & \quad (2n-1)2^i, (2n-1)2^i+1, \ldots, n2^{i+1}-1\,. \end{cases}$$

The first λ_ℓ symbols of $x^{\lambda_\ell} S_{a_\ell}^{(f)}$, $[(a_\ell)_{L-\lambda_\ell+c},\ c = 0, \ldots, \lambda_\ell - 1]$, are $(a_\ell)_{L-\lambda_\ell+c} = 1$, $c = 0,1, \ldots, \lambda_\ell-1$. The first λ_ℓ symbols of $S_g = S_{a_i} + x^{\lambda_\ell} S_{a_{i\ell}}^{(f)}$ are

$$g_d = \begin{cases} 1 & d = 0,1, \ldots, 2^i-1;\ 2^{i+1}, \ldots, 3\cdot 2^i-1;\ \ldots; \\ & \quad n2^{i+1}, \ldots, n2^{i+1}+w-1 \\ 0 & d = 2^i, 2^i+1, \ldots, 2^{i+1}-1;\ 3\cdot 2^i, \ldots, 4\cdot 2^i-1;\ \ldots; \\ & \quad (2n-1)2^i, \ldots, n2^{i+1}-1\,. \end{cases}$$

From the symbol structure indicated above, it is seen that there are "w" more ones than zeros in the first $\lambda_{\ell} = n2^{i+1} + w$ digits of S_g. Thus from (5.7), $\rho_{i\ell}^{(f)}(n2^{i+1} + w) = - 2w/L$ $(L = 2^k)$ for $n = 0, \ldots, 2^{\ell-i-1}-1$, and $w = 0, 1, \ldots, 2^i$.

For the same constraint on n, but with $w = 2^i, 2^i + 1, \ldots, 2^{i+1}$, the "flipped" cross-correlation is found to be, $\rho_{i\ell}^{(f)}(n2^{i+1} + w) = - 2(2^{i+1}-w)/L$.

For $n = 2^{\ell-i-1}, 2^{\ell-i-1} + 1, \ldots, 2^{\ell-i} - 1$,

$$\rho_{i\ell}^{(f)}[n2^{i+1}+w] = \begin{cases} + 2w/L & w = 0, 1, \ldots, 2^i \\ 2(2^{i+1}-w)/L & w = 2^i, \ldots, 2^{i+1} \end{cases}$$

Finally for $n = 2\sigma(2^{\ell-i-1}), 2\sigma(2^{\ell-i-1}) + 1, \ldots, 2\sigma(2^{\ell-i-1}) + 2^{\ell-i-1} - 1$, $(\sigma = 0, 1, \ldots, 2^{k-\ell-1} - 1)$,

$$\rho_{i\ell}^{(f)}(n2^{i+1}+w) = \begin{cases} - 2w/L & w = 0, 1, \ldots, 2^i \\ - 2(2^{i+1}-w)/L & w = 2^i, \ldots, 2^{i+1}, \end{cases}$$

and with $n = (2\sigma+1)2^{\ell-i-1}, \ldots, (2\sigma+1)2^{\ell-i-1} + 2^{\ell-i-1} - 1$,

$$\rho_{i\ell}^{(f)}(n2^{i+1}+w) = \begin{cases} + 2w/L & w = 0, 1, \ldots, 2^i \\ + 2(2^{i+1}-w)/L & w = 2^i, \ldots, 2^{i+1} \end{cases}$$

APPENDIX D: Derivation of Probability of Error With Basic Walsh Functions For k=2

In this appendix, the average probability of error, when correlating with the carriers associated with the Basic Walsh function sequences S_{a_0} or S_{a_1}, with two carriers on the channel, (k=2) is determined. We are given the density functions, for i=0, ℓ=1,

$$p(\rho_{on}) = \frac{1}{\sqrt{\frac{\pi N_o S}{T}}} \exp - \left[\frac{(\rho_{in}-S)^2}{N_o S/T}\right], \tag{D.1}$$

and

$$p(\rho_{i\ell}) = p(\rho_{o1}) = \begin{cases} \frac{1}{2}\,\delta(\rho_{o1}) + \frac{1}{2S} & -\frac{S}{2} \leq \rho_{o1} \leq \frac{S}{2} \\ 0 & \text{elsewhere} \end{cases} \tag{D.2}$$

Then $p(Z \mid d_o=+1)$ is given by the convolution of $p(\rho_{on})$ and $p(\rho_{o1})$, or

$$P(Z \mid d_i=+1) = \int_{-\infty}^{\infty} p(\rho_{o1}) p_{on}(Z-\rho_{o1}) d\rho_{o1}$$

$$= \int_{-S/2}^{S/2} \frac{1}{2}\left[\delta(\rho_{o1}) + \frac{1}{S}\right] \cdot \frac{1}{\sqrt{\frac{N_o S}{T}}} \exp$$

$$- \left[\frac{(Z-\rho_{o1}-S)^2}{N_o S/T}\right] d\rho_{o1} \tag{D.3}$$

Thus the expression for the probability of error, $P(e_0) = P(e_1)$ becomes

$$P(e_1) = P(e_0) = \int_{-\infty}^{0} p(Z \mid d_1=+1)dZ =$$

$$\tfrac{1}{2}\sqrt{\frac{ST}{2\pi N_0}} \int_{-\infty}^{0}\int_{-S/2}^{S/2} \exp\left[-\frac{(Z-\rho_{01}-S)^2}{N_0 S/T}\right] d\rho_{01}\,dZ$$

$$+ \tfrac{1}{2}\sqrt{\frac{T}{\pi N_0 S}} \int_{-\infty}^{0} \exp\left[-\frac{(Z-S)^2}{N_0 S/T}\right] dz \qquad (D.4)$$

$$= \frac{1}{4S}\int_{-S/2}^{S/2}\left[1-\operatorname{erf}\left(\frac{\rho_{01}+S}{\sqrt{N_0 S/T}}\right)\right]d\rho_{01} + \tfrac{1}{4}\left[1-\operatorname{erf}\sqrt{\frac{ST}{N_0}}\right] \qquad (D.5)$$

where, $\operatorname{erf}(v)$, the error function of v is defined as

$$\operatorname{erf}(v) = \frac{2}{\sqrt{\pi}}\int_0^v e^{-x^2}dx \quad . \qquad (D.6)$$

The integration of the error function in (D-5) is performed by parts. The final result for the average probability of error is then

$$P(e_0) = P(e_1) = \tfrac{1}{2} - \tfrac{1}{4}\operatorname{erf}\sqrt{\frac{ST}{N_0}} - \tfrac{3}{8}\operatorname{erf}\left(\tfrac{3}{2}\sqrt{\frac{ST}{N_0}}\right)$$

$$+ \tfrac{1}{8}\operatorname{erf}\left(\tfrac{1}{2}\sqrt{\frac{ST}{N_0}}\right) - \frac{1}{\sqrt{\pi}}\sqrt{\frac{N_0}{ST}}\,e^{-ST/4N_0} + \frac{1}{\sqrt{\pi}}\sqrt{\frac{N_0}{ST}}\,e^{-9ST/4N_0}$$

(D.7)

APPENDIX E: Asymptotic Series Approximation to $P(e_o)$

An asymptotic series approximation to the integral expression (5.26) for i = o, which yields accurate results for $k \geq 4$ will now be derived. For i = o (5.26) can be transformed to

$$P(e_o) = \frac{1}{2} - \frac{1}{\pi} \int_o^\infty \frac{\sin 2^{k-1} y}{y} \left[\frac{\sin y}{2y} + \frac{1}{2}\right]^{k-1} e^{-y^2 2^{2k-4}/G^2} dy \qquad (E.1)$$

The procedure to be used for the above expression is similar to the procedure previously used for the asymptotic series approximation to[35,36]

$$\int_o^\infty \left(\frac{\sin x}{x}\right)^n dx \quad .$$

An approximation to $\left[\frac{\sin y}{2y} + \frac{1}{2}\right]^{k-1}$ will first be derived. It is noted that

$$\frac{d}{dy}\left[\ell n\left(\frac{\sin y}{2y} + \frac{1}{2}\right)\right] = \frac{y \cos y - \sin y}{y \sin y + y^2} \qquad (E.2)$$

Writing the series approximation to the right hand side of (E.2) we find

$$\frac{d}{dy}\left[\ell n\left(\frac{\sin y}{2y} + \frac{1}{2}\right)\right] = \frac{-y^3\left[\frac{2}{3!}\right] + y^5\left[\frac{4}{5!}\right] - y^7\left[\frac{6}{7!}\right] + \cdots}{2y^2 - \frac{y^4}{3!} + \frac{y^6}{5!} - \frac{y^8}{7!} + \cdots} \qquad (E.3)$$

Performing the long division and integration, and retaining the first

three terms

$$\ln\left(\frac{\sin y}{2y} + \frac{1}{2}\right) \sim -\frac{y^2}{12} + \frac{y^4}{1440} + \frac{y^6}{18,144} \tag{E.4}$$

Thus:

$$\left(\frac{\sin y}{2y} + \frac{1}{2}\right)^{k-1} \approx e^{-(k-1)y^2/12}\, e^{k-1\left[\frac{y^4}{1440} + \frac{y^6}{18,144}\right]}, \tag{E.5}$$

which can be approximated as

$$\left(\frac{\sin y}{2y} + \frac{1}{2}\right)^{k-1} \approx e^{-(k-1)y^2/12}\left[1 + \frac{(k-1)y^4}{1440} + \frac{(k-1)y^6}{18,144}\right] \tag{E.6}$$

Substituting (E.6) into (E.1) the expression for $P(e_o)$ is approximated as

$$P(e_o) \approx \frac{1}{2} - \frac{1}{\pi}\int_0^\infty \frac{\sin 2^{k-1}y}{y} \exp\left[-y^2\left(\frac{k-1}{12} + \frac{2^{2k-4}}{G^2}\right)\right] dy$$

$$- \frac{1}{\pi}\int_0^\infty [\sin 2^{k-1}y]\left[\frac{(k-1)y^3}{1440}\right] \exp\left[-y^2\left(\frac{k-1}{12} + \frac{2^{2k-4}}{G^2}\right)\right] dy$$

$$- \frac{1}{\pi}\int_0^\infty [\sin 2^{k-1}y]\left[\frac{(k-1)y^5}{18,144}\right] \exp\left[-y^2\left(\frac{k-1}{12} + \frac{2^{2k-4}}{G^2}\right)\right] dy \tag{E.7}$$

The contribution of the third integral can be shown to be negligible for $0 \leq G^2 \leq 20$. Also for G^2 in this range and $k \geq 4$ we can use the

approximation

$$\exp\left[-y^2\left(\frac{k-1}{12}+\frac{2^{2k-2}}{G^2}\right)\right] \approx \left(\exp\left[-\frac{y^2\,2^{2k-2}}{G^2}\right]\right)\left[1-\frac{y^2(k-1)}{12}\right] \tag{E.8}$$

Incorporating these approximations into (E.7) and performing the integration with the aid of integral 337-2b in Gröbner,[34] we get the approximation

$$P(e_o) \sim \frac{1}{2}-\frac{1}{2}\operatorname{erf}(G)+\left(\frac{k-1}{12\pi}\right)\left(\frac{G^3}{2^{2k-2}}\right)\Gamma\left(\frac{3}{2}\right)e^{-G^2}$$

$$-\frac{(k-1)}{1440\pi}\frac{G^5}{2^{4k-8}}\Gamma\left(\frac{5}{2}\right)e^{-G^2}\quad F\left[-1,\frac{3}{2},G^2\right]$$

$$+\frac{(k-1)^3}{(17,280)\pi}\frac{G^7}{2^{6k-12}}\Gamma\left(\frac{7}{2}\right)e^{-G^2}\quad F\left[-2,\frac{3}{2},G^2\right] \tag{E.9}$$

where $F[x,y,z]$ is a confluent hypergeometric function.

It is seen that the resultant approximation for $P(e_o)$ is the binary PSK error probability plus some error terms which approach zero for $k \to \infty$.

APPENDIX F: Probability of Error Averaged Over k Basic Walsh Function Carriers

In this appendix the probability of error averaged over all k carriers on the channel, for $k \to \infty$, will be derived. When correlating with the carrier associated with $S_{a_i}=S_{a_{k-E}}$, the output of the i^{th} correlator becomes Gaussian distributed with mean zero and variance, $\sigma^2_{Z_{k-E}}$, $E=1, 2, \ldots, k \to \infty$,

$$\sigma^2_{Z_{k-E}} = \frac{N_o S}{2T} + \frac{S^2}{3}\left[(E-1)2^{-2E+1}+\left(\frac{4}{3}\right)\left(2^{-2E-1}\right)\right] \quad . \tag{F.1}$$

Let

$$\sigma^2_E = \sigma^2_{Z_{k-E}} - \frac{N_o S}{2T} \quad . \tag{F.2}$$

Then the probability of error $P(e_{k-E})$ when correlating with the i=k-E carrier is

$$P(e_{k-E}) = \tfrac{1}{2} - \tfrac{1}{2}\,\mathrm{erf}\left[\frac{1}{\left[\frac{1}{G^2}+\frac{2\sigma_E^2}{S^2}\right]^{\frac{1}{2}}}\right] \quad , \tag{F.3}$$

where

$$G = \sqrt{ST/N_o} \quad .$$

We are interested in $\bar{P}_w$, the error probability averaged over all of the carriers. Thus

$$\bar{P}_w = \lim_{k\to\infty} \frac{1}{k} \sum_{E=1}^{k} P(e_{k-E}) \quad , \tag{F.4}$$

or

$$\bar{P}_w = \lim_{k\to\infty} \frac{1}{k} \sum_{E=1}^{k} \left\{ \tfrac{1}{2} - \tfrac{1}{2} \operatorname{erf}\left[\frac{1}{\left(\frac{1}{G^2} + \frac{2\sigma_E^2}{S^2} \right)^{\frac{1}{2}}} \right] \right\} \tag{F.5}$$

Expand the error function in the series

$$\operatorname{erf}(x_E) = \frac{2}{\sqrt{\pi}} \sum_{c=1}^{\infty} (-1)^{c+1} \frac{x_E^{2c-1}}{(2c-1)(c-1)!} \tag{F.6}$$

where

$$x_E = \frac{1}{\left[\frac{1}{G^2} + \frac{2\sigma_E^2}{S^2} \right]^{\frac{1}{2}}} = \frac{G}{\left[1 + \frac{2\sigma_E^2 G^2}{S^2} \right]^{\frac{1}{2}}} \tag{F.7}$$

If $\frac{2\sigma_E^2 G^2}{S^2} < 1$ then x_E can be expanded in a power series in ascending powers of $\frac{2\sigma_E^2 G^2}{S^2}$. Now $\frac{2\sigma_E^2 G^2}{S^2}$ achieves its maximum value for

E=1 or E=2, with $\frac{2\sigma_1^2}{S^2} = \frac{2\sigma_2^2}{S^2} = \frac{1}{9}$. Hence for all $G^2 < 9$*, x_E is equivalent to

$$x_E = G \sum_{d=0}^{\infty} \frac{1}{2^{2d}} \binom{2d}{d} (-1)^d \left[\frac{2\sigma_E^2 G^2}{S^2}\right]^d . \qquad (F.8)$$

Then

$$\overline{P}_W = \lim_{k\to\infty} \frac{1}{k} \sum_{E=1}^{k} \left\{\frac{1}{2} - \frac{1}{2} \cdot \frac{2}{\sqrt{\pi}} \sum_{c=1}^{\infty} \frac{(-1)^{c+1} G^{2c-1}}{(2c-1)(c-1)!}\right.$$

$$\left. \cdot \sum_{d=0}^{\infty} \left[\frac{(-1)^d}{2^{2d}} \binom{2d}{d} \left[\frac{2\sigma_E^2 G^2}{S^2}\right]^d\right]^{2c-1}\right\} \qquad (F.9)$$

Since all of these infinite series are uniformly convergent we can interchange the summation and limiting operations in an arbitrary manner. Thus the expression for $\overline{P}_W$ can be reduced to

$$\overline{P}_W = \left\{\frac{1}{2} - \frac{1}{2} \cdot \frac{2}{\sqrt{\pi}} \sum_{c=1}^{\infty} \frac{(-1)^{c+1} G^{2c-1}}{(2c-1)(c-1)!} \cdot \lim_{k\to\infty} \frac{1}{k} \sum_{E=1}^{k} \left[\sum_{d=0}^{\infty} \frac{(-1)^d}{2^{2d}} \binom{2d}{d}\right.\right.$$

$$\left.\left. \left(\frac{2\sigma_E^2 G^2}{S^2}\right)^d\right]^{2c-1}\right\} \qquad (F.10)$$

*The average probability of error for binary PSK signalling with $G^2=9$ is $1.1 \cdot 10^{-5}$.

It will now be shown that

$$\lim_{k\to\infty} \frac{1}{k} \sum_{E=1}^{k} \left[\sum_{d=0}^{\infty} \frac{(-1)^d}{2^{2d}} \binom{2d}{d} \left(\frac{2\sigma_E^2 G^2}{S^2} \right)^d \right]^{2c-1} = 1 \qquad \text{(F.11)}$$

The first term of the above summation is 1.

A typical remaining term is of the form

$$\lim_{k\to\infty} \frac{c_1}{k} \sum_{E=1}^{k} \left(\frac{\sigma_E^2}{S^2} \right)^{\beta} , \qquad \text{(F.12)}$$

where β is a positive integer and c_1 is a finite constant.

But,

$$\left(\frac{\sigma_E^2}{S^2} \right)^{\beta} = \left(\frac{4}{9} \right)^{\beta} 2^{-\beta 2E-\beta} \left[\sum_{m=0}^{\beta} \binom{\beta}{m} (E-1)^m 3^m \right] \qquad \text{(F.13)}$$

It is then verified that

$$\lim_{k\to\infty} \frac{c_1}{k} \sum_{E=1}^{k} 2^{-\beta 2E} \sum_{m=0}^{\beta} \binom{\beta}{m} (E-1)^m 3^m = 0$$

Hence the probability of error, $\overline{P}_w$, averaged over the k Basic Walsh

functions, $k \to \infty$, is

$$\overline{P}_w = \tfrac{1}{2} - \tfrac{1}{2} \cdot \frac{2}{\pi} \sum_{c=1}^{\infty} \frac{(-1)^{c+1} G^{2c-1}}{(2c-1)(c-1)!}$$

$$= \tfrac{1}{2} - \tfrac{1}{2} \operatorname{erf}(G) \quad ,$$

for $G^2 \leq 9$.

REFERENCES

1. Golomb, S. W., et.al., Digital Communications with Space Applications. Englewood Cliffs: Prentice-Hall, Inc., 1964.

2. Singer, J., "A Theorem in Finite Projective Geometry and Some Applications to Number Theory," Trans. American Math. Society, 43, (1938) pp.377-85.

3. Zierler, N., "Linear Recurring Sequences," Journal of the Society for Industrial and Applied Mathematics, 7, (1959), pp.31-48.

4. Golomb, S.W., Sequences with Randomness Properties, Terminal Progress Report under Contract Req. No.639498, Baltimore, Maryland: Glenn L. Martin Company, June 1955.

5. Paley, R. E. A. C., "On Orthogonal Matrices," Journal of Mathematics and Physics, 12, (1933), pp.311-20.

6. Brauer, A., "On a New Class of Hadamard Determinants," Mathematische Zeitschrift, 58, (1953), pp.219-25.

7. Hall, M., Jr., "A Survey of Difference Sets," Proceedings of the American Mathematical Society, 7, (1956), pp.975-86.

8. Heimiller, R. C., "Phase Shift Pulse Codes with Good Periodic Correlation Properties," IRE Transactions, IT-7, (1961), pp.254-57.

9. Franck, R. L. and S. A. Zadoff, "Phase Shift Pulse Codes with Good Periodic Correlation Properties," IRE Transactions, IT-8, (1962), pp.381-2.

10. Tompkins, D. N., "Codes with Zero Correlation," Paper presented at International Conference on Microwaves, Circuit Theory and Information Theory, Pt.3, Information Theory, Tokyo, 1964.

11. Titsworth, R. C., The Algebra of Periodic Sequences, Technical Report No.32-381, Pasadena: Jet Propulsion Laboratory, January 1963.

12. Titsworth, R. C., Correlation Properties of Cyclic Sequences, Technical Report No.32-388, Pasadena: Jet Propulsion Laboratory, July 1963.

13. Turyn, R., Incidence Matrix Design, Final report under contract No. AF30(602)-3334, Waltham, Mass., Sylvania Electronic Systems, April 1965.

14. Wolf, J. K., and B. Elspas, "On the Number of Possible Almost-Orthogonal Waveforms," Report R-108, Multiple Access to a Communication Satellite with a Hard-Limiting Repeator, Arlington: Institute for Defense Analysis, April 1965.

15. Gilbert, E. N., "Cyclically Permutable Error-Correcting Codes," IEEE Transactions, IT-7 (1963), pp.175-82.

16. Turyn, R., Research in Non-Linear Codes, Final Report AFCRL-64-137, Cambridge: Air Force Cambridge Research Laboratories, March 1964.

17. Birdsall, T.G., and M.P. Ristenbatt, Introduction to Linear Shift-Register Generated Sequences, EDG Technical Report No.90, University of Michigan Research Institute, 1958.

18. Elspas, B., "The Theory of Autonomous Linear Sequential Networks," IRE Transactions, CT-6 (1959), pp.45-60.

19. Raphael, J., Non-Linear Filtering of Pseudo-Random Sequences, M.S.E.E. Project Report, New York University, New York, 1964.

20. Viterbi, A. J., "Systematic Coding for the Continuous Gaussian Channel," Ph.D. Dissertation, University of Southern California, August 1962.

21. Reed, I.S., and R. A. Scholtz, N-Orthogonal Phase-Modulated Codes, USCEE Report 134, University of Southern California, Electronic Sciences Laboratory, May 1965.

22. Stiffler, J. J., "Self-Synchronizing Binary Telemetry Codes," Ph.D. Dissertation, Dept. of Electrical Engineering, California Institute of Technology (1962).

23. Titsworth, R. C., "A Boolean-Function-Multiplexed Telemetry System," IEEE Transactions, SET-9 (1963), pp.42-45.

24. Peterson, W. W., Error-Correcting Codes. Cambridge: M.I.T. Press, 1961.

25. Wolf, J. K., et al, The Shift and Add Property of Maximal Length Binary Sequences Using Cyclotomic Polynomials, RADC-TDR 64-66, Rome Air Development Center, March 1964.

26. Elspas, B., and R. Short, A Table of Indices for Polynomials Over GF(2), RADC TR 61-259, Rome Air Development Center, October 1961.

27. Turyn, R., Private Communication.

28. Bose, R. C., and D. K. Ray-Chaudhuri,"On a Class of Error-Correcting Binary Group Codes," Inf. and Control, 3 (1960), pp.68-79.

29. Elspas, B., Design and Instrumentation of Error-Correcting Codes, RADC-TDR 62-511, Rome Air Development Center, 1962.

30. Levitt, K. N., and J. K. Wolf, "On the Interleaving of Two-Level Periodic Binary Sequences," Paper presented at 1965 National Electronics Conference.

31. Van Der Waerden, B. L., Modern Algebra Vol. 1, New York: Frederick Ungar Company, 1931, pp. 114-115.

32. Hall, M., Jr., "Block Designs," in Applied Combinatorial Mathematics, edited by Beckenbach, E. F., New York: John Wiley and Sons, 1964, pp. 369-87.

33. Aein, J. M., and J. W. Schwartz, Multiple Access to a Communication Satellite with a Hard Limiting Repeater, Vol. II, Report R-108, Institute for Defense Analysis, April 1965.

34. Grobner, W., and Hofreiter, N., Integral-tafel Zweiter Teil Bestimate Integrale, Vienna: Springer-Verlag, 1950.

35. Goddard, L. S., "The Accumulation of Chance Effects and the Gaussian Frequency Distribution," Philos. Mag. 36, 1945, pp. 428-33.

36. Medhurst, R. G. and J. H. Roberts, "Evaluation of the Integral

$$I_n(b) = 2/\pi \int_0^\infty (\sin x/x)^n \cos bx \, dx \, ,"$$

Mathematics of Computation, 19 (1965), pp. 113-18.

37. Wolf, J. K. and B. Elspas, "Mutual Interference Due to Correlated Constant-Envelope Signals," Report R-108, Multiple Access to a Communication Satellite with a Hard Limiting Repeater, Arlington: Institute for Defense Analysis, April 1965.

38. Wolf, J. K., "Cumulative Codes as Variable Redundancy Codes," IEEE International Convention Record, Part 5, 1964, pp. 66-72.

39. Schillinger, A. G., "A Class of Solid-Burst Error-Correcting Codes," Paper presented at International Conference on Microwaves, Circuit Theory and Information Theory, Part 3, Information Theory, Tokyo, 1964.

40. Magnavox Research Laboratories, Study of Correlation Properties of Binary Sequences, Report R-692, Torrance, California, January 1964.

41. Zygmund, A., Trigonometric Series, New York: Dover Publications Inc., 1955.

UNCLASSIFIED

Security Classification

DOCUMENT CONTROL DATA · R&D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY *(Corporate author)* NEW YORK UNIVERSITY, SCHOOL OF ENGINEERING AND SCIENCE, Department of Electrical Engineering, Laboratory for Electroscience Research, University Hts., Bx., N.Y. 10453	2a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED 2b. GROUP

3. REPORT TITLE

CORRELATION PROPERTIES OF MULTI-LEVEL CYCLIC SEQUENCES

4. DESCRIPTIVE NOTES *(Type of report and inclusive dates)*

Final Report - Part II

5. AUTHOR(S) *(Last name, first name, initial)*

Levitt, Karl N. (Jack K. Wolf, P.I.)

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
November 1965	166 + viii	41

8a. CONTRACT OR GRANT NO. DA-31-124-ARO-D-253 b. PROJECT NO. 4949E c. TASK d.	9a. ORIGINATOR'S REPORT NUMBER(S) TECHNICAL REPORT 400-125 9b. OTHER REPORT NO(S) *(Any other numbers that may be assigned this report)*

10. AVAILABILITY/LIMITATION NOTICES

U.S. Government agencies may obtain copies of this report directly from DDC. All other users shall request through Clearinghouse for Federal Scientific and Technical Information, (CFSTI), Sills Building, Springfield, Virginia 22151

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
	U.S. Army Research Office - Durham Box CM, Duke Station Durham, North Carolina 27706

13. ABSTRACT

DD FORM 1 JAN 64 1473

UNCLASSIFIED

Security Classification

14. KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Coding Theory Cyclic Sequences Correlation Non-binary Sequences Orthogonal Sequences						

INSTRUCTIONS

1. ORIGINATING ACTIVITY: Enter the name and address of the contractor, subcontractor, grantee, Department of Defense activity or other organization *(corporate author)* issuing the report.

2*a*. REPORT SECURITY CLASSIFICATION: Enter the overall security classification of the report. Indicate whether "Restricted Data" is included. Marking is to be in accordance with appropriate security regulations.

2*b*. GROUP: Automatic downgrading is specified in DoD Directive 5200.10 and Armed Forces Industrial Manual. Enter the group number. Also, when applicable, show that optional markings have been used for Group 3 and Group 4 as authorized.

3. REPORT TITLE: Enter the complete report title in all capital letters. Titles in all cases should be unclassified. If a meaningful title cannot be selected without classification, show title classification in all capitals in parenthesis immediately following the title.

4. DESCRIPTIVE NOTES: If appropriate, enter the type of report, e.g., interim, progress, summary, annual, or final. Give the inclusive dates when a specific reporting period is covered.

5. AUTHOR(S): Enter the name(s) of author(s) as shown on or in the report. Enter last name, first name, middle initial. If military, show rank and branch of service. The name of the principal author is an absolute minimum requirement.

6. REPORT DATE: Enter the date of the report as day, month, year, or month, year. If more than one date appears on the report, use date of publication.

7*a*. TOTAL NUMBER OF PAGES: The total page count should follow normal pagination procedures, i.e., enter the number of pages containing information.

7*b*. NUMBER OF REFERENCES: Enter the total number of references cited in the report.

8*a*. CONTRACT OR GRANT NUMBER: If appropriate, enter the applicable number of the contract or grant under which the report was written.

8*b*, 8*c*, & 8*d*. PROJECT NUMBER: Enter the appropriate military department identification, such as project number, subproject number, system numbers, task number, etc.

9*a*. ORIGINATOR'S REPORT NUMBER(S): Enter the official report number by which the document will be identified and controlled by the originating activity. This number must be unique to this report.

9*b*. OTHER REPORT NUMBER(S): If the report has been assigned any other report numbers *(either by the originator or by the sponsor)*, also enter this number(s).

10. AVAILABILITY/LIMITATION NOTICES: Enter any limitations on further dissemination of the report, other than those imposed by security classification, using standard statements such as:

(1) "Qualified requesters may obtain copies of this report from DDC."

(2) "Foreign announcement and dissemination of this report by DDC is not authorized."

(3) "U. S. Government agencies may obtain copies of this report directly from DDC. Other qualified DDC users shall request through

_____."

(4) "U. S. military agencies may obtain copies of this report directly from DDC. Other qualified users shall request through

_____."

(5) "All distribution of this report is controlled. Qualified DDC users shall request through

_____."

If the report has been furnished to the Office of Technical Services, Department of Commerce, for sale to the public, indicate this fact and enter the price, if known.

11. SUPPLEMENTARY NOTES: Use for additional explanatory notes.

12. SPONSORING MILITARY ACTIVITY: Enter the name of the departmental project office or laboratory sponsoring *(paying for)* the research and development. Include address.

13. ABSTRACT: Enter an abstract giving a brief and factual summary of the document indicative of the report, even though it may also appear elsewhere in the body of the technical report. If additional space is required, a continuation sheet shall be attached.

It is highly desirable that the abstract of classified reports be unclassified. Each paragraph of the abstract shall end with an indication of the military security classification of the information in the paragraph, represented as *(TS), (S), (C), or (U).*

There is no limitation on the length of the abstract. However, the suggested length is from 150 to 225 words.

14. KEY WORDS: Key words are technically meaningful terms or short phrases that characterize a report and may be used as index entries for cataloging the report. Key words must be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location, may be used as key words but will be followed by an indication of technical context. The assignment of links, rules, and weights is optional.