CORRELATION PROPERTIES OF CYCLIC SEQUENCES

Thesis by

Robert C. Titsworth

In Partial Fulfillment of the Requirements

For the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1962

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my advisor, Dr. S. W. Golomb, for his very capable direction and his many helpful suggestions.

I also wish to acknowledge the financial support provided by International Business Machines and by the Jet Propulsion Laboratory during the period over which this thesis was written.

ABSTRACT

In the unconstrained channel with additive Gaussian noise, where the optimum detector is based on correlation or matched filters, the quality of a code can be expressed as a function of the correlation values between code words. For a cyclic-sequence code, optimality reduces to a criterion to be met by the autocorrelation function of the sequence. Methods are presented here for determining cyclic sequences with given correlation properties.

When the amount of equipment in the receiver is limited, matched filtering is no longer the optimal detection scheme. A better system, as is shown here, is one which, by the use of a Boolean function, combines several "component" sequences to generate the transmitted signal; the receiver consists of filters matched to each component. The logic, the number of components, the requirements of the component sequences to optimize the system, and a general method for treating Boolean logics are given in this work.

TABLE OF CONTENTS

INTRODUCTION

Over the past few years, cyclic sequences have played an increasingly important role as information codes in digital communications. They have found a welcome place in secret and secure communications schemes, missile command and telemetry systems, and interplanetary and satellite ranging experiments. Each such scheme exerts its own particular need on the type of code it uses; but, due to the fact that the optimal detectors for the Gaussian channel are correlating devices, part of each need can be described as a requirement on the correlation of a code.

The performance of such systems relies heavily upon the types of sequence correlation properties available to the designer. He desires a code which will tend to minimize the errors caused by noise. By this, we mean that each of the possible situations presented to the receiver must be as mutually distinguishable as possible. When the information of a code is contained in the phase-shift of a transmitted sequence, maximal distinguishability means that the autocorrelation function of the sequence must be much higher in-phase than out-of-phase.

On the other hand, suppose that the combined phase-shifts of several sequences are the information carriers and suppose that we combine, at the transmitter, these several sequences together into a single code. This combined code now carries information concerning the phase of each "component" sequence; but it is necessary to find an optimal set of sequences to correlate with the received signal to decode the information. At some phase-shift the correlation between the combined code and an element of the decoding set must be as large, and at all other shifts as small, as possible. With the knowledge of such shifts and the decoding procedure, one must be

able to interpret the phase information of components uniquely. In this way, a very long code can be made whose phase may be determined, component by component, in a comparatively short time and with a limited amount of receiver equipment.

It is the purpose of this thesis to investigate autocorrelations of single and multi-component sequences, cross-correlations between a sequence and its components, and to develop methods by which sequences having given correlation properties can be synthesized.

Binary sequences with two-level autocorrelation functions have been characterized elsewhere[1,2,3,4], and methods have been devised to synthesize them when they exist (for example, linear shift-registers, quadratic residues). When the two-level property does not exist, there has been, up to now, no method, except exhaustive search, to find nearest-to-ideal sequences. There are, however, iterative methods which yield near-optimum sequences of any cyclic length. There are other methods, which apply to certain periods, which produce the most distinguishable sequences for those periods. These methods are developed here, as well as general methods for the analysis of modulation and sequences generated by Boolean functions of component sequences.

Insofar as it was feasible, the author tried to make this thesis a self-contained entity, starting with motivating arguments based on modulation by sequences, continuing with the subsequent detection and extending to synthesis of sequences with given properties. It was, of course, impossible to make it entirely self-contained, and there are numerous references to texts and articles throughout the thesis.

The requisites necessary to read the sequel are limited to elementary calculus, number theory and modern algebra. The latter two may be somewhat unfamiliar to most engineers, but no more than the first few chapters of

Nagell's Introduction to Number Theory (John Wiley, 1951) and Birkhoff's and MacLane's A Survey of Modern Algebra (MacMillan, 1950) should be needed to follow the argument.

Chapter 1

MODULATION OF SIGNALS BY SEQUENCES

The notion of having a signal or set of signals modulated by a digital sequence is not new in communications; in fact, multiplex, frequency-shift keying (FSK), CW telegraphy, etc., have been using this concept for years.

In these systems, it is usually assumed that the modulation is binary, not coherent with the carrier, and not periodic. However, it has become necessary in many more modern schemes to modulate by codes which are cyclic, coherent, and/or non-binary.

A coded interplanetary- and space-radar recently developed at the Jet Propulsion Laboratory[5,6] is coherent throughout and uses periodic modulation. Many improvements in jam-proof, secure, or missile commands systems are also being based on such principles. Certain cyclic non-binary codes have much to recommend their use and can be used to advantage in telemetry systems[7].

In the case of non-coherent, non-periodic modulation, calculations could be made regarding spectral distribution by assuming that the carrier and modulation were statistically independent. Such an assumption no longer remains valid for coherent systems. In fact, such an assumption may often lead to basically erroneous results.

For example, let a sinusoidal carrier be phase modulated $\pm 90^{\circ}$, changing randomly at integral multiples of some basic time interval t_0. This may be treated as amplitude modulation where the modulation is ± 1. When the carrier and modulation are independent, the spectrum rolls off at 6 db/octave, and the spectrum is merely the convolution of modulation with carrier. But when

the carrier shifts 180° only as it passes through zero, the spectrum falls off at 12 db/octave. For more complicated carriers or modulation, the change due to coherence can be even more drastic.

A general method for computing the power spectrum of signals produced by such sequence-modulation schemes was given in 1959[8,9] by the author in collaboration with Dr. L. R. Welch. Part of this method is repeated here to give an efficient method for spectral calculation, to demonstrate that it is possible to express the spectrum as a linear function of the sequence correlation values, to indicate the type of sequence correlation desirable from a spectral simplicity point-of-view, and to illustrate the form of the spectrum in some practical cases.

A. The Spectral Equation

Let

$$\left\{ h_i(t):\ i = 1, 2, \ldots, b;\ \ h_i(t) = 0 \text{ for } t \text{ not in } \left[0, t_o\right) \right\}$$

be a set of distinct, Fourier-transformable functions, and let

$$\underline{a} = \left\{ a_n:\ n = \ldots, -2, -1, 0, 1, 2, \ldots \right\}$$

be a doubly-infinite sequence of elements belonging to a finite set

$$\left\{ e_i:\ i = 1, 2, \ldots, b \right\}$$

of objects, or states; that is, $\underline{a}$ is a mapping of the integers onto the set

$\{e_i\}$. Let δ_n^i be a type of Kronecker delta defined by

$$\delta_n^i = \left\{ \begin{array}{l} 1 \text{ if } a_n = e_i \\ \\ 0 \text{ if } a_n \neq e_i \end{array} \right\} = \delta(e_i, a_n) . \qquad (1.1)$$

The sequences

$$\delta^i = \left\{ \delta_n^i: \; n = \ldots, -2, -1, 0, 1, 2, \ldots \right\} \quad , (i = 1, 2, \ldots, b)$$

are <u>projections</u> of the separate states onto binary (0, 1) sequences.

We allow the functions $\{h_i(t)\}$ to be chosen by the sequence states to form a signal (see Figure 1.1)

$$x(t) = \sum_{i=1}^{b} \sum_{n=-\infty}^{+\infty} \delta_n^i \, h_i(t - nt_0), \qquad (1.2)$$

whose spectrum we wish to determine. We describe $x(t)$ as the result of <u>modulating</u> $\{h_i(t)\}$ by the sequence <u>a</u>.

We can visualize $x(t)$ as the output of a b-port linear filter (see Figure 1.2) whose inputs are δ-function trains

$$\delta^i(t) = \sum_{n=-\infty}^{+\infty} \delta_n^i \; \delta(t - nt_0), \qquad (1.3)$$

and whose unit impulse responses are $h_i(t)$. This is true because the filter output is[10]

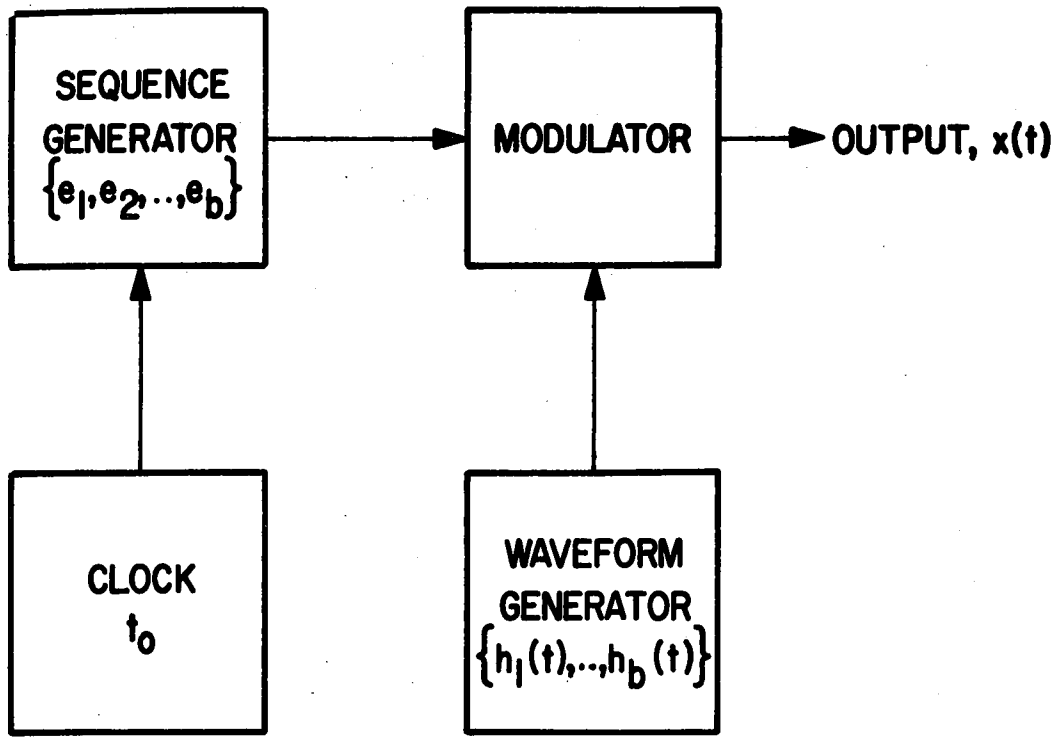

FIGURE I.I. SEQUENCE MODULATION TECHNIQUE

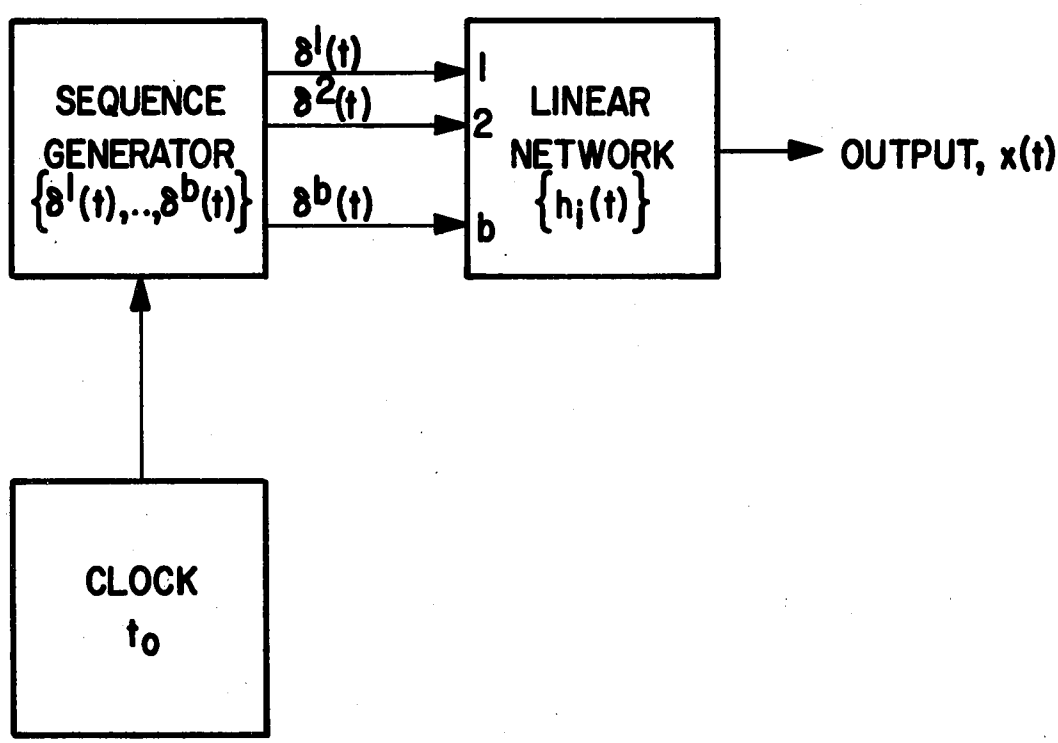

FIGURE I.2. MATHEMATICAL MODEL OF MODULATION BY SEQUENCE

$$\sum_{i=1}^{b} \int_{-\infty}^{+\infty} h_i(t') \sum_{n=-\infty}^{+\infty} \delta_n^i \, \delta(t-nt_0-t') \, dt'$$

$$= \sum_{i=1}^{b} \sum_{n=-\infty}^{+\infty} \delta_n^i \; h_i(t-nt_0) \; = \; x(t) \; . \qquad (1.4)$$

With this input time series, the output spectrum of a linear filter is given by[11]

$$S_{xx}(f) \; = \; \sum_{i=1}^{b} \sum_{k=1}^{b} H^*_i(f) \, H_k(f) \, S_{ik}(f) \; , \qquad (1.5)$$

where (*) indicates complex conjugation, $H_i(f)$ is the transform of the impulse response,

$$H_i(f) \; = \; \int_{0}^{t_0} h_i(t) \; e^{-j2\pi ft} \; dt \; , \qquad (1.6)$$

and $S_{ik}(f)$ is the transform of the (time) cross-correlation $c_{ik}(\tau)$ between the i<u>th</u> and k<u>th</u> inputs.

$$c_{ik}(\tau) \; = \; \lim_{T \longrightarrow \infty} \; \frac{1}{2T} \int_{-T}^{+T} \delta^i(t) \, \delta^k(t+\tau) \; dt \; . \qquad (1.7)$$

By substituting for $\delta^i(t)$ and $\delta^k(t+\tau)$, their δ-function representatives, the last equation expands to

$$c_{ik}(\tau) \; = \; \lim_{T \longrightarrow \infty} \; \frac{1}{2T} \int_{-T}^{+T} \sum_{n=-\infty}^{+\infty} \sum_{m=-\infty}^{+\infty} \delta_n^i \delta_m^k \, \delta(t-nt_0) \qquad (1.8)$$

$$\delta(t+\tau-mt_0) \; dt \; .$$

The sifting action of the integral means that we can set $T = Nt_0$; consequently, the limits in the sum over n must be replaced by

$$-N \leq n \leq N \, . \tag{1.9}$$

Completing the integration and simplifying the result yield

$$c_{ik}(\tau) = \frac{1}{t_0} \sum_{m=-\infty}^{+\infty} \left[\lim_{N \longrightarrow \infty} \frac{1}{2N} \sum_{n=-N}^{+N} \delta_n^i \delta_{n+m}^k \right] \delta(\tau - mt_0). \tag{1.10}$$

We can then take the transform of $c_{ik}(\tau)$ to get

$$S_{ik}(f) = \frac{1}{t_0} \sum_{m=-\infty}^{+\infty} \left[\lim_{N \longrightarrow \infty} \frac{1}{2N} \sum_{n=-N}^{+N} \delta_n^i \delta_{n+m}^k \right] e^{-j2\pi fmt_0} \, . \tag{1.11}$$

The term in brackets is of particular interest because it represents correlation between the ith and kth states of the sequence.

If a is stochastic, we average $c_{ik}(\tau)$ over the ensemble of stochastic variables, and if a is periodic, we may let N take on only integral multiples of the period. Whenever we can assure ourselves that the limit will exist, we define the normalized state-correlation of the sequence by

$$r_{ik}(m) = \lim_{N \longrightarrow \infty} \frac{1}{2N} \sum_{m=-N}^{+N} \delta_n^i \delta_{n+m}^k \, . \tag{1.12}$$

The final resulting spectral equation for a sequence modulated process is

$$S_{xx}(f) = \frac{1}{t_0} \sum_{i=1}^{b} \sum_{k=1}^{b} H^*_i(f)\, H_k(f) \left(\sum_{m=-\infty}^{+\infty} r_{ik}(m)\, e^{-j2\pi f m t_0} \right) . \tag{1.13}$$

Note in this equation that $S_{xx}(f)$ is very simply related to the signals $h_i(t)$ and to the correlation values $r_{ik}(m)$; $S_{xx}(f)$ is a function of carrier properties and sequence properties in which the sequence correlation properties enter linearly into the calculations and in which the carrier and sequence properties influence each other in a simple, multiplicative way.

By defining

$$\begin{aligned} \underset{\sim}{H}(f) &= \left[H_1(f), \ldots, H_b(f) \right]^T \\ \underset{\sim}{r}(m) &= \left[r_{ik}(m) \right] \\ \underset{\sim}{S}(f) &= \sum_{m=-\infty}^{+\infty} \underset{\sim}{r}(m)\, e^{j2\pi f m t_0} , \end{aligned} \tag{1.14}$$

the spectral equation can be put in matrix form:

$$S_{xx}(f) = \underset{\sim}{H}^*(f)\, \underset{\sim}{S}(f)\, \underset{\sim}{H}(f) . \tag{1.15}$$

To find the autocorrelation function of $x(t)$, we merely take the inverse Fourier transform of $S_{xx}(f)$

$$\begin{aligned} R_{xx}(\tau) &= \int_{-\infty}^{+\infty} S_{xx}(f)\, e^{j2\pi f \tau}\, df \\ &= \frac{1}{t_0} \int_{-\infty}^{+\infty} \sum_{i=1}^{b} \sum_{k=1}^{b} \left(\sum_{n=-\infty}^{+\infty} r_{ik}(n)\, e^{-j2\pi f n t_0} \right) \end{aligned} \tag{1.16}$$

$$H^*_i(f)\, H_k(f)\, e^{j2\pi f \tau}\, df .$$

Express $\tau = mt_0 + \tau_0$, where $0 \leq \tau_0 < t_0$, and substitute the corresponding Fourier integral forms for $H^*_i(f)$ and $H_k(f)$. This yields

$$R_{xx}(mt_0 + \tau_0) = \frac{1}{t_0} \sum_{i=1}^{b} \sum_{k=1}^{b} \sum_{n=-\infty}^{+\infty} r_{ik}(n) \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} h_i(s)\, h_j(t)\, e^{j2\pi f(s-t+\tau_0-(n-m)t_0} df\, ds\, dt. \tag{1.17}$$

In the integration over f, we use the expression relating the δ-function to its Fourier integral,

$$\delta(t) = \int_{-\infty}^{+\infty} e^{j2\pi ft}\, df, \tag{1.18}$$

to give the equation

$$R_{xx}(\tau) = \frac{1}{t_0} \sum_{i=1}^{b} \sum_{k=1}^{b} \sum_{n=-\infty}^{+\infty} r_{ik}(n) \int_{-\infty}^{+\infty} h_i(s)\, h_k(s+\tau_0-(n-m)t_0)\, ds. \tag{1.19}$$

All of the terms in the sum over n vanish except those with $n = m$ and $n = m+1$. Now define

$$\psi_{ik}(\tau) = \frac{1}{t_0} \int_{-\infty}^{+\infty} h_i(s)\, h_k(s+\tau)\, ds. \tag{1.20}$$

The final expression for the autocorrelation of x(t) is

$$R_{xx}(mt_0 + \tau_0) = \sum_{i=1}^{b} \sum_{k=1}^{b} \left[r_{ik}(m)\ \psi_{ik}(\tau_0) + r_{ik}(m+1)\ \psi_{ik}(\tau_0 - t_0) \right] . \tag{1.21}$$

When $\tau_0 = 0$, there is no overlapping of intervals and the second terms above vanish.

$$R_{xx}(mt_0) = \sum_{i=1}^{b} \sum_{k=1}^{b} r_{ik}(m)\ \psi_{ik}(0). \tag{1.22}$$

Here, $\psi_{ik}(0)$ takes on the special form

$$\psi_{ik}(0) = \frac{1}{t_0} \int_0^{t_0} h_i(t)\ h_k(t)\ dt . \tag{1.23}$$

The average power S in x(t) is then

$$S = R_{xx}(0) = \frac{1}{t_0} \sum_{i=1}^{b} r_{ii}(0) \int_0^{t_0} h_i^{\,2}(t)\ dt \tag{1.24}$$

$$S = \frac{1}{t_0} \sum_{i=1}^{b} E_i\ r_{ii}(0)$$

where E_i is the energy in $h_i(t)$.

The correlation matrix $\underset{\sim}{r}(m)$ defined above can be further decomposed to reveal a few properties of $\underline{a}$. First, $\underset{\sim}{r}(0)$ is a diagonal matrix; $r_{ii}(0)$ is the relative frequency (probability) p_i with which state e_i occurs in $\underline{a}$. (We will assume that all $r_{ii}(0) \neq 0$, so that all states are non-null.) Second, $r_{ik}(m)$ is the relative frequency (probability) which states e_i

and e_k occur separated by m steps. And third, we can apply a Bayes' rule to get conditional relative frequencies (probabilities), $p_{ik}(m)$ that e_i is followed m steps later by e_k, given that e_i has occurred in $\underline{a}$:

$$p_{ik}(m) = \frac{r_{ik}(m)}{r_{ii}(0)} . \tag{1.25}$$

In matrix notation, we write $\underset{\sim}{r}(0) = \underset{\sim}{r}_0$

$$\underset{\sim}{r}(m) = \underset{\sim}{r}_0 \underset{\sim}{P}(m) . \tag{1.26}$$

B. Markov Modulation

In this section we let $\underline{a}$ be a stationary, irreducible, aperiodic Markov chain[12]. The outstanding property of such a chain is that

$$\underset{\sim}{r}(m) = \begin{cases} r_\Theta \left[\underset{\sim}{P}(1)\right]^m ; & m \geq 1 \\ \left[\underset{\sim}{P}^T(1)\right]^{-m} \underset{\sim}{r}_0 ; & m \leq -1 \end{cases} . \tag{1.27}$$

For convenience, we then set $\underset{\sim}{P}(1) = \underset{\sim}{P}$, so

$$\underset{\sim}{r}(m) = \begin{cases} \underset{\sim}{r}_0 \underset{\sim}{P}^m ; & m \geq 1 \\ (\underset{\sim}{P}^T)^{-m} \underset{\sim}{r}_0 ; & m \leq -1 \end{cases} . \tag{1.28}$$

The expression for $\underset{\sim}{S}(f)$ is then a geometric series

$$\underset{\sim}{S}(f) = \underset{\sim}{r}_0 \left[\underset{\sim}{I} + \sum_{n=1}^{\infty} \underset{\sim}{P}^n (e^{-j2\pi f t_0})^n\right] + \left[\sum_{n=1}^{\infty} (\underset{\sim}{P}^T)^n (e^{+j2\pi f t_0})^n\right] \underset{\sim}{r}_0 . \tag{1.29}$$

The form of $\underset{\sim}{P}$ is that of a stochastic matrix[13,14] whose eigenvalues must then lie on or within the unit circle. There is always at least one

eigenvalue equal to unity, and by restricting the chain to being irreducible and aperiodic we insure that there is only one unity magnitude eigenvalue[15]. But then $\underset{\sim}{S}(f)$ converges[16] for every f except possibly those for which

$$\begin{aligned} e^{-j2\pi t_0 f} &= 1 \\ e^{+j2\pi t_0 f} &= 1 . \end{aligned} \tag{1.30}$$

Consequently, $\underset{\sim}{S}(f)$ has removable discontinuities possibly at

$$f = \frac{m}{t_0}, \quad m = \ldots, -2, -1, 0, 1, 2, \ldots \tag{1.31}$$

We investigate these points by looking at the asymptotic behavior of $\underset{\sim}{r}(m)$. Asymptotically, $\lim_{n \to \infty} r_{ik}(n) = p_i p_k$, because after many transitions the states become independent.

$$S_{ik}(f) = \sum_{m=-\infty}^{+\infty} (r_{ik}(m) - p_i p_k)\, e^{-j2\pi t_0 fm} + p_i p_k \sum_{m=-\infty}^{+\infty} e^{-j2\pi t_0 fm} . \tag{1.32}$$

The latter sum is a well known one, being the Fourier-series expansion of a δ-function train

$$\sum_{m=-\infty}^{+\infty} e^{-j2\pi t_0 fm} = \frac{1}{t_0} \sum_{n=-\infty}^{+\infty} \delta\left(f - \frac{n}{t_0}\right) . \tag{1.33}$$

At all $f \neq \frac{n}{t_0}$, this sum is zero:

$$S_{ik}(f) = \sum_{m=-\infty}^{+\infty} r_{ik}(m)\, e^{-j2\pi t_0 fm}, \quad f \neq \frac{n}{t_0}, \tag{1.34}$$

so $S_{xx}(f)$ converges here to a spectral density. At $f = \frac{n}{t_0}$, we may, for the present, omit the contribution due to the spectral density:

$$S_{ik}(f) = \frac{p_i p_k}{t_0} \sum_{n=-\infty}^{+\infty} \delta(f - \frac{n}{t_0}) \, . \tag{1.35}$$

Substituting these into the spectral equation, we get

$$S_{xx}(f) = \frac{1}{t_0^2} \sum_{n=-\infty}^{+\infty} \left[\sum_{i=1}^{b} p_i \, H_i(f) \right]^2 \delta(f - \frac{n}{t_0}) + \frac{1}{t_0} \sum_{i=1}^{b} \sum_{k=1}^{b} H^*_i(f) \, H_k(f) \left[\sum_{m=-\infty}^{+\infty} r_{ik}(m) \; e^{-j2\pi f t_0 m} \right] . \tag{1.36}$$

There will be an absence of spectral lines if, and only if,

$$\sum_{i=1}^{b} p_i \, H_i(\frac{n}{t_0}) = 0 \qquad \text{for all } n. \tag{1.37}$$

But if we periodically extend the $h_i(t)$ outside $\left[0, \, t_0\right]$, the function

$$K(t) = \sum_{m=-\infty}^{+\infty} \sum_{i=1}^{b} p_i \, h_i(t - mt_0) \, , \tag{1.38}$$

aside from a constant factor, has its Fourier coefficients equal to

$\sum_{i=1}^{b} p_i \, H_i(\frac{n}{t_0})$, which are all zero, and therefore $K(t) = 0$.

We reach the conclusion that there are no spectral lines if, and only if,

$$\sum_{i=1}^{b} p_i \, h_i(t) = 0 \qquad \text{for } t \text{ in } \left[0, \, t_0\right] \, . \tag{1.39}$$

C. Examples of Markov Modulation

Let us assume that a Markov chain modulates a set of sinusoids

$$h_i(t) = \sin(\omega_i t + \phi_i) \tag{1.40}$$

$$\omega_i = \left(\frac{\pi}{t_0}\right) n_i$$

with n_i an integer (the number of half-cycles in $\left[0, t_0\right]$). We will choose simple chains so that $S_{xx}(f)$ takes a simplified form. In each case we will judiciously pick p_i, n_i and ϕ_i to eliminate spectral spikes.

1. Symmetric processes. Suppose that for every $h_k(t)$ in $\left\{h_i(t)\right\}$ there exists an r such that $h_r(t) = -h_k(t)$ is in $\left\{h_i(t)\right\}$ and $p_r = p_k$. This eliminates spikes in the spectrum. Further, assume that $p_{jk} = p_{rs}$ whenever $h_j(t) = \pm h_r(t)$ and $h_k(t) = \pm h_s(t)$; that is, we assume $r_{jk}(m) = r_{rs}(m)$. The spectral equation reduces to

$$S_{xx}(f) = \frac{1}{t_0} \sum_{i=1}^{b} p_i \left|H_i(f)\right|^2 . \tag{1.41}$$

From this equation we note that the over-all power spectrum is merely the weighted sum of the energy spectra of each individual component $h_i(t)$ in the modulated set.

As a special case, we allow unrestricted transitions

$$p_i = p_{ik} = \frac{1}{b} \tag{1.42}$$

Routine calculation yields

$$S_{xx}(f) = \frac{t_0}{b} \sum_{i=1}^{b} \left[\frac{\sin\left(\frac{\omega-\omega_i}{2}\right)t_0}{\left(\frac{\omega-\omega_i}{2}\right)t_0} \right]^2 \left[\frac{\cos^2 \phi_i + \left(\frac{\omega}{\omega_i}\right)^2 \sin^2 \phi_i}{\left(1 + \frac{\omega}{\omega_i}\right)^2} \right] \quad (1.43)$$

where $\omega = 2\pi f$. According to this equation, the phase angles ϕ_i are of importance in the region $\omega >> \omega_i$. Each term is a sine-square enveloped by

$$S_{env}(f) = \frac{4}{bt_0} \frac{\omega_i^2 \cos^2 \phi_i + \omega^2 \sin^2 \phi_i}{(\omega^2 - \omega_i^2)^2} \quad . \quad (1.44)$$

If ϕ_i is not a multiple of π, the spectrum ultimately decays at 6 db/octave; but if ϕ_i is a multiple of π, there is a 12 db/octave roll-off. The rate of approach to the 6 db asymptote is determined by ϕ_i, since for ϕ_i near zero, the spectrum seems to approach a 12 db limit; but as ω grows sufficiently large, the roll-off ultimately changes to 6 db/octave.

When each independent ϕ_i is considered to be a random variable uniformly distributed over $[0, 2\pi]$, the resulting spectrum is the average over this range; each term is of the form

$$S_{xx}(f) = \frac{t_0}{2} \left[\frac{\sin \frac{\omega - \omega_i}{2} t_0}{\frac{\omega - \omega_i}{2} t_0} \right]^2 \left[\frac{1 + \left(\frac{\omega}{\omega_i}\right)^2}{\left(1 + \frac{\omega}{\omega_i}\right)^2} \right] \quad (1.45)$$

This is exactly the same equation of spectral density obtained by assuming independence between carrier and modulation or obtained by setting each $\phi_i = \frac{\pi}{4}$. Figure 1.3 shows examples of the spectral distribution of modulated sinusoids with different phases, compared to the spectrum when the sinusoids are replaced by unit square waves of the same period (maxima are set equal so that roll-off can be compared). Note the 90 deg-shifted

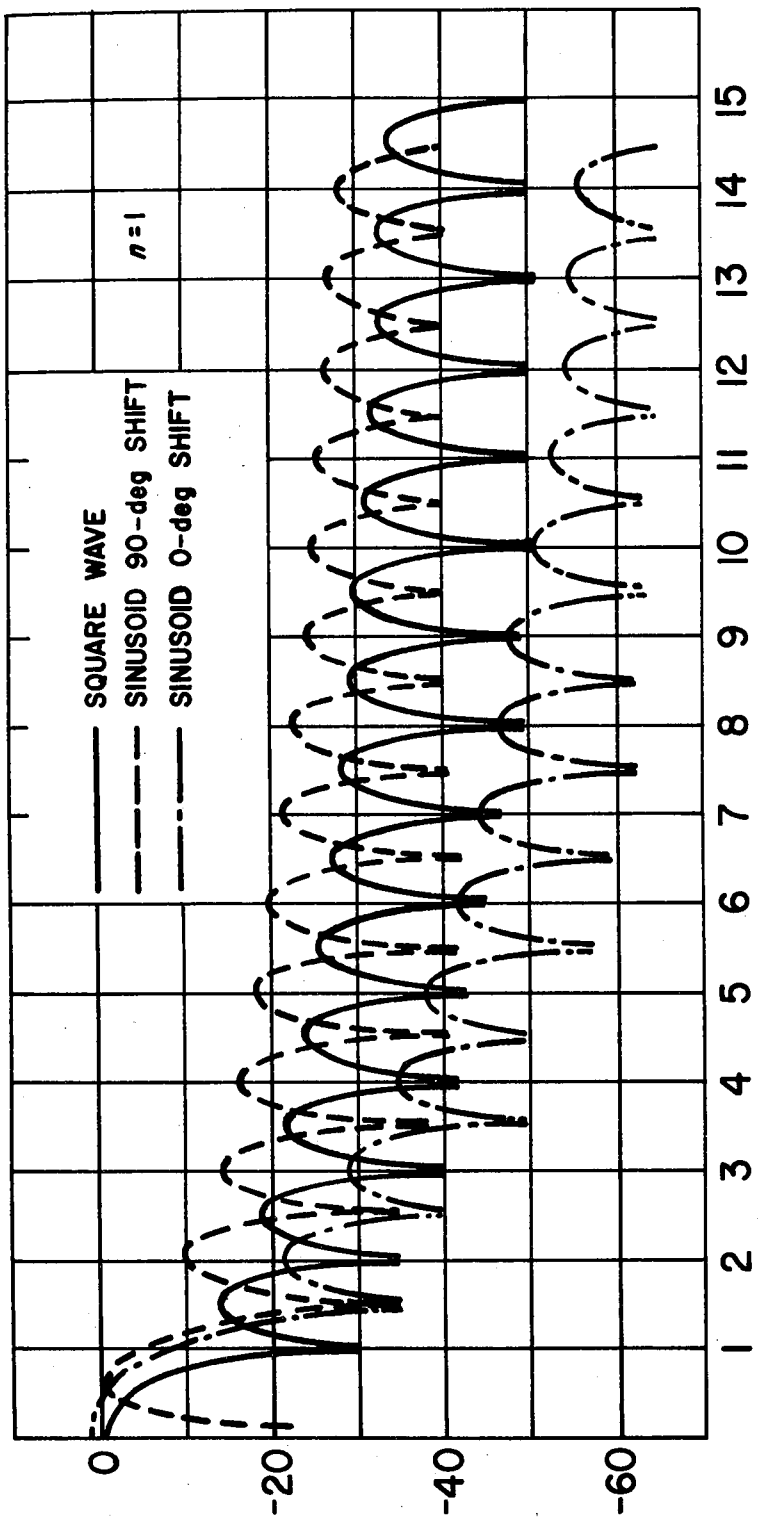

FIGURE 1.3a. SPECTRA OF SIGNALS MODULATED BY MARKOV CHAINS, FOR $t_0 = 1$ (NORMALIZED)

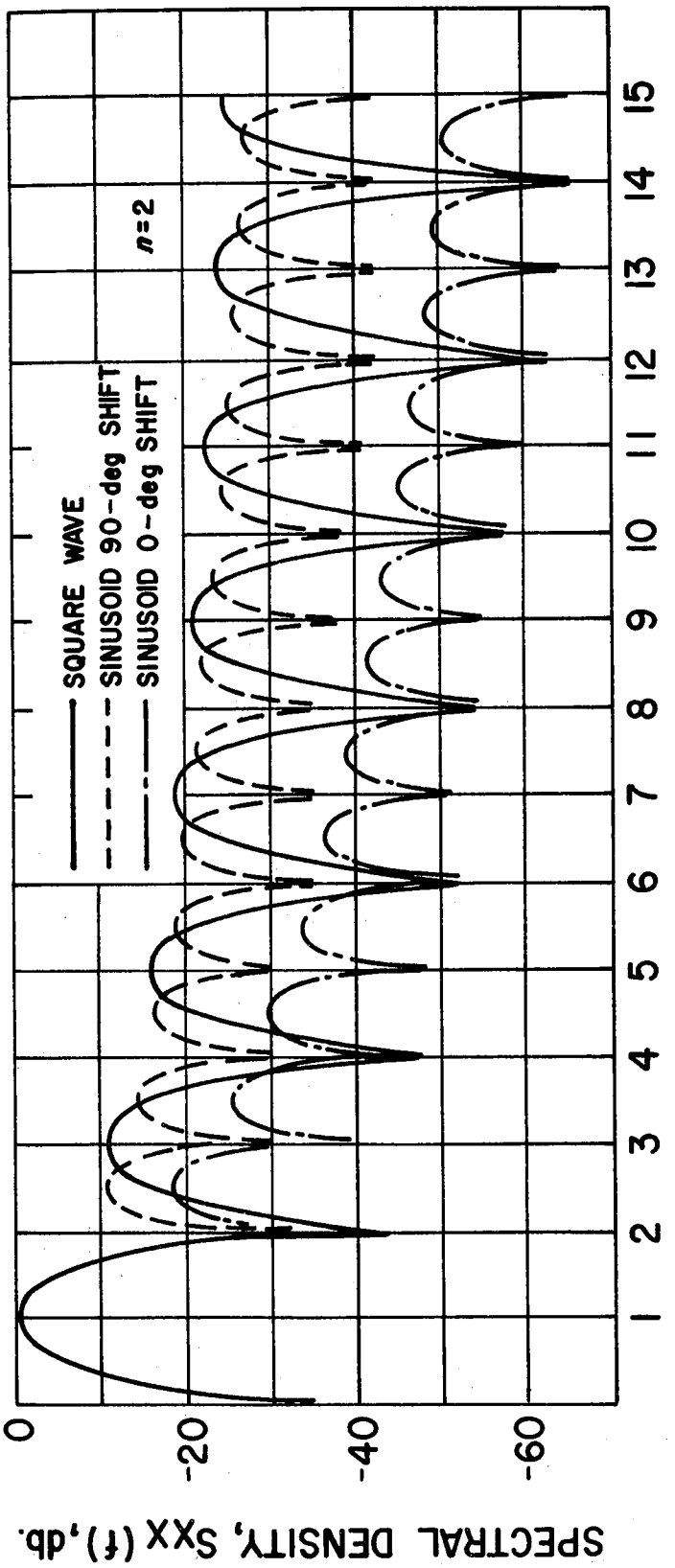

FIGURE 1.3b. SPECTRA OF SIGNALS MODULATED BY MARKOV CHAINS, FOR $t_0 = 1$ (NORMALIZED)

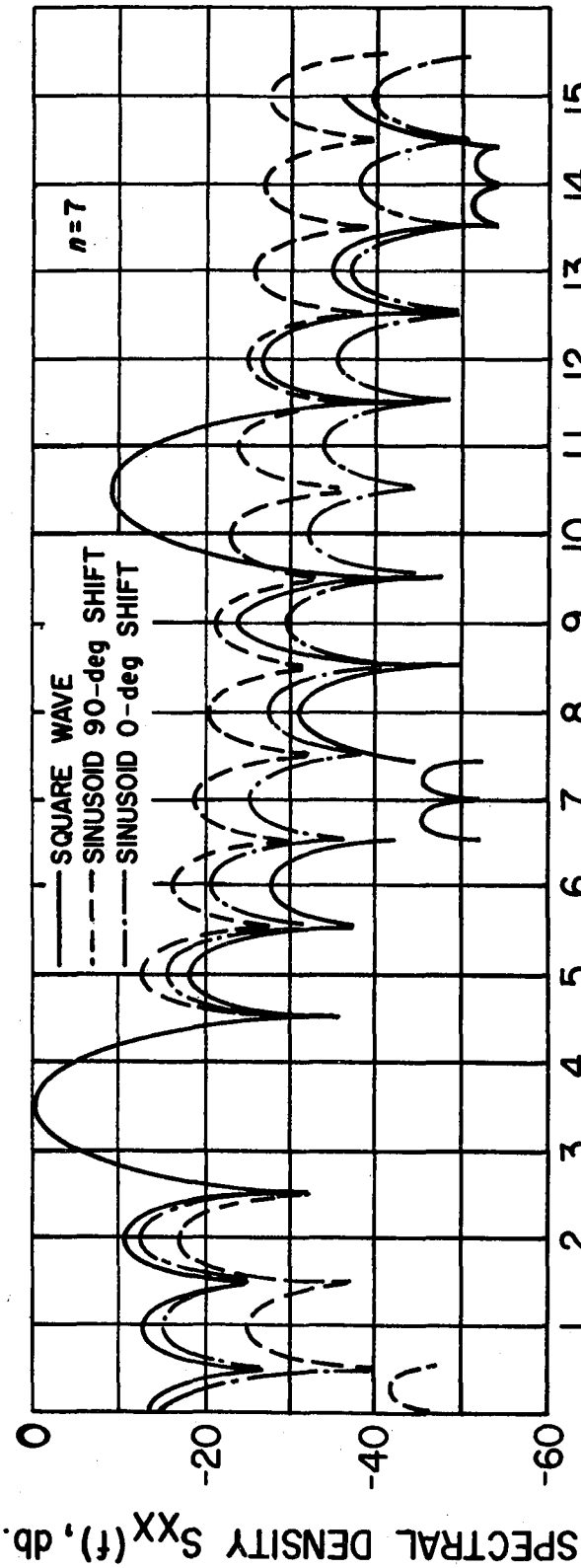

FIGURE 1.3c. SPECTRA OF SIGNALS MODULATED BY MARKOV CHAINS, FOR $t_0 = 1$. (NORMALIZED)

sinusoid rolls off at about the same rate as the square wave but that the 0 deg-shifted sinusoid decays much faster.

2. Equi-phase modulation. Suppose all ω_i are the same, but $\phi_i = \frac{2\pi i}{b}$. The common value of ω_i we designate ω_0. One may verify that there are again no spectral lines, and the spectrum is given by

$$S_{xx}(f) = \frac{t_0(\omega^2 + \omega_0^2)}{2(\omega + \omega_0)^2} \left[\frac{\sin(\frac{\omega-\omega_0}{2})t_0}{(\frac{\omega-\omega_0}{2})t_0} \right] \tag{1.46}$$

This is the same equation for random-phase modulation given earlier.

3. Slope-preserving modulation. We now restrict $\underline{a}$ to be a Markov chain which excludes transitions except between waveforms which preserve the sign of the slope at the changeover times $t = nt_0$. Again, for every $h_i(t)$ there is a corresponding $h_r(t) = -h_i(t)$, and again $p_i = p_r$. However, if we partition $\{h_i(t)\}$ into the subsets

$$\begin{aligned}
\{h_{++}\} &= \{ h_i(t): \text{ slope (+) at } t = 0, \text{ (+) at } t_0 \} \\
\{h_{+-}\} &= \{ h_j(t): \text{ slope (+) at } t = 0, \text{ (-) at } t_0 \} \\
\{h_{--}\} &= \{ -h_{++} \} \\
\{h_{-+}\} &= \{ -h_{+-} \} \quad .
\end{aligned} \tag{1.47}$$

The transition matrix is then similarly partitioned

$$\underset{\sim}{P} = \left[\begin{array}{cc|cc}
\underset{\sim}{P}_{++} & \underset{\sim}{P}_{+-} & \underset{\sim}{Q} & \underset{\sim}{Q} \\
\underset{\sim}{Q} & \underset{\sim}{Q} & \underset{\sim}{P}_{-+} & \underset{\sim}{P}_{--} \\
\hline
\underset{\sim}{Q} & \underset{\sim}{Q} & \underset{\sim}{P}_{++} & \underset{\sim}{P}_{+-} \\
\underset{\sim}{P}_{-+} & \underset{\sim}{P}_{--} & \underset{\sim}{Q} & \underset{\sim}{Q}
\end{array}\right] . \tag{1.48}$$

Using equation 1.29, we calculate the spectrum

$$S_{xx}(f) = \frac{2}{t_0} \sum_{i=1}^{\frac{b}{2}} p_i \left| H_i(f) \right|^2 + \frac{4}{t_0} \mathrm{Re} \left\{ \tilde{\underset{\sim}{H}}^*(f) \, \tilde{\underset{\sim}{S}}(f) \, \tilde{\underset{\sim}{H}}(f) \right\} , \quad (1.49)$$

which involves only the "positive" waveforms h_{++} and h_{+-}, with

$$\tilde{\underset{\sim}{H}}(f) = \begin{bmatrix} H_1(f) \\ H_2(f) \\ \cdot \\ \cdot \\ \cdot \\ H_{b/2}(f) \end{bmatrix}$$

$$\underset{\sim}{r}_0 = \mathrm{diag} \left[p_1, p_2, \cdots, p_{b/2} \right]$$

$$\underset{\sim}{S}(f) = \underset{\sim}{r}_0 \sum_{n=1}^{+\infty} \begin{bmatrix} \underset{\sim}{P}_{++} & \underset{\sim}{P}_{+-} \\ -\underset{\sim}{P}_{-+} & -\underset{\sim}{P}_{--} \end{bmatrix}^n e^{-j2\pi f t_0 n} . \quad (1.50)$$

We now work a particular example of a slope-preserving sinusoidal process described by

$$b = 4$$

$$n_1 = n_3 \text{ is even}$$

$$n_2 = n_4 \text{ is odd}$$

$$P = \frac{1}{2} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix} \quad (1.51)$$

Substitution of these parameters into the spectrum yields, upon simplification,

$$S_{xx}(f) = \frac{1}{t_0}\left[\left(\frac{\omega_1}{\omega^2-\omega_1^2}\right) - \left(\frac{\omega^2}{\omega^2-\omega_2^2}\right)\right]^2 \sin^2 \omega t_0 \quad . \tag{1.52}$$

For large $f = \frac{\omega}{2\pi}$, $S_{xx}(f)$ decreases at approximately 12 db/octave. This is again because of the chosen phase relations. Examples of such spectra are illustrated in Figure 1.4. If n_1 and n_2 are adjacent integers, $S_{xx}(f)$ falls off very rapidly near the fundamental peaks.

D. Random-like Periodic Modulation

It is well known that periodic signals possess periodic correlation functions and that their spectra are composed entirely of impulse functions at multiples of the fundamental frequency determined by the correlation period. Furthermore, it is known that the Fourier transform of a periodic process x(t) is of the form[17]

$$X(f) = \frac{X_0(f)}{T} \sum_{m=-\infty}^{+\infty} \delta\left(f - \frac{m}{T}\right), \tag{1.53}$$

where T is the period of x(t) and $X_0(f)$ is the Fourier transform of one cycle of x(t). If x(t) were a correlation function, $R(\tau)$, the corresponding transform is a power spectrum

$$\begin{aligned} S(f) &= \frac{S_0(f)}{T} \sum_{m=-\infty}^{+\infty} \delta\left(f - \frac{m}{T}\right) \\ S_0(f) &= \int_{-T/2}^{T/2} R(\tau)\, e^{-j2\pi f}\, d\tau \quad . \end{aligned} \tag{1.54}$$

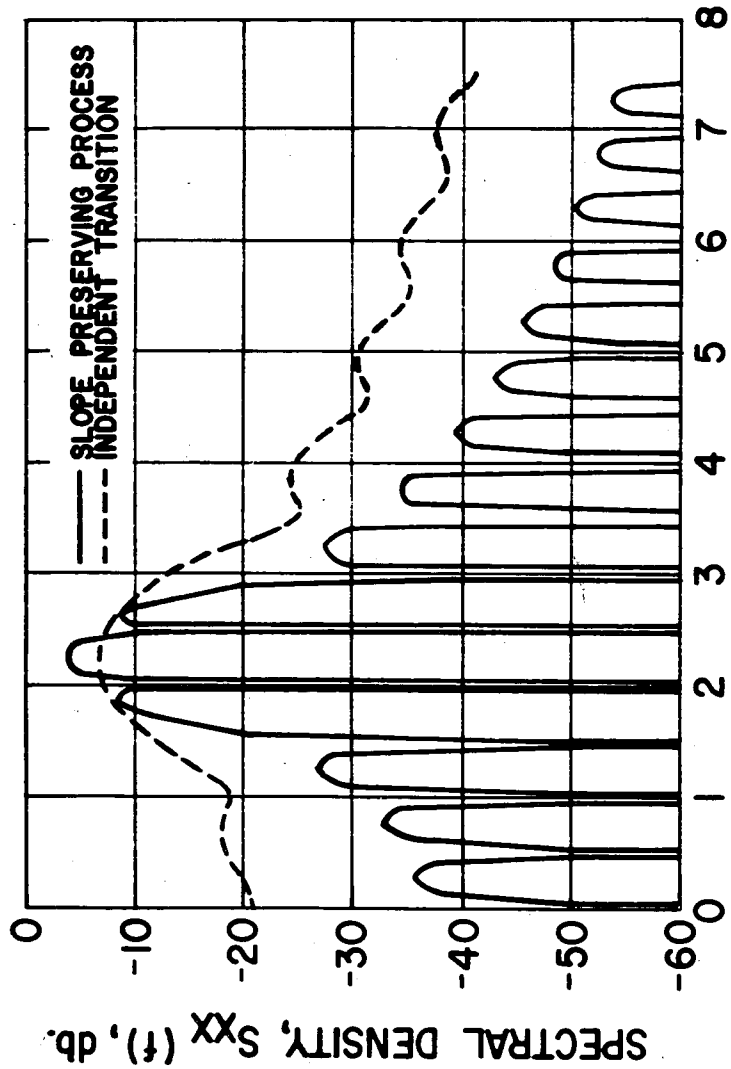

FIGURE 1.4a. SPECTRA OF TWO-FREQUENCY PROCESSES, $t_0=1$, $n_1=4$, $n_2=5$

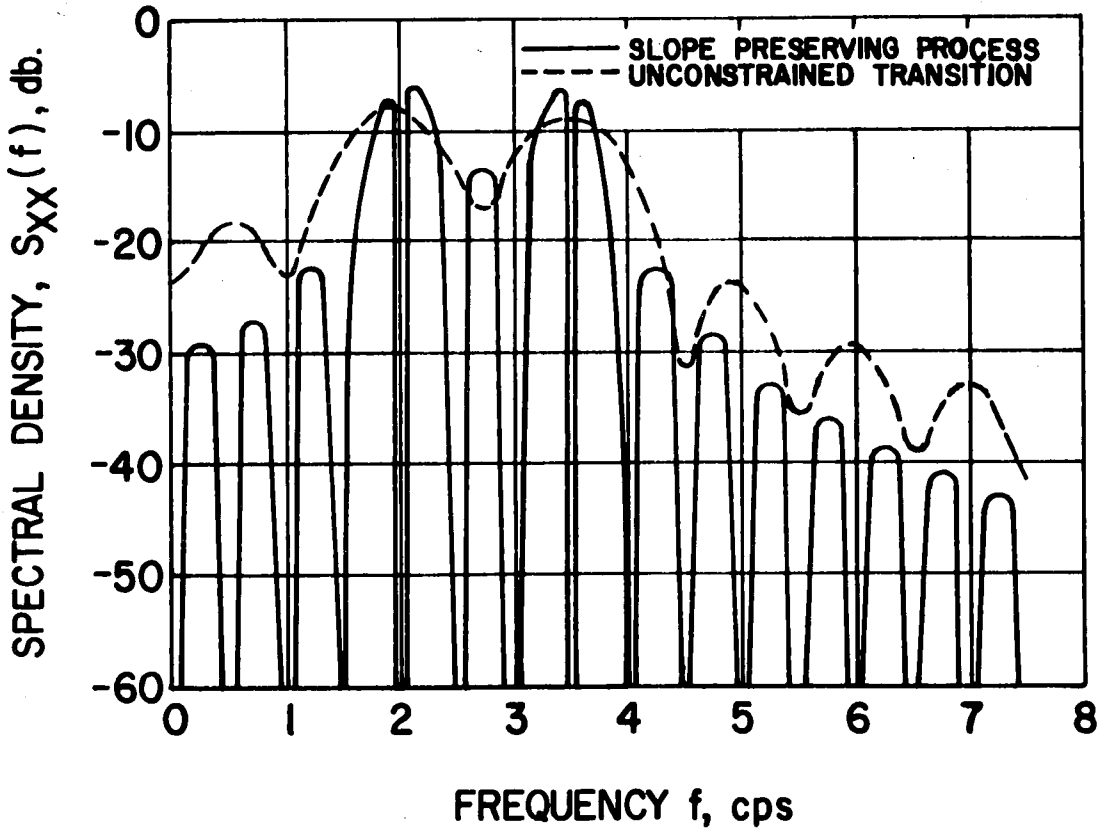

FIGURE 1.4b. SPECTRA OF TWO FREQUENCY PROCESSES, $t_0=1$, $n_1=4$, $n_2=7$

A periodic signal thus has a spectrum of "spikes", weighted by an "envelope"; this envelope is the power spectrum of an aperiodic process having identical correlation in (-T/2, +T/2) and zero elsewhere. If this autocorrelation were some non-zero constant outside this range there would be a change in the dc value and if only approximately constant, the envelope and dc would be in some slight error, depending on the seriousness of the fluctuations outside the specified range. Whenever a periodic sequence has sufficient random-like correlation properties, we can approximate the envelope of its spectral behavior by that of a random process. For example, a binary Markov sequence with independent states has a two-level correlation function and can be approximated by periodic binary sequences which also possess two-level correlation functions. The accuracy of this approximation is surprisingly good, as we shall see.

Linear recurring sequences. Given a sequence $\underline{a} = \alpha$ whose states $e_i = \epsilon_i$ are elements of a finite field $\mathcal{K}$, and a set $\{\gamma_0, \gamma_1, \ldots, \gamma_m\}$ of elements also in $\mathcal{K}$, then $\underline{a}$ is said to be linearly recurring if for all n

$$\sum_{i=0}^{m} \alpha_{n-i} \gamma_i = 0 . \tag{1.55}$$

Such a sequence is easily mechanized by shift-registers as shown in Figure 1.5. Much work[18,19,20] has been done on such sequences, and an abundance of information about them is available. The major portion of the theory is not of concern here, but a few significant properties are given.

Because each α_n belongs to a finite field, the number of states $b = q^k$ where q is prime. For a given m, the maximum period p is $p = b^m - 1$; these maximum - length linear recurring sequences are usually

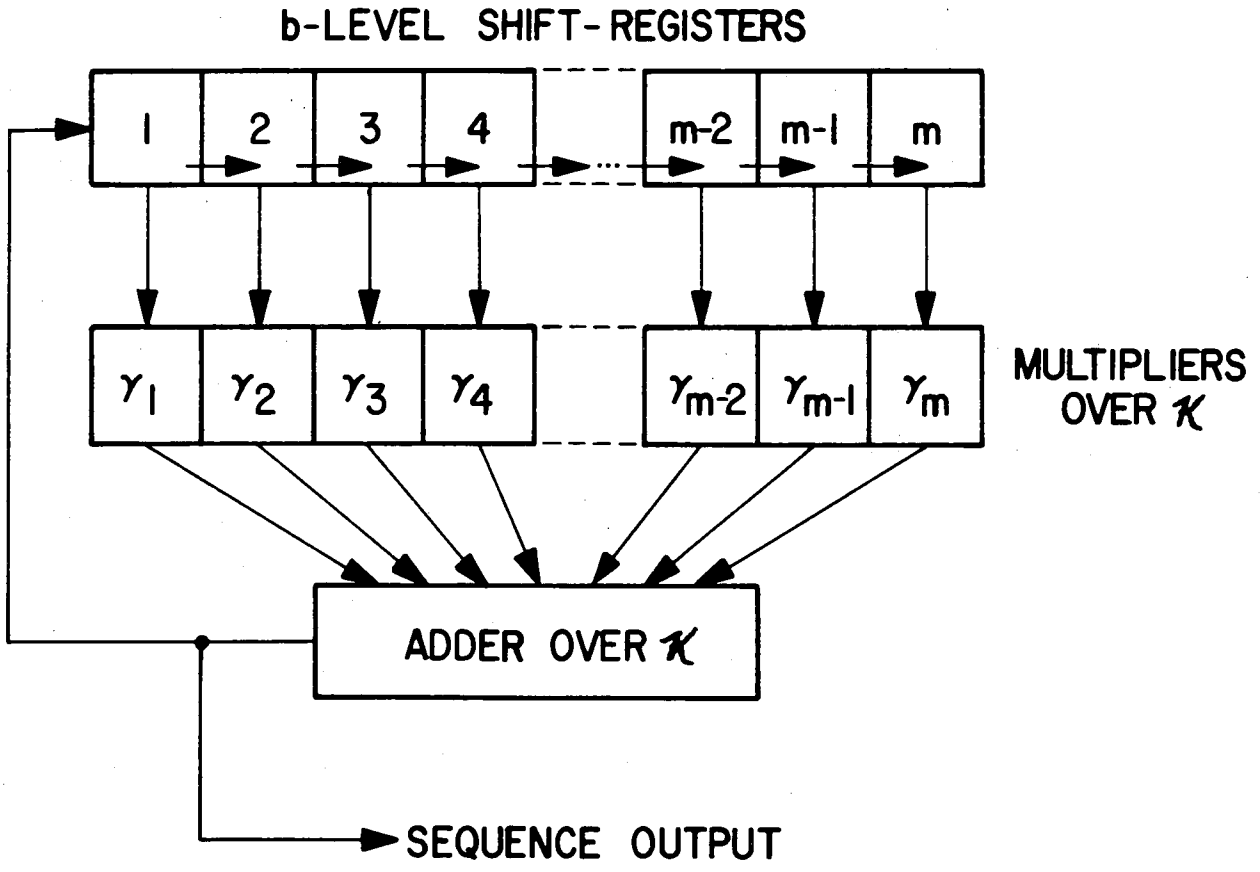

FIGURE 1.5.
LINEAR SHIFT-REGISTER SEQUENCE GENERATOR

referred to merely as linear sequences or m-sequences (this latter terminology is due to Zierler). All states except one occur b^{m-1} times per period. The excepted state is the zero of $\mathcal{K}$ which only occurs $b^{m-1}-1$ times.

The frequencies of occurrence (designating ϵ_b as the zero element of $\mathcal{K}$) are

$$\begin{aligned} p_i &= \frac{p+1}{bp}\,; \qquad (i = 1, 2, \ldots, b-1) \\ p_b &= \frac{p+1-b}{bp}\,. \end{aligned} \tag{1.56}$$

The correlation properties of α are almost like those of a Markov chain with unrestricted transitions.

$$\underset{\sim}{P}(t) = \begin{bmatrix} \frac{1}{b} & \frac{1}{b} & \cdots & \frac{1}{b} \\ \frac{1}{b} & \frac{1}{b} & \cdots & \frac{1}{b} \\ \frac{1}{b-b^{-m+2}} & \frac{1}{b-b^{-m+2}} & \cdots & \frac{1-b^{-m+2}}{b-b^{-m+2}} \end{bmatrix} \tag{1.57}$$

for all $t \not\equiv 0 \bmod p/(b-1)$. When $t \equiv 0 \bmod p/(b-1)$,

$$p_{ik}\left(\frac{Mp}{b-1}\right) = \delta(\epsilon_k, \mu^M \epsilon_i)\,, \tag{1.58}$$

for some primitive element μ of the field and $\delta(\,,\,)$ is the Kronecker delta. The primitive μ is the element

$$\mu = \alpha_{t+s}\,\alpha_t^{-1} \tag{1.59}$$

for all non-zero α_t of α, with $s = p/(b-1)$.

If the correlation function is inserted into the fundamental equation, 1.13, the spectral distribution is finally found to be

$$S_{xx}(f) = \frac{1}{t_0^2}\left\{\frac{1}{p}\left[\left(\frac{p+1}{b^2}\right)\sum_{i=1}^{b}\sum_{k=1}^{b} H^*_i(f)\,H_k(f) - \left|H_b(f)\right|^2\right]\sum_{n=-\infty}^{+\infty}\delta\left(f-\frac{n}{t_0}\right)\right.$$

$$+\frac{p+1}{p^2}\left(\frac{b-1}{b}\right)\left[\left|H_b(f)\right|^2 - \frac{1}{b}\sum_{i=1}^{b}\sum_{k=1}^{b} H^*_i(f)\,H_k(f)\right]\sum_{n=-\infty}^{+\infty}\delta\left(f-\frac{n(b-1)}{pt_0}\right)$$

$$+\frac{p+1}{bp^2}\left[\sum_{i=1}^{b-1}\sum_{k=1}^{b-1}\sum_{r=1}^{b-1} H^*_i(f)\,H_k(f)\;e^{-\frac{j2\pi frpt_0}{b-1}}\;\delta(\epsilon_k, \mu^r\epsilon_i)\right]$$

$$\left.\sum_{n=-\infty}^{+\infty}\delta\left(f-\frac{n}{pt_0}\right)\right\} \quad . \tag{1.60}$$

E. Examples of Linear Sequence Modulation

By choosing processes similar to those treated in our previous Markov model, we can show a great similarity between the spectra of signals modulated by linear sequences and by Markov chains. There are, of course, certain differences and these, too, we wish to illustrate.

1. Binary modulation. When we limit $b = 2$ and $h_1(t) = -h_2(t)$, many terms vanish from $S_{xx}(f)$. The result has exactly the same form as the corresponding Markov spectrum except at frequencies $f = \frac{n}{t_0}$. At these points, $S_{xx}(f)$ drops to about $\frac{1}{p}$ of the value predicted by the Markov modulation. The linear sequence spectrum is

$$S_{xx}(f) = \frac{|H(f)|^2}{p^2 t_0^2}\left[(p+1)\sum_{n=-\infty}^{+\infty}\delta\left(f-\frac{n}{pt_0}\right) - p\sum_{n=-\infty}^{+\infty}\delta\left(f-\frac{n}{t_0}\right)\right]. \tag{1.61}$$

If the period is long, this appears essentially to be the spectrum of a Markov process with two equally-likely states.

2. Equi-phase modulation of sinusoids. Here we choose the $h_i(t)$ to be the same as those in Markov equi-phase modulation; i.e.

$$h_i(t) = \sin(\omega_0 t + \frac{2\pi i}{b}) \qquad \omega_0 = \frac{r\pi}{t_0} \quad . \tag{1.62}$$

After completing the calculations, we arrive at

$$S_{xx}(f) = \frac{1}{(\omega+\omega_0)^2}\left[\frac{\sin(\frac{\omega-\omega_0}{2})t_0}{(\frac{\omega-\omega_0}{2})t_0}\right]^2 \left\{ \begin{array}{l} (\frac{p+1}{p^2})\omega_0^2 \sum_{n=-\infty}^{+\infty} \delta(f - \frac{2n}{pt_0}) \\ + (\frac{p+1}{p^2})\omega^2 \sum_{n=-\infty}^{+\infty} \delta(f - \frac{2n+1}{pt_0}) \\ - \frac{\omega_0^2}{p^2} \sum_{n=-\infty}^{+\infty} \delta(f - \frac{n}{t_0}) \end{array} \right\} \tag{1.63}$$

Comparing this formula with that of the corresponding Markov process, one sees that, except at frequencies which are multiples of $\frac{1}{t_0}$, the average of adjacent spikes in the linear-sequence spectrum gives the same general shape as that of the Markov. To a frequency analyzer whose bandwidth of resolution is insufficient to distinguish individual lines, the linear spectrum appears to have a Markovian character.

At frequencies which are multiples of $\frac{1}{t_0}$, $S_{xx}(\frac{n}{t_0})$ is smaller than the spikes surrounding it by a factor of $\frac{1}{p}$. This is the same behavior exhibited by binary modulation at these frequencies.

One thing important to note at this point is that the correlation of α is not Markovian for $b > 2$, because certain states become highly correlated at delays less than the period of α (see Figure 1.6). However, by proper choice of modulating waveform, this apparent difficulty does not give anomalous results.

F. Discussion of Modulation Spectra

We have shown that random and random-like sequences may modulate carriers in such a way that the concentrations of power at specific frequencies are not apparent. This is important when the receiver employs a phase-locked loop[21], for then the loop could possibly lock onto an undesired frequency.

We have also seen that by choosing the correlation function of the periodic sequence to be similar to that of the random one, the two spectra resemble each other, sometimes with amazing accuracy. Random sequences are generally easier to work with mathematically because statistical averaging is usually easier than time averaging. Hence, by proper periodic modulation, we can use statistical means to compute spectra with little loss in accuracy.

Although no exact formulae have been calculated for slope-preserving linear sequence processes, experiments have shown that the measured linear sequence spectra are extremely well approximated by a Markov envelope (Figure 1.7). Although the spectra here ultimately decay at the same rate as the unrestricted transition processes, larger, more pronounced peaks located near fundamental frequencies of $h_i(t)$ occur. These processes are then doubly important: first, such processes may be easier to mechanize by reason of smoother transition between states, and, second, it is possible to create a broad-band spectrum which falls off rapidly outside the band. To a transmitter, this means that power is not wasted outside the desired band.

SEQUENCE $\alpha=\{E_1,E_1,E_2,E_1,E_0,E_3,E_3,E_1,E_3,E_0,E_2,E_2,E_3,E_2,E_0\}$

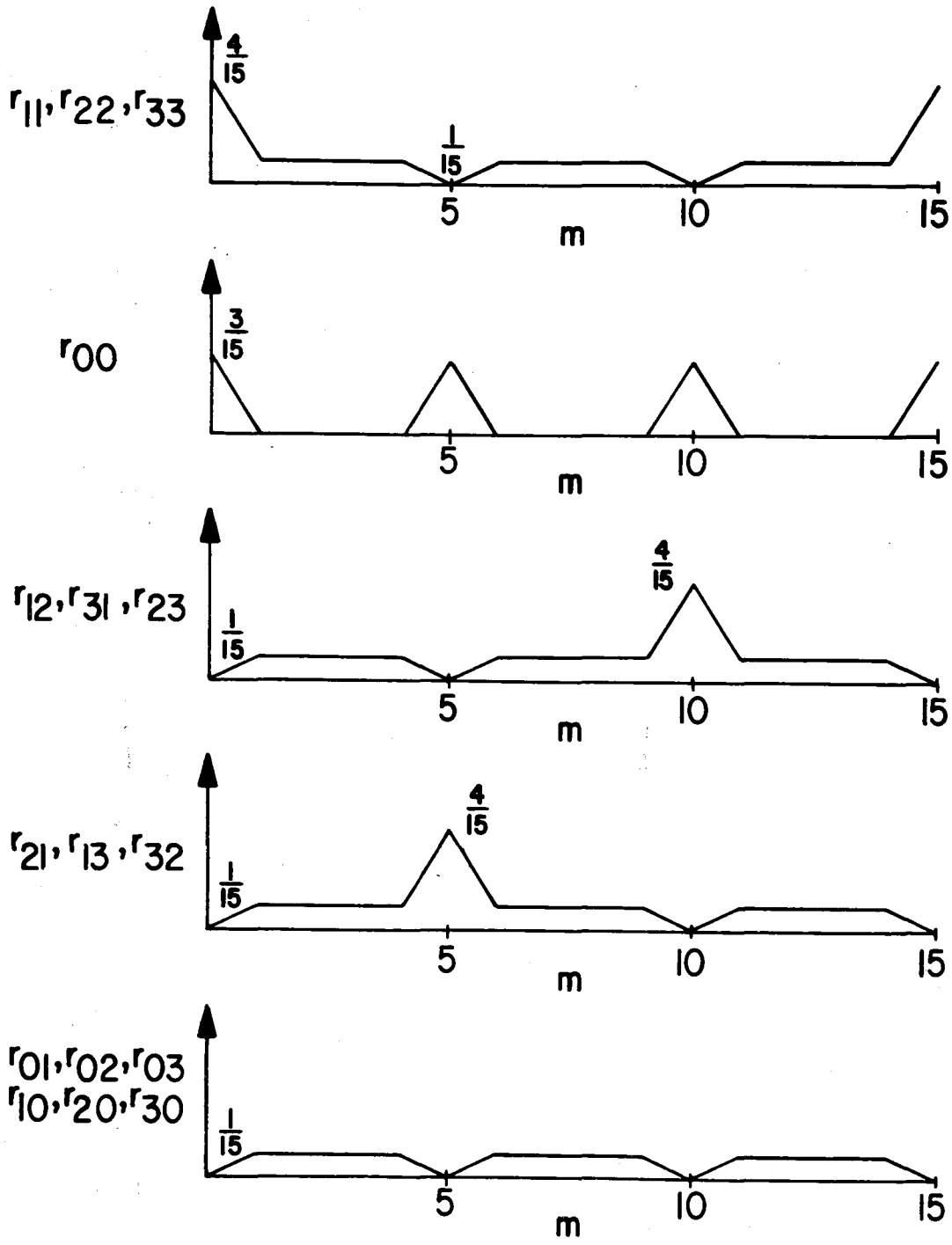

FIGURE 1.6.
STATE CORRELATIONS OF THE PERIOD 15 2-SEQUENCE OVER GF (4)

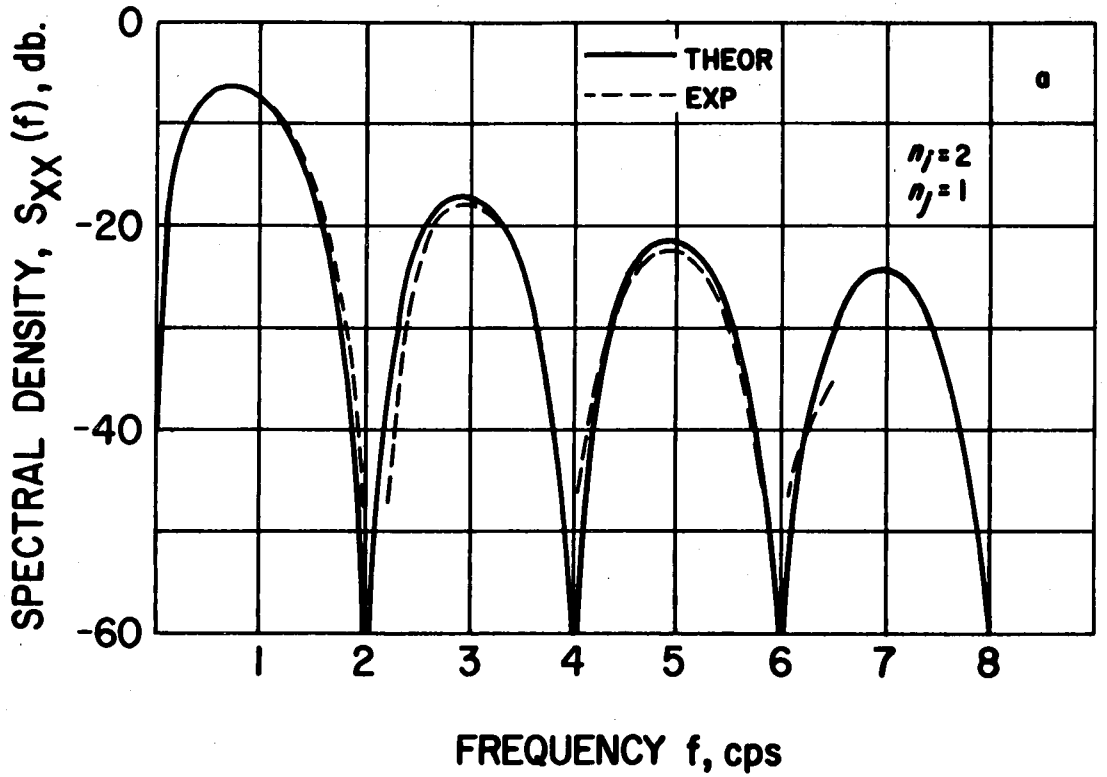

FIGURE 1.7a. COMPARISON OF SLOPE PRESERVING THEORETICAL MARKOV-MODULATED AND MEASURED LINEAR SEQUENCE-MODULATED SPECTRAL DENSITIES (NORMALIZED), FOR $t_0 = 1$. SIGNAL SETS ARE SQUARE WAVES.

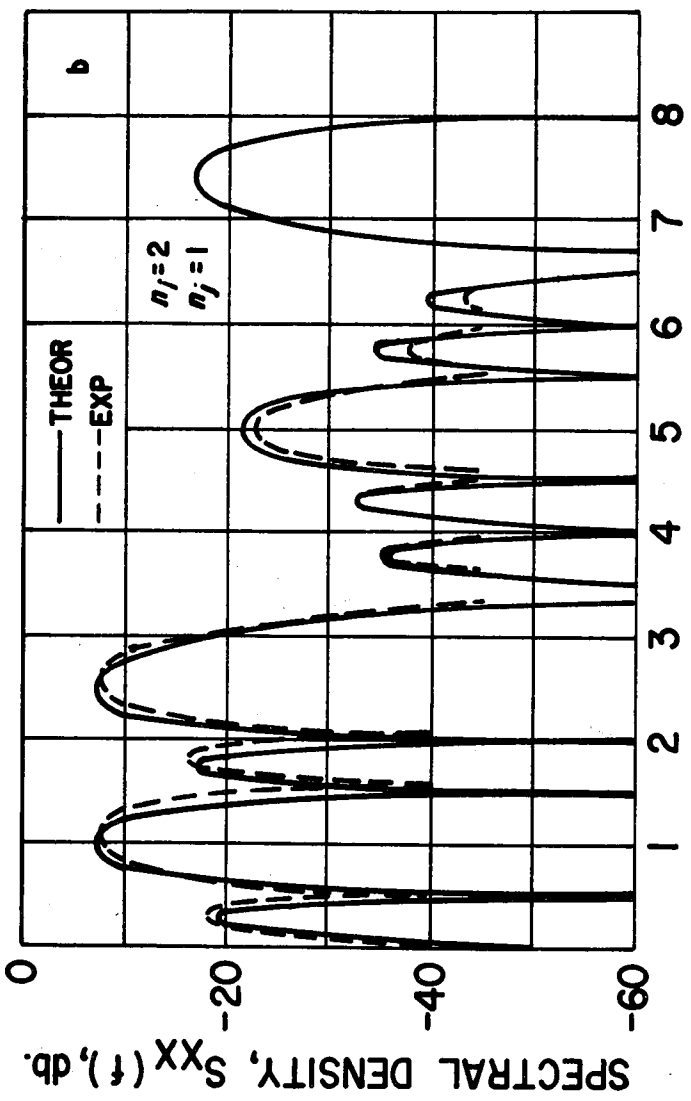

FIGURE I.7b COMPARISON OF SLOPE PRESERVING THEORETICAL MARKOV MODULATED AND MEASURED LINEAR SEQUENCE MODULATED SPECTRAL DENSITIES (NORMALIZED), FOR $t_0=1$. SIGNAL SETS ARE SQUARE WAVES.

Chapter 2

DETECTION OF SEQUENCE-MODULATED SIGNALS

A. Description of the Detection Process

Suppose that a signal $x(t)$, generated by modulating a carrier set $\{h_i(t)\}$ by a sequence $\underline{a}$ having period p, is sent through a simple continuous channel with additive white Gaussian noise of zero mean, as shown in Figure 2.1. The time series $y(t)$ presented to the receiver is

$$y(t) = x(t-\tau) + n(t) . \tag{2.1}$$

Here we have assumed no attenuation in the channel; we may do this without loss in generality by assuming that the receiver is capable of amplifying $y(t)$ to recover any channel loss. The noise is, of course, also amplified, and this must be taken into account.

The receiver knows the statistics of the noise, bounds on the time delay τ (τ assumed constant), the sequence $\underline{a}$, except for its phase, the carrier set $\{h_i(t)\}$, and the modulating scheme (i.e., the correspondence $e_i \longrightarrow h_i(t)$). The receiver is to estimate either the unknown phase of $\underline{a}$, or the channel time-delay, or both.

If τ is known, the channel is telemetry using a cyclic code $\underline{a}$; if the receiver knows the transmitted phase of $\underline{a}$, the transmitter-receiver is a coded, continuous radar-device measuring the "length" τ of the channel. If both τ and the phase of $\underline{a}$ are unknown, with

$$\tau = k\, t_0 + \tau_0, \quad (0 \leq \tau_0 \leq t_0) , \tag{2.2}$$

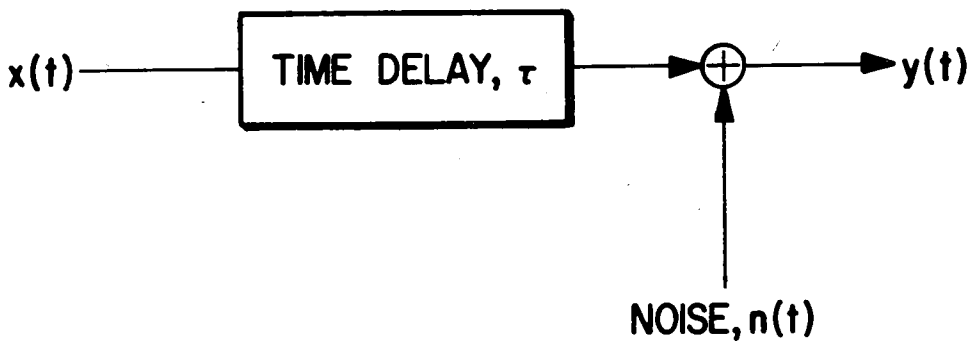

FIGURE 2.1. THE CONTINUOUS CHANNEL

then the phase of $\underline{a}$ at the receiver is its initial phase plus k additional units delay. By transmitting a carrier modulated by the clock rate t_0, τ_0 can be measured by a phase-locked receiver[22]. Once τ_0 is found, the receiver "locks" this quantity out of the measurement on τ. We then only need consider cases with $\tau = kt_0$.

We will assume for the remainder of the present discussion then that such an initial synchronization or modulation lock is in effect. The receiver we investigate is one which estimates the phase of $\underline{a}$ as if it were for a radar system. Then we can make suitable interpretation to include the telemetry channel or the telemetry + radar device (but the latter requires additional information, or time-sharing of the device, or some such scheme to separate the phase of $\underline{a}$ from the channel delay).

Both the receiver and the modulating periodic sequence $\underline{a}$ are to be chosen to minimize the $\underline{a}$ posteriori probability of error in estimating the unknown phase of $\underline{a}$. It is a well-known fact that the receiver in such cases is a correlating device (Figure 2.2); but for the sake of completeness, we will show the form the correlations must take and the properties which $\underline{a}$ must have. The argument is not a rigorous one but indicates the form of the solution much more easily than more mathematical treatments[23,24].

We assume $\tau = kt_0$, so $y(t) = x(t - kt_0) + n(t)$, and that $y(t)$ may be observed for one period pt_0 of $x(t)$. To minimize the probability of error, we must choose our estimate m so as to maximize the conditional probability $\Pr\left\{ k = m \,\middle|\, y(t);\ 0 \le t \le pt_0 \right\}$. Then the probability of error, given by

$$P_e = \sum_{r \neq m} \Pr\left\{ k = r \,\middle|\, y(t);\ 0 \le t \le pt_0 \right\} \tag{2.3}$$

is surely a minimum.

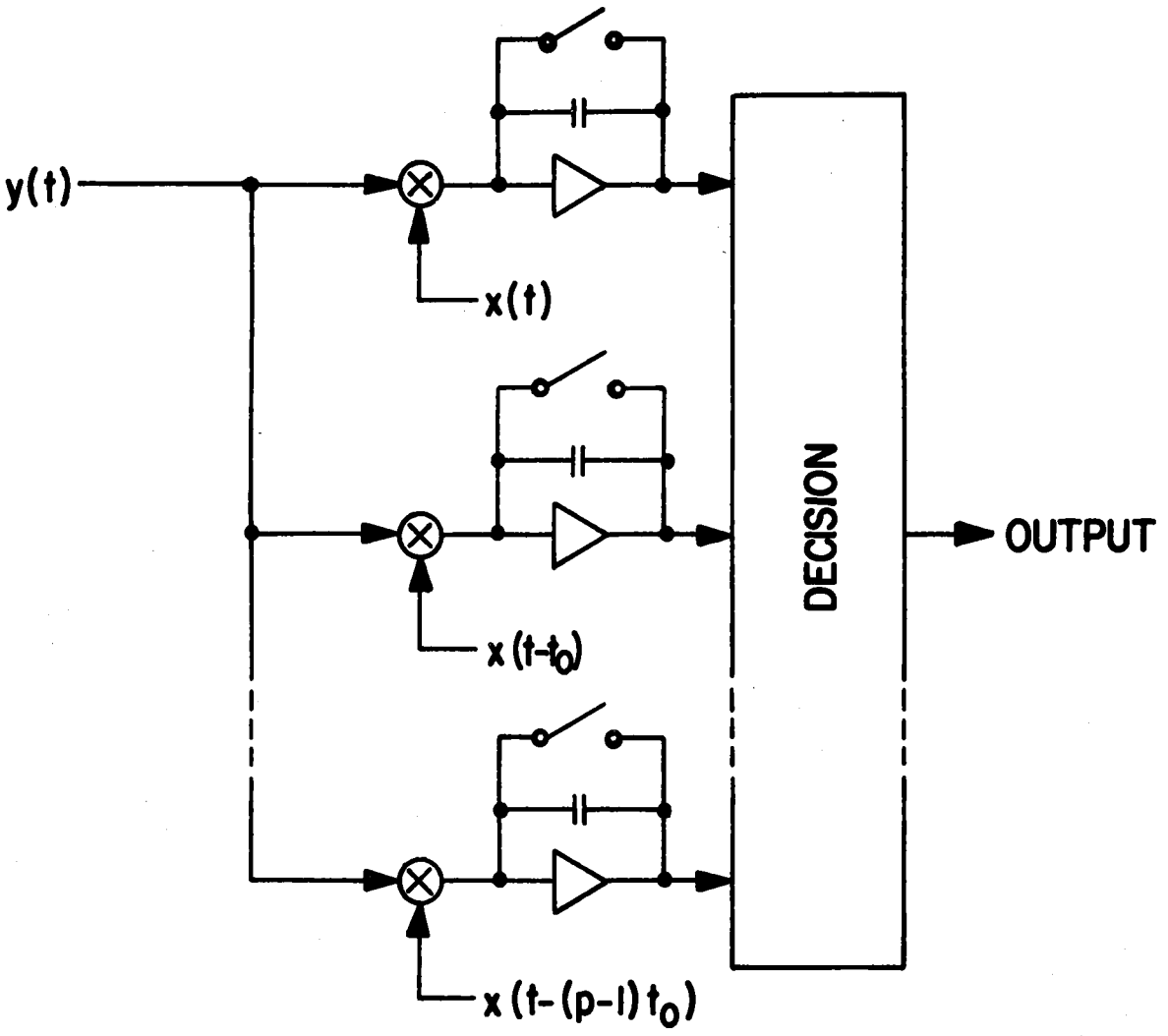

FIGURE 2.2. THE OPTIMUM RECEIVER FOR THE WHITE-NOISE GAUSSIAN CHANNEL.

By Bayes' rule[25], we can reverse the conditional relationship.

$$\Pr\left\{ k = m \middle| y(t) \right\} \Pr\left\{ y(t) \right\} = \Pr\left\{ y(t) \middle| k = m \right\} \Pr\left\{ k = m \right\} \tag{2.4}$$

The likelihood ratio between possibilities k = m and k = n is

$$\frac{\Pr\left\{ k = m \middle| y(t) \right\}}{\Pr\left\{ k = r \middle| y(t) \right\}} = \frac{\Pr\left\{ k = m \right\} \Pr\left\{ y(t) \middle| k = m \right\}}{\Pr\left\{ k = r \right\} \Pr\left\{ y(t) \middle| k = r \right\}} . \tag{2.5}$$

Considering all admissible candidates for the phase of a equally likely, we reduce the problem to that of choosing m so as to minimize the probability that n(t) was the corrupting influence in the channel giving rise to y(t) when $x(t-kt_0)$ was sent. On the condition that k = m,

$$n(t) = y(t) - x(t-mt_0) . \tag{2.6}$$

It can be shown[26] that the density of a particular sample function, n(t), of white Gaussian noise lasting from time 0 to pt_0 may be expressed as

$$\Pr \text{ density}\left\{ n(t) \right\} = J \exp\left[- \frac{1}{N_0} \int_0^{pt_0} n^2(t)\, dt \right] \tag{2.7}$$

where $\frac{N_0}{2}$ is the (double-sided) spectral density of the noise, and J is a constant not dependent on n(t). (The space on which this probability density exists must be carefully defined, but need not concern us here.)

Hence, if $\Pr\left\{ k = m \middle| y(t) \right\} > \Pr\left\{ k = r \middle| y(t) \right\}$ for all $r \neq m$,

$$\frac{\Pr\left\{ k = r \middle| y(t) \right\}}{\Pr\left\{ k = m \middle| y(t) \right\}} < 1 , \tag{2.8}$$

and, as a result

$$\exp\left[\frac{1}{N_0}\int_0^{pt_0}\left(y(t)-x(t-mt_0)\right)^2 dt - \int_0^{pt_0}\left(y(t)-x(t-rt_0)\right)^2 dt\right] < 1 \quad . \tag{2.9}$$

Simplifying the exponent and taking logarithms of both sides leads to a sufficient statistical criterion: estimate $k = m$ whenever, for all $r \neq m$,

$$\int_0^{pt_0} y(t)\, x(t-mt_0)dt > \int_0^{pt_0} y(t)\, x(t-rt_0)\, dt \quad . \tag{2.10}$$

B. Error Probability and Optimal Signals

For convenience we may consider that $\tau = 0$. By making the substitution $y(t) = x(t) + n(t)$, and by using the periodicity of $x(t)$ in the equation above, the decision criterion becomes: choose the estimate m such that for all $r \neq m$,

$$R_{xx}(mt_0) + v_m > R_{xx}(rt_0) + v_r \quad , \tag{2.11}$$

where the noise v_r is a zero-mean, Gaussian random variable

$$v_r = \frac{1}{pt_0}\int_0^{pt_0} n(t)\, x(t-rt_0)\, dt \quad . \tag{2.12}$$

The noise covariances $\mu_{rm} = \xi\,(v_r v_m)$ are, of course, given by

$$\mu_{rm} = \frac{N_0}{2} R_{xx}((m-r) t_0) . \tag{2.13}$$

If the decision was correct, then m = 0, and the vector

$$\underset{\sim}{v} = (v_0, v_1, \ldots, v_{p-1})^T \tag{2.14}$$

must have been in the region cut out by

$$S - R_{xx}(rt_0) > v_r - v_0 , \quad S = R_{xx}(0) \tag{2.15}$$

for each non-zero admissible candidate rt_0 for the phase. When all of the p values of r are admissible, the error probability is given by

$$P_e = 1 - \int_{-\infty}^{\infty} \int_{-\infty}^{S - R_{xx}(t_0) + v_0} \cdots \int_{-\infty}^{S - R_{xx}((p-1)t_0) + v_0} \tag{2.16}$$

$$p(v_0, v_1, \ldots, v_{p-1}) \, dv_0 \, dv_1 \cdots dv_{p-1} .$$

It is not clear from equation 2.16 what the optimal correlation function for x(t) would be, since $R_{xx}(\tau)$ appears in both $p(\underset{\sim}{v})$ and the integral limits. In fact, a complete solution to this problem is not known. It is conjectured that x(t) should be chosen to have its maximum out-of-phase correlation minimized, and there are several arguments which tend to bear this out.

From the form of detection criterion, we might at first think that for optimal distinguishability we should clearly want large separations

between the in-phase and out-of-phase correlations. Then $S - R_{xx}(rt_0)$, we would reason, would be more likely to be bigger than $v_r - v_0$. This reasoning is not necessarily valid, because the noise term $v_r - v_0$ has variance

$$\xi\left\{(v_r - v_0)\right\}^2 = N_0(S - R_{xx}(rt_0)) \tag{2.17}$$

which increases with separation. It is this trade-off between separation and noise variance that causes the difficulty in finding the optimal correlation function, and it is strongly reflected in the integral expression for P_e.

It is also conceivable that the optimal correlation function might change as a function of the signal-to-noise ratio in the channel.

Perhaps the strongest result at present is due to Balakrishnan[27] which states that if there exists a region of signal-to-noise over which a unique optimal code of M signals exists, and if the dimensionality of the signal space is at least M-1, then the signals, envisaged as points in signal space, should be placed at the vertices of an (M-1)-dimension simplex; that is, a polyhedron, each vertex of which is equally (and maximally) distant from every other vertex. The common value of cross-correlation is $-\frac{1}{M-1}$ (normalized). The problem of a signal space of smaller dimensionality than M-1 has not been solved in general. Whenever an (M-1)-degree simplex is cyclic, the signal corresponding to it has the optimum correlation.

For all values of $\frac{S}{N_0}$, it is further known[28,29] that the simplex correlations provide a local optimum. That is, P_e, as a function of the

correlation values (assumed to be independent variables), takes on a relative minimum when each correlation is equal to the simplex value.

By differentiation it can be shown that a P_e is a monotonic non-decreasing function of each correlation as well as the signal-to-noise.

$$\frac{\partial P_e}{\partial \gamma} \geq 0 \tag{2.18}$$

where γ is either a (normalized) correlation or the signal-to-noise ratio. This, too, hints that one should choose $x(t)$ to minimize the out-of-phase correlations, for then P_e would surely be minimum also. Of course, all the correlations are <u>not</u> independent, so this reasoning is not really valid either but indicates what would be desirable if a sufficient degree of freedom were available. We can show that if all correlations are taken to be equal, then the best value to pick for this correlation is the simplex value. This is done easily with a result of Kot'elnikov[30]: let $P_e(\lambda, \rho)$ be the probability of error for a code, all of whose cross-correlations are equal to $\rho < 1$, at a signal-to-noise ratio λ; then

$$P_e\left(\frac{\lambda}{1-\rho}, \rho\right) = P_e(\lambda, 0) . \tag{2.19}$$

Immediately we see that the larger $1-\rho$ becomes, the smaller the <u>effective</u> signal-to-noise becomes and by the monotoneness of P_e, we reason that $1-\rho$ should be as large as possible. Hence, ρ should be the simplex value for such codes.

The foregoing discussion was presented to justify, to some extent, the assumption which we shall make about the type of correlation which we

desire $x(t)$ to have, and this is that it is desirable for $x(t)$ to have the lowest possible out-of-phase correlation.

As we shall see, it is not always possible to achieve a simplex correlation, especially when $\underline{a}$ is a binary sequence with fixed period. Then, we not only desire that the $x(t)$ have its maximum out-of-phase correlation minimized but that the number of times this maximum is attained also be minimized. This is a heuristic optimizing necessity, borne out by considering bounds on P_e. Applying the mean-value theorem, one can show[31]

$$P_e(\lambda, R_{xx}(m)) \leq P(\lambda, R_{max}) . \tag{2.20}$$

This indicates that the error probability, at a given signal-to-noise ratio, is improved if the correlation is not equal to the maximum everywhere. By the monotoneness of P_e with each correlation, we reason that the fewer times R_{max} is attained, the better signal we will have.

C. Perturbed Additive Gaussian Channels

Suppose we restrict ourselves, for the moment, to binary sequence-modulation of an antipodal sinusoidal set. We can implement this mathematically by either amplitude modulation

$$x(t) = a(t) \sin \omega_0 t \tag{2.21}$$

or by phase modulation $\pm 90^\circ$

$$x(t) = \sin(\omega_0 t + \frac{\pi}{2} a(t)) . \tag{2.22}$$

The series a(t) is a binary (±1) sequence

$$a(t) = \sum_{n=-\infty}^{\infty} (\delta_n^{\,1} - \delta_n^{\,2})\ u(t-nt_0) \tag{2.23}$$

where u(t) is the unit pulse from 0 to t_0.

In the channel, white Gaussian noise is added, as in preceding sections of this chapter, and, in addition, the <u>phase</u> of x(t) is perturbed by an additive noise, $\psi(t)$.

$$y(t) = \sin(\omega_0 t + \frac{\pi}{2} a(t) + \psi(t)) + n(t)\ . \tag{2.24}$$

Such a received signal would result if the sine wave generator had a phase instability or if the medium were randomly varying.

If $\psi(t)$ were known, the ideal receiver would correlate y(t) against $\sin(\omega_0 t + \frac{\pi}{2} a(t-mt_0) + \psi(t))$, comparing the shifts of a(t) to find a maximum. Not knowing $\psi(t)$, the receiver estimates the noise, say, as $\psi_0(t)$. Now define

$$\begin{aligned}
\tilde{\Lambda}(m) &= \frac{1}{pt_0} \int_0^{pt_0} y(t) \sin(\omega_0 t + \tfrac{\pi}{2} a(t-mt_0) + \psi_0(t))\, dt \\
&= \tfrac{1}{2} \frac{1}{pt_0} \int_0^{pt_0} \cos\left[\tfrac{\pi}{2} a(t) - a(t-mt_0) + \psi(t) - \psi_0(t)\right] dt \\
&\quad - \tfrac{1}{2} \frac{1}{pt_0} \int_0^{pt_0} \cos\left[2\omega_0 t + \tfrac{\pi}{2} (a(t) + a(t-mt_0)) + \psi(t) + \psi_0(t)\right] dt \\
&\quad + \frac{1}{pt_0} \int_0^{pt_0} n(t) \sin(\omega_0 t + \tfrac{\pi}{2} a(t-mt_0) + \psi_0(t_0))\, dt\ .
\end{aligned} \tag{2.25}$$

The second of these integrals can be omitted with little loss in error probability since it represents the integral of a high frequency sinusoid. We thus re-define $\Lambda(m)$ to exclude this term, and we drop the factor of $\frac{1}{2}$ by normalizing.

$$\Lambda(m) = \frac{1}{pt_0} \int_0^{pt_0} a(t)\, a(t-mt_0) \cos\left[\psi(t) - \psi_0(t)\right] dt + v_m \,. \tag{2.26}$$

We can estimate $\psi(t)$ by inserting a phase-locked loop in the receiver to get a fairly good approximation, $\psi_0(t)$. Consequently, our test statistic will be something like

$$\Lambda(m) = \Theta R_{xx}(mt_0) + v_m \,, \tag{2.27}$$

where Θ is a random variable indicating the degree of lock, presumably slowly varying and positive if pt_0 is long.

The additive noise channel with phase noise is thus really different from the additive noise channel without phase noise only by a change in the signal-to-noise ratio. The detection schemes are the same, and coding for both requires sequences with minimal out-of-phase correlations.

D. Correlation Time as a Function of Distinguishability

We now wish to compare the integration time T required to give a constant probability of error as a function of correlation separation. Suppose a unit-power signal $x(t)$ is transmitted, $y(t) = x(t-m) + n(t)$ is received, and the receiver correlates $y(t)$ against a unit-power waveform $z(t)$ for a time T. The output $\Lambda(m, T)$ of the integrator is then

$$\begin{aligned} \Lambda(m, T) &= \int_0^T y(t)\, z(t)\, dt \\ &= \int_0^T x(t-m)\, z(t)\, dt + \int_0^T n(t)\, z(t)\, dt \\ &= T\, C_{xz}(m) + N(T) \,. \end{aligned} \tag{2.28}$$

The noise term at the termination of integration has variance

$$\begin{aligned} \sigma_N^2 = \xi(N^2) &= \int_0^T \int_0^T \frac{N_0}{2} \delta(t-s)\, z(t)\, z(s)\, dtds \\ &= \frac{N_0}{2} \int_0^T z^2(t)\, dt = \tfrac{1}{2} N_0 T \,. \end{aligned} \tag{2.29}$$

Let ΔC_{xz} represent the <u>distinguishability</u> of the normalized cross-correlation values $C_{xz}(m)$:

$$\Delta C_{xz} = \left| C_{xz}(m') - C_{xz}(m'') \right| \tag{2.30}$$

where $\left| C_{xz}(m') \right| \geq \left| C_{xz}(m) \right|$ for all m, and m'' is chosen to minimize the difference above. The distinguishability-to-noise ratio, as we have seen, fixes the error probability; that is, two correlation detectors will have approximately the same probability of error if they have the same distinguishability-to-noise ratio, $\overline{\Delta \Lambda} / \sigma_N$,

$$\frac{\overline{\Delta \Lambda}}{\sigma_N} = \frac{T \Delta C_{xz}}{\sqrt{\frac{1}{2} N_0 T}} = \sqrt{\frac{2T}{N_0}}\, \Delta C_{xz} \,. \tag{2.31}$$

As a result, the integration time for a given probability of error (more precisely, for a given $\overline{\Delta \Lambda} / \sigma_N$) increases as the inverse-square of distinguishability of cross-correlation values.

$$T = \frac{N_0}{2} \left(\frac{\overline{\Delta \Lambda}}{\sigma_N} \right) \left[\Delta C_{xz} \right]^{-2} \quad . \tag{2.32}$$

The ratio of the times T' and T for two such systems is hence

$$\frac{T'}{T} = \left(\frac{\Delta C_{xz}}{\Delta C_{x'z'}} \right)^2 \quad . \tag{2.33}$$

E. Minimum Acquisition-Time Receivers

The optimal receivers we have considered up to this point minimize the probability of error for a given detection time, or analogously, the detection time for a given probability of error. It consists of filters (or correlators) matched to each possible transmitted signal, and this generally requires a large amount of equipment. Sometimes, however, we are limited to a certain amount of equipment or receiver complexity, and we must operate on the incoming signal accordingly.

For example, suppose that a sequence a is transmitted in a continuous radar situation, and we wish to "acquire", or detect, the delayed received replica of a. By using p correlators, we are able to estimate the received shift of a with a certain probability of error after integrating for, say, T seconds. From the foregoing discussion, this is the least T giving this probability of error. However, if we were limited to using one correlator in the receiver, we must correlate the incoming signal serially against every phase-shift of a, which requires pT seconds to achieve the same prob-

ability of error. There is thus a trade-off between receiver complexity and acquisition time which we can relate by

$$T_{acq} = \frac{\text{time for a one-correlator receiver to acquire } \underline{a}}{\text{number of correlators in receiver}} \qquad (2.34)$$

Now as an alternative, let us build a receiver which cross correlates $\underline{a}$ against several locally-generated sequences; say $\underline{c}_1, \underline{c}_2, \ldots, \underline{c}_n$. When $\underline{a}$ and $\underline{c}_i$ are cross-correlated for T' seconds, $R_{\underline{ac}_i}(m)$ will have maximum values at multiples of the highest common factor v_i of $\underline{a}$ and $\underline{c}_i$; denoting the period of $\underline{c}_i$ as u_i, these are

$$v_i = (p, u_i) .$$

Knowing the vector $\underline{m} = (m_1, m_2, \ldots, m_n)$ containing the delays m_i at which $R_{\underline{ac}_i}(m)$ are maximum, we want to be able to decide the most probable shift of $\underline{a}$ uniquely. The number of these vectors $\underline{m}$ must thus be greater than the number of phases of $\underline{a}$. Each m_i can be reduced modulo v_i without loss in distinguishability, and we may assume then that each m_i is the least positive integer giving the maximum $R_{\underline{ac}_i}(m)$. But the number of distinct pairs (m_i, m_j) of maximal indications is the least common cycle length $\left[v_i, v_j\right]$ of the two cross-correlations $R_{\underline{ac}_i}(m)$, $R_{\underline{ac}_j}(m)$. Also, if v_k were to divide $\left[v_i, v_j\right]$, no information would be carried in m_k. We can exclude such cases and extend, by induction, to

$$p \leq \left[v_1, v_2, \ldots, v_n\right]. \qquad (2.36)$$

With one integrator observing T' seconds per step, the time required serially to perform all correlations of $\underline{a}$ with the $\underline{c}_i$, phase-by-phase and sequence-by-sequence, is $(v_1 + v_2 + \ldots + v_n)T'$. We choose T' sufficiently long that the confidence limits in this scheme are the same as the previous ones using integration time T. The acquisition ratio, defined as

$$\frac{T'_{acq}}{T_{acq}} = \frac{(v_1 + v_2 + \ldots + v_n)T'}{pT}, \tag{2.37}$$

represents the relative saving (if any) between the two schemes, each with the same specified number of integrators.

If it were possible to pick $\underline{c}_i$, n and T' in such a way that the ratio is less than unity, the alternate scheme would prove a more desirable receiver in that for a given receiver complexity and error probability, the total time to acquire is less in the second method. We will not only show that this is possible, but we will also give a way by which a great saving can be achieved.

First, T' depends on the distinguishability among the $R_{\underline{ac}_i}(m)$ at various m. If, for each n, the $\underline{c}_i$ and $\underline{a}$ are chosen in some systematic manner, T' is a function of n and T, exclusively.

Second, the period u_i of $\underline{c}_i$ cannot be relatively prime to p, for if it were, $R_{\underline{ac}_i}(m)$ would be the same for all m because $v_i = (u_i, p)$. By Euclid's algorithm, there exist positive integers s and t $(0 \leq t < p)$ with the property that

$$sp + t = \left[v_1, v_2, \ldots, v_n\right]. \tag{2.38}$$

It is possible for each v_i to divide p only if t = 0 and s = 1.

$$p = \left[v_1, v_2, \ldots, v_n \right] . \tag{2.39}$$

To minimize the acquisition ratio for a fixed n, we minimize $(v_1 + \ldots + v_n)$ keeping $p = \left[v_1, \ldots, v_n\right]$ constant. Recall that for each i and j, v_i and v_j must have been chosen to have some non-unity relative prime factors.

There will always exist v_i', i = 1, ..., n, relatively prime in pairs (assuming $p \neq v_1 v_2 \ldots v_n$) with

$$p = v_i' v_2' \ldots v_n' \tag{2.40}$$

such that $(v_1' + v_2' + \ldots + v_n') < (v_1 + v_2 + \ldots + v_n)$. To demonstrate that this is possible, we proceed as follows: stepwise, consider all pairs v_i, v_j, and arbitrarily set $v_i = v_i'$ and $v_j' = v_j/(v_i, v_j)$ at each step. The final set $\left\{v_i'\right\}$ is relative prime and $v_1' v_2' \ldots v_n' = p$, with either $v_i' < v_i$ or $v_i' = v_i$. Hence, $(v_1 + v_2 + \ldots + v_n) > (v_1' + v_2' + \ldots + v_n')$.

Since we wish to pick v_i to minimize the acquisition ratio, we must let the v_i be relatively prime, for otherwise we could follow the procedure above to pick a relatively prime set of v_i' giving a smaller acquisition ratio.

It is a well-known result[32] that $(v_1 + \ldots + v_n)$ is minimized, relative to the constraint that $p = v_1 v_2 \ldots v_n$, by choosing each v_i equal to $\sqrt[n]{p}$. Of course, the distinctness of each v_i makes this impossible. We must, in consolation, group the v_i as close to $\sqrt[n]{p}$ as possible, keeping them relatively prime. We now have a strong reason for finding optimum cross-correlating sequences of <u>all</u> lengths.

For a minimum acquisition-time receiver, we seek n well-chosen sequences $\underline{c}_i$, i = 1, 2, ..., n, whose cross-correlations $R_{\underline{a}\underline{c}_i}(m)$ with $\underline{a}$ have periods v_i which are relatively prime and close to $\sqrt[n]{p}$ and which have a maximum distinguishability between phases. Over all such schemes, we then choose n to further minimize the acquisition ratio

$$\frac{T'_{acq}}{T_{acq}} \approx n\, p^{\frac{1-n}{n}}\, \frac{T'(n)}{T} \quad . \tag{2.41}$$

We have indicated that T' is dependent only on n (and T) when there is a systematic way of choosing $\underline{c}_1, \underline{c}_2, \ldots, \underline{c}_n$ and $\underline{a}$ for each n. We investigate, in the final chapter, acquisition of $\underline{a}$ by taking $\underline{a}$ to be the optimal Boolean function of the "component" sequences $\underline{c}_1, \underline{c}_2, \ldots, \underline{c}_n$.

Chapter 3

EQUIVALENCE CLASSES OF SEQUENCES

Fine[33], in 1957, and Gilbert and Riordan[34], in 1961, treated the following problem: if two sequences $\underline{a}$ and $\underline{a}'$ can be made alike by either a shift in origin or a permutation of the states e_i, or both, how many distinct (inequivalent) sequences or symmetry types of sequences are there? The solution to this problem, the so-called "necklace" problem[35], is important because it reveals the number of different sequence generators which can be implemented to a given period. We are not interested in sequence generators as such, but the method used to count the equivalence classes, namely Pòlya's formula[36,37], can be applied to a problem of specific importance to us.

In the next chapter, it will be shown that certain transformations of sequences do not change the values which the correlation function assumes, but only the order in which these values appear. It is of interest, then, to determine the number of sequences which are distinct under such transformations, for then we need be able to synthesize only one sequence in each equivalence class.

Let $\underline{a} = \{a_n\}$ be a cyclic sequence of length L (L may be a multiple of the period), each of whose elements a_n may assume one of b values. There are b^L such sequences. Define the operator g_k^t on $\{a_n\}$ by

$$g_k^t\{a_n\} = \{a_{kn+t}\}. \tag{3.1}$$

Obviously, k, t and kn+t may be treated as integers modulo L because the sequences involved are cyclic. Define the set

$$\mathcal{G} = \left\{ g_k^t : (k, L) = 1; \; t, \; k \bmod L \right\} . \tag{3.2}$$

It is easily shown that $\mathcal{G}$ is a group of order $L\,\phi(L)$ (ϕ is Euler's totient function[38]). This set $\mathcal{G}$ of permutations forming a group of operators on the domain of cyclic sequences is called an Affine Group[39]. By applying Pólya's formula, the number of equivalence classes of sequences under this group can thus be obtained.

A. Properties of the Affine Group $\mathcal{G}$

Two sequences $\underline{a}$ and $\underline{a}'$ are equivalent under $\mathcal{G}$ if there exists a g_r^t in $\mathcal{G}$ such that $g_r^t \underline{a} = \underline{a}'$. The number of sequences $\underline{a}$ with the property that, given g_k^t, $g_k^t \underline{a} = \underline{a}$, is denoted

$$\mathcal{I}(g_k^t) = \text{number of sequences invariant under } g_k^t .$$

It is obvious that

$$g_k^t \left\{ a_n \right\} = \left\{ a_n \right\} \quad \text{if and only if } a_n = a_{nk+t} ;$$

the constraints made upon a sequence by invariance under g_k^t are that $a_m = a_n$ whenever n and m are in the same cycle of the decomposition of the integers modulo L by the permutation

$$n \longrightarrow nk+t . \tag{3.3}$$

The first such cycle of g_k^t is $(0, t, t(k+1), \ldots, t(k^{q-1} + \ldots + 1))$ where q is chosen so that it is the least positive integer such that $t(k^q + k^{q-1} + \ldots + 1) = 0$. If v is the least integer modulo L not in this cycle, then we form the second cycle $(v, vk+t, vk^2 + t(k+1), \ldots, vk^{x-1} + t(k^{x-2} + \ldots + 1))$, and so on until every integer from 0 to L-1 is placed in a cycle. We call such a disjoint decomposition of L the <u>cycles</u> of the permutation g_k^t, or the <u>equivalence classes</u>, or <u>orbits</u> of integers under the relation g_k^t, etc., as we choose. Denote the number of such classes by $\mathcal{C}(k, t)$.

$$\mathcal{C}(k, t) = \text{number of cycles in decomposition of integers mod L by } g_k^t . \tag{3.4}$$

For each k relatively prime to L, there is some least positive integer q such that $k^q = 1 (\text{mod } L)$. This integer $E_k(L)$ is the <u>exponent</u>, or <u>index</u>, of k modulo L.

<u>LEMMA</u>: $q = E_k(L)$ if and only if q is the least integer such that $1 + k + \ldots + k^{q-1} = 0$ modulo $\frac{L}{(L, k-1)}$.

<u>Proof</u>: Assume $q = E_k(L)$, and let $d = (L, k-1)$. Then q is the least integer such that, for some m,

$$k^q - 1 = (k-1)(k^{q-1} + \ldots + 1) = mL \equiv 0(L) . \tag{3.5}$$

But $(\frac{L}{d}, \frac{k-1}{d}) = 1$; hence if it is true that $(\frac{k-1}{d})(k^{q-1} + \ldots + 1) \equiv 0(L/d)$, then it must also be true that $k^{q-1} + \ldots + 1 \equiv 0(L/d)$. This proves the first half of the lemma.

Assume now that q is the least integer such that $k^{q-1} + \ldots + 1 \equiv 0(L/d)$. Since $\frac{k-1}{d}$ is relatively prime to L/d, q is also the least integer such that $\frac{k-1}{d}(k^{q-1} + \ldots + 1) \equiv 0(L/d) = mL/d$, for some m. Therefore $k^q - 1 = mL$, and q is the exponent of k.

We now define a concept similar to the exponent of k. Define $\mathcal{N}(k, L)$ to be the least integer x such that

$$1 + k + \ldots + k^{x-1} \equiv 0 \bmod L . \tag{3.6}$$

A relatively simple lemma follows:

LEMMA: $\mathcal{N}\left(k, \frac{L}{(L, k-1)}\right) = E_k(L)$.

Proof: $\mathcal{N}\left(k, \frac{L}{(L, k-1)}\right) = q$ means that q is the least integer such that $1 + k + \ldots + k^{q-1} \equiv 0 \bmod L/(L, k-1)$; hence that q is the exponent of k.

The main result involving $\mathcal{N}(k, L)$ is the following:

THEOREM:

$$\mathcal{N}(k, L) = \begin{cases} L & ; \text{ if } k = 1 \\ LE_k(L)/\left(L, \frac{k^{E_k(L)} - 1}{k-1}\right); & \text{if } k \neq 1 \end{cases} .$$

Proof: $1 + k + \ldots + k^{N-1} \equiv 0(L)$ implies $k^N - 1 \equiv 0(L)$, hence that $E_k(L)$ divides N; that is, $N = rE_k(L)$ for some r, where if $N = \mathcal{N}(k, L)$, r is the least such integer. But then mod L, $1 + \ldots + k^{N-1} \equiv r(1 + \ldots + k^{E_k(L) - 1}) = nL$, for some n. Let $v = (L, 1 + \ldots + k^{E_k(L) - 1})$. If $k = 1$, $v = L$; and if $k \neq 1$, $v = \left(L, \frac{k^{E_k(L)} - 1}{k-1}\right)$. Then

$$r\left(\frac{1 + k + \ldots + k^{E_k(L) - 1}}{v}\right) = n\frac{L}{v} . \tag{3.7}$$

Since L/v and $(1 + \ldots + k^{E_k(L) - 1})/v$ are relatively prime, r is the least non-zero integer such that

$$r \equiv 0 \bmod \frac{L}{v} . \tag{3.8}$$

Therefore, $r = L/v$, and $N = \frac{L}{v} E_k(L)$.

THEOREM: The number of elements in the cycle of g_k^t containing the element u is

$$\mathcal{N}\left(k, \frac{L}{(L, u(k-1) + t}\right) . \tag{3.9}$$

Proof: Let the cycle containing u have x elements. Then x is the least integer such that

$$uk^x + t(k^{x-1} + \ldots + 1) \equiv u(L) . \tag{3.10}$$

That is, $\left[u(k-1) + t\right](k^{x-1} + \ldots + 1) \equiv 0\ (L) = nL$, for some n. Let $v = (L, u(k-1) + t)$. Then x is the least integer such that

$$k^{x-1} + \ldots + 1 = 0 \text{ modulo } L/v . \tag{3.11}$$

Therefore, $x = \mathcal{N}(k, L/v)$.

As a special consequence of this theorem, we see that the number of elements in each cycle divides L.

For convenience, let us denote the number of elements in the cycle of g_k^t to which u belongs by

$$H(u;\, k,\, t) = \mathcal{N}\left(k,\, \frac{L}{(L,\, u(k-1) + t)}\right)$$
$$= \left[\text{number of elements in the cycle of } g_k^t \text{ to which u belongs}\right]. \tag{3.12}$$

We readily compute the number of cycles $\mathcal{C}(k,\, t)$ in the decomposition of g_k^t.

COROLLARY: $\mathcal{C}(k,\, t) = \sum_{u=0}^{L-1} \frac{1}{H(u;\, k,\, t)}$.

Proof: Let $\mathcal{U} = \{u_1, u_2, \ldots, u_{\mathcal{C}}\}$ be a set of representatives of the cycles of g_k^t each u_i from a different cycle. Then

$$\sum_{u=0}^{L-1} \frac{1}{H(u;\, k,\, t)} = \sum_{i=1}^{\mathcal{C}} H(u_i;\, k,\, t)\left[\frac{1}{H(u_i;\, k,\, t)}\right] = \mathcal{C}(k,\, t). \tag{3.13}$$

B. Counting the Equivalence Classes

We now apply the Pòlya formula: Let $\mathcal{G}$ be a finite group of operators on a finite set $\mathcal{S}$. The number of equivalence classes $\mathcal{Q}$ established in $\mathcal{S}$ by $\mathcal{G}$ is given by

$$\mathcal{Q} = |\mathcal{G}|^{-1} \sum_{g \in \mathcal{G}} \mathcal{L}(g) \tag{3.14}$$

where $|\mathcal{G}|$ is the order of $\mathcal{G}$.

THEOREM: The number $\mathcal{P}(L)$ of equivalence classes of sequences under $\mathcal{G}$ is

$$\left.\begin{aligned}
\mathcal{P}(L) &= \frac{1}{L\,\phi(L)} \sum_{t=0}^{L-1} \sum_{\substack{k=1 \\ (k,L)=1}}^{L-1} b^{\mathcal{C}(k,\,t)} \\
&\text{where} \\
L &= \text{cyclic length of sequences} \\
\phi &= \text{Euler's totient function} \\
b &= \text{number of sequence states} \\
\mathcal{C}(k,\,t) &= \sum_{u=0}^{L-1} H^{-1}(u;\,k,\,t), \text{ the number of cycles of } g_k^t \\
H(u;\,k,\,t) &= \mathcal{N}\left(k,\ \frac{L}{(L,\ u(k-1)+t)}\right) \\
\mathcal{N}(k,\,d) &= \begin{cases} d & ;\ \text{if } k = 1 \\ d\,E_k(d)/\left(d,\ \dfrac{k^{E_k(d)}-1}{k-1}\right) & ;\ \text{if } k \neq 1 \end{cases} \\
E_k(d) &= \text{least integer such that } k^E - 1 \equiv 0 \bmod d.
\end{aligned}\right\} \qquad (3.15)$$

Proof: Pòlya's formula, in this case, reads,

$$\mathcal{P}(L) = \frac{1}{L\,\phi(L)} \sum_{g_k^t \in \mathcal{G}} \mathcal{J}(g_k^t) . \qquad (3.16)$$

To compute $\mathcal{J}(g_k^t)$: any sequence such that $a_n = a_m$ whenever n and m are in the same cycle of g_k^t is left invariant by g_k^t. Hence $\mathcal{J}(g_k^t) = b^{\mathcal{C}(k,\,t)}$. Therefore,

$$\mathcal{P}(L) = \frac{1}{L\,\phi(L)} \sum_{k,t} b^{\mathcal{C}(k,\,t)} . \qquad (3.17)$$

COROLLARY: If $(L,\ k-1)$ divides t, then $\mathcal{C}(k,\,t) = \sum_{d\ L} \frac{\phi(d)}{E_k(d)}$.

Proof: If $(L, k-1)$ divides t, there exists a u_0 such that $u_0(k-1) + t \equiv 0(L)$. The mapping $v \longrightarrow v+u_0$ of the integers modulo L onto itself is 1 to 1, and $(v+u_0)(k-1) + t = v(k-1)$. Then denote $d = (L, v)$, so

$$H(v+u_0; k, t) = N(k, \frac{L}{(L, v(k-1))}) = N(k, \frac{L/d}{(\frac{L}{d}, k-1)}) = E_k(\frac{L}{d}) . \quad (3.18)$$

As v ranges over all the residues modulo L, d passes through every divisor of L, as does L/d. Hence

$$\mathcal{C}(k, L) = \sum_{d|L} \frac{M(d)}{E_k(d)} = \sum_{d|L} \frac{M(L/d)}{E_k(L/d)} . \quad (3.19)$$

Where $M(q)$ is the number of residue classes v modulo L such that $L/(L, v) = q$; v must be such that $(L, v) = L/q = d$. Thus $v = rd$, where $(r, L) = 1$ and $rd = rL/q < L$, or $r < q$. Hence $M(q)$ is the number of integers less than q, relatively prime to q; that is, $M(q) = \phi(q)$.

This last theorem establishes the fact that anytime $(L, k-1)$ divides t, the number of cycles of g_k^t is the same as the number of cycles of g_k^0.

LEMMA: As a function of x, $x(k-1) + t$ takes on $L/(L, k-1)$ values as $x = 0, 1, \ldots, L-1$, each $(L, k-1)$ times.

Proof: $x(k-1) + t = y(k-1) + t$ means that $x = y \bmod L/(L, k-1)$. Hence, $1, 2, \ldots, L/(L, k-1)$) are the distinct values, each assumed $(L, k-1)$ times.

By this lemma, the task of computing (k, t) is somewhat lessened:

$$\mathcal{C}(k, t) = (L, k-1) \sum_{u=1}^{\frac{L}{(k-1, L)}} H^{-1}(u; kt) . \quad (3.20)$$

In the special case that L is prime, k-1 is relatively prime to L for all k, (k, L) = 1, except k = 1. For k = 1, $\mathcal{N}(1, \frac{L}{(L, t)}) = H(u; 1, t) = \frac{L}{(L, t)}$.

$$\mathcal{Q}(L) = \frac{1}{L(L-1)} \left\{ b^L + b(L-1) + L \sum_{\substack{k=2 \\ (k,L)=1}}^{L-1} b^{\sum_{d \mid L} \frac{\phi(d)}{E_k(d)}} \right\} \tag{3.21}$$

The values of $\mathcal{Q}(L)$ for the first few values of L are given in Table 3-1.

Although the above formula presents an explicit way of expressing $\mathcal{Q}(L)$ in terms of elementary functions, it involves upwards of $L^2\phi(L)$ calculations which, if done without an electronic computer, can become a long and tedious process. It seems that a simpler way to determine $\mathcal{Q}(L)$ is by

$$\mathcal{Q}(L) = \frac{1}{L\,\phi(L)} \sum_{t=0}^{L-1} \sum_{\substack{k=1 \\ (k,L)=1}}^{L-1} b^{\mathcal{C}(k, t)} \tag{3.22}$$

where $\mathcal{C}(k, t)$ is computed by looking directly at the decompositions of L by the permutation $n \longrightarrow nk+t$ for each desired k, t.

The number $\tilde{\mathcal{Q}}(L)$ of sequences with period exactly L can be found by

$$\tilde{\mathcal{Q}}(L) = \begin{cases} \mathcal{Q}(L) - \mathcal{Q}(1) & ; \text{ for prime L} \\ 2\mathcal{Q}(L) - \sum_{d\ L} \tilde{\mathcal{Q}}(d) & ; \text{ for all L} \end{cases} \tag{3.23}$$

where the sum is extended over all divisors d of L. This number is also given by applying the Möbius inversion formula[40]:

$$\tilde{\varphi}(L) = \sum_{d \mid L} \mu(L/d)\, \varphi(d) \tag{3.24}$$

where $\mu(d)$ is the Mobius function: $\mu(1) = 1$, $\mu(d) = (-1)^r$ if d is the product of r distinct primes, $\mu(d) = 0$ otherwise.

Both $\varphi(L)$ and $\tilde{\varphi}(L)$ are given in Table 3-1 and plotted in Figure 3-1. From the figure, one may note that $\varphi(L)$ is roughly exponential in L. For large L, the number of equivalence classes is approximated by

$$\mathcal{Q}(L) \approx b^{h(L-1)} \tag{3.25}$$

for some appropriate constant h, which, according to the figure, is about 0.6 for b = 2.

The analysis above indicates that the problem of finding a particular sequence or a representative of an equivalence class is reduced to about $2^{-(.4L + .6)}$ of an exhaustive search. However, the number of equivalence classes still grows exponentially.

It should be pointed out that it is possible for two sequences to have the same autocorrelation function and be in different equivalence classes. This is the case, for example, for the binary linear and Legendre sequences of period 31. Hence, even though equivalence was defined to leave the correlation properties of sequences invariant, these classes are insufficient to characterize the correlation types uniquely.

TABLE 3-1

Number of Inequivalent Sequences of Length L, $\mathcal{Q}(L)$, and of Period L, $\tilde{\mathcal{Q}}(L)$

L	$\mathcal{Q}(L)$	$\tilde{\mathcal{Q}}(L)$
1	2	2
2	3	1
3	4	2
4	6	3
5	6	4
6	13	8
7	10	8
8	24	18
9	22	18
10	45	38
11	30	28
12	158	142
13	74	72
14	245	234
15	368	361
16	693	669
17	522	520
18	2,637	2,576
19	1,610	1,608
20	7,341	7,293
30	4,499,852	4,499,436
31	2,311,468	2,311,466

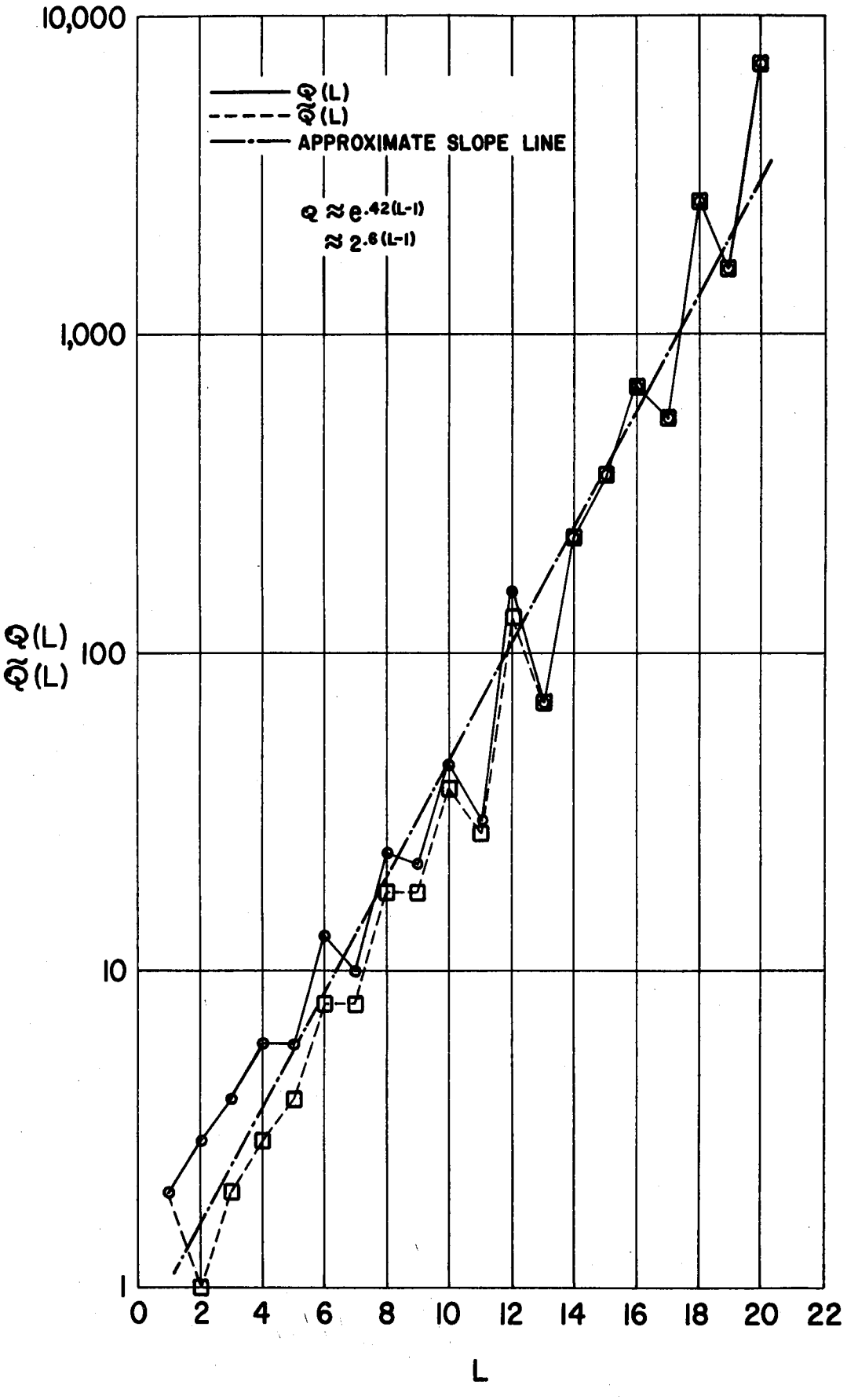

FIGURE 3.1. NUMBERS OF INEQUIVALENT SEQUENCES OF LENGTH L, Q(L), AND OF PERIOD L, Q̃(L)

Chapter 4

THE CYCLIC SEQUENCE CORRELATION FUNCTION

A. General Correlation Properties

A cyclic sequence (or merely a sequence) $\underline{a} = \{a_n\}$ is a mapping of the integers onto b objects or states, $e_1, e_2, \ldots, e_b$, for which there exists a positive integer L, called a cycle length, such that for all n,

$$a_n = a_{n+L} . \tag{4.1}$$

The least positive such L is the period, p.

We have defined a correlation of a sequence-modulated signal, and we have defined the correlation between states of a sequence. (4.2)

There are several ways to define what we might call a "correlation" function on a sequence. We choose to define the correlation of $\{a_n\}$ relative to a function: Let f be a real or complex-valued function on the states.

$$f(\underline{a}) = f\{a_n\} = \{f(a_n)\} . \tag{4.3}$$

The (unnormalized) autocorrelation of $\underline{a} = \{a_n\}$ relative to f is

$$R_{f(\underline{a})}(m) = \sum_{n=1}^{L} f(a_n) f^*(a_{n+m}) . \tag{4.4}$$

The (unnormalized) cross-correlation of $\underline{a} = \{a_n\}$ and $\underline{c} = \{c_n\}$ relative to f and g is similarly defined.

$$R_{f(\underline{a}),\, g(\underline{c})}(m) = \sum_{n=1}^{V} f(a_n)\, g^*(c_{n+m}) \tag{4.5}$$

where $V = \left[L(\underline{a}),\, L(\underline{c}) \right]$, the least common multiple of the cyclic lengths of $\underline{a}$ and $\underline{c}$. Whenever we deal with only one sequence, we shall quite frequently omit this fact from the notation and merely write $R_f(m)$, $R_{fg}(m)$. We shall also have occasion to use normalized correlations.

$$\begin{aligned} C_f(m) &= \frac{R_f(m)}{L(\underline{a})} \\ C_{f(\underline{a}),\, g(\underline{c})}(m) &= \frac{R_{f(\underline{a}),\, g(\underline{c})}(m)}{V} \end{aligned} \tag{4.6}$$

As an example, let δ^i $(i = 1, \ldots, b)$ be projective functions; that is,

$$\delta^i(a_n) = \left\{ \begin{array}{ll} 1 & \text{if } a_n = e_i \\ 0 & \text{otherwise} \end{array} \right\} = \delta(e_i, a_n) \,. \tag{4.7}$$

The set of images of $\underline{a}$ under these projections completely specifies $\underline{a}$, and vice-versa. That state correlations, or correlations of projections defined earlier, are then merely

$$r_{ij}(m) = C_{\delta i,\, \delta j}(m) \,. \tag{4.8}$$

These are put into a matrix in the obvious way

$$\underset{\sim}{r}(m) = \left[r_{ij}(m) \right] ; \; m = 1, \ldots, L \,, \tag{4.9}$$

to form the correlation matrix of the sequence.

In Chapter 1 we showed that the spectral density of a sequence whose states are waveforms of the same basic time durations is directly related to this matrix function and the Fourier transforms of the sequence states. Also, the correlation of $\underline{a}$ relative to any function f can be expressed as a linear combination of the elements of $\underset{\sim}{r}(m)$.

Let δ^i and δ^k be two projections of $\underline{a}$ and define corresponding p x p circulants $\underset{\sim}{\Delta}^i$ and $\underset{\sim}{\Delta}^k$:

$$\begin{aligned} \underset{\sim}{\Delta}^i &= \left[\Delta^i_{rs}\right] \\ \Delta^i_{rs} &= \delta^i_{r-s} \,. \end{aligned} \tag{4.10}$$

Similarly, for the element $r_{ik}(m)$ in $\underset{\sim}{r}(m)$, define the circulant

$$\underset{\sim}{r}_{ik} = \left[r_{ik}(r-s)\right] \,. \tag{4.11}$$

Now $\underset{\sim}{\Delta}^i$, $\underset{\sim}{\Delta}^k$ and $\underset{\sim}{r}_{ik}$ are related by

$$(\underset{\sim}{\Delta}^i)^T \underset{\sim}{\Delta}^k = \underset{\sim}{r}_{ik} \,, \tag{4.12}$$

as may be verified by routine matrix multiplication. Hence, if $\underset{\sim}{r}_{ik}$ is given, and if $\underset{\sim}{\Delta}^i$ is non-singular, we can find $\underset{\sim}{\Delta}^k$ immediately,

$$\underset{\sim}{\Delta}^k = (\underset{\sim}{\Delta}^i)^{-T} \underset{\sim}{r}_{ik} \,. \tag{4.13}$$

Circulants are a form of a group-ring algebra we shall have occasion to use in the next chapter.

Equation 4.13 states that if the correlation matrix $\underset{\sim}{r}(m)$, m = 1, ..., L, and one of the projections, whose circulant is non-singular, are given, then all projections can be found, and from these a sequence having $\underset{\sim}{r}(m)$ as its correlation matrix can be made.

Therefore, in order to find a sequence having a given correlation matrix, it is sufficient to be able to find a single binary projection (assuming that one exists whose circulant is non-singular), given its autocorrelation function.

Since the spectral density of a sequential process is directly related to $\underset{\sim}{r}(m)$, since the correlation of $\underline{a}$ relative to any function is a linear combination of the terms in $\underset{\sim}{r}(m)$, and since a sequence having $\underset{\sim}{r}(m)$ as its correlation matrix involves finding only a single projection, we see that a study of binary sequences is not restrictive. Therefore, for the remainder of this thesis, we will assume that the functions on sequence states are binary.

There is an obvious transformation between binary (0, 1) sequences and binary (±1) sequences, and likewise, there is one between their correlation functions. Hence, there is no loss in generality in speaking of binary sequences either, as (0, 1) or (±1) sequences. As a matter of convention, we will denote functions on a binary sequence, for the most part, by lower-case Greek letters. For example, we will write α for $\alpha(\underline{a})$, with

$$\alpha_n = \alpha(a_n)$$

$$\alpha_n = \pm 1. \tag{4.14}$$

When we have occasion to use binary (0, 1) sequences, we modify the notation: $\hat{\alpha} = \hat{\alpha}(\underline{a})$ with

$$\begin{aligned} \hat{\alpha}_n &= \hat{\alpha}(a_n) \\ \alpha_n &= (-1)^{\hat{\alpha}_n} . \end{aligned} \tag{4.15}$$

The second part of this last equation can also be written explicitly for $\hat{\alpha}_n$ as

$$\hat{\alpha}_n = \frac{1 - \alpha_n}{2} . \tag{4.16}$$

B. Correlation of Binary Sequences

In the remainder of this chapter we will deal with the correlation function of a binary (±1) sequence without regard to the states which produced the (±1) terms. We treat a more general case in Chapter 7 in which the sequence states are binary vectors.

Let $\alpha = \{\alpha_n\}$ denote a binary (±1) sequence of period p. Its autocorrelation functions are, per period,

$$\begin{aligned} R_\alpha(m) &= \sum_{n=1}^{p} \alpha_n \, \alpha_{n+m} \\ C_\alpha(m) &= \frac{1}{p} \sum_{n=1}^{p} \alpha_n \, \alpha_{n+m} . \end{aligned} \tag{4.17}$$

Obviously, $R_\alpha(m) = R_\alpha(p-m)$, for

$$R_\alpha(p-m) = \sum_{n=1}^{p} \alpha_n \alpha_{n+p-m}$$

$$= \sum_{n=1}^{p} \alpha_n \alpha_{n-m} \qquad (4.18)$$

$$= \sum_{n=1-m}^{p-m} \alpha_{n+m} \alpha_n = R_\alpha(m) ,$$

and trivially, $R_\alpha(0) = p$. The difference between the number of ones and the number of minus ones, per period, will be called the <u>imbalance</u> D_α of α ,

$$D_\alpha = \sum_{n=1}^{p} \alpha_n . \qquad (4.19)$$

Whenever $\left|D_\alpha\right| \leq 1$, α is said to be <u>balanced</u>.

<u>LEMMA</u>: $\sum_{m=1}^{p} R_\alpha(m) = D_\alpha^2 .$

<u>Proof</u>: We merely apply definitions of $R_\alpha(m)$ and D_α:

$$\sum_{m=1}^{p} R_\alpha(m) = \sum_{m=1}^{p} \sum_{n=1}^{p} \alpha_n \alpha_{n+m} = \sum_{n=1}^{p} \alpha_n \sum_{m=1}^{p} \alpha_{n+m}$$

$$= D_\alpha^2 . \qquad (4.20)$$

The next theorem limits the values which $R_\alpha(m)$ assumes to numbers congruent to p modulo 4.

<u>THEOREM</u>: $p - R_\alpha(m)$ is divisible by 4 for all m.

Proof: Let $\{t_1, t_2, \ldots, t_k\}$ be the set of all indices within one period of α such that $\alpha_{t_i} = -1$. Define $\alpha^{(t)}$ as that sequence derived from α by changing α_t to $-\alpha_t$. For example, $\alpha^{(t_1, t_2, \ldots, t_k)}$ is the all-ones sequence of length p. By the structure of the autocorrelation function,

$$R_\alpha(t_1, \ldots, t_r)^{(m)} - R_\alpha(t_1, \ldots, t_{r-1})^{(m)} = 2\alpha_{t_r}(\alpha_{m+t_r} + \alpha_{m-t_r}) \tag{4.21}$$

a change of 0, +4 or -4. Hence, 4 divides each term in

$$\begin{aligned} &\left[R_\alpha(t_1, \ldots, t_k)^{(m)} - R_\alpha(t_1, \ldots, t_{k-1})^{(m)}\right] \\ &+ \left[R_\alpha(t_1, \ldots, t_{k-1})^{(m)} - R_\alpha(t_1, \ldots, t_{k-2})\right] \\ &+ \ldots + \left[R_\alpha(t_1)^{(m)} - R_\alpha(m)\right] = p - R_\alpha(m) \cdot \end{aligned} \tag{4.22}$$

We postulated, in Chapter 2, that sequences with minimal out-of-phase correlations were the best signals in the Gaussian channel. The next theorems give bounds on the optimal types of correlation function.

THEOREM: $$\min_\alpha \operatorname*{Ave}_{m\neq p} R_\alpha(m) = \left\{\begin{array}{l} -1 \text{ if p is odd} \\ \\ -(1+1/p) \text{ if p is even} \end{array}\right\} \cdot$$

Proof: Taking the average as indicated yields

$$\begin{aligned} \operatorname*{Ave}_{m\neq p} R_\alpha(m) &= \frac{1}{p-1}\sum_{m=1}^{p-1} R_\alpha(m) \\ &= \frac{D_\alpha^2 - p}{p-1} \end{aligned} \tag{4.23}$$

To minimize the average by choice of α, we must make D_α^2 as small as possible: $D_\alpha^2 = 1$ if p is odd and $D_\alpha = 0$ if p is even. Substitution of these values gives the theorem.

This bound on the minimum average correlation, along with the congruence of p and $R_\alpha(m)$ modulo 4, produces the following result:

THEOREM: Let α be a binary (± 1) sequence with period p. Then

$$\max_{m \not\equiv 0(p)} R_\alpha(m) \geq \left\{ \begin{array}{l} -1, \text{ if } p \equiv 3(4) \\ 0 \text{ , if } p \equiv 0(4) \\ 1 \text{ , if } p \equiv 1(4) \\ 2 \text{ , if } p \equiv 2(4) \end{array} \right\} .$$

Proof: The maximum value of R(m) is certainly larger than the average, and a forteriori larger than the minimum average.

$$\max_{m \not\equiv 0(p)} R_\alpha(m) \geq \operatorname*{Ave}_{m \not\equiv 0(p)} R_\alpha(m) \geq \min_{\alpha} \operatorname*{Ave}_{m \not\equiv 0(p)} R_\alpha(m) . \tag{4.24}$$

If $\max R_\alpha(m)$ is less than any one of the bounds stated in the theorem, then because $p \equiv R(m) \bmod 4$, we must have

$$-2 \geq \max_{m \not\equiv 0(p)} R(m) \geq -(1 + 1/p) , \tag{4.25}$$

a contradiction.

Next, we will prove the theorem referred to in Chapter 2; namely, the following:

THEOREM: Let α and β be (± 1) sequences whose autocorrelations are $R_\alpha(m)$ and $R_\beta(m)$, respectively. Assume that there exists an operator g_k^t

in $\mathcal{G}$ such that $\beta = g_k^t \alpha$. Then $R_\beta(m) = R_\alpha(km) = g_k^0 R_\alpha(m)$.

Proof: The correlation of β is

$$R_\beta(m) = \sum_{n=1}^{p} \beta_n \beta_{n+m} = \sum_{n=1}^{p} \alpha_{kn+t} \alpha_{k(n+m)+t} \cdot \tag{4.26}$$

But since (k, p) = 1, kn+t, as a function of n, passes through all residue classes modulo p; in this case,

$$R_\beta(m) = \sum_{n=1}^{p} \alpha_n \alpha_{n+km} = R_\alpha(km) , \tag{4.27}$$

which is $g_k^0 R_\alpha(m)$.

As stated in Chapter 2, operators of the affine group do not alter the set of values which $R_\alpha(m)$ takes on, but merely the order in which they appear. In the transformation $\alpha_n \longrightarrow \alpha_{nk+t}$, we say that α has undergone a t-phase-shift and a k-decimation.

C. Term-By-Term Products of Sequences

In the sequel we shall need to know relationships between the properties of (±1) sequences and those of their term-by-term product. The emphasis will be on the period and correlation function of such a product.

Let $\alpha = \{\alpha_n\}$ and $\beta = \{\beta_n\}$ be binary (±1) sequences having periods p and q, respectively. The term-by-term product sequence $\gamma = \alpha * \beta$ of α and β is defined term-wise by

$$\gamma_n = \alpha_n \beta_n . \tag{4.28}$$

We shall often refer to this as merely the *-product. Denote the period of γ by t, and let v = (p, q), V = $\left[p, q\right]$.

If v = 1, γ clearly has maximal period t = V = pq. But if v $\neq$ 1, it is not necessarily true that t = V. For example,

$$\begin{aligned}
\alpha&: + + + + + - - - - - + + + + + - - - - - + + + + + - - - - - \\
\beta&: + + + - - - + + + - - - + + + - - - + + + - - - + + + - - - \\
\gamma&: + + + - - + - - - + - - + + + + + + - - + - - - + - - + + +
\end{aligned} \tag{4.29}$$

Here p = 10, q = 6, v = 2 and V = 30, but t = 15.

The fact that a maximum period is not attained indicates that the sequences are not really "independent" but have some common structure.

LEMMA: If $\alpha_n = \alpha_{n+p}$ and $\alpha_n = \alpha_{n+p'}$ hold for all n, then $\alpha_n = \alpha_{n+(p, p')}$ is also true for all n.

Proof: Since $\alpha_n = \alpha_{n+p} = \alpha_{n+p'}$, it follows that for all u and y, $\alpha_n = \alpha_{n+up} = \alpha_{n+yp'} = \alpha_{n+(up+yp')}$. But there exist certain values[41] of u and y, say u_0 and y_0, such that $u_0 p + y_0 p' = (p, p')$, and therefore $\alpha_n = \alpha_{n+(p, p')}$.

For any positive integer x, we can decimate a sequence α to form a set of sequences $\alpha^{u)}_x$ as follows:

$$\alpha^{u)}_{k\,x} = \alpha_{u+kx}; \quad u = 0, 1, \ldots, x-1 . \tag{4.30}$$

The periods of these decimations are denoted $p_{u/x}$. Whenever a particular x is understood, or when no confusion arises from its omission, we merely write α^u and p_u.

LEMMA: p_u divides $p/(x, p)$.

Proof: The period of α^u must divide $p/(x, p)$ because for a given u, $u+kx \equiv u+(k+p/(p, x)x$ modulo p; i.e., because $p/(x, p)$ is an integer such that $\alpha^u_k = \alpha^u_{k+p/(x, p)}$.

We leave considerations concerning the period of $\gamma = \alpha^* \beta$, for a moment, and turn to the correlation function. By definition,

$$R\gamma(m) = \sum_{n=0}^{t-1} \gamma_n \gamma_{n+m} = \sum_{n=0}^{t-1} \alpha_n \alpha_{n+m} \beta_n \beta_{n+m}$$

$$= \frac{t}{pq} \sum_{n=0}^{pq-1} \alpha_n \alpha_{n+m} \beta_n \beta_{n+m} . \qquad (4.31)$$

Expand α and β to their decimated forms $\alpha^u)_v$ and $\beta^y)_v$.

$$R\gamma(m) = \frac{t}{pq} \sum_{u=0}^{v-1} \sum_{k=0}^{V-1} \alpha^u_k \alpha^{u+y}_{k+r} \beta^u_k \beta^{u+y}_{k+r} , \qquad (4.32)$$

where y is chosen, for a particular u, so that $0 \leq u+y < v$ and $u+kv+m = (u+y) + (k+r)v$. Set $k = i + j;/v$; $0 \leq i < p/v$. This gives

$$R\gamma(m) = \frac{t}{pq} \sum_{u=0}^{v-1} \sum_{i=0}^{(p/v)-1}$$

$$\sum_{j=0}^{\frac{Vv}{p}-1} \alpha^u_{i+jp/v} \alpha^{u+y}_{i+r+jp/v} \beta^u_{i+jp/v} \beta^{u+y}_{i+r+jp/v} . \qquad (4.33)$$

But each α^u has period dividing p/v; therefore, if we sum over i first and recognize that i + jp/v runs through all residues mod q/v, then

$$R_{\gamma}(m) = \frac{t}{pq} \sum_{u=0}^{v-1} \left(\sum_{i=0}^{(p/v)-1} \alpha_i^u \alpha_{i+r}^{u+y} \right) \left(\sum_{j=0}^{(\frac{Vv}{p})-1} \beta_j^u \beta_{j+r}^{u+y} \right) . \tag{4.34}$$

Since $V = \frac{pq}{v}$, we see that $\frac{Vv}{p} = q = v(q/v)$. Define

$$\begin{aligned} R_{\alpha}^u(m) &= \sum_{i=0}^{(p/v)-1} \alpha_i^u \alpha_{i+r}^{u+y} \\ R_{\beta}^u(m) &= \sum_{j=0}^{(q/v)-1} \beta_j^u \beta_{j+r}^{u+y} \end{aligned} \tag{4.35}$$

where m = y+rv with y chosen such that $0 \leq u+y < v$. The correlation of the *-product thus becomes

$$R_{\gamma}(m) = \frac{t}{V} \sum_{u=0}^{v-1} R_{\alpha}^u(m) R_{\beta}^u(m) . \tag{4.36}$$

<u>THEOREM</u>: If $\gamma = \alpha * \beta$, where α and β have period p and q, respectively, and if v = (p, q), define

$$\begin{aligned} R_{\alpha}^u(m) &= \sum_{i=0}^{p/v - 1} \alpha_i^u \alpha_{i+r}^{u+y} \\ R_{\beta}^u(m) &= \sum_{j=0}^{q/v - 1} \beta_j^u \beta_{j+r}^{u+y} \end{aligned} \tag{4.37}$$

where m = y+rv with y chosen such that $0 \leq u+y < v$. Then if t denotes the period of γ ,

$$R_\gamma(m) = \frac{t}{V} \sum_{u=0}^{v-1} R_\alpha^u(m)\, R_\beta^u(m) . \tag{4.38}$$

When p and q are relatively prime, this reduces to a well-known form,

$$R_\gamma(m) = R_\alpha(m)\, R_\beta(m) . \tag{4.39}$$

We can use the formula above to infer the nature of the period of γ. However, it is more instructive to evaluate t more directly.

LEMMA: If $P = \text{lcm}\left\{p_{u/x}\right\}$, then P divides p and p divides Px.

Proof: For each fixed u

$$\alpha_k^u = \alpha_{k+p_u}^u = \alpha_{u+kx+xp_u} . \tag{4.40}$$

Since P is a multiple of every p_u, then

$$\alpha_{u+kx} = \alpha_{u+kx+Px} \tag{4.41}$$

holds for all u. Thus $\alpha_n = \alpha_{n+Px}$, so that p divides Px. Also, the preceding lemma states that p_u divides p, and hence P must also.

LEMMA: If x divides p, then $p = x\ \text{lcm}\left\{p_{u/x}\right\}$.

Proof: By hypothesis, p = mx for some m. Therefore,

$$\alpha_k^u = \alpha_{k+m}^u . \tag{4.42}$$

Hence every p_u divides m, from which it follows that lcm $\left\{p_u\right\}$ divides m. Clearly, then, x lcm $\left\{p_u\right\}$ divides p. Conversely,

$$\alpha_n = \alpha_{u+kx} = \alpha_{u+kx+xp_u} = \alpha_{u+kx+Px} = \alpha_{n+Px} . \tag{4.43}$$

This means p divides xP = x lcm $\left\{p_{u/x}\right\}$, and the lemma is proved.

THEOREM: $p = (x, p)$ lcm $\left\{p_{u/x}\right\}$.

Proof: Let $w = (x, p)$ and $x = mw$. By the lemma above, $p = w$ lcm $\left\{p_{u/w}\right\}$. Note that $\alpha_k^u)_x = \alpha_{u+kx} = \alpha_{u+kmw} = \alpha_{km}^u)_w$. Since $(m, p) = 1$, α_{u+kx} is a co-prime decimation of α_{u+kmw}, which, by virtue of the last theorem in Section A, means that $p_{u/x} = p_{u/w}$. Therefore, $p = (x, p)$ lcm $\left\{p_{u/x}\right\}$.

Let us now apply this to $\gamma = \alpha * \beta$.

THEOREM: Let $\gamma = \alpha * \beta$ have period t, when α and β have periods p and q, respectively. Then $t = V(v,t)/v$, where $v = (p,q)$, $V = \left[p, q\right]$.

Proof: By the preceding theorem,

$$\begin{aligned} t &= (v, t) \text{ lcm } \left\{t_{u/v}\right\} \\ p &= (v, p) \text{ lcm } \left\{p_{u/v}\right\} = v \text{ lcm } \left\{p_{u/v}\right\} \end{aligned} \tag{4.44}$$

$$q = (v, q) \text{ lcm } \left\{q_{u/v}\right\} = v \text{ lcm } \left\{q_{u/v}\right\} . \tag{4.45}$$

But p_u divides p/v and q_y divides q/v; hence $(p_u, q_y) = 1$. Then $\gamma^u = \alpha^u * \beta^u$ has period $t_u = p_u q_u$, and, as a result,

$$t = (v, t)\ \mathrm{lcm}\left\{p_{u/v}\right\}\ \mathrm{lcm}\left\{q_{u/v}\right\} = (v, t)\ \frac{pq}{v^2} = V(v, t)/v\ . \tag{4.46}$$

According to this theorem, the minimal period of γ is V/v, and the maximal period is, of course, V. The maximal period is attained if and only if v divides t. Given two sequences, t is generally unknown before the actual combination and α and β, and so it is not known whether v divides t or not. We therefore seek conditions relating the structure of α and β to the period of γ.

COROLLARY: If v^2 divides V, t = V.

Proof: V/v divides t. Hence, if v divides V/v (i.e., v^2 divides V), it also divides t, and the theorem above applies.

If we substitute V/v for x and $\gamma = \alpha * \beta$ in the previous theorems, we get

$$t = V/v\ \mathrm{lcm}\left\{t_{u/(V/v)}\right\}. \tag{4.47}$$

The condition for minimal period then becomes

$$t_{u/(V/v)} = 1 \qquad \text{for } u = 0, 1, \ldots, (V/v)-1\ . \tag{4.48}$$

Under this condition

$$\alpha^u = \pm \beta^u; \qquad u = 0, 1, \ldots, (V/v)-1\ . \tag{4.49}$$

COROLLARY: $\gamma = \alpha^* \beta$ has minimum period if and only if $\alpha^{u)}_{V/v} = \pm \beta^{u)}_{V/v}$ for all u.

To see what happens if a minimal period is encountered, consider $\gamma = \alpha^* \beta$ whose decimations $\gamma^{u)}_{V/v}$ all have period 1 (the necessary and sufficient condition). Multiply β by +1 or -1 so that $\alpha^0 = \beta^0$ (this clearly does not affect the period behavior of γ). Let u_0, k_0 be such that $u_0 + k_0\, V/v \equiv 0(p)$. Designate $p' = (V/v, p)$. There are exactly p/p' such values of u_0 mod p: $u_0 = m\, p'$ $(m = 0, 1, \ldots, p/p'-1)$. For any u_0, k_0, we note that $\alpha^0_k = \alpha^{u_0}_{k_0+k}$. That is, α^0 and α^{u_0} are identical except for phase-shift.

This may be repeated to find u_i, k_i such that $u_i + k_i\, V/v \equiv i(p)$, and we see that generally $\alpha^i_k = \alpha^{u_i}_{k_i+k}$. This process may be repeated using β and q, in which case $\beta^i_k = \beta^{y_i}_{m_i+k}$.

We recognize that $(p', q') = 1$. Hence, the values of $u_0 = m\, p'$ taken modulo q' exhaust all equivalence classes mod q'. Hence, α^0 differ from the β^i at most by a phase shift, and hence the α^i and β^j differ from each other by at most a phase shift.

THEOREM: If $\gamma = \alpha^* \beta$ has minimum period, then all decimations $\alpha^{u)}_{V/v}$ and $\beta^{y)}_{V/v}$ differ only by phase-shift and possible inversion.

The V/v-decimations can also be analyzed for maximal period conditions. Note that γ takes on maximal period only when $\operatorname{lcm}\left\{t_{u/(V/v)}\right\} = v$. There are several ways to make this occur, two of which are given in the corrollaries below:

COROLLARY: If v is prime, and if there exists a u such that $\alpha^{u)}_{V/v} \neq \pm \beta^{u)}_{V/v}$, then $\gamma = \alpha^* \beta$ has maximum period.

COROLLARY: If there exist u and y such that $p_{u(V/v)}$ and $q_{y(V/v)}$ are relatively prime, and $p_{u(V/v)}\, q_{y(V/v)} = v$, then $\gamma = \alpha^* \beta$ has maximum period.

The latter of these corollaries is true because some phase-shift of every α^u is paired with some phase-shift of every β^y in the products $\alpha^{u'} * \beta^{u'}$. There must then exist a value of u' which pairs α^u with β^y, giving $t_{u'} = v$.

D. The Kronecker Product of Sequences

In this section, a second kind of sequence product is investigated to find the period and correlation function of the resulting sequence.

The Kronecker product $\gamma = \alpha \otimes \beta$ of two sequences α and β having periods p and q, respectively, is defined for all n = uq + y by

$$\gamma_{uq+y} = \alpha_u \beta_y , \tag{4.50}$$

where $0 \leq y < q$. We shall refer to this product merely as the $\otimes$-product.

If t denotes the period of γ, then t is the least positive integer such that

$$\gamma_n = \gamma_{n+t} . \tag{4.51}$$

This periodicity can also be expressed in terms of the component sequences

$$\alpha_u \beta_y = \alpha_{u+x} \beta_{y+z} \tag{4.52}$$

where $t = xq + z$, $0 \leq z+y < q$ (x and z thus depend on y). Clearly, t divides pq, because $\alpha_u \beta_y = \alpha_{u+p} \beta_y$.

And pq is also the <u>least</u> multiple of q which t will divide. However, the period need not be pq and, in fact, may even be less than q. For example,

$$\begin{aligned} \alpha&: \ + - \\ \beta&: \ + - + - + \\ \alpha \boxtimes \beta&: \ + - + - + - + - + - \end{aligned} \tag{4.53}$$

In this case, $p = 2$, $q = 5$ and $t = 2$.

We note also that this product is not a commutative one; that is, $\alpha \boxtimes \beta$ is not generally the same as $\beta \boxtimes \alpha$. For the example above,

$$\beta \boxtimes \alpha: \ + - - + + - - + + - \tag{4.54}$$

has period $t = 10$.

<u>THEOREM</u>: If $p > 2$, $t = pq$.

<u>Proof</u>. Let $t = xq+z$, $0 \leq z+y < q$ for any given fixed y such that $0 \leq y < q$. Then for all u,

$$\alpha_u \beta_y = \alpha_{u+x} \beta_{z+y} . \tag{4.55}$$

Now either $\alpha_u = \alpha_{u+x}$ for all u, in which case p divides x, or else $\alpha_u = -\alpha_{u+x}$ for all u, in which case p divides 2x. In either case, p divides 2x;

let us set mp = 2x. Then $t = \left(\frac{mp}{2}\right) q+z$ divides pq. For some $k \geq 0$,

$$\begin{aligned} kt &= k\left(\frac{mp}{2}\right) q+kz = pq \\ \left(\frac{km}{2} - 1\right)pq &= -kz \ . \end{aligned} \tag{4.56}$$

This can be true only when km = 2 and z = 0, or else m = 0 and kz = pq. In the first case, z = 0 implies t = xq from which it follows that t = pq, since p is the least multiple of q such that t divides xp.

In the second case, m = 0 implies $t = z < q$. This produces two conditions on the sequences

$$\begin{aligned} \alpha_u \beta_y &= \alpha_u \beta_{y+t} \quad ; \ 0 \leq y < q-t \\ \alpha_u \beta_y &= \alpha_{u+1} \beta_{y+t-q} \ ; \ q-t \leq y < q \end{aligned} \tag{4.57}$$

We cancel α_u from the first and note β has period q in the second to give

$$\begin{aligned} \beta_y &= \beta_{y+t} \quad ; \ 0 \leq y < q-t \\ \alpha_u \beta_y &= \alpha_{u+1} \beta_{y+t} \ ; \ q-t \leq y < q \end{aligned} \tag{4.58}$$

Since the second of these equations holds for all u, and since $q > t > 0$, there is some y_0 such that $q-t \leq y_0 < q$ and either $\beta_{y_0} = -\beta_{y_0+t}$, or else $\beta_{y_0} = \beta_{y_0+t}$. For this y_0, the second equation above becomes

$$\left.\begin{aligned} \alpha_u &= -\alpha_{u+1} \\ \alpha_u &= \alpha_{u+1} \end{aligned}\right\} \quad \text{for all u.} \tag{4.59}$$

or

But this would require $p \leq 2$, contrary to hypothesis. Thus, for $p > 2$, the only valid case is $t = pq$, proving the theorem.

In the proof above, it is seen that for $p = 2$ the structure of β determines t; t is the least integer such that t divides 2q and

$$\begin{aligned} \beta_y &= \beta_{y+t} \; ; \quad 0 \leq y < q-t \\ \beta_y &= -\beta_{y+t} \; ; \quad q-t \leq y < q \end{aligned} \tag{4.60}$$

Naturally, if q is prime and $p = 2$, either $t = 2$ or else $t = 2q$.

The correlation function of $\gamma = \alpha \boxtimes \beta$ is, by definition

$$R_\gamma(m) = \frac{t}{pq} \sum_{n=0}^{pq-1} \gamma_n \gamma_{n+m} \tag{4.61}$$

If $m = rq + s$, and $0 \leq s \leq q$,

$$\begin{aligned} R_\gamma(rq+s) &= \frac{t}{pq} \sum_{u=0}^{p-1} \left\{ \sum_{y=0}^{q-s-1} \alpha_u \alpha_{u+r} \beta_y \beta_{y+r} + \sum_{y=q-s}^{q-1} \alpha_u \alpha_{u+r+1} \beta_y \beta_{y+s-q} \right\} \\ &= \frac{t}{pq} \left\{ R_\alpha(r) \sum_{y=0}^{q-r-1} \beta_y \beta_{y+s} + R_\alpha(r+1) \sum_{y=q-s}^{q-1} \beta_y \beta_{y+s} \right\} \end{aligned} \tag{4.62}$$

Define the <u>aperiodic correlation</u> of β as

$$T_\beta(s) = \sum_{y=0}^{q-s-1} \beta_y \beta_{y+s} \; . \tag{4.63}$$

Then the second summand above becomes

$$\sum_{y=q-s}^{q-1} \beta_y \beta_{y+s} = R_\beta(s) - T_\beta(s) \ . \qquad (4.64)$$

Substitution of this in the equation for $R_\gamma(rq+s)$ gives the final result:

THEOREM: If $\gamma = \alpha \otimes \beta$, where α, β and γ have periods p, q and t, respectively, then

$$R_\gamma(rq+s) = \frac{t}{pq} \left\{ R_\alpha(r+1)\, R_\beta(s) + T_\beta(s) \left[R_\alpha(r) - R_\alpha(r+1) \right] \right\} \qquad (4.65)$$

We will almost always be interested in the case $p > 2$; we can therefore drop the t/pq factor in $R_\gamma(m)$.

$$R_\gamma(rq+s) = R_\alpha(r+1)\, R_\beta(s) + T_\beta(s) \left[R_\alpha(r) - R_\alpha(r+1) \right] \qquad (4.66)$$

In a later chapter, we will work specific examples using this formula to show existence of certain classes of sequences having desirable correlation functions.

E. Self-Noise of Incomplete Integration

It is often advantageous, in the interest of saving detection time and equipment, to estimate the autocorrelation function of a sequence by summing the received terms, multiplied by a delayed replica, for only a fraction of the total period. We show in this section that this estimate is unbiased and that the variance decreases monotonically to zero as more and more terms are admitted to the sum.

Suppose we observe a binary (±1) sequence α for only t terms, whereas the period of α is $p \geq t$. Let $C_\alpha(m|t, s)$ denote the normalized estimate:

$$C_\alpha(m|t, s) = \frac{1}{t} \sum_{n=1}^{t} \alpha_{n+s}\, \alpha_{n+s+m} \,. \tag{4.67}$$

We will suppose that the origin of α is unknown; i.e., that s is a uniformly distributed random variable. For any m and t,

$$\begin{aligned} \overline{C}_\alpha(m|t) &= \underset{s}{\text{average}}\; C_\alpha(m|t, s) \\ &= \frac{1}{p} \sum_{s=1}^{p} C_\alpha(m|t, s) \\ &= \frac{1}{pt} \sum_{s=1}^{p} \sum_{n=1}^{t} \alpha_{n+s}\, \alpha_{n+s+m} \end{aligned} \tag{4.68}$$

By summing first over s, and then on t, we see that $C_\alpha(m|t, s)$ is unbiased,

$$\overline{C}_\alpha(m|t) = C_\alpha(m) \,, \tag{4.69}$$

since the expected value of the estimate equals the true, or full-period, value.

The self-noise, fluctuation about this mean, or the variance of the estimate will be a function of m. Many times, however, the delay variable is either unknown beforehand or unimportant. Hence we treat m as a random variable, with all values of m (within a period) equally likely. The variance in the estimate is

$$\sigma^2(t) = \frac{1}{p} \sum_{m=1}^{p} \left[\frac{1}{p} \sum_{s=1}^{p} C_\alpha^2(m|t, s) - C_\alpha^2(m) \right]$$

$$= \frac{1}{t^2 p^2} \left[\sum_{m=1}^{p} \sum_{s=1}^{p} \sum_{n=1}^{t} \sum_{r=1}^{t} \alpha_{n+s} \alpha_{n+s+m} \alpha_{r+s} \alpha_{r+s+m} \right] - \frac{1}{p} \sum_{m=1}^{p} C_\alpha^2(m)$$

$$= \frac{1}{t^2} \sum_{n=1}^{t} \sum_{r=1}^{t} C_\alpha^2(n-r) - \frac{1}{p} \sum_{m=1}^{p} C_\alpha^2(m)$$

$$= \frac{1}{t} - \frac{1}{p} + \frac{1}{t^2} \sum_{n \neq r}^{t} \sum_{r}^{t} C_\alpha^2(n-r) - \frac{1}{p} \sum_{m=1}^{p-1} C_\alpha^2(m) . \qquad (4.70)$$

Designate the largest out-of-phase value of $C_\alpha^2(m)$ by $|C|^2_{max}$, and, similarly, the smallest value by $|C|^2_{min}$. Then we can bound the variance by

$$\sigma^2(t) \leq \frac{1}{t} - \frac{1}{p} + \left(\frac{t-1}{t} \right) |C|^2_{max} - \left(\frac{p-1}{p} \right) |C|^2_{min} \qquad (4.71)$$

This inequality degenerates to equality when α has two-level autocorrelation, $|C|^2_{max} = |C|^2_{min}$.

$$\sigma^2(t) \leq \frac{1}{t}(1 - |C|^2_{max}) - \frac{1}{p}(1 - |C|^2_{min}) + (|C|^2_{max} - |C|^2_{min}) \qquad (4.72)$$

The upper bound is clearly positive and monotone decreasing in t.

As a special case, suppose that $|C|^2_{max} = |C|^2_{min} = C^2$. Equality holds, so that the standard deviation of the estimate is precisely

$$\sigma(t) = \sqrt{\frac{(p-t)}{tp}\ (1 - C^2)}\ . \tag{4.73}$$

When C^2 is much less than one it may be omitted; such will be the case for the so-called pseudo-noise sequences[42], as well as many other sequences given in later chapters. For these sequences,

$$\sigma(t) = \sqrt{\frac{p-t}{tp}} = \frac{1}{\sqrt{p}} \sqrt{\frac{1-(t/p)}{(t/p)}}\ . \tag{4.74}$$

The significance of this result is that correlation can be estimated to a desired degree by proper choice of t. With a given ratio t/p, the accuracy is improved by increasing p. When $p >> t$, the variance is the same as that of a Markov chain with independent states[43].

$$\sigma(t) \sim \frac{1}{\sqrt{t}}\ . \tag{4.75}$$

In the more general case, if $|C|^2_{max}$ and $|C|^2_{min}$ are much less than one, we estimate the upper bound relation

$$\sigma^2(t) \leq \frac{p-t}{pt} + (|C|^2_{max} - |C|^2_{min})\ . \tag{4.76}$$

There are many sequences, which we will study later, with three-level autocorrelation for which $|C|_{max} = 3/p$, $|C|_{min} = 1/p$:

$$|C|^2_{max} - |C|^2_{min} = \frac{8}{p^2}\ . \tag{4.77}$$

For these, the upper bound on deviation is slightly larger than the previous value:

$$\sigma(t) \leq \sqrt{\frac{p-1}{pt} + \frac{8}{p^2}} \quad . \tag{4.78}$$

At $t = p/2$, and large p,

$$\sigma(p/2) \leq \sqrt{\frac{1}{p}} \quad . \tag{4.79}$$

When we are dealing with maximum-length linear shift-register sequences, it is interesting to note that we can determine the variance in partial-time correlation without resorting to an average over correlation delay. That is, we can determine the variance of $C(m|t, s)$ for any fixed m.

If α is a maximal-length linear sequence, it possesses the following property: for every $m \not\equiv 0(p)$, there exists a $u = u(m)$ such that

$$\alpha_n \, \alpha_{n+m} = \alpha_{n+u} \quad . \tag{4.80}$$

This is due to the so-called "cycle-and-add" property of these sequences. The variance is then easily computed as before.

$$\sigma^2(m|t) = \frac{1}{p} \sum_{s=1}^{p} C^2(m|t, s) - \frac{1}{p^2}$$

$$= \frac{1}{pt^2} \sum_{s=1}^{p} \sum_{n=1}^{t} \sum_{k=1}^{t} \alpha_{n+s+u} \, \alpha_{k+s+u} - \frac{1}{p^2} \quad . \tag{4.81}$$

For those values of $n \neq k$, there exist $v = v(n, k)$ such that

$$\alpha_{n+s+u} \, \alpha_{k+s+u} = \alpha_{s+u+v} \quad . \tag{4.82}$$

Consequently, by summing first on s and then over u and k,

$$\sigma^2(m|t) = \frac{1}{pt^2}\left[\sum_{n=1}^{t}\sum_{\substack{k=1\\ n\neq k}}^{t}\sum_{s=1}^{p}\alpha_{s+u+v} + pt\right] - \frac{1}{p^2}$$

$$= \frac{(p-t)(p+1)}{p^2 t} \quad . \tag{4.83}$$

The standard deviation for each m is independent of m

$$\sigma(m|t) = \sqrt{\frac{(p-t)(p+1)}{p^2 t}} \quad . \tag{4.84}$$

When $\sigma^2(m\ t)$ is averaged over all m, as was done for the other less specialized sequences, the same answer is obtained

$$\sigma^2(t) = \frac{(p-t)(p^2-1)}{p^3 t} \quad . \tag{4.85}$$

F. Cross-Correlation of Binary Sequences

Let α and β be binary (± 1) sequences, each having period p, auto-correlations $R_\alpha(m)$, $R_\beta(m)$, and cross correlation $R_{\alpha\beta}(m)$. We then prove the following theorem:

THEOREM: $R_\alpha(0) - R_\alpha(m) \geq R_{\alpha\beta}(0) - R_{\alpha\beta}(m)$.

Proof: Let $\gamma = \{i: \alpha_i \neq \beta_i\}$. Then we write β in terms of α as follows:

$$\beta_i = \begin{cases} \alpha_i\ ; & i \notin \gamma \\ -\alpha_i; & i \in \gamma \end{cases} \tag{4.86}$$

Now, it is clear that

$$R_{\alpha}(n) - R_{\alpha\beta}(n) = \sum_{i=1}^{p} \alpha_{i-n}(\alpha_i - \beta_i)$$

$$= 2 \sum_{i \in \gamma} \alpha_i \alpha_{i-n} \tag{4.87}$$

Hence, by the triangle inequality,

$$R_{\alpha}(n) - R_{\alpha\beta}(n) \leq 2|\gamma| = R_{\alpha}(0) - R_{\alpha\beta}(0) \tag{4.88}$$

and the theorem follows immediately.

Without loss in generality, we can pick the origin of β (or α) such that $R_{\alpha\beta}(0)$ is the maximum cross-correlation value. The theorem above then states that, for any sequence α, its autocorrelation is more distinguishable than its cross-correlation with any other sequence β of the same period.

Chapter 5

SYNTHESIS OF BINARY SEQUENCES

We have discussed so far the need for sequences with desirable correlation properties and have shown the sufficiency of considering only binary sequences. We have given no method, as yet, by which such sequences can be found, and indeed, there is no efficient general method known. Many methods are presented in the next chapters which give extremely good results for a wide class of sequences.

There are two problems we wish to consider in sequence synthesis. First, since the sufficiency of binary synthesis was based on finding a binary sequence when the correlation function is specified exactly, we need a method for doing this. And second, since in communications we want to use sequences with low out-of-phase correlations, we need a method to find them.

One method which always works is an exhaustive search to find the desired sequence. Even if we examine only one representative from each of the different equivalence classes, this is a greal deal of work due to the fact that the number of equivalence classes increases roughly proportionate to $2^{.6p}$. Hence we seek shorter methods to find solutions.

The problem of finding a sequence whose correlation function is specified is a comparatively old one[46,47,48,49,50,51], and it is still unresolved in the general case. One class of notable solutions contains the synthesis procedures for certain classes of pseudo-noise sequences, and another partial solution, developed in the next section, covers synthesis of binary sequences having specified symmetries. As we shall see, an infinite class of optimum and near-optimum sequences belong to this class.

Synthesis of sequences with the best correlation function is sometimes even more difficult, because the exact form of the correlation is not usually known. Many extremely good sequences can be found by combining sequences of smaller periods, and this is done in the next chapters.

An iterative method yielding very good approximate solutions to both problems appears in the final sections of this chapter.

A. An Algebra of Periodic Sequences

Let $\mathcal{F}$ be an arbitrary field and let $\mathcal{F}[x]$ denote the ring of polynomials with coefficients in $\mathcal{F}$. We will denote by $\mathcal{F}_x$ the ring of polynomials modulo x^L-1:

$$\mathcal{F}_x = \mathcal{F}[x]/(x^L-1) . \tag{5.1}$$

This ring is a hypercomplex system[52] (or vector space) over $\mathcal{F}$ with basis $(1, x, x^2, \ldots, x^{L-1})$ and structure constraints

$$x^i x^j = x^{i+j} ; \quad (i+j \text{ taken modulo } L) . \tag{5.2}$$

Every element A of $\mathcal{F}_x$ has the form

$$A = \alpha_0 + \alpha_1 x + \ldots + \alpha_{L-1} x^{L-1} . \tag{5.3}$$

The basis elements $\{x^i\}$ may be construed as the elements of a cyclic group of order L; elements of $\mathcal{F}_x$ are formal sums of field elements paired with group elements. Such a ring is called the group ring[53] of the group (x) over $\mathcal{F}$.

By straightforward calculation we can show

$$1.\quad A + B = \sum_{i=0}^{L-1} (\alpha_i + \beta_i)x^i$$

$$2.\quad AB = \sum_{n=0}^{L-1} \Big(\sum_{i=0}^{L-1} \alpha_i \, \beta_{n-i} \Big) x^n \tag{5.4}$$

$$3.\quad A = B \text{ if and only if } \alpha_i = \beta_i,\ i = 0, 1, \ldots, L-1 .$$

We define the <u>reverse</u> A* of an element A to be the polynomial with the coefficients in reverse order

$$A^* = \sum_{i=0}^{L-1} \alpha_{-i} \, x^i . \tag{5.5}$$

Then, by using (2) above,

$$\begin{aligned} AB^* &= \sum_{n=0}^{L-1} \Big(\sum_{i=0}^{L-1} \alpha_i \, \beta_{n+i} \Big) x^n \\ &= \sum_{n=0}^{L-1} R_{\alpha\beta}(n) x^n . \end{aligned} \tag{5.6}$$

The fact that correlation is a type of product in $\mathcal{F}_x$ allows us to state the first sequence synthesis problem as one involving factorizations in rings: If an autocorrelation R is given, we seek an A such that

$$AA^* = R , \tag{5.7}$$

under the constraint that the α_i be binary valued.

The problem thus reduces to one in the theory of a cyclic group-ring, and all the powerful tools of algebra and the structure of rings are available to aid in the solution. However, even these have not given a satisfactory general solution as yet, and this is chiefly due to the fact that solutions are not unique and, moreover, generally not even equivalent under transformations of the affine group of Chapter 3. The constraint of α_i to binary values is an unnatural one, insofar as algebraic methods are concerned. If we sufficiently restrict the form of either R or A, or both, solutions are available. Being interested in low-out-of-phase correlations, we may investigate methods of synthesizing the pseudo-noise sequences, for example.

Before making any such restrictions, however, there are a few statements concerning the structure of $\mathcal{F}_x$. A fundamental theorem of group rings[54] applied to $\mathcal{F}_x$ allows us to decompose $\mathcal{F}_x$ into a direct sum of orthogonal fields $\mathcal{F}_i$ whenever the characteristic of $\mathcal{F}$ does not divide L. This condition (semi-simplicity) is always satisfied if $\mathcal{F}$ is the field of rational numbers or any other field of characteristic zero. If $\mathcal{F}$ is a finite field, say, the integers modulo a prime q, then the condition is met if (q, L) = 1. We will always assume the condition is fulfilled. Then

$$\mathcal{F}_x = \mathcal{F}_1 \oplus \mathcal{F}_2 \oplus \ldots \oplus \mathcal{F}_m . \tag{5.8}$$

Each $\mathcal{F}_i$ is isomorphic to a simple algebraic extension of $\mathcal{F}$ by a root of an irreducible factor of x^L-1. Every element A in $\mathcal{F}_x$ can be uniquely decomposed into a sum of elements from fields:

$$\begin{aligned} A &= A_1 + A_2 + \ldots + A_m \\ A_i A_j &= 0 \quad \text{if } i \neq j . \end{aligned} \tag{5.9}$$

Denote unit element of $\mathcal{F}_i$ as I_i. By the orthogonality of units,

$$A_i = A I_i . \tag{5.10}$$

The decomposition of $\mathcal{F}_x$ is thus completely specified by the field units $\{I_i\}$.

An element θ with the property

$$\theta^2 = \theta \tag{5.11}$$

is called an <u>idempotent</u>. In each field $\mathcal{F}_i$

$$\begin{aligned} \theta_i^2 &= \theta_i \\ \theta_i &= I_i \text{ or } 0 . \end{aligned} \tag{5.12}$$

All idempotents are thus the sum of field units, and

$$1 = I_1 + I_2 + \ldots + I_m . \tag{5.13}$$

Another way of describing the units is to say that $\{I_i\}$ is the maximal set of mutually orthogonal idempotents.

The following theorem characterizes the rational group ring.

<u>THEOREM</u>: Let $\mathcal{R}_x$ be the group ring of a cyclic group (x) of order L over the rational numbers $\mathcal{R}$. There is a unique field $\mathcal{R}_d$ corresponding to each different divisor d of L, and the period of every element in $\mathcal{R}_d$ is d. The unit I_d of $\mathcal{R}_d$ is of the following form:

(1) If $d = 1$, then

$$I_1 = \frac{1}{L} \sum_{i=0}^{L-1} x^i .$$

(2) If $d = q^m$ for some prime q, then

$$I_d = \frac{d}{qL} \sum_{i=0}^{L/d - q} \left[(q-1) - x^{d/q} - x^{2d/q} - \ldots - x^{(q-1)d/q}\right] x^{id} .$$

(3) If $d = q_1^{m_1} q_2^{m_2} \ldots q_k^{m_k}$, a composition of k distinct primes $q_1, \ldots, q_k$, each having multiplicity $m_i > 0$, and $d_i = q_i^{m_i}$, then the coefficients of I_d are given by

$$\text{coeff. of } x^n \text{ in } I_d = L^{k-1} \prod_{i=1}^{k} (\text{coeff. of } x^n \text{ in } I_{d_i}) .$$

The proof of this theorem consists of a straightforward verification that the set $\{I_i\}$ is a set of $\tau(L)$ (where $\tau(L)$ = number of divisors of L) mutually orthogonal idempotents. This, coupled with the fact that $x^L - 1$ has precisely $\tau(L)$ irreducible factors, implies that $\{I_i\}$ is a maximal set of mutually orthogonal idempotents and must, therefore, be the field units.

B. The Correlation Equation

If $\hat{a}$ is a binary (0, 1) sequence and A is its representation in $\mathcal{F}_x$, then A can be written as

$$A = B + C \tag{5.15}$$

where B represents the "even" part and C represents the "odd" part of A, as follows:

$$B = \sum \hat{\alpha}_i \hat{\alpha}_{-i} x^i$$

$$C = \sum \hat{\alpha}_i (1-\hat{\alpha}_{-i}) x^i \ . \qquad (5.16)$$

Let us define other sequences

$$\tilde{B} = \sum (1 - \hat{\alpha}_i)(1 - \hat{\alpha}_{-i}) x^i$$

$$U = \sum x^i \ . \qquad (5.17)$$

$\tilde{B}$ has ones where $\hat{\alpha}$ has zeros symmetric about $\hat{\alpha}_0$, and U is the all-ones sequence. By construction,

$$B^* = B$$

$$C^* = U - (B + \tilde{B}) - C \ . \qquad (5.18)$$

This reduces the correlation equation to

$$AA^* = A(B + U - B - \tilde{B} - C)$$

$$R = A(U - \tilde{B} - A + B) \ . \qquad (5.19)$$

By moving all terms to one side of the equation,

$$A^2 - (B - \tilde{B})A - k\,U + R = 0 \ , \qquad (5.20)$$

k being the number of ones in A.

$$A^2 - (B - \tilde{B})A + (R - k\,U) = 0\,. \tag{5.21}$$

Hence, if the symmetric structure of A is known, A can be found by solving quadratic equations in the fields $\mathcal{F}_i$.

C. Synthesis of Symmetric Sequences

Suppose A is symmetric about $\hat{\alpha}_0$; that is, $A = A^*$. Then, to solve

$$A^2 = R\,, \tag{5.22}$$

we need to find a binary (0, 1) square root in $\mathcal{F}_x$. If L is odd, we can let $\mathcal{F}$ be the integers modulo 2; then all cross-terms in the square, being even, vanish:

$$A^2 = \sum \hat{a}_i x^{2i} = \sum R_{\hat{\alpha}}(2i)x^{2i}\,. \tag{5.23}$$

Upon equating coefficients, we have a general solution to the first synthesis problem for odd period symmetric sequences.

THEOREM: Let $\hat{\alpha}$ be a binary (0, 1) sequence having odd period and symmetry about $\hat{\alpha}_0$. Then $\hat{\alpha}_i \equiv R_{\hat{\alpha}}(2i) \bmod 2$.

Coefficients in a product AB are convolutions of the sequence α and β. So, in general,

$$A^2 = K \tag{5.24}$$

where we use K to denote the generator of A's convolution function.

$$K(m) = \sum_{i=0}^{L-1} \alpha_i \, \alpha_{m-i} \, . \tag{5.25}$$

When we postulate symmetry of A in the correlation problem, we are really saying that R(m) is a valid convolution function for α. The general problem we have solved is that of finding a sequence with a given arbitrary convolution function.

$$\hat{\alpha}_i \equiv K_{\hat{\alpha}}(2i) \bmod 2 \, . \tag{5.26}$$

The quadratic residues for primes of the form 4t+1 are sequences of this type and, as we shall see later, are very important because their correlation is the best among all binary sequences of the same period.

THEOREM: Let $\hat{\alpha}$ be a non-trivial binary (0, 1) cyclic sequence with two-level autocorrelation, period L, and symmetry about $\hat{\alpha}_0$. Let the sequence have k terms equal to $\hat{\alpha}_1$ per period. Then L must be even and

$$\frac{k}{L} \geq \frac{1}{1 + \frac{(2^s + 1)^2}{(L-1)}}$$

if L has s distinct prime divisors.

Proof: Let A be the generator of $\hat{\alpha}$ in the rational group ring $\mathcal{R}_x$. We must solve

$$A^2 = R \, . \tag{5.27}$$

Case I (odd L): Let L be odd and assume that a non-trivial $\hat{\alpha}$ exists. By the previous theorem,

$$\hat{a}_n \equiv R_{\hat{a}}(2n) \ . \tag{5.28}$$

But R has only two distinguishable coefficients, R(0) and R(1) = R(2) ... = R(L-1). The reduction modulo 2 reveals that $\hat{a}$ can only be one of the trivial sequences (all-zeros, all-ones, all-zeros with a one or all-ones with a zero), contrary to hypothesis. Therefore, if $\hat{a}$ is a non-trivial, symmetric sequence with two-level autocorrelation, L may not be odd.

Case II (L even): Let L be even and assume $\hat{a}$ is a non-trivial symmetric sequence with two-level autocorrelation. The complement of a binary sequence which has two-level autocorrelation also has two-level autocorrelation. We choose $\hat{a}$ to be the one with $\hat{a}_1 = 1$. Then we can write

$$A^2 = R = (k - \lambda) + \lambda U \ . \tag{5.29}$$

From Section A, U is a multiple of I_1:

$$U = L I_1 \ . \tag{5.30}$$

Upon decomposing R into its field components

$$R = \left[k + (L-1)\lambda\right] I_1 + (k - \lambda)I_2 + \ldots + (k - \lambda)I_L \ . \tag{5.31}$$

Subscripts d on I_d refer to the divisors of L. Since $A_1^2 = k^2 I_1$,

$$k^2 I_1 = \left[k + (L-1)\lambda\right] I_1 \tag{5.32}$$

which gives the Bruck-Ryser condition[55] on a difference set (another name for two-level autocorrelation sequences)

$$k^2 = k + (L-1)\lambda \ . \tag{5.35}$$

Other components must satisfy

$$A_d^{\,2} = (k - \lambda)I_d \tag{5.34}$$

for all divisors d of L. These are equations in fields, and therefore $\sqrt{k - \lambda}$ must be in $\mathcal{R}$ if there is to be <u>any</u> solution $\hat{a}$.

$$\begin{aligned} A_1 &= k\, I_1 \\ A_d &= \pm \sqrt{(k - \lambda)I_d} \ , \quad d \neq 1 \ . \end{aligned} \tag{5.35}$$

According to the theorem in Section A, only those idempotents in fields indexed by a d such that

$$d = q_1^{\,m_1} q_2^{\,m_2} \cdots q_s^{\,m_s} \ , \tag{5.36}$$

with each $m_i = 0$ or 1, have non-zero coefficients of x^1. Let s be the number of primes which divide L; there are then 2^s such non-zero coefficients of x^1, each equal to 1/L. Therefore,

$$\hat{a}_1 = 1 = \frac{1}{L}\left[k + \sqrt{k - \lambda} \sum_{\substack{d \ L \\ d \neq 1}} a_d\right]. \tag{5.37}$$

The 2^s-1 numbers a_d above are either plus or minus one. Use of the triangle inequality yields

$$k + \sqrt{k - \lambda}\,(2^s - 1) \geq L \,. \tag{5.38}$$

By subtracting k from each side, squaring, dividing by $k - \lambda$, and substituting $\lambda = (k^2 - k)/(L-1)$, we obtain

$$(2^s-1)^2 \geq \frac{(L - k)(L - 1)}{k} = \frac{1 - (k/L)}{(k/L)}\,(L-1) \,, \tag{5.39}$$

which can easily be solved for k/L, giving the value stated in the theorem.

$$k/L \geq \frac{1}{1 + \dfrac{(2^s - 1)^2}{(L-1)}} \,. \tag{5.40}$$

This inequality is least stringent for $L = \pi_s$, the product of the first s primes. Hence, for any given s, a bound r_0 on the ratio k/L is given by

$$r_0(s) = \frac{1}{1 + \dfrac{(2^s - 1)^2}{\pi_s - 1}} \,. \tag{5.41}$$

For any ratio $k/L < r_0$, no sequences may exist. We may properly speak only about integer values of s as in Table 5-1; however, for visual facility, Figure 5.1 shows $r_0(s)$ with the points connected by a smooth curve. At s = 7, k/L lies within 2% of unity, and at s = 8, within 0.7%.

TABLE 5.1

TABULATION OF LOWER BOUND r_0 ON k/L

s	π_s	r_0
0	1	1.000
1	2	.500
2	6	.357
3	30	.371
4	210	.481
5	2,310	.706
6	30,030	.881
7	510,510	.981
8	9,699,690	.993

s = number of primes dividing cycle length L

π_s = product of first s primes

k = number of ones (or zeros) per cycle.

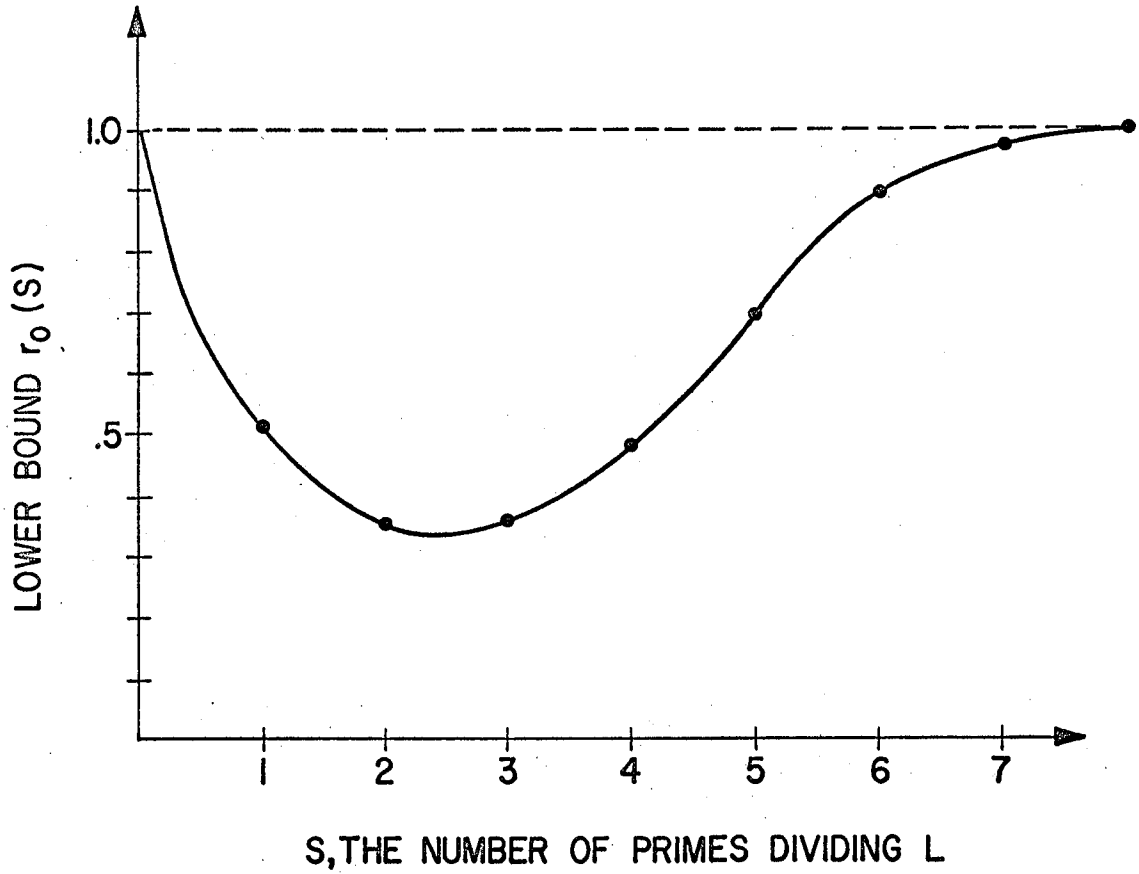

FIGURE 5.1. LOWER BOUND ON THE RATIO k/L AS A FUNCTION OF S, THE NUMBER OF PRIMES DIVIDING L.

D. Synthesis of Anti-Symmetric Binary Sequences

Suppose that α is anti-symmetric about α_0; that is,

$$\begin{cases} \hat{\alpha}_1 = 1 - \hat{\alpha}_{-i} , & (i = 1, 2, \ldots, L-1) \\ \hat{\alpha}_0 = \hat{\alpha}_0 . \end{cases} \tag{5.42}$$

Clearly, L is restricted to being odd. In the correlation equation, $B = \hat{\alpha}_0$ and $\tilde{B} = 1 - \alpha_0$. Then

$$A^2 - A + (R - k\,U) = 0 . \tag{5.43}$$

If we choose to solve this in $\mathcal{R}_x$, we must solve a quadratic equation

$$A_d^{\,2} - A_d + R_d = 0 \tag{5.44}$$

in every field R_d with $d > 1$; for $d = 1$, of course,

$$A_1 = k\,I_1 . \tag{5.45}$$

The number of ones k in A must, because of the anti-symmetry hypothesis, be

$$k = \frac{L+1}{2} . \tag{5.46}$$

Rather than trying to solve the quadratic equations in $\mathcal{R}_x$, as stated formally by

$$A_d = \tfrac{1}{2}(I_d \pm \sqrt{(I_d - 4R_d)}\ )$$

$$= \tfrac{1}{2}(1 \pm \sqrt{1 + 4(k\,U - R)}\ )\ I_d, \qquad (5.47)$$

which is often difficult because of the square root involved, we may revert back to equation 5.43 directly. Since L is odd, we may reduce 5.43 modulo 2 and equate coefficients, giving

$$\alpha_n + \alpha_{2n} \equiv R(2n) + k \pmod 2\ . \qquad (5.48)$$

Since R(m) and k are given, we have only a few choices to make to determine α.

$$\left.\begin{aligned} \alpha_0 &= \alpha_0 \\ \alpha_2 &= \alpha_1 + R(2) + k \\ \alpha_4 &= \alpha_1 + R(2) + R(4) \\ &\text{etc.} \end{aligned}\right\} \quad \text{mod } 2$$

There is only one choice to make in each of the sets corresponding to the cycles of g_2^0: (0) (1, 2, 4, ...) ... (v, 2v, 4v, ...), a total of $\mathcal{C}(2, 0)$ choices (see equation 3.19).

Then, too, if we seek sequences with two-level autocorrelation functions $R = (k - \lambda) + \lambda U$, direct substitution into the correlation equation yields

$$A^2 - A + \left(\frac{L+1}{4}\right)(1 - U) = 0\ . \qquad (5.49)$$

Let q be a prime dividing $\frac{L+1}{4}$, and reduce the equation modulo q. Then

$$A^2 = A\ . \qquad (5.50)$$

The sequence we seek is one of the binary idempotents in $GF(q)_x$. Moreover, since $A^q = A$, and we are working modulo q,

$$\hat{\alpha}_i = \hat{\alpha}_{qi} . \tag{5.51}$$

The sequence we seek is not only an idempotent, but it is also left fixed by the operator g_q^0 of Chapter 3; there are $2^{\mathcal{C}(q, 0)}$ such sequences where, as in Chapter 3,

$$\mathcal{C}(q, 0) = \sum_{d\ L} \frac{\phi(d)}{E_q(d)} . \tag{5.52}$$

Of these $2^{\mathcal{C}(q, 0)}$, many are not eligible because they have an improper number of ones; these can be discarded immediately.

Among the sequences of this anti-symmetric type are found the linear binary sequences mentioned in Chapter 1 and the quadratic residue sequences of period 4t+3 to be discussed in the next chapter.

E. Sequences with Specified Symmetries

Given the correlation R, we can solve the quadratic equation for A formally whenever $(B - \tilde{B})$ is specified. As in the preceding section, this solution has the form

$$A = \tfrac{1}{2}\left[(B - \tilde{B}) + J\sqrt{(B - \tilde{B})^2 + 4(k\ U - R)}\right] \tag{5.53}$$

in the group-ring over a field with characteristic not equal to 2, $J^2 = 1$ being chosen to make A binary. Conceptually, then, the symmetric part of A along with its correlation is sufficient to specify A.

The difficulty arises when one seeks the square root. One need find only a "positive" square root, the rest being taken into account by J. Taking a square root in an arbitrary field is not always an easy thing to do, unless the radicand takes on a form recognized as a square. Otherwise it may require less work to perform an exhaustive search for the sequence with the given correlation.

We can often reduce the amount of search in some special cases by looking for multipliers. A multiplier of a sequence $\hat{a}$ is an integer m such that, for some t, there is an operator g_m^t in $\mathcal{G}$ which leaves $\hat{a}$ fixed. That is, $g_m^t \hat{a} = \hat{a}$. According to the theorem in 4-B, m must also be a multiplier for the correlation function

$$R(n) = R(mn) .$$

Since $\mathcal{G}$ is a group, the multipliers also form a group. Let q be a prime not dividing L, and designate $s = q^r$. If we raise equation 5.21 to the s-th power, reduce modulo q, and apply Fermat's theorem,

$$A^{2s} - (B^s - \tilde{B}^s)A^s + (R^s - k\,U) = 0 .$$

Suppose that $R^s = R$, $B^s = B$ and $\tilde{B}^s = B$; that is, that s is a multiplier of R, B and $\tilde{B}$. Then

$$A^{2s} - (B - \tilde{B})A^s + (R - k\,U) = 0$$

$$A^2 - (B - \tilde{B})A + (R - k\,U) = 0 .$$

Subtracting these two last expressions, it is seen that

$$(A^s + A)\,(A^s - A) \;=\; (B - \tilde{B})\,(A^s - A)\,.$$

But this means that in each of the fields of $GF(q)_x$, either $A_i^s = A_i$ or else $A_i^s + A_i = B_i - \tilde{B}_i$. If the former holds in every field, s is a multiplier of A; let us assume, then, there there is some j such that $A_j^s \neq A_j$. If we had used s^2 instead of s, we would have reasoned that in every field, either $A_i^{s^2} = A_i$ or else $A_i^{s^2} + A_i = B_i - \tilde{B}_i$. But then we cannot have $A_j^{s^2} + A_j = B_j - \tilde{B}_j$ because this would imply

$$A_j^{s^2} \;=\; A_j^s$$

or

$$A_j^s \;=\; A_j\,,$$

contrary to hypothesis. Hence if $A_j^s \neq A_j$ for some j, then $A_j^{s^2} = A_j$. But then

$$A^{s^2} \;=\; A$$

and $m = s^2$ is a multiplier.

THEOREM: If $s = q^r(L)$ for some integer r and prime q relatively prime to L, and $R^s = R$, $B^s = B$ and $\tilde{B}^s = \tilde{B}$ modulo q, then either $m = s$ or $m = s^2$ is a multiplier of A.

For example, suppose we wish to find a ±1 sequence α having

R(n): 13, 1, -3, 1, 1, -3, -3, -3, -3, 1, 1, -3, 1 .

The multipliers of R are $\{1, 3, 4, 9, 10, 12\}$, as easily can be verified, and each of these is of the form $4^r(27)$ or $10^t(27)$. Hence, if we were to assume that either 4 or 10 were multipliers, $12 \equiv -1(13)$ would be also; then $A^* = A$, and we can use the methods of section C to find an $\hat{\alpha}$. We must check the correlation of α to verify that the α we find actually satisfies $AA^* = R$. A solution does exist:

$$\alpha: \quad - - - + - - + + + + - - + - \ .$$

As a special case, we go back to the two-level autocorrelation case:

$$A^2 - (B - \tilde{B})A + (k - \lambda)(1 - U) = 0 \ . \tag{5.54}$$

Let q be a prime divisor of $k - \lambda$ relatively prime to L. If we reduce mod q, then A, B and $\tilde{B}$ are elements of $GF(q)_x$ related by

$$A^2 = (B - \tilde{B})A \ . \tag{5.55}$$

In each field, either

$$A_d = 0 \quad \text{or} \quad A_d = \tilde{B}_d - B_d \ . \tag{5.56}$$

Hence, knowing the symmetry of A limits the forms which A can take rather severly, and it cuts down on the number of trial solutions from 2^L to $2^{\mathcal{C}-1}$, where $\mathcal{C} = \mathcal{C}(q, 0)$, the number of fields. Generally, for any m $(1 \leq m \leq n)$,

$$A^n = (B - \tilde{B})^{n-m} A^m \tag{5.57}$$

so that for $n = q^r+1$,

$$A^{q^r+1} = (B - \tilde{B})^{q^r} A = (B^{q^r} - \tilde{B}^{q^r})A . \tag{5.58}$$

Let us now assume that the only effect of raising B and $\tilde{B}$ to the q^r-th power is a shift in phase: for some t,

$$\begin{aligned} B^{q^r} &= x^t B \\ \tilde{B}^{q^r} &= x^t \tilde{B} . \end{aligned} \tag{5.59}$$

Referring back to Chapter 4, we would say that B and $\tilde{B}$ are invariant under $g^t_{q^r}$ for some t. As a result,

$$A^{q^r+1} = x^t(B - \tilde{B})A = x^t A^2 , \tag{5.60}$$

and therefore A is invariant under the same operator.

$$A^{q^r} = x^t A. \tag{5.61}$$

THEOREM: If α is a binary (0, 1) sequence with two-level autocorrelation, if the symmetric part of A is undisturbed by some operator $g^t_{q^r}$ in the affine group $\mathcal{G}$, and if q is a prime which divides $k - \lambda$, then A is also invariant under this operator.

Stated in terms of multipliers, this reads: if $(q, L) = 1$, q is a prime which divides $k - \lambda$, and if q^r is a multiplier of the symmetric part of A, then q^r is a multiplier of A also.

This theorem is similar to Hall's multiplier theorem[56] which states: If $(q, L) = 1$, q divides $k - \lambda$, and $q^r > \lambda$, then q^r is a multiplier of A. The theorem above can be used to show that all known pseudo-noise sequences have symmetries such that the restriction $q^r > \lambda$ of Hall's theorem is never needed. There is an unproved conjecture that this restriction is never needed.

F. Iterative Methods and Approximations

Often, when we seek a solution to the first correlation problem, we must assume some form for $R(m)$, not knowing whether a solution exists or not. Almost equally as often, for engineering purposes, we do not need to find a sequence which has the given correlation exactly but one whose correlation approximates the given one to a desired degree. This is related to the second correlation problem, that of finding a sequence with low out-of-phase correlation, in that we wish to approximate the ideal (or two-level) autocorrelation to as close a degree as possible.

Let $r(m)$ be a given function. We desire to find a binary (± 1) sequence α, whose autocorrelation $R(m)$ in some sense approximates $r(m)$. Now define a "loss" criterion $\mathcal{L}(\alpha)$ on α relating to the quality of this approximation. For example, $\mathcal{L}(\alpha)$ might be the total square-error,

$$\mathcal{L}(\alpha) = \sum_{m=1}^{p} \left[r(m) - R(m)\right]^2 . \tag{5.62}$$

Implicit in any definition of $\mathcal{L}(\alpha)$, we assume α is a "better" sequence than β if $\mathcal{L}(\alpha) < \mathcal{L}(\beta)$.

Suppose that α is a given sequence; then for any fixed k, denote by $\alpha^{(k)}$ that sequence whose terms satisfy

$$\alpha_i^{(k)} = \begin{cases} \alpha_i \ ; \ i \neq k \\ \\ -\alpha_k ; \ i = k \end{cases} . \tag{5.63}$$

Considering the set $\left\{ \alpha^{(k)} ; \ k = 1, 2, \ldots, p \right\}$ to be a neighborhood of α, the loss assumes minima relative to these neighborhoods and, of course, at least one absolute minimum. This absolute minimum corresponds to the best approximation possible. By proper choice of loss functions, it is hoped that relative minimal loss sequences also can give good approximations.

To find a relative minimum loss, we may start with an arbitrary or randomly chosen periodic sequence β and find a sequence of indices i_1, i_2, ..., i_k such that

$$\mathcal{L}(\beta) > \mathcal{L}(\beta^{(i_1)}) > \mathcal{L}(\beta^{(i_1, i_2)}) > \ldots > \mathcal{L}(\beta^{(i_1, i_2, \ldots, i_k)}) . \tag{5.64}$$

When this finally leads to $\alpha = \beta^{(i_1, i_2, \ldots, i_k)}$ such that for all i,

$$\mathcal{L}(\alpha) \leq \mathcal{L}(\alpha^{(i)}) , \tag{5.65}$$

then α is a <u>minimal loss sequence</u>. There is no guarantee, of course, that this iteration will <u>ever</u> give the true minimum loss.

If we were to start our iterative procedure at a <u>maximal</u> loss sequence υ and finish with a relatively minimal loss α,

$$\alpha = \upsilon^{(i_1, i_2, \ldots, i_k)}, \tag{5.66}$$

the total change in loss would be

$$\mathcal{L}(\upsilon) - \mathcal{L}(\alpha) = \sum_{j=0}^{k-1} \left[\mathcal{L}(\upsilon^{(i_1, i_2, \ldots, i_j)}) - \mathcal{L}(\upsilon^{(i_1, i_2, \ldots, i_{j+1})}) \right]$$

$$= k(\Delta\mathcal{L})_{\text{average}} . \tag{5.67}$$

When we want to have $\mathcal{L}(\alpha)$ as small as possible, we want to choose the indices $i_1, i_2, \ldots, i_k$ to maximize $\mathcal{L}(\upsilon) - \mathcal{L}(\alpha)$; i.e., to make both k and $(\Delta\mathcal{L})_{\text{ave}}$ as large as possible. In practical cases, k and $\Delta\mathcal{L}$ are not entirely independent. However, k is usually related to the number of minus (or plus) ones in α and is, consequently, somewhat fixed. Heuristically, then, we desire to maximize the change in loss at each state of the approximation.

$$\mathcal{L}(\alpha) = \mathcal{L}(\upsilon) - k(\Delta\mathcal{L})_{\text{ave}} . \tag{5.68}$$

When we begin the iteration, with a sequence chosen at random, we may still use this maximal-change policy to advantage.

Whether iteration from a randomly chosen sequence leads to a true minimum or merely a minimal loss depends on the relative abundance of optimal sequences in the set of minimal loss sequences. In the cases where only a few optimal sequences of a given period exist, the iterative procedure has shown reluctance to find them. On the other hand, the sequences found in almost every case are surprisingly good ones.

1. Quadratic loss and minimal variance sequences. Because we seek sequences with low out-of-phase correlations, we will assume that $r(m) = -r$ for all $m \neq 0$ and $r(0) = p$; that is, we seek, by the iterative method above, to find an approximation to the ideal two-level autocorrelation function. For any binary (± 1) sequence α, define the loss function to be the total square-error

$$\mathcal{L}(\alpha) = \sum_{m=1}^{p} \Big[r(m) - R(m)\Big]^2 = \sum_{m=1}^{p-1} \Big[R(m) + r\Big]^2 . \tag{5.69}$$

Now by changing α_i to $-\alpha_i$, the value of $R(m)$ changes by $2\alpha_i(\alpha_{i+m} + \alpha_{i-m})$, because

$$R(m) = \alpha_i(\alpha_{i+m} + \alpha_{i-m}) + \sum_{\substack{n=1 \\ n\neq i, n\neq i-m}} \alpha_n \alpha_{n+m} . \tag{5.70}$$

The change in loss is therefore given by

$$\mathcal{L}(\alpha) - \mathcal{L}(\alpha^{(i)}) = \sum_{m=1}^{p-1} \Big[(R(m) + r)^2 - (R(m) + r - 2\alpha_i(\alpha_{i+m} + \alpha_{i-m}))^2\Big]$$

$$\Delta_i\mathcal{L} = 4 \sum_{m=1}^{p-1} \Big[(R(m) + r)(\alpha_{i+m} + \alpha_{i-m})\alpha_i - (\alpha_{i+m} + \alpha_{i-m})^2\Big]. \tag{5.71}$$

Averaging these $\Delta_i\mathcal{L}$ over i,

$$\underset{i}{\text{ave}}(\Delta_i\mathcal{L}) = \frac{8}{p}\left[\sum_{m=1}^{p-1} R^2(m) - p^2 - (r-1)p + rD^2 - \delta\right] . \tag{5.72}$$

Here we have inserted

$$D = \sum_{n=1}^{p} \alpha_n$$

$$\delta = \sum_{m=1}^{p-1} \sum_{i=1}^{p} \alpha_{i-m}\, \alpha_{i+m} = \sum_{m=1}^{p-1} \sum_{i=1}^{p} \alpha_{2i-m}\, \alpha_m \,. \tag{5.73}$$

When p is odd, note that the latter reduces to

$$\delta = D^2 - D\,\alpha_0 \,, \tag{5.74}$$

and when p is even, to

$$\delta = 2(D_o^{\,2} + D_e^{\,2}) - D_e\,\alpha_0 = 2D^2 - 4D_o\,D_e - D_e\,\alpha_0 \,. \tag{5.75}$$

D_o and D_e represent the sum $\sum \alpha_n$ over odd and even n, respectively.

At the termination of iteration, $\Delta_i \mathcal{L} \leq 0$ for all i. Clearly, then, the average is also less than zero, whence

$$\sum_{m=1}^{p-1} R^2(m) \leq p^2 + (\,\delta - rD^2) + (r-1)p \,. \tag{5.76}$$

For a minimal loss α based on $\mathcal{L}(\alpha)$, the loss $\mathcal{L}'(\alpha)$ about $r'(m) = -1$ is bounded by

$$\mathcal{L}'(\alpha) = \sum_{m=1}^{p-1} \Big[R(m) + 1\Big]^2 \leq p^2 + (r-2)p + \delta - (r-2)D^2 - 1 \,, \tag{5.77}$$

which, for large p, nearly balanced sequences, and r = 2, gives an approximate upper bound on the RMS of $\Big[R(m) + 1\Big]$:

$$\mathrm{RMS}\left[R(m) + 1\right] = \sqrt{\underset{m \neq 0}{\text{ave}} \left[R(m) + 1\right]^2} \leq \sqrt{p}$$

$$\mathcal{L}'(\alpha) \leq p^2 \quad . \tag{5.78}$$

In practice, sequences found by iteration on a quadratic loss are much better than the bound above indicates. The reason for this is that $\Delta_i \mathcal{L} \leq 0$ is too weak a statement for most i. An indication of the sensitivity of this bound can be obtained by estimating the average $\Delta \mathcal{L}$ per iteration step. Starting with a maximal loss sequence v, the all-ones,

$$\mathcal{L}(v) = (p-1)(p+1)^2 \quad . \tag{5.79}$$

The maximum $\Delta \mathcal{L}$ occurs when v is changed to $v^{(i)}$, any i.

$$\mathcal{L}(v^{(i)}) = (p-1)(p-3)^2 \quad . \tag{5.80}$$

Hence, the maximum change per step is

$$(\Delta \mathcal{L})_{\max} = 8(p-1)^2 \quad . \tag{5.81}$$

On the other hand, the minimum change in loss can be nearly zero, or a very small fraction of the maximum, for large p.

For a fixed decision rule, let h be defined by

$$(\Delta \mathcal{L})_{\text{ave}} = \frac{(\Delta \mathcal{L})_{\max}}{h} = \frac{8(p-1)^2}{h} \quad . \tag{5.82}$$

We expect k to be close to the number of minus ones in α (it will be precisely the number of minus ones if no minus is changed back to plus in the iteration), and this number should be something like p/2 so that the average correlation is near -1.

We then estimate

$$\mathcal{L}(\alpha) = (p-1)(p+1)^2 - \frac{4p}{h}(p-1)^2 . \tag{5.83}$$

Now certainly $\mathcal{L}(\alpha) \geq 0$, and if α is minimal loss, $\mathcal{L}(\alpha) \leq p(p-1) + D^2 + \delta - 1$. Dropping $D^2 + \delta - 1$ from the latter term as being negligible for large p, we get tight upper and lower bounds on h.

$$4\left(1 - \frac{3p+1}{(p+1)^2}\right) \leq h \leq 4\left(1 - \frac{2p+1}{p^2+p+1}\right) . \tag{5.84}$$

For large p, h is less than, but very close to, 4. The lower bound on h produces the lower bound on $\mathcal{L}(\alpha)$ and likewise, the upper bound yields the upper bound on $\mathcal{L}(\alpha)$.

By using a maximum-decision rule in the iteration procedure, we attempt to increase the average, thereby lowering h. As shown by the analysis above, we do not have to increase the average very much to get a sizeable decrease in $\mathcal{L}(\alpha)$ over the loss produced by the worst decision rule.

When, at a given stage, negation of the ith element in the sequence produces a maximum change in loss, we may expect that many such i will also produce this change. As a matter of convenience, we always decide to negate the least i which gives the proper change.

2. Even-moment loss sequence. In using a quadratic criterion to generate a minimal loss sequence, it is conceivable that the final result has a large number of places where correlation is close to -1 and a few places where the correlation is large but in which the decrease in loss gained by negating some element, causing a decrease in the maximum correlation (which is what we want), is counteracted by a large number of small increases of R(m) away from -1. Experimentally, it is found that this does occur and becomes more serious as the period increases.

One way to counteract this is by using a criterion in which a large deviation from -1 costs much more than the total cost of the small increases. To do this, we can use an sth even-moment loss function

$$\mathscr{L}(\alpha) = \sum_{m=1}^{p-1} \left[R(m) + 1\right]^{2s} . \tag{5.85}$$

For any given s, there exists a period p at which the criterion will begin failing to minimize the maximum out-of-phase correlation. Up to this period, the iteration reduces the maximal $\left| R(m) + 1 \right|$ to a relative minimal point and the reduces the number of these maxima to a relative minimum. For this reason, minimal loss sequences for any $s = s_0$ are also minimal loss for $s < s_0$.

Reducing the maximal distance of the correlation from -1 is not exactly the same as reducing the maximal correlation, since the even-moment of a large negative correlation will also cause the negative correlation to be increased. On the whole, then, even-moment cost criteria tend to make the final sequence nearly constant in out-of-phase correlation.

Experimentally, s = 1 in the criterion gives good sequences up to about p = 28, and s = 2 increases this up to p = 46. For s = 4, good results were

obtained up to the largest period considered, p = 63. We shall have more to say about these experiments later. It is of interest to note (see Tables 5.2 - 5.4) that the maximum correlation remained about the same for s = 1, 2 and 4 at a given value of p; however, the number of maxima decreased as s was increased. Note also the effect of different values of r.

3. Maximum-correlation loss criterion. We can take, as a valid loss function, the double criterion

$$\mathcal{L}(\alpha) = (R_{\alpha M}, N_\alpha) \tag{5.87}$$

where $R_{\alpha M} = \max\left\{R_\alpha(m)\right\}$, and N_α is the number of times $R_\alpha(m) = R_{\alpha M}$. We order $\mathcal{L}(\alpha)$ lexiographically as follows:

$$\mathcal{L}(\alpha) \leq \mathcal{L}(\beta), \text{ if } R_{\alpha M} < R_{\alpha M}$$
$$\text{or } R_{\alpha M} = R_{\beta M} \text{ and } N_\alpha \leq N_\beta . \tag{5.88}$$

Expressed another way, we may take

$$\mathcal{L}(\alpha) = p\, R_{\alpha M} + N_\alpha . \tag{5.89}$$

Then, naturally, $\mathcal{L}(\alpha) \leq \mathcal{L}(\beta)$ if and only if the lexiographic ordering above holds, because $N_\alpha < p$.

The advantage of this criterion lies in the fact that only maximal correlations affect $\mathcal{L}(\alpha)$, a property not exactly true of the even-moment losses. The disadvantage of this loss is that negative correlation excursions are ignored, and the final sequence may possibly be far from two-

level and not have as few maxima as the even-moment cost sequences (see Table 5.2).

G. Results of Iterative Techniques

Tables 5.2 - 5.4 compare the quality of sequences found by each of four methods: even-moment losses for s = 1, 2, 4, and the maximum-correlation loss. The best sequence of a given period found by these techniques are compiled in the Appendix along with some of the sequences found by methods given in the next chapter. A small, relatively slow digital computer was used to make the iterations.

To compute a correlation function, computer time increases as p^2; the loss computation requires summing roughly p of these correlation terms; and the effect of negating any one of the p sequence elements means that p losses must be computed. The number of iterations is near the number of minus ones, or about p/2. The total computer time thus increases as a polynomial in proportion to p^3. (A search through equivalence classes would increase in proportion to $p^2 2^{0.6p}$.) If, on the other hand, we start with randomly chosen sequences, there is less iteration necessary, and the time increases less rapidly than a p^3 polynomial.

To introduce an initial starting sequence for iteration in the (p+1) case, the p-period sequence previously found was augmented by inserting an extra one per period. After finding the sequence of length p, the computer performed the augmentation and began iteration for p+1.

TABLE 5.2

MINIMUM LOSS SEQUENCES, r = 2

p	sth Even-Moment Loss s = 1	s = 2	s = 4	Max. Correlation Loss	First Positive Charge, s = 1
4	0	0	0	0(opt)	0(opt)
5	1(opt)	1(opt)	1(opt)	1(opt)	1(opt)
6	2(opt)	2(opt)	2(opt)	2(opt)	2(opt)
7	-1(opt)	-1(opt)	-1(opt)	-1(opt)	-1(opt)
8	0	0	0	0(opt)	0
9	1(opt)	1(opt)	1(opt)	1(opt)	1(opt)
10	2(opt)	2(opt)	2(opt)	2(opt)	2(opt)
11	-1(opt)	-1(opt)	-1(opt)	-1(opt)	3
12	0(opt)	0(opt)	0(opt)	0(opt)	0(opt)
13	1(opt)	1(opt)	1(opt)	1(opt)	1(opt)
14	2(opt)	2(opt)	2(opt)	2	2(opt)
15	-1(opt)	-1(opt)	-1(opt)	-1(opt)	3
16	0(opt)	0(opt)	0(opt)	0(opt)	4
17	1(opt)	1(opt)	1(opt)	1(opt)	1(opt)
18	2(opt)	2(opt)	2(opt)	2	2(opt)
19	3	3	3	3	3
20	0(opt)	0(opt)	0(opt)	0	4
21	1(opt)	1(opt)	1(opt)	1(opt)	1(opt)
22	2(opt)	2(opt)	2(opt)	2	6
23	3	3	3	-1(opt)	3
24	4	4	4	4	4
25	1(opt)	1(opt)	1(opt)	1(opt)	5

TABLE 5.2 (continued)

p	sth Even-Moment Loss s = 1	s = 2	s = 4	Max. Correlation Loss	First Positive Charge, s = 1
26	2(opt)	2(opt)	2(opt)	2	6
27	3	3	3	3	3
28	4	4	4	4	4
29	1	1	1	5	5
30	2	2	2	2	2
31	3	3	3	3	3
32	0(opt?)	0(opt?)	0(opt?)	4	4
33	1	1(opt?)	1(opt?)	5	5
34	6	2	2	2	6
35	3	3	3	3	3
36	4	4	4	4	4
37	5	5	5	5	5
38	2	2	2	2	2
39	7	3	3	3	3
40	4	4	4	4	4
41	1	5	5	5	1
42	6	2	2	6	2
43	7	3	3	3	3
44	4	4	4	4	4
45	1	5	5	5	5
46	2	2	2	2	6
47	3	3	3	3	7
48	4	4	4	4	8
49	5	5	5	5	5

TABLE 5.2 (continued)

p	sth Even-Moment Loss s = 1	s = 2	s = 4	Max. Correlation Loss	First Positive Charge, s = 1
50	2	6	6	6	6
51	3	3	3	3	3
52	8	4	4	4	8
53	5	5	5	5	5
54	6	6	6	6	6
55	3	3	7	7	7
56	4	4	4	4	4
57	5	5	5	5	5
58	6	6	6	6	6
59	7	3	3	3	7
60	4	4	4	4	4
61	5	5	5	5	5
62	6	6	2	6	6
63	3	3	3	7	7

NOTE: Figures are maximum out-of-phase correlation values.

TABLE 5.3

MINIMUM LOSS SEQUENCES, r = 3

p	sth Even-Moment Loss s = 1	s = 2	s = 4	First Positive Decision s=1
4	0(opt)	0(opt)	0(opt)	0(opt)
5	1(opt)	1(opt)	1(opt)	1(opt)
6	2(opt)	2(opt)	2(opt)	2(opt)
7	-1(opt)	-1(opt)	-1(opt)	-1(opt)
8	0(opt)	0(opt)	0(opt)	0(opt)
9	1(opt)	1(opt)	1(opt)	1(opt)
10	2(opt)	2(opt)	2(opt)	2(opt)
11	-1(opt)	-1(opt)	-1(opt)	-1(opt)
12	0(opt)	0(opt)	0(opt)	0(opt)
13	1(opt)	1(opt)	1(opt)	1(opt)
14	2(opt)	2(opt)	2(opt)	2(opt)
15	-1(opt)	-1(opt)	-1(opt)	3
16	0(opt)	0(opt)	0(opt)	0(opt)
17	1(opt)	1(opt)	1(opt)	1(opt)
18	2(opt)	2(opt)	2(opt)	2(opt)
19	3	3	3	3
20	0(opt)	0(opt)	0(opt)	4
21	1(opt)	1(opt)	1(opt)	1
22	2(opt)	2(opt)	2(opt)	2
23	3	3	3	3
24	0	0	0	4
25	1(opt)	1	1	5

TABLE 5.3 (continued)

p	sth Even-Moment Loss s = 1	s = 2	s = 4	First Positive Decision s = 1
26	2	2	2	2
27	3	3	3	3
28	4	4	4	4
29	1	1(opt)	1(opt)	5
30	6	2	2	6
31	3	3	3	3
32	4	4	4	4
33	5	1	1	5
34	2	2	2	2
35	3	3	3	3
36	4	4	4	4
37	1(opt)	5	1	5
38	2	2	2	6
39	3	3	3	3
40	4	4	4	4
41	5	5	5	5
42	2	2	2	6
43	3	3	3	3
44	4	4	4	8
45	5	5	5	5
46	6	2	2	6
47	3	3	3	7
48	4	4	4	4

TABLE 5.3 (continued)

p	sth Even-Moment Loss s = 1	s = 2	s = 4	First Positive Decision s = 1
49	5	5	5	5
50	2	6	2	2
51	7	3	3	3
52	4	4	4	4
53	5	5	5	5
54	6	6	2	6
55	7	3	3	7
56	12	4	4	4
57	9	5	5	5
58	6	6	2	6
59	3	3	3	3
60	4	4	4	4
61	5	5	5	5
62	6	6	6	6
63	7	3	3	3

TABLE 5.4

MINIMUM LOSS SEQUENCES, r = 1

p	sth Even-Moment Loss s = 1	s = 2	s = 4	First Positive Change s = 1
4	0	0	0	0
5	1(opt)	1(opt)	1(opt)	1
6	2(opt)	2(opt)	2(opt)	2(opt)
7	-1(opt)	-1(opt)	-1(opt)	-1(opt)
8	0	0	0	0
9	1	1	1	1
10	2(opt)	2(opt)	2(opt)	2(opt)
11	-1(opt)	-1(opt)	-1(opt)	3
12	0	0	0	0
13	1(opt)	1(opt)	1(opt)	1
14	2(opt)	2(opt)	2(opt)	2(opt)
15	3	3	3	3
16	0	0	0	0
17	1(opt)	1(opt)	1(opt)	1
18	2(opt)	2(opt)	2(opt)	2(opt)
19	3	3	3	3
20	0	0(opt)	0(opt)	4
21	1	1	1	1
22	2(opt)	2	2	2
23	3	3	3	3
24	0(opt)	4	4	4
25	5	5	5	5

TABLE 5.4 (continued)

p	sth Even-Moment Loss s = 1	s = 2	s = 4	First Positive Change s = 1
26	2(opt)	2	2	6
27	3(opt)	3	3	3
28	4	4	4	4
29	5	5	5	5
30	6	2	2	6
31	3	3	3	3
32	4	4	4	8
33	5	5	5	5
34	2	2	2	6
35	3	3	3	3
36	4	4	4	4
37	5	5	5	5
38	2	2	2	6
39	3	3	3	7
40	4	4	4	8
41	5	5	1(opt)	5
42	2	2	2	6
43	3	3	3	3
44	4	4	4	4
45	9	5	5	9
46	6	6	6	6
47	7	3	7	7
48	4	4	4	4
49	9	5	5	9

TABLE 5.4 (continued)

p	sth Even-Moment Loss s = 1	s = 2	s = 4	First Positive Change s = 1
50	10	2	6	6
51	7	7	7	7
52	4	4	4	8
53	5	5	5	5
54	2	2	6	2
55	11	3	7	3
56	4	4	4	4
57	9	5	5	5
58	2	6	6	6
59	7	3	7	7
60	4	4	4	4
61	9	5	5	9
62	6	6	6	6
63	3	7	7	7

Chapter 6

OPTIMUM AND MINIMAX SEQUENCES

A. Optimally Distinguishable Sequences

For any sequence α having period p, let $R_{\alpha M}$ denote the largest value of out-of-phase correlation

$$R_{\alpha M} = \underset{m \not\equiv 0(p)}{\text{maximum}} \left\{ R_\alpha(m) \right\} \quad . \tag{6.1}$$

The minimum of such maximum correlations taken over all sequences α with the specified period will be denoted R_M:

$$R_M = \underset{\alpha}{\text{minimum}} \left\{ R_{\alpha M} \right\} \quad . \tag{6.2}$$

As shown in Chapter 4, there are certain lower bounds on the maximum out-of-phase correlation values of a sequence, according to its period. Those sequences which achieve these lower bounds, when they exist, will be called <u>minimax</u> sequences.

Those sequences whose maximum out-of-phase correlation is R_M are the best that can be hoped for, as far as seeking sequences having low out-of-phase correlation. In some sense, however, it is advantageous and desirable, if α is a sequence having R_M as its maximum out-of-phase correlation, that $R_\alpha(m)$ assume the value R_M a minimum number of times for m = 1, 2, ..., p-1, because this would tend to increase the probability of correct detection. For this reason, we define an <u>optimal</u> sequence, for a specified period p, as one whose maximum out-of-phase correlation is R_M and whose correlation function R(m) takes on the value R_M the least number of times per period.

When p is of the form 4t+3 there often exist sequences with $R_M = 1$; these are the so-called pseudo-noise sequences[57,58]. They are ideal from the point of view that they are minimax, optimal, and R_M is the least of all lower bounds for any period. In fact, it does not necessarily follow that optimal sequences are minimax, or conversely.

The known cases for which such ideal or pseudo-noise sequences exist are[59]

1. $p = 2^n - 1$ (linear sequences)
2. $p = 4t-1$ is prime (Legendre sequences)
3. $p = 4x^2 + 27$ is prime (Hall sequences)
4. $p = t(t+2)$, both t and t+2 are prime (twin-prime sequences).

When there are no sequences having ideal two-level autocorrelation, there are often those whose correlation takes on only three values: an in-phase value (p) and two out-of-phase values. A particularly important case arises when the two out-of-phase correlation values are separated by 4 (the minimum separation). In fact, we may treat two-level correlation as a special case of three-level correlations in which one of the levels occurs 0 times. In our treatment of three-level correlations here, we do not exclude the possibility that one of the three levels does not occur.

In case $p \equiv 3(4)$, but no pseudo-noise sequence of this period exists, we relax the minimax condition somewhat to include an upper bound of +3. A minimax sequence is thus one whose maximum out-of-phase correlation R_M is given by

$$R_M = \begin{cases} 0; & \text{if } p \equiv 0(4) \\ 1; & \text{if } p \equiv 1(4) \\ 2; & \text{if } p \equiv 2(4) \\ -1; & \text{if } p \equiv 3(4) \text{ and a p-n sequence exists} \\ 3; & \text{if } p \equiv 3(4) \text{ and no p-n sequence exists.} \end{cases} \tag{6.3}$$

We connect optimal and minimax sequences by the following theorem:

THEOREM: If α is a balanced sequence with three-level autocorrelation, in which the two out-of-phase correlation values differ by 4, than α is both optimal and minimax.

Proof: The three correlation values are p, the in-phase value, R, the maximum and R-4. Suppose R occurs $N_\alpha (\geq 0)$ times in the correlation function. Then

$$\sum_{n=1}^{p} R_\alpha(n) = p + N_\alpha R + (p-N_\alpha-1)(R-4) = D_\alpha^2 \qquad (6.4)$$

where D_α is the imbalance of α. Solving for N_α produces the relation

$$N_\alpha = - \frac{(R-4)(p-1) + (p-D_\alpha^2)}{4} . \qquad (6.5)$$

By hypothesis, α is balanced: $D_\alpha^2 = 0$ or 1. The fact that $N_\alpha \geq 0$ implies that

$$(R-4)(p-1)(p-D_\alpha^2) \leq 0$$

$$R-4 \leq -\left(\frac{p-D_\alpha^2}{p-1}\right) \leq -1 + \frac{D_\alpha^2 - 1}{p-1} . \qquad (6.6)$$

But since R is an integer, we may omit the fraction $(D_\alpha^2-1)/(p-1)$. This produces the result that

$$R \leq 3 . \qquad (6.7)$$

In the cases $p \equiv 0$, 1 or 2 mod 4, α is clearly a minimax sequence. If $p = 3(4)$, we may either have $R = -1$ or $R = 3$. Let us assume $R = 3$ in this case and show that this includes the other also. Substitution of $R = 3$ into the equation for N_α gives

$$N_\alpha = -\frac{-1(p-1) + (p-1)}{4} = 0 . \tag{6.8}$$

This states that if $p \equiv 3(4)$ and $R = 3$, then this value of 3 is taken on 0 times, and hence α is pseudo-noise.

We should interrupt the proof at this point to note from the above that if no pseudo-noise sequence of length $p \equiv 3(4)$ exists, then neither does a balanced three-level sequence.

In all the cases above, the fact that α is a balanced three-level sequence implies that it is also minimax. To prove that it is optimal, we need to show that N_α is the least integer preserving the minimax property. From the foregoing discussion, we need consider only $p \equiv 0$, 1, 2(4), since balanced three-level sequences of length 3 mod 4 are pseudo-noise and thus optimal.

Let β be an optimal sequence having the same period as α; β is then a minimax sequence whose maximum correlation value occurs, say, N_0 times in the correlation function and $N_0 \leq N_\alpha$. Let R_1 denote its average non-maximum out-of-phase correlation and D_β its imbalance:

$$D_\beta = \sum_{i=1}^{p} \beta_i \qquad (\text{and clearly } D_\beta^2 \geq D_\alpha^2) . \tag{6.9}$$

The sum of correlation values over a period is

$$\sum_{n=1}^{p} R_{\beta}(n) = D_{\beta}^2 = p + N_0 R_M + (p-N_0-1)\, R_1 \ . \tag{6.10}$$

Solving this for N_0 produces the relation

$$N_0 = -\frac{(p-1)\, R_1 + (p-D_{\beta}^2)}{R_M - R_1} \ . \tag{6.11}$$

Clearly, $R_1 \leq R_M-4$. If $R_1 = R_M-4$, β is a three-level sequence; the condition $N_0 \leq N_{\alpha}$ implies

$$D_{\beta}^2 \leq D_{\alpha}^2 \ . \tag{6.12}$$

Due to the balance of α, the inequality cannot hold, consequently, $D^2 = D_{\alpha}^2$ and $N_0 = N_{\alpha}$. Therefore, if $R_1 = R_M-4$, α is optimal.

Suppose, on the other hand, that $R_1 < R_M-4$. The condition $N_0 \leq N$ is equivalent to

$$\frac{R_1(p-1) + (p-D_{\beta}^2)}{R_M - R_1} \geq \frac{(R_M-4)\,(p-1) + (p-D_{\alpha}^2)}{4} \ . \tag{6.13}$$

By simple manipulation, we can rearrange this to read

$$D_{\alpha}^2\left(\tfrac{1}{4} - \frac{1}{R_M-R_1}\right) \geq \left[R_M(p-1) + p\right]\left(\tfrac{1}{4} - \frac{1}{R_M-R_1}\right) + \frac{D_{\beta}^2 - D_{\alpha}^2}{R_M-R_1} \ . \tag{6.14}$$

This inequality is not affected if $\frac{D_{\beta}^2-D_{\alpha}^2}{R_M-R_1}$ is dropped (it is non-negative), nor if we divide both sides of the resulting inequality by the positive term $\left(\tfrac{1}{4} - \frac{1}{R_M-R_1}\right)$. When this is done, we obtain

$$D_\alpha^2 \geq R_M(p-1) + p \ . \tag{6.15}$$

The balance of α assures us that $D_\alpha^2 \leq 1$. Consequently,

$$1 \geq R_M(p-1) + p$$

$$R_M \leq -1 \ . \tag{6.16}$$

This can certainly not hold for $p \equiv 0, 1, 2\ (4)$ if $p > 2$. The case $p \equiv 3(4)$ has already been disposed of. Hence a contradiction is reached, indicating that R_1 is not strictly less than $R_M - 4$. We thus revert back to the case $R_1 = R_M - 4$, and α is optimum, completing the proof of the theorem.

The Legendre[60] symbol $\left(\frac{x}{p}\right)$ is defined by

$$\left(\frac{x}{p}\right) = \begin{cases} 0 & \text{if } x \equiv 0 \bmod p \ (p \text{ is a prime}) \\ 1 & \text{if } x \text{ is a square, mod } p \\ -1 & \text{if } x \text{ is a non-square, mod } p \ . \end{cases}$$

Those x with $\left(\frac{x}{p}\right) = 1$ are called <u>quadratic residues</u>.

An equivalent way of defining the Legendre symbol is as follows: since the integers modulo p form a finite field, the multiplicative group is cyclic. Let μ be primitive in this group; then for every $n \not\equiv 0$ there exists a unique r in the range $1 \leq r \leq p-1$ such that

$$\mu^r = n \ . \tag{6.17}$$

Then define

$$\left(\frac{n}{p}\right) = \begin{cases} (-1)^r & n \not\equiv 0\ (p) \\ 0 & n \equiv 0\ (p) \end{cases} \ . \tag{6.18}$$

That these two definitions define the same quantity can be shown as follows: if n is a square, there exists an r such that $\mu^r = x^2 = n$. Suppose r is odd. If this is the case, $\mu^{2m+1} = x^2$ would imply $\mu = (x\mu^{-m})^2$. But μ is primitive and hence must have order p-1, whereas a square can have at most order $\frac{p-1}{2}$. This contradiction indicates that r is even and $(\frac{n}{p}) = 1$ for square n. Similarly, $(\frac{n}{p}) = -1$ for non-square n.

It follows trivially from the latter definition that

$$(\frac{n}{p})(\frac{m}{p}) = (\frac{nm}{p}) \tag{6.19}$$

for all n and m modulo p (that is, the Legendre symbol is a group character)[61].

THEOREM: The Legendre sequences for every prime p produce a balanced, optimal, minimax sequence of period p whose autocorrelation has three-or-fewer levels.

Proof: Define α as follows

$$\alpha_n = \begin{cases} 1 & ; \quad n \equiv 0(p) \\ (\frac{n}{p}); & n \not\equiv 0(p) \end{cases} \tag{6.20}$$

First, α is balanced because

$$D_\alpha = 1 + \sum_{n=1}^{p-1} (\frac{n}{p}) = 1 + \sum_{n=1}^{p-1} (-1)^n$$
$$= 1 + 0 = 1. \tag{6.21}$$

The group property of the Legendre symbol allows us to compute $R_\alpha(m)$ easily:

$$R_\alpha(m) = \sum_{n=1}^{p} \alpha_n \alpha_{n+m} = \alpha_0(\alpha_m + \alpha_{-m}) + \sum_{\substack{n=1 \\ n\neq p-m}}^{p-1} \alpha_n \alpha_{n+m}$$

$$= \alpha_m + \alpha_{-m} + \sum_{n=1}^{p-1} \left(\frac{n}{p}\right)\left(\frac{n+m}{p}\right) . \tag{6.22}$$

Since $n \neq 0$ in the summation terms, there exists some integer, call it n^{-1}, such that $n(n^{-1}) \equiv 1(p)$. Then

$$\left(\frac{n+m}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{1 + m\, n^{-1}}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{x}{p}\right) . \tag{6.23}$$

As n goes through the values 1, 2, ..., p-1, x goes through 2, 3, ..., p, in some order. As a result,

$$R_\alpha(m) = \left(\frac{m}{p}\right) + \left(\frac{-m}{p}\right) + \sum_{x=2}^{p} \left(\frac{x}{p}\right)$$

$$= \left(\frac{m}{p}\right)\left[1 + \left(\frac{-1}{p}\right)\right] + \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) - \left(\frac{1}{p}\right)$$

$$= \left(\frac{m}{p}\right)\left[1 + \left(\frac{-1}{p}\right)\right] - 1 . \tag{6.24}$$

We now need to know when -1 is a quadratic residue; if μ is primitive modulo p,

$$\mu^{\frac{p-1}{2}} = -1 . \tag{6.25}$$

Therefore, -1 is a residue whenever $\frac{p-1}{2}$ is even; i.e., when $p \equiv 1(4)$. Otherwise, when $p \equiv 3(4)$, -1 is a non-residue. Consequently, if $p \equiv 3(4)$,

$$R_\alpha(m) = -1; \; m \not\equiv 0(p) , \tag{6.26}$$

and α is pseudo-noise, as stated earlier. If $p \equiv 1(4)$, on the other hand, α has three-level autocorrelation:

$$R_\alpha(m) = 2 \left(\frac{m}{p} \right) - 1 , \tag{6.27}$$

and $R_\alpha(m)$ takes on the values p, 1 and -3.

In either case, we apply the preceding theorem and optimality of α is assured. If α_0 had been set equal to -1 instead of +1 the result would be unchanged for $p \equiv 3(4)$, but for $p \equiv 1(4)$

$$R_\alpha(m) = -2 \left(\frac{m}{p} \right) - 1 , \tag{6.28}$$

also an optimal correlation function.

B. Minimax Sequences

From the preceding section, optimal minimax sequences are known to exist whenever the period is prime, or of the form $p = 2^n-1$, or $p = t(t+2)$, with both t and t+2 prime. In this section we shall show the existence of several other classes of minimax sequences. We extend the quadratic residue concept and derive conditions under which sequences made by term-by-term and Kronecker products may be made minimax. Some near-optimal sequences result and, in a few special cases (e.g., p = 9) a three-level optimal sequence exists.

1. Jacobi sequences. We begin by extending the quadratic residue sequences. If p and q are different primes, the Jacobi[62] symbol $\left(\frac{n}{pq} \right)$ is defined

$$\left(\frac{n}{pq}\right) = \left(\frac{n}{p}\right)\left(\frac{n}{q}\right) . \tag{6.29}$$

Brauer[63] showed that if proper values of ±1 are inserted in the sequence $\left\{ \beta_n = \left(\frac{n}{pq}\right) \right\}$ where $\left(\frac{n}{pq}\right) = 0$, a pseudo-noise sequence could be made if $q = p \pm 2$. We can prove an analogous theorem.

THEOREM: If p and q are prime and $|p-q|$ is 4 or 6, then a minimax sequence of period pq exists. Furthermore, when $p = q+4$, there exists a sequence with three-level autocorrelation and imbalance 3.

To prove the theorem, define the sequence α termwise as follows:

$$\alpha_n = \begin{cases} \left(\frac{n}{pq}\right); & n \not\equiv 0(p),\ n \not\equiv 0(q) \\ a \quad ; & n \equiv 0(pq) \\ b \quad ; & n \equiv 0(p),\ n \not\equiv 0(q) \\ c \quad ; & n \not\equiv 0(p),\ n \equiv 0(q) \end{cases} \tag{6.30}$$

We wish to choose a, b and c either +1 or -1 so that the correlation function of α is most desirable. Let A be the generating function of α:

$$A = \sum_{n=0}^{pq-1} \alpha_n x^n . \tag{6.31}$$

Likewise, define the component generating functions

$$Q = \sum_{n=1}^{pq-1} \left(\frac{n}{pq}\right) x^n$$

$$B = b \sum_{n=0}^{q-1} x^{pn} \tag{6.32}$$

$$C = c \sum_{n=0}^{p-1} x^{qn} .$$

We may then express A as a sum of these components in the following way:

$$A = Q + B + C + (a-b-c) . \tag{6.33}$$

According to the analysis in Chapter 5, the generator R of $R_\alpha(m)$ is merely

$$AA^* \equiv R \quad \text{modulo } x^{pq}-1 . \tag{6.34}$$

From the structure of the components, $B^* = B$ and $C^* = C$. By routine calculations, we can verify that

$$\left.\begin{aligned} B^2 &= qbB \\ C^2 &= pcC \\ BC &= bc \sum_{n=0}^{pq-1} x^n \end{aligned}\right\} \pmod{x^{pq}-1} \tag{6.35}$$

For convenience, set $h = a-b-c$. The correlation of α is

$$\begin{aligned} AA^* &= QQ^* + (Q + Q^*)(B + C) + h(Q + Q^*) \\ &\quad + (2h + qb)B + (2h + pc)C + 2BC + h^2 . \end{aligned} \tag{6.36}$$

The terms in QQ^* are the correlations of quadratic residues which, because p and q are coprime, are of the form

$$\sum_{n=0}^{pq-1} \left(\frac{n}{pq}\right)\left(\frac{n+m}{pq}\right) = \begin{cases} (p-1)(q-1); & m \equiv 0(pq) \\ -(p-1) & ; m \equiv 0(p),\ m \not\equiv 0(q) \\ -(q-1) & ; m \not\equiv 0(p),\ m \equiv 0(q) \\ +1 & ; m \not\equiv 0(p),\ m \not\equiv 0(q) \end{cases} \tag{6.37}$$

Coefficients in $Q+Q^*$ are $\left(\frac{n}{pq}\right) + \left(\frac{-n}{pq}\right)$; we thus have $Q+Q^* = 2Q$ or 0, according as -1 is a square or non-square modulo pq. Recall that -1 is a square modulo k whenever k is a prime of the type $4r+1$, and a non-square when k is a prime of the type $4r+3$. Hence, if p and q are prime of the same type,

$$Q + Q^* = 0 . \tag{6.38}$$

Finally, consider the product

$$QB = b \sum_{n=0}^{pq-1} \sum_{m=0}^{q-1} \left(\frac{n}{pq}\right) x^{n+mp}$$

$$= b \sum_{k=0}^{pq-1} \sum_{m=0}^{q-1} \left(\frac{k+mp}{pq}\right) x^{k} . \tag{6.39}$$

Since $\left(\frac{k+mp}{pq}\right) = \left(\frac{k}{p}\right)\left(\frac{k+mp}{q}\right)$, the sum on m causes $k+mp$ to go through all residues modulo q exactly once and gives a vanishing sum

$$QB = 0 . \tag{6.40}$$

By symmetry, likewise

$$QC = 0 . \tag{6.41}$$

Substitution of these values in the expression

$$R = QQ^* + h(Q + Q^*) + (2h + qb)B + (2h + pc)C + h^2 \tag{6.42}$$

yields the following correlation values:

$$R(m) = \begin{cases} pq & ; \quad m \equiv 0(pq) \\ 1 + 2bc + 2(a-b-c)\left(\frac{m}{pq}\right) g & ; \quad m \not\equiv 0(p),\ m \not\equiv 0(q) \\ -1 + 2ac - q + p & ; \quad m \not\equiv 0(p),\ m \equiv 0(q) \\ -1 + 2ab - p + q & ; \quad m \equiv 0(p),\ m \not\equiv 0(q) \end{cases} \tag{6.43}$$

where $g = 0$ if p and q are different type primes, and $g = 1$ if p and q are primes of the same type.

Note that if $p = q + 2$, $a = b = -c = 1$, then $R(m)$ takes on the value -1 for all out-of-phase m. This verifies the previous assertion concerning the existence of pseudo-noise sequences whose periods are products of twin primes.

If p and q differ by 6, set $a = b = -c = 1$. By equation 6.43 above,

$$R(m) = \begin{cases} pq; & m \equiv 0(pq) \\ -1; & m \not\equiv 0(p),\ m \not\equiv 0(q) \\ +3; & m \not\equiv 0(p),\ m \equiv 0(q) \\ -5; & m \equiv 0(p),\ m \not\equiv 0(q) \end{cases} \tag{6.44}$$

This is a minimax sequence if no pseudo-noise sequence of length $p(p+6)$ exists (of which none are known at present). A sequence of period 55 made this way appears in the Appendix.

In the case $p = q+4$, set $a = b = -c = 1$. As a consequence,

$$R(m) = \begin{cases} pq & ; \quad m \equiv 0(pq) \\ -1 + 2\left(\frac{m}{pq}\right); & m \not\equiv 0(p),\ m \not\equiv 0(q) \\ 1 & ; \quad m \not\equiv 0(p),\ m \equiv 0(q) \\ -3 & ; \quad m \equiv 0(p),\ m \not\equiv 0(q) \end{cases} \tag{6.45}$$

We compute the square of imbalance by

$$D_\alpha^2 = \sum_{n=0}^{pq-1} R(m) = pq + (p-1) - 3(q-1) - (pq-p-q+1) + 2 \sum_{m=0}^{pq-1} \left(\frac{m}{pq}\right)$$

$$= 9 \tag{6.46}$$

giving an imbalance of 3. If no three-level balanced sequence of such periods exist, these are optimal. The first possible example would have period 77 (the Appendix gives a p = 21 sequence which <u>is</u> balanced).

This completes the proof of the theorem. We note in passing that if p and q differ by more than 6, the maximum out-of-phase value of R(m) is always greater than the minimax value.

Going back to the definition of the quadratic residue, one sees that there are rather obvious symmetries involved. The quadratic residue sequences for $p \equiv 1(4)$ are symmetric about α_0, and for $p \equiv 3(4)$ are anti-symmetric about α_0. These symmetries are carried over into the Jacobi sequences as well. The point is this: all these sequences could have been synthesized by the methods of Chapter 5, given the correlation function (had it been known).

2. <u>Term-by-term product sequences</u>. Suppose p and q are relatively prime and let α and β have periods p and q, respectively. The correlation of $\gamma = \alpha * \beta$ is, of course,

$$R_{\gamma}(m) = R_{\alpha}(m)\, R_{\beta}(m) . \tag{6.47}$$

THEOREM: If $\gamma = \alpha^{*}\beta$ is minimax, α has period p, β period q, (p, q) = 1, and p is divisible by 4, then $R_{\alpha}(m) = 0$ for $m \not\equiv 0(p)$, β is pseudo-noise and γ has three-level autocorrelation.

Proof: Under the hypothesis that γ is minimax, for all $m \not\equiv 0(pq)$,

$$R_{\gamma}(m) = R_{\alpha}(m)\, R_{\beta}(m) \leq 0 . \tag{6.48}$$

For $m = nq$, $R_{\gamma}(nq) = qR_{\alpha}(nq) \leq 0$. This yields

$$R_{\alpha}(m) \leq 0 , \tag{6.49}$$

for all $m \not\equiv 0(p)$. Hence α is minimax. Similarly, when $m = np$, $R(np) = p\, R_{\beta}(np) \leq 0$, and $R_{\beta}(m)$ must be less than or equal to zero for all $m \not\equiv 0(q)$. But this can only occur if β is a pseudo-noise sequence, because q must be odd. If β is taken to be pseudo-noise, for each $m \not\equiv 0(p)$ we get

$$R_{\gamma}(m) = -R_{\alpha}(m) \leq 0 , \tag{6.50}$$

or $R_{\alpha}(m) \geq 0$. This is compatable with $R_{\alpha}(m) \leq 0$ only if

$$R_{\alpha}(m) = 0 ; \qquad m \not\equiv 0(p) . \tag{6.51}$$

There are, then, only three levels in $R_{\gamma}(m)$: pq, 0 and -p.

The only known sequence having the property of equation 6.51 has period 4, equivalent to

$$\alpha: \; + + + - . \tag{6.52}$$

It is conjectured that there are no others; in fact, it has been shown[64] that if others do exist, $p \geq 144$.

To compute the imbalance of γ when $p = 4$,

$$D_\gamma^2 = D_\alpha^2 D_\beta^2 = 4 , \tag{6.53}$$

giving $|D_\gamma| = 2$. The out-of-phase values are, then, 0 and -4. This three-level autocorrelation and near-balance indicate the near-optimality of term-by-term product sequences of period 4q when a pseudo-noise sequence exists having period q. Examples of such sequences are given in the Appendix with periods 28, 44 and 60.

We may now assume that neither p nor q is divisible by 4 and assign $p > q$. If $m = np \not\equiv 0(pq)$,

$$\begin{aligned} R_\gamma(np) &= p\, R_\beta(np) \leq R_M \\ R_\beta(m) &\leq \frac{R_M}{p} . \end{aligned} \tag{6.54}$$

If $p > 3$, $R_\beta(m) < 1$, which implies β is pseudo-noise. Likewise,

$$\begin{aligned} R_\gamma(nq) &= q\, R_\alpha(nq) \leq R_M \\ R_\alpha(m) &\leq \frac{R_M}{q} , \end{aligned} \tag{6.55}$$

and if $q > 3$, α must also be pseudo-noise. Since we have chosen $p > q$, we have the result that if $\gamma = \alpha^* \beta$, $q > 3$, and γ is minimax, then both α and β are pseudo-noise. It is clear that if α and β are pseudo-noise then γ is minimax.

If $q = 2$, $R_M = 2$ and $R_\alpha(m) \leq 1$; so $p \equiv 1$ or $3(4)$.

$$R_\gamma(m) = (-1)^m \, 2R_\alpha(m) \leq 2 . \tag{6.56}$$

Since $(2, p) = 1$, $R_\alpha(m)$ must satisfy both

$$\begin{aligned} R_\alpha(m) &\geq -1 \\ R_\alpha(m) &\leq 1 \end{aligned} \tag{6.57}$$

Consequently, α must have two-level autocorrelation with the out-of-phase value equal to +1 or -1.

The remaining case is $q = 3$; β is then pseudo-noise, because the only sequences of period 3 are pseudo-noise. When $p \equiv 1(4)$, and when no pseudo-noise has period $3p$, $R_M = 3$; α is minimax by equation 6.55. The values $R_\gamma(m)$ assumes are then $3p$, $-R_\alpha(m)$ and $3R_\alpha(m)$. Hence, if α has minimax three(or less)-level autocorrelation $(p, 1, -3)$, γ is minimax.

When $q = 3$ and $p \equiv 3(4)$, equation 6.55 requires that $R_\alpha(m) < 0$, and α must be pseudo-noise. This proves the following theorem:

THEOREM: If $\gamma = \alpha^* \beta$ is minimax, the periods p and q of α and β, respectively, are relatively prime, and $p > q$, then

(1) $q = 2$, and α has minimax two-level autocorrelation, or

(2) $q = 3$, $p \equiv 1(4)$, and α has three(or less)-level minimax autocorrelation $(p, 1, -3)$, or

(3) $q \geq 3$ and both α and β are pseudo-noise.

3. Kronecker-product sequences. Kronecker products sometimes yield minimax sequences if the factors are properly chosen. By considering the cases which arise, we prove the following:

THEOREM: Let $\gamma = \alpha \boxtimes \beta$ be a minimax sequence for which the period p of α is greater than 2. Denote the period of β by q and assume that no pseudo-noise sequence has period pq. Then

(1) If $p \equiv 0(4)$, then $R_\alpha(m) = 0$ for $m \not\equiv 0(p)$, and β is a Barker sequence with q = 2, 3, 7 or 11.

(2) If $p \equiv 1(4)$, α must be minimax, and either

(a) q = 2 and $R_\alpha(m) + R_\alpha(m+1) \geq -2$ for all m, or else

(b) q = 3, α has three-level (or less) autocorrelation (p, 1, -3) and β is either + + − or − + + , or their complements.

(3) $p \equiv 2(4)$ may not occur.

(4) If $p \equiv 3(4)$, α is pseudo-noise, and either

(a) $p \geq 7$, β is a Barker sequence with q = 2, 3, 7 or 11, or else

(b) p = 3, β has three-level (or less) autocorrelation, and an aperiodic correlation function $T_\beta(n)$ satisfying

$$T_\beta(n) \leq \left\{ \begin{matrix} 0; & R_\beta(n) < 0 \\ 1; & R_\beta(n) > 0 \end{matrix} \right\} \quad \text{for all } n \not\equiv 0(q) \ .$$

Proof: Recall that when $mq+n \not\equiv 0(pq)$, $0 \leq n < q$, the condition that γ is minimax is

$$R_\gamma(mq+n) = R_\alpha(m+1)\, R_\beta(n) + T_\beta(n) \left[R_\alpha(m) - R_\alpha(m+1) \right] \leq R_M$$

$$R_\beta(n) = T_\beta(n) + T_\beta(q-n) \ . \tag{6.58}$$

If we alternately set m and n to zero, we derive two conditions on α and β : for out-of-phase values of m,

$$R_\alpha(m) \leq \frac{R_M}{q} \leq \frac{3}{q} ,$$

$$R_\beta(m) \leq \frac{2R_M}{p+R_\alpha(1)} , \tag{6.59}$$

($p+R_\alpha(1)$ cannot vanish for $p > 2$). The minimax value R_M is congruent to pq modulo 4. For every q, α must be a minimax sequence, and in fact,

$$R_\alpha(m) < 2 . \tag{6.60}$$

This rules out $p \equiv 2(4)$ immediately. For every $q > 3$,

$$R_\alpha(m) \leq 0 . \tag{6.61}$$

Before considering specific cases for p, we show $q \not\equiv 0(4)$: let us assume q is divisible by 4 and show this leads to a contradiction. Both α and β are such that

$$R_\alpha(m) \leq 0$$

$$R_\beta(n) \leq 0 . \tag{6.62}$$

Let $\mathcal{N} = \left\{ n: R_\beta(n) = 0 \right\}$; $\mathcal{N}$ is not empty because 0 is the minimax value of $R_\beta(m)$. For every n_0 in $\mathcal{N}$

$$T_\beta(n_0) = -T_\beta(q-n_0) . \tag{6.63}$$

But then, by equation 6.58,

$$
\begin{aligned}
R_{\gamma}(n_0) &= T_{\beta}(n_0)\left[p - R_{\alpha}(1)\right] \leq 0 \\
R_{\gamma}(q-n_0) &= T_{\beta}(q-n_0)\left[p - R_{\alpha}(1)\right] \leq 0 \\
&= -T_{\beta}(n_0)\left[p - R_{\alpha}(1)\right] \leq 0
\end{aligned}
\tag{6.64}
$$

This occurs only if $T_{\beta}(n_0) = 0$ for every n_0 in $\mathcal{N}$, indicating every such n_0 must be even. In Chapter 5, we showed that the minimax value must be attained at least a certain number of times, namely

$$
N_{\beta} \geq \frac{3q}{4} - 1 . \tag{6.65}
$$

But there are only $\frac{q}{2} - 1$ even integers in the range 1, 2, ..., q-1. There must, therefore, be some odd integer n, with $R_{\alpha}(n_1) = 0$; n_1 then belongs to $\mathcal{N}$, contrary to the fact that only even integers may belong to $\mathcal{N}$.

We need only consider Kronecker products with $q \not\equiv 0(4)$ and $p \not\equiv 2(4)$.

Case 1: $p \equiv 0(4)$: By equation 6.59

$$
\begin{aligned}
R_{\alpha}(m) &\leq 0 \\
R_{\beta}(m) &\leq 0 .
\end{aligned}
\tag{6.66}
$$

First, $R_{\alpha}(m)$ must be zero for all $m \not\equiv 0(p)$, for suppose there exists a value of m, say m_0, such that $R_{\alpha}(m_0)$ were less than zero, but $R(m_0 + 1) = 0$. For each $n \not\equiv 0(q)$,

$$
\begin{aligned}
R_{\gamma}(m_0 q+n) &= T_{\beta}(n)\, R_{\alpha}(m_0) \leq 0, \\
T_{\beta}(n) &\geq 0 .
\end{aligned}
\tag{6.67}
$$

But then, by equations 6.58, 6.59 and 6.67,

$$0 \geq R_\beta(n) = T_\beta(n) + T_\beta(q-n) \geq 0, \text{ or}$$
$$R_\beta(n) = 0 , \tag{6.68}$$

and this contradicts the hypothesis that $q \neq 0(4)$. Consequently, there can be no such m_0 and as a result,

$$R_\alpha(m) = 0, \text{ all } m \neq 0(p) . \tag{6.69}$$

The only sequences known to have this property are those equivalent to $+ + + -$.

The second equation of 6.66 limits the values q may take to either 2 or the period of a pseudo-noise sequence. For $q = 2$, equation 6.58 reduces to

$$R_\gamma(2m) = 2R_\alpha(m)$$
$$R_\gamma(2m+1) = -R_\alpha(m) - R_\alpha(m+1) , \tag{6.70}$$

giving a three-level autocorrelation $(2p, 0, -p)$.

Evaluation of equation 6.58 for $m = 0$ gives

$$T_\beta(n) \left[p - R_\alpha(1) \right] \leq 0$$
$$T_\beta(n) \leq 0 . \tag{6.71}$$

This, coupled with the fact that when n is even, q-n is odd, and vice-versa, and

$$R_\beta(n) = T_\beta(n) + T_\beta(q-n) = -1 \tag{6.72}$$

restricts the aperiodic correlation $T_\beta(n)$ to either 0 or -1.

Sequences β such that

$$|T_\beta(n)| \leq 1, \quad 1 \leq n < q \ , \tag{6.73}$$

are called Barker sequences[65]. There are only three pseudo-noise Barker sequences, and these are[66]

$$\begin{aligned} q &= 3, \qquad \beta: \ + + - \\ q &= 7, \qquad \beta: \ + + + - - + - \\ q &= 11, \qquad \beta: \ + + + - - - + - - + - \ , \end{aligned} \tag{6.74}$$

all of which have $T_\beta(n) \leq 0$. Inserting these values in equation 6.58,

$$R_\gamma(mq+n) = \begin{cases} qR_\alpha(m) & \text{when } n = 0 \\ -R_\alpha(m+1) & \text{when } T_\beta(n) = 0 \\ -R_\alpha(m) & \text{when } T_\beta(n) = -1 \ . \end{cases} \tag{6.75}$$

The resulting Kronecker product has three-level autocorrelation (pq, 0, -p).

There are, therefore, minimax sequences with $R_M = 0$ of periods 2p, 3p, 7p and 11p which can be made by Kronecker products whenever a sequence α has $R_\alpha(m) = 0$, all $m \not\equiv 0(p)$.

Case 2: $p \equiv 1(4)$. By equation 6.59, q must be 3 or less, and α is minimax. Consider q = 2. The correlation of γ is restricted by

$$\begin{aligned} R_\gamma(2m) &= 2R_\alpha(m) \leq 2 \\ R_\gamma(2m+1) &= -\left[R_\alpha(m+1) + R_\alpha(m)\right] \leq 2 \ . \end{aligned} \tag{6.76}$$

The second of these is the condition stated in the theorem.

Next, let q = 3. All period 3 sequences are equivalent to + + −, − + +, or + − +. The first two of these have

$$T_{\beta}(n): \ 3, \ 0, \ -1 \ , \tag{6.77}$$

and the third has

$$T_{\beta}(n): \ 3, \ 0, \ +1 \ . \tag{6.78}$$

When β is one of the first two types, $R_{\alpha}(m)$ must satisfy

$$\begin{aligned} R_{\gamma}(3m) &= 3R_{\alpha}(m) \leq 3 \\ R_{\gamma}(3m+1) &= -R_{\alpha}(m+1) \leq 3 \\ R_{\gamma}(3m+2) &= -R_{\alpha}(m) \leq 3 \ . \end{aligned} \tag{6.79}$$

Whenever α has three-level autocorrelation (p, 1, −3), these equations are satisfied, resulting in four-level autocorrelation of α (3p, 3, −1, −p). When α has two-level autocorrelation (p, 1), γ also has four-level autocorrelation (3p, 3, −1, −p). If α has any correlation less than −3, γ is no longer minimax.

Next, when β is the third type,

$$\begin{aligned} R_{\gamma}(3m) &= 3R_{\alpha}(m) \leq 3 \\ R_{\gamma}(3m+1) &= -R_{\alpha}(m+1) \leq 3 \\ R_{\gamma}(3m+2) &= R_{\alpha}(m) - 2R_{\alpha}(m+1) \leq 3. \end{aligned} \tag{6.80}$$

In particular, the third of these, evaluated at m = 0, gives

$$R_\gamma(2) = p - 2R_\alpha(1) \leq 3 , \tag{6.81}$$

which can be rearranged to read

$$\frac{p-3}{2} \leq R_\alpha(1) \leq 1 . \tag{6.82}$$

This can hold only for $p = 5$; but there exists a pseudo-noise sequence with period 15, contrary to the theorem hypothesis. There are, then, no sequences of this third type.

Case 3: $p \equiv 3(4)$. The restriction in the first half of 6.59 limits α to pseudo-noise; the remainder of 6.59, together with equation 6.58, evaluated $m = 1$ limit β as follows:

$$\begin{aligned} R_\beta(n) &\geq -R_M && \text{for all } n \\ R_\beta(n) &\leq \frac{2R_M}{p-1} && \text{for all } n \not\equiv 0(q) . \end{aligned} \tag{6.83}$$

Consequently, β must be minimax three-level or less; equation 6.83, together with equation 6.58, evaluated for $m = 0$, provide the necessary and sufficient conditions which β must satisfy.

$$T_\beta(n) \leq \frac{R_M + R_\beta(n)}{p+1} \leq \frac{4}{p+1} . \tag{6.84}$$

For all $p \geq 7$, the periodic correlation of β would have an upper bound of zero, and thus an out-of-phase correlation bounded above by zero. As a result, either $q = 2$ or else β, as well as α, is pseudo-noise. Further, the upper bound $T_\beta(n) \leq 0$ plus the restriction of β to pseudo-noise requires that

β be one of the pseudo-noise Barker sequences. For each of these, q = 2, 3, 7 or 11, both equation 6.83 and equation 6.84 are satisfied, giving the result stated in the theorem.

On the other hand, if p = 3, the necessary and sufficient conditions reduce to

$$-R_M \leq R_\beta(n) \leq R_M$$

$$T_\beta(n) \leq \frac{R_M + R_\beta(n)}{4} \leq 1 . \tag{6.85}$$

When $q \equiv 3(4)$, $R_M = 1$, so β must be a pseudo-noise Barker sequence, q = 3, 7 or 11; also, q = 2 satisfies 6.85.

In the final two cases, $q \equiv 1(4)$ and $q \equiv 2(4)$, $q > 2$, β must have three-level (or less) minimax (periodic) correlation and an aperiodic autocorrelation which satisfies

$$T_\beta(n) \leq \begin{cases} 0; & \text{if } R_\beta(n) < 0 \\ 1; & \text{if } R_\beta(n) > 0 \end{cases} \tag{6.86}$$

That sequences of this type exist may be verified by example: suppose $q = 6$, β = + − + − − +. Then

$$R_\beta(n): \quad 6, -2, -2, 2, -2, -2 ,$$

$$T_\beta(n): \quad 6, -3, 0, +1, -2, +1 . \tag{6.87}$$

Next, for $q = 9$, β = + + − + + − − − + ,

$$R_\beta(n): \quad 9, 1, -3, -3, 1, 1, -3, -3, 1 ,$$

$$T_\beta(n): \quad 9, 0, -3, 0, 1, 0, -3, 0, 1 . \tag{6.88}$$

There are also Barker sequences with q = 5 and 13, which naturally satisfy 6.85 and 6.86.

This completes the proof of the theorem.

Coll[67] has shown that Kronecker squares of pseudo-noise Barker sequences satisfy equation 6.86. Equations 6.87 and 6.88 were made, respectively, from Kronecker products we can designate as 3 ⊠ 2, and 3 ⊠ 3, the latter being one of Coll's squares. However, Coll's squares, except for the 3 ⊠ 3, violate the first part of 6.85.

C. Compiling the Minimax Sequences

By using the three methods indicated in Section B, we can compute optimum and minimax sequences for all periods commensurate with theory. The first theorem of Section A can be applied as a guide to optimality. Even when this theorem is not applicable, namely, when we have found a non-balanced or non-three-level minimax sequence, the desirable qualities of minimax sequences are evident: near-balance and as few autocorrelation levels as possible.

Table 6.1 shows the existence of minimax sequences synthesized by the methods of this chapter. When more than one method produces minimax sequences of a given period, only the one whose autocorrelation has the least number of out-of-phase maxima is listed.

If we were to compare minimax sequences made from products to those found by iterative computer search, we would see, for periods less than 63, at least, that the computer-found sequences usually have fewer out-of-phase maxima. Of course, when a sequence synthesized by methods of this chapter are optimal, or extremely near optimal, the computer results prove inferior. For this reason, only a few product-sequences appear in the Appendix of Minimax Sequences.

TABLE 6.1

THEORETIC MINIMAX SEQUENCES

period p	generation method	status
4	2 ⊠ 2	optimum
5	quad. res.	optimum
6	3 ⊠ 2	optimum
7	lin. shift-reg.	optimum
8	4 ⊠ 2	optimum
9	3 ⊠ 3	optimum
10	5 ⊠ 2	(10, 2, -2, -6)
11	quad. res.	optimum
12	3 * 4	near optimum
13	quad. res.	optimum
14	7 ⊠ 2	(14, 2, -2, -6)
15	lin. shift-reg.	optimum
16		
17	quad. res.	optimum
18	9 ⊠ 2	(18, 2, -2, -6)
19	quad. res.	optimum
20		
21	7 ⊠ 3	(21, 1, -3, -7)
22	11 ⊠ 2	(22, 2, -2, -10)
23	quad. res.	optimum
24		
25		
26	13 ⊠ 2	(26, 2, -2, -14)
27	3 ⊠ 3 ⊠ 3	(27, 3, -1, -5)
28	4 * 7	optimum (?)
29	quad. res.	optimum
30	15 ⊠ 2	(30, 2, -2, -14)
31	lin. shift-reg.	optimum
32		
33	3 ⊠ 11	(33, 1, -3, -11)

TABLE 6.1 (continued)

period p	generation method	status
34		
35	Jacobi symbol	optimum
36		
37	quad. res.	optimum
38	19 * 2	(38, 2, -2, -18)
39	13 ⊠ 3	(39, 3, -1, -13)
40		
41	quad. res.	optimum
42	21 ⊠ 2	(42, 2, -2, -6, -22)
43	quad. res.	optimum
44	11 * 4	optimum (?)
45	15 ⊠ 3	(45, 1, -3, -15)
46	23 ⊠ 2	(46, 2, -2, -22)
47	quad. res.	optimum
48		
49	7 ⊠ 7	(49, 1, -7)
50	25 ⊠ 2	(50, 2, -2, -6, -26)
51	17 ⊠ 3	(51, 3, -1, -9, -17)
52		
53	quad. res.	optimum
54		
55	Jacobi symbol	(55, 2, -1, -5)
56		
57	19 ⊠ 3	(57, 1, -3, -19)
58		
59	quad. res.	optimum
60	15 * 4	optimum (?)
61	quad. res.	optimum
62	31 ⊠ 2	(62, 2, -2, -30)

SYMBOLS: p ⊠ q (=) Kronecker product of sequences with periods p and q.
p * q (=) termwise product of sequences with periods p and q.
The numbers in parenthesis indicate the correlation levels.

CHAPTER 7

TRANSFORM THEORY OF BOOLEAN SEQUENCES

In this chapter a Fourier-type theory is developed for Boolean functions. Through this theory we will be able to develop optimal sequences to be used in the minimum acquisition-time receiver.

A. Analysis of Discrete Real Functions

Suppose f is any real function of binary (0, 1) variables $x_1, x_2, \ldots, x_n$. The domain $\mathcal{X}$ of f is then a set of 2^n binary vectors $\underline{x} = (x_1, x_2, \ldots, x_n)$

$$\mathcal{X} = \left\{ \underline{x} = (x_1, x_2, \ldots, x_n);\ x_i = 0 \text{ or } 1,\ i = 1, 2, \ldots, n \right\}. \tag{7.1}$$

Since f is completely specified by its value at each of these 2^n points in $\mathcal{X}$, we may consider f as a member of a 2^n-dimensional vector space $\mathcal{V}$.

$$\mathcal{V} = \left\{ f = (f_1, f_2, \ldots, f_{2^n});\ f_i \text{ real} \right\}. \tag{7.2}$$

For any two elements $\underline{s}$ and $\underline{x}$ of $\mathcal{X}$, define the function

$$\phi(\underline{s}, \underline{x}) = 2^{-n/2} \prod_{i=1}^{n} (-1)^{s_i x_i} . \tag{7.3}$$

When $\underline{s}$ is fixed, ϕ is a function of $\underline{x}$ lying in $\mathcal{V}$. These are the Rademacher-Walsh functions[68] and will form the basis of our Fourier theory.

LEMMA: The set $\left\{ \phi(\underline{s}, \underline{x});\ \underline{s} \text{ in } \mathcal{X} \right\}$ is an orthonormal basis of $\mathcal{V}$.

Proof: We merely need to show that any two elements in the set are orthonormal. Let $\underline{s}$ and $\underline{w}$ be members of $\mathcal{X}$. Then

$$\sum_{\underline{x}} \phi(\underline{s}, \underline{x})\, \phi(\underline{w}, \underline{x}) = 2^{-n} \sum_{\underline{x}} \prod_{i=1}^{n} (-1)^{(s_i+w_i)x_i}$$

$$= 2^{-n} \prod_{i=1}^{n} \sum_{x_i=0}^{1} (-1)^{(s_i+w_i)x_i} . \qquad (7.4)$$

This inner product vanishes if any $s_i \neq w_i$; when all $w_i = s_i$, each sum is 2, or

$$\sum_{\underline{x}} \phi(\underline{s}, \underline{x})\, \phi(\underline{w}, \underline{s}) = \begin{cases} 1; & \underline{s} = \underline{w} \\ 0; & \underline{s} \neq \underline{w} \end{cases} \qquad (7.5)$$

The set $\{\phi\}$ is a set of 2^n orthogonal unit vectors in $\mathcal{V}$ and must therefore be a basis.

Now, given any function f in $\mathcal{V}$, we can expand f in terms of this basis

$$f(x) = \sum_{\underline{s}} F(\underline{s})\, \phi(\underline{s}, \underline{x}) \qquad (7.6)$$

There are 2^n coefficients $F(\underline{s})$, and hence F is a member of $\mathcal{V}$; these two corresponding members of $\mathcal{V}$ are a transform-pair.

LEMMA: f and its transform F are related by

$$f(\underline{x}) = \sum_{\underline{s}} F(\underline{s})\, \phi(\underline{s}, \underline{x})$$

$$F(\underline{s}) = \sum_{\underline{x}} f(\underline{x})\, \phi(\underline{x}, \underline{s}) .$$

Proof: The first equation defines the coefficients $F(\underline{s})$; the second is obtained by finding the inner products of f with the new basis:

$$\sum_{\underline{x}} f(\underline{x})\, \phi(\underline{x}, \underline{s}) = \sum_{\underline{s}} \sum_{\underline{x}} F(w)\, \phi(\underline{w}, \underline{x})\, \phi(\underline{s}, \underline{x})$$

$$= F(\underline{s}) . \tag{7.7}$$

From this a dual of Parseval's theorem[69] follows:

THEOREM (Parseval):

$$\sum_{\underline{x}} f^2(\underline{x}) = \sum_{\underline{s}} F^2(\underline{s}) .$$

Proof: An orthonormal linear transformation in a vector space preserves distances.

Now if $\underline{x}$ and $\underline{y}$ are in $\mathcal{X}$, denote by $\underline{x} \oplus \underline{y} = \underline{z}$ the modulo 2 vector sum in $\mathcal{X}$:

$$z_i = x_i + y_i \bmod 2 . \tag{7.8}$$

For any fixed $\underline{y}$, $f(\underline{x} \oplus \underline{y})$ is the $\underline{y}$-translate of $f(\underline{x})$.

LEMMA: If $g(\underline{x}) = f(\underline{x} \oplus \underline{y})$, then $G(\underline{s}) = 2^{n/2}\, \phi(\underline{s}, \underline{y})\, F(\underline{s})$.

Proof:

$$G(s) = \sum_{\underline{x}} g(x)\, \phi(\underline{x}, \underline{s}) = \sum_{\underline{u}} f(\underline{u})\, \phi(\underline{s}, \underline{u} \oplus \underline{y}).$$

But

$$\phi(\underline{s}, \underline{u} \oplus \underline{y}) = 2^{-n/2} \prod_{i=1}^{n} (-1)^{s_i(u_i+y_i)} = 2^{n/2}\, \phi(\underline{s}, \underline{u})\, \phi(\underline{s}, \underline{y}) ,$$

and the theorem follows.

THEOREM (convolution): $f(\underline{x}) = g(\underline{x})\ h(\underline{x})$ if and only if

$$F(\underline{s}) = 2^{-n/2} \sum_{\underline{w}} G(\underline{s} \oplus \underline{w})\ H(\underline{w}) = 2^{-n/2} \sum_{\underline{w}} G(w)\ H(\underline{s} \oplus \underline{w})\ .$$

Proof: By the lemma above, it follows that $f(\underline{x}) = g(\underline{x})\ h(\underline{x})$ if and only if

$$f(x) = \sum_{\underline{s}} \sum_{\underline{w}} G(s)\ H(w)\ \phi(\underline{s}, \underline{x})\ \phi(\underline{w}, \underline{x})$$

$$= \sum_{\underline{s}} \left(\sum_{\underline{w}} 2^{-n/2}\ G(\underline{w})\ H(\underline{w} \oplus \underline{s}) \right) \phi(\underline{s}, \underline{x}) \qquad (7.9)$$

from which the theorem is clear.

COROLLARY: $F(s) = G(s)\ H(s)$ if and only if

$$f(\underline{x}) = 2^{-n/2} \sum_{\underline{y}} g(\underline{x} \oplus \underline{y})\ h(\underline{y})\ .$$

Next, there is the dual to the "initial" value theorem.

THEOREM (initial value): Let f and F be a transform pair in $\mathcal{V}$. Then

$$\sum_{\underline{x}} f(\underline{x}) = 2^{n/2}\ F(\underline{0})$$

and

$$\sum_{\underline{s}} F(\underline{s}) = 2^{n/2}\ f(\underline{0})\ .$$

Proof: $f(\underline{x}) = \sum_{\underline{s}} F(\underline{s})\, \phi(\underline{s}, \underline{x})$. Note, however, that $2^{n/2}\, \phi(\underline{0}, \underline{x}) = 1$ for all $\underline{x}$. Hence, summing on $\underline{x}$,

$$\sum_{\underline{x}} f(\underline{x}) = \sum_{\underline{s}} F(\underline{s})\, \phi(\underline{s}, \underline{x}) 2^{n/2}\, \phi(\underline{0}, \underline{x}) = F(\underline{0}) . \tag{7.10}$$

The same analysis applies with slight modification to give the "final" value.

COROLLARY (final value): Let f and F be a transform pair in $\mathcal{V}$. Then

$$\sum_{\underline{x}} f(\underline{x})\, (-1)^{x_1+x_2+\ldots+x_n} = 2^{n/2}\, F(1, 1, \ldots, 1) ,$$

and

$$\sum_{\underline{s}} F(\underline{s})\, (-1)^{s_1+s_2+\ldots+s_n} = 2^{n/2}\, f(1, 1, \ldots, 1) .$$

Using the initial value theorem, we get an important bound on the transform coefficients.

THEOREM: Suppose that f is bounded: $|f(\underline{x})| \leq M$, all $\underline{x}$. Then

$$-2^{n/2}\, M \leq F_{min}(\underline{s}) \leq 2^{-n/2}\, f(\underline{0}) \leq F_{max}(\underline{s}) \leq 2^{n/2}\, M .$$

Proof: By the initial value theorem, $\sum F(\underline{s}) = 2^{n/2}\, f(\underline{0})$. Obviously, then,

$$2^n\, F_{min} \leq 2^{n/2}\, f(\underline{0}) \leq 2^n\, F_{max} . \tag{7.11}$$

By hypothesis, f is bounded by M; by the triangle inequality,

$$|F(s)| = \left|\sum f(\underline{x})\ \phi(\underline{x},\ \underline{s})\right| \leq 2^{-n/2} \sum |f(\underline{x})| \leq 2^{n/2}\ M, \qquad (7.12)$$

from which the theorem follows.

Let π be an operator on $\mathcal{X}$ which, when applied to $\underline{x}$, permutes the indices:

$$\underline{x} = (x_1,\ x_2,\ \ldots,\ x_n)$$

$$\pi\underline{x} = (x_{\pi 1},\ x_{\pi 2},\ \ldots,\ x_{\pi n})\ . \qquad (7.13)$$

THEOREM: If $g(\underline{x}) = f(\pi\underline{x} \oplus \underline{v})$, then $G(\underline{s}) = 2^{n/2}\ \phi(\underline{v}, \pi\underline{s})\ F(\pi\underline{s})$.

Proof: By direct evaluation,

$$G(s) = \sum_{\underline{x}} f(\pi\underline{x} \oplus \underline{y})\ \phi(\underline{x}, \underline{s}) = \sum_{\underline{x}} f(\underline{x} \oplus \pi^{-1})\ \phi(\pi^{-1}\underline{x}, \underline{s})$$

$$= \sum_{\underline{x}} f(x)\ \phi(\pi^{-1}\underline{x} \oplus \pi^{-1}\underline{v}, \underline{s})$$

$$= 2^{n/2}\ \phi(\pi^{-1}\underline{v}, \underline{s}) \sum_{\underline{x}} f(\underline{x})\ \phi(\pi^{-1}\underline{x}, \underline{s})$$

$$= 2^{n/2}\ \phi(\underline{v}, \pi\underline{s})\ F(\pi\underline{s})\ , \qquad (7.14)$$

and the theorem is proved.

Let $\mathcal{S}_k$ be the set of distinct permutations σ which map $\underline{u}^k = (1, 1, \ldots, 1, 0, \ldots, 0)$ of k ones onto all vectors of k ones.

$$\mathcal{S}_k = \left\{\sigma : \sigma\,\underline{u}^k \neq \sigma'\,\underline{u}^k \text{ if } \sigma' \neq \sigma\right\}\ . \qquad (7.15)$$

Then f can be expressed in terms of $\mathcal{S}_k$ and $\underline{u}^k$ as follows:

$$f(\underline{x}) = \sum_{k=0}^{n} \sum_{\sigma \in \mathcal{S}_k} F(\sigma\, \underline{u}^k)\, \phi(\sigma\, \underline{u}^k, \underline{x}) \,. \tag{7.16}$$

By the previous theorem, if $g(x) = f(\pi\, \underline{x} \oplus \underline{v})$, then

$$G(\sigma\, \underline{u}^k) = 2^{n/2}\, \phi(\underline{v}, \pi\, \sigma\, \underline{u}^k)\, F(\pi\, \sigma\, \underline{u}^k) \,. \tag{7.17}$$

The importance of this expression lies in the fact that, as Golomb noted[70] for Boolean functions, for each k = 0, 1, ..., n, the sets

$$\left\{2^{n/2}\, \phi(\underline{v}, \pi\, \underline{u}^k)\, F(\pi\, \underline{u}^k)\right\}$$

are invariant under permutations π and complementations $\underline{v}$ of variables. Golomb calls these sets <u>invariants</u> of the logical family $\left\{ f(\pi\, \underline{x} \oplus \underline{v})\right\}$. Ninomiya[71] recognized this in an earlier paper, in which he defined the Boolean functions $\left\{f(\pi\, \underline{x})\right\}$ as <u>congruence classes</u>, and the Boolean functions $\left\{f(\pi\, \underline{x} \oplus \underline{v})\right\}$ as <u>generic</u> classes. A function f which is left unchanged by such operations must be invariant in each of the n classes; stated more precisely, we have the following result.

<u>THEOREM</u>: $f(\underline{x}) = f(\pi\, \underline{x} \oplus \underline{v})$ for all $\underline{x}$ if and only if

$$F(\underline{s}) = 2^{n/2}\, \phi(\underline{v}, \pi\, \underline{s})\, F(\pi\, \underline{s}) \,.$$

<u>COROLLARY</u>: If $f(\underline{x}) = f(\underline{x} \oplus \underline{v})$ for all x, then for each $\underline{s}$, either $F(\underline{s}) = 0$ or else the inner product $(\underline{v}, \underline{s}) = 0 \bmod 2$.

<u>Proof</u>: $f(\underline{x}) = f(\underline{x} \oplus \underline{v})$ implies $F(\underline{s}) = 2^{n/2}\, \phi(\underline{v}, \underline{s})\, F(\underline{s})$. Hence, for each $\underline{s}$, $F(\underline{s})$ must be zero or else $2^{n/2}\, \phi(\underline{v}, \underline{s}) = 1$. The latter result is

possible only when $\prod_{i=1}^{n} (-1)^{s_i v_i} = (-1)^{\sum s_i v_i} = 1$, indicating that $(\underline{s}, \underline{v}) = 0 \bmod 2$.

B. Boolean Functions

Any member f of $\mathcal{V}$ whose values on $\mathcal{X}$ are ±1 we will call a Boolean function. The set of Boolean functions we denote $\mathcal{B}$.

$$\mathcal{B} = \left\{ f: \ f \text{ in } \mathcal{V} \ ; \ |f(\underline{x})| = 1 \text{ for all } \underline{x} \text{ in } \mathcal{X} \right\}. \tag{7.18}$$

In the more usual notation, a Boolean function takes on the values 0 or 1. If we have recourse to such notation, we will denote the function as $\hat{f}$ and relate it to f by

$$f(\underline{x}) = (-1)^{\hat{f}(\underline{x})} . \tag{7.19}$$

THEOREM: $F(\underline{s})$ is the transform of a Boolean function $f(\underline{x})$ if and only if

$$\sum_{\underline{s}} F(\underline{s}) \, F(\underline{s} \oplus \underline{w}) = 2^n \, \delta(\underline{w}, \underline{0}) \ ;$$

that is, if and only if it has norm 2^n and is orthogonal to all of its $\underline{w}$-translates.

Proof: First, f is Boolean if and only if

$$f^2(\underline{x}) = f(\underline{x}) \, f(\underline{x}) = 1 = 2^{n/2} \, \phi(\underline{0}, \underline{x}) . \tag{7.20}$$

By the convolution theorem, the result is immediate:

$$2^{n/2}\ \delta(\underline{0},\ \underline{w})\ =\ 2^{-n/2} \sum F(\underline{s})\ F(\underline{s} \oplus \underline{w})\ . \tag{7.21}$$

THEOREM: If f is a Boolean function

$$-2^{n/2} \le F_{min} \le 2^{-n/2}\ f(0) \le F_{max} \le 2^{n/2}\ .$$

Proof: f is bounded by M = 1.

THEOREM: If f is a Boolean function, then $2^{n/2}\ F(\underline{s})$ is an even integer for all $\underline{s}$.

Proof: Let $\hat{f}$ be the (0,1) Boolean function corresponding to f. We can always express $\hat{f}$ as a modulo 2 sum of products (for example, see Calingaert[72]) which can be reduced, by factoring x from the terms in which it appears, to

$$\hat{f}(\underline{x})\ =\ x_1\ \hat{f}_1(x_2,\ x_3,\ \ldots,\ x_n) \oplus \hat{f}_2(x_2,\ \ldots,\ x_n)\ . \tag{7.22}$$

Now, $F(\underline{s})$ is the transform of $(-1)^{\hat{f}}$, or

$$F(\underline{s})\ =\ 2^{-n/2} \sum_{\underline{x}} (-1)^{x_1\hat{f}_1+\hat{f}_2+s_1x_1+\ldots+s_nx_n}$$

$$=\ 2^{-n/2} \sum_{x_2=0}^{1} \cdots \sum_{x_n=0}^{1} (-1)^{s_2x_2+\ldots+s_nx_n+\hat{f}_2} \left[\sum_{x_1=0}^{1} (-1)^{(s_1+\hat{f}_1)x_1} \right] \tag{7.23}$$

For those $\underline{s}$ with $s_1 \neq \hat{f}_1$, the sum in brackets is zero; and for those with $s_1 = \hat{f}_1$, the term is 2, both even. Hence, $2^{n/2} F(s)$ is a sum of even terms.

In this proof, note that all terms in the sum vanish except those for which $s_1 = \hat{f}_1(x_2, \ldots, x_n)$. Suppose that $\hat{f}_1$ has k_1 ones in its truth-table; then

$$F(\underline{s}) = 2^{1-n/2} \sum_{\substack{x_2,\ldots,x_n \\ \hat{f}_1(x_2,\ldots,x_n)=s_1}} (-1)^{\hat{f}_2+s_2x_2+\ldots+s_nx_n} \qquad (7.24)$$

is a sum of either k_1 or 2^n-k_1 terms, depending on whether s_1 is 1 or 0. This proves the theorem.

COROLLARY: If $\hat{f}_1(x_2,\ldots,x_n)$ has an odd number of ones in its truth-table, then $F(s) \neq 0$ for all $\underline{s}$.

We may combine this with a previous result to obtain the following:

THEOREM: If $\hat{f}_1(x_2, \ldots, x_n)$ has an odd number of ones in its truth-table, and if there exists complementation vector $\underline{v}$ such that $f(\underline{x}) = f(\underline{x} \oplus \underline{v})$ for all $\underline{x}$, then $\underline{v} = \underline{0}$.

Proof: An $\hat{f}_1$ having an odd number of ones implies that $F(\underline{s}) \neq 0$, all $\underline{s}$. Hence, $(\underline{s}, \underline{v}) = 0 \pmod 2$ must apply for all $\underline{s}$, a requirement which can be met only when $\underline{v} = \underline{0}$.

THEOREM: If for some k, $\hat{f}(\underline{x}) = cx_k \oplus \hat{f}_k(x_1,\ldots,x_{k-1},x_{k+1},\ldots,x_n)$, then $F(\underline{s}) = 0$ whenever $s_k = 1 \oplus c$.

Proof:

$$F(\underline{s}) = 2^{-n/2} \left(\sum_{\substack{x_1,\ldots,x_{k-1} \\ x_{k+1},\ldots,x_n}} (-1)^{f_k + s_1 x_1 + \ldots + s_{k-1} x_{k-1} + s_{k+1} x_{k+1} + \ldots + s_n x_n} \right) \left(\sum_{x_2=0}^{1} (-1)^{(c+s_k)x_k} \right) \quad (7.25)$$

This is zero whenever $c + s_k = 1$.

C. Boolean Sequences and the Minimum Acquisition-Time Receiver

In Chapter 2, we introduced the possibility of increasing the desirability of a fixed-complexity receiver by cross-correlating the incoming sequence, call it α, against several component sequences, call them $\xi_1, \xi_2, \ldots, \xi_n$, and decoding the vector of maximal correlations $(m_1, m_2, \ldots, m_n)$ into the phase estimate $\underline{m}$ of α.

To optimize the set of ξ_i, we pick them to have cross-correlation periods v_i which are relatively prime in pairs and each approximately $\sqrt[n]{p}$, where $p = v_1 v_2 \ldots v_n$ is the period of α. The correlations, themselves, $R_{\alpha \xi_i}(m)$, are to have maximum distinguishability.

We have seen in Chapter 4 that the separation of autocorrelation values is always greater than the separation of cross-correlation values. To make cross-correlations as mutually distinguishable as possible, then, we would like for them to appear to be as near to autocorrelations as possible. One may attempt this by defining α as a combination of the ξ_i, hopefully obtaining a highly distinguishable set of cross-correlation functions by proper choice of the combining function. That is, we would like to be able to combine the $\xi_1, \xi_2, \ldots, \xi_n$ in some way to produce α, choosing this function to

maximize the distinguishability. We are dealing with binary sequences, and it is thus natural to use Boolean functions to combine the ξ_i. We will assume that, for an arbitrary Boolean function f,

$$\hat{\alpha} = \hat{f}(\hat{\xi}_1, \hat{\xi}_2, \ldots, \hat{\xi}_n) , \tag{7.26}$$

where the function is applied termwise, as though α were the output of a switching network when the inputs are $\xi_1, \xi_2, \ldots, \xi_n$ (see Figure 7.1).

$$\hat{\alpha}_i = f(\hat{\xi}_{1i}, \hat{\xi}_{2i}, \ldots, \hat{\xi}_{ni}) . \tag{7.27}$$

We assume α and the ξ_i are binary (± 1) sequences so that f is a (± 1) Boolean function, and the $\hat{\alpha}$, $\hat{\xi}_i$, and $\hat{f}$ are defined on (0, 1) accordingly:

$$\begin{aligned} \alpha_i &= (-1)^{\hat{\alpha}_i} \\ \xi_{ij} &= (-1)^{\hat{\xi}_{ij}} \\ f &= (-1)^{\hat{f}} . \end{aligned} \tag{7.28}$$

By using the Kronecker delta we can separate the sequence from the Boolean function much in the same way as we separated the sequence from the modulation in Chapter 1.

$$\alpha = \sum_{\underline{x}} f(\underline{x})\, \delta(\underline{x}, \hat{\underline{\xi}}) . \tag{7.29}$$

The cross-correlation of α with a sequence β, defined by

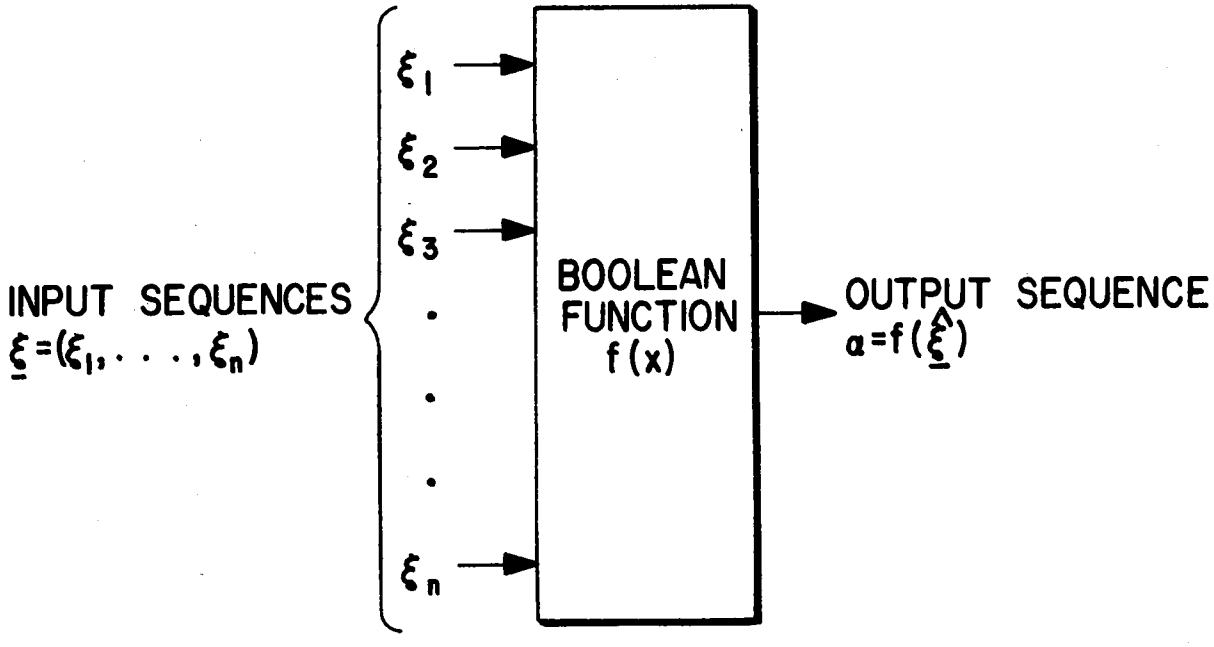

FIGURE 7.1. SEQUENCE GENERATION BY LOGICAL COMBINATION OF COMPONENT SEQUENCES.

$$\beta = \sum_{\underline{x}} g(\underline{x})\ \delta(\underline{x}, \hat{\underline{\xi}}) \ , \tag{7.30}$$

can be easily computed by standard means. Since we assume the v_i are relatively prime in pairs,

$$R_{\alpha\beta}(m) = \sum_{\underline{x}} \sum_{\underline{y}} f(\underline{x})\ g(\underline{y}) \prod_{k=1}^{n} \left[\sum_{i=1}^{v_k} \delta(x_k, \hat{\xi}_{ki})\ \delta(y_k, \hat{\xi}_{k,i+m}) \right]$$

$$= \sum_{\underline{x}} \sum_{\underline{y}} f(\underline{x})\ g(\underline{y}) \prod_{k=1}^{n} r_{x_k y_k}(m) \tag{7.31}$$

where the (<u>un-normalized</u>) cross-correlations of projections are defined as in equation 1.12

$$r_{x_k y_k}(m) = \sum_{i=1}^{v_k} \delta(x_k, \hat{\xi}_{ki})\ \delta(x_k, \hat{\xi}_{k,i+m}) \ . \tag{7.32}$$

At this point, we make use of the Boolean transform.

$$f(\underline{x}) = \sum_{\underline{s}} F(\underline{s})\ \phi(\underline{s}, \underline{x})$$

$$g(\underline{x}) = \sum_{\underline{s}} G(\underline{s})\ \phi(\underline{s}, \underline{x}) \ . \tag{7.33}$$

Direct substitution into $R_{\alpha\beta}(m)$ results in the equation

$$R_{\alpha\beta}(m) = \sum_{\underline{x}} \sum_{\underline{y}} \sum_{\underline{s}} \sum_{\underline{w}} F(\underline{s})\ G(\underline{w})\ \phi(\underline{s}, \underline{x})\ \phi(\underline{w}, \underline{y}) \prod_{j=1}^{n} r_{x_j y_j}(m)$$

$$= \sum_{\underline{s}} \sum_{\underline{w}} F(\underline{s})\ G(\underline{w}) \left[2^{-n} \sum_{\underline{x}} \sum_{\underline{y}} \prod_{j=1}^{n} r_{x_j y_j}(m)\ (-1)^{s_j x_j + w_j y_j} \right]$$

$$R_{\alpha\beta}(m) = \sum_{\underline{s}} \sum_{\underline{w}} F(\underline{s})\, G(\underline{w}) \left[2^{-n} \prod_{j=1}^{n} \left(\sum_{x_j=0}^{1} \sum_{y_j=0}^{1} r_{x_j y_j}(m)\, (-1)^{s_j x_j + w_j y_j} \right) \right] . \tag{7.34}$$

Let us turn our attention, for the moment, to the term in brackets above. The r(m) are correlations of projections $\delta(x_j, \hat{\xi}_j)$, and these projections are related as follows:

$$\delta(0, \hat{\xi}_j) = 1 - \delta(1, \hat{\xi}_j) . \tag{7.35}$$

We can thus reduce all r(m) to terms involving $r_{1_j 1_j}(m)$

$$\begin{aligned} r_{0_j 0_j}(m) &= p_j - 2k_j + r_{1_j 1_j}(m) \\ r_{0_j 1_j}(m) &= k_j - r_{1_j 1_j}(m) = r_{1_j 0_j}(m) \end{aligned} \tag{7.36}$$

where k_j is the number of ones in $\hat{\xi}_j$ per cycle.

On the other hand, $R_{\xi_j}(m)$ also is related to these r(m) in a simple way

$$\begin{aligned} R_{\xi_j}(m) &= r_{0_j 0_j}(m) - r_{0_j 1_j}(m) + r_{1_j 1_j}(m) \\ &= p_j - 4k_j + 4\, r_{1_j 1_j}(m) . \end{aligned} \tag{7.37}$$

When $s_j = w_j = 1$, the term in brackets in 7.34 is thus precisely equal to $R_{\xi_j}(m)$; when $s_j \neq w_j$, this term is $(v_j - 2k_j) = D_j$, the imbalance in ξ_j, and for $s_j = w_j = 0$, the bracket term becomes v_j.

At this point, let us normalize $R_{\alpha\beta}(m)$ to $C_{\alpha\beta}(m)$ and denote the normalized bracket term to be $C(m; \underline{s}, \underline{w})$; if we assume $X^0 = 1$ as a convention, we can write

$$C(m;\ \underline{s},\ \underline{w}) = \frac{1}{p} \prod_{j=1}^{n} D_j^{|s_j - w_j|} \left[R_{\xi_j}(m)\right]^{\delta(s_j,1)\,\delta(w_j,1)}_{v_j}\ \delta(s_j,0)\ \delta(w_j,0)$$

$$= \prod_{j=1}^{n} \left[\frac{D_j}{v_j}\right]^{|s_j - w_j|} \left[C_{\xi_j}(m)\right]^{s_j w_j} . \tag{7.38}$$

The final expression for the normalized cross-correlation between α and β is then

$$C_{\alpha\beta}(m) = 2^{-n} \sum_{\underline{s}} \sum_{\underline{w}} F(\underline{s})\ G(\underline{w})\ C(m;\ \underline{s},\ \underline{w}) . \tag{7.39}$$

This formula is of fundamental importance in finding the minimum acquisition-time receiver. Note that, by using it, one may express the cross-correlation between any two Boolean functions of the ξ_i as a sum of transform coefficients of the two functions weighted by <u>autocorrelation</u> properties of the ξ_i. One thing worthwhile to note about the equation for $C(m;\ \underline{s},\ \underline{w})$ is that when $s_j \neq w_j$,

$$\left|C(m;\ \underline{s},\ \underline{w})\right| \leq \frac{D_j}{v_j} \tag{7.40}$$

and when both $s_j \neq w_j$ and $s_i \neq w_i$,

$$\left|C(m;\ \underline{s},\ \underline{w})\right| \leq \frac{D_j D_i}{v_j v_i} , \text{ etc.} \tag{7.41}$$

From these considerations, when the $\frac{D_j}{v_j}$ are sufficiently small, we may often omit the terms with $\underline{s} \neq \underline{w}$ from the correlation equation.

D. Design of the Minimal Acquisition-Time Receiver

Our original reason for studying Boolean functions was so that we could determine the best function $f(\underline{x})$ to define α.

$$\alpha = f(\hat{\underline{\xi}}) . \tag{7.42}$$

We desire to pick f and the ξ_i, i = 1, 2, ..., n, in such a way that the cross-correlations of α with each ξ_i have maximum distinguishability. By choosing $g(\underline{x}) = (-1)^{x_i}$, we can write ξ_i as

$$\xi_i = g(\hat{\underline{\xi}}) . \tag{7.43}$$

The transform of g is easily computed, for we note that $g(\underline{x}) = 2^{n/2}\, \phi(\underline{x}, \underline{e}^i)$, defining $\underline{e}^i$ to be the ith unit vector

$$\underline{e}^i = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$$

$$e^i_j = \delta(i, j) . \tag{7.44}$$

The transform of g is then

$$G(\underline{s}) = 2^{n/2}\, \delta(\underline{s}, \underline{e}^i) . \tag{7.45}$$

Consequently, the cross-correlation equation reduces to

$$C_{\alpha\xi_i}(m) = 2^{-n/2} \sum_{\underline{s}} F(\underline{s}) \prod_{j=1}^{n} (D_j/v_j)^{|s_j - e^i_j|} \left[C_{\xi_j}(m)\right]^{s_j e^i_j}$$

$$C_{\alpha\,\xi_i}(m) = 2^{-n/2}\left\{\left[\sum_{\underline{s},s_i=1} F(\underline{s}) \prod_{j\neq i} (D_j/v_j)^{s_j}\right] C_{\xi_i}(m) + \left[\sum_{\underline{s},s_i=0} F(\underline{s}) \prod_{j\neq i} (D_j/v_j)^{s_j}\right]\left(\frac{D_i}{v_i}\right)\right\}. \tag{7.46}$$

For any two values m' and m" of m, the difference in correlation values $C_{\alpha\,\xi_i}(m)$ (and specifically, the distinguishability) is dependent separately on the autocorrelation of ξ_i and the Boolean function

$$C_{\alpha\,\xi_i}(m') - C_{\alpha\,\xi_i}(m'') = 2^{-n/2}\left[\sum_{\underline{s},s_i=1} F(\underline{s}) \prod_{j\neq i} \left(\frac{D_j}{p_j}\right)^{s_j}\right]\left[C_{\xi_i}(m') - C_{\xi_i}(m'')\right] \tag{7.47}$$

Our course to optimize the acquisition receiver is now clear; first, each ξ_i is to have minimum out-of-phase autocorrelation values so that $C_{\xi_i}(m)$ has maximum separation, and second, f is to be chosen such that $\left[\sum_{\underline{s},s_i=1} F(\underline{s}) \prod_{j\neq i} (D_j/v_j)^{s_j}\right]$ is maximized -- also for each i. Further, we can always choose the sum to be <u>positive</u> by proper choice of f_i; for suppose the sum were negative. By choosing $g'(\underline{x}) = (-1)^{x_i+1}$, we correlate α against ξ_i', given by

$$\xi_i' = g'(\hat{\underline{\xi}}) = -\xi_i\,, \tag{7.48}$$

and have $C_{\alpha\,\xi_i'}(m) = -C_{\alpha\,\xi_i}(m)$, which has the sum in question positive. By duality, we can thus always complement x_i in $f(\underline{x})$, if need be, to make

$$\sum_{\underline{s},s_i=1} F(\underline{s}) \prod_{j\neq i} (D_j/v_j)^{s_j} > 0 \,. \tag{7.49}$$

If the α received is delayed by m steps, our decoding scheme is also clear: after having found the delays m_i giving maximum cross-correlations of α with each of ξ_i, we declare that m is that integer such that, for each i,

$$m \equiv m_i \text{ modulo } v_i \tag{7.50}$$

which has a unique solution by the "Chinese" remainder theorem[73] of number theory.

Now, consider the sum to be maximized, $\sum_{\underline{s},\, s_i=1} F(\underline{s}) \prod_{j\neq i} (D_j/v_j)^{s_j}$,

One of the terms in the sum is $F(\underline{e}^i)$, but the remainder have products of (D_j/v_j) as factors. Denote

$$\begin{aligned} D'/v' &= \max_{i\neq j} \left\{ |D_j/v_j| \right\} \\ F_M &= \max_{\substack{\underline{s},s_i=1 \\ \underline{s}\neq\underline{e}^i}} \left\{ |F(s)| \right\} \,. \end{aligned} \tag{7.51}$$

Using the triangle inequality, we can bound the sum of remaining terms, call it F, as follows:

$$F = \left| \sum_{\substack{\underline{s},s_i=1 \\ \underline{s}\neq\underline{e}^i}} F(\underline{s}) \prod_{j\neq i} (D_j/v_j)^{s_j} \right| \leq \sum_{\substack{\underline{s},s_i=1 \\ \underline{s}\neq\underline{e}^i}} \left|F(\underline{s})\right| \prod_{j\neq i} \left|D_j/v_j\right|^{s_j}$$

$$|F| \le F_M \sum_{\substack{\underline{s}, s_i = 1 \\ \underline{s} \neq \underline{e}^i}} \prod_{j \neq i} (D'/v')^{s_j}$$

$$\le F_M \left[\sum_{k=0}^{n-1} \binom{n-1}{k} (D'/v')^k - 1 \right] . \tag{7.52}$$

The binomial theorem can be applied to the inequality to give

$$\left| \sum_{\substack{\underline{s}, s_i = 1 \\ \underline{s} \neq \underline{e}^i}} F(\underline{s}) \prod_{j \neq i} (D_j/v_j) \right| \le F_M \left[(1 + (D'/v'))^{n-1} - 1 \right] \tag{7.53}$$

Note that when D'/v' is small, this upper bound can be replaced by $F_M\, n(D'/v')$.

$$|F| \le n\, F_M(D'/v') . \tag{7.54}$$

We recognize that by using nearly balanced sequences for the ξ_i (which we want to do to optimize distinguishability), it is highly efficient to maximize $F(\underline{e}^i)$ by proper choice of $f(\underline{x})$. In fact, any time that $n\, D'/v' < 1$, this is the course we must follow to insure the largest possible $F(\underline{e}^i) \div F$.

The best logical function $f(\underline{x})$ is therefore one whose transform $F(\underline{s})$ has $F(\underline{e}^i)$ as large as possible, for each i. In order not to present bias to any component, we may restrict

$$F(\underline{e}^i) = F(\underline{e}^j), \text{ all } j = 1, 2, \ldots, n, \tag{7.55}$$

and maximize $F(\underline{e}^1)$ by proper choice of f.

E. The Maximality of Majority Logic

We are now is a position to prove that the Boolean function which minimizes acquisition time is the majority function.

THEOREM: Let $\hat{f}(\underline{x})$ be the (0, 1) Boolean function of n binary (0, 1) variables associated with a (±1) Boolean function f(x) chosen such that, among the transform values $F(\underline{s})$, $F(\underline{e}^i) = F(\underline{e}^1)$ for all i, and $F(\underline{e}^1)$ is maximum over all such Boolean functions. Then if n is odd, $\hat{f}(\underline{x}) = 1$ if and only if $\underline{x} = (x_1, x_2, \ldots, x_n)$ has a majority of its variables equal to 1 and is unique; if n is even, f is not unique, but necessarily $\hat{f}(\underline{x}) = 1$ whenever $\underline{x}$ has a strict majority of ones; and $\hat{f}(\underline{x}) = 0$ when $\underline{x}$ has a strict majority of zeros.

Proof: Define $\mathcal{X}_{k1} = \left\{\underline{x} = (x_1, \ldots, x_n) : \hat{f}(\underline{x}) = 1, x_k = 1\right\}$, and $\mathcal{X}_{k0} = \left\{\underline{x} : \hat{f}(\underline{x}) = 1, x_k = 0\right\}$. Then $\mathcal{X}_{k1} \cup \mathcal{X}_{k0} = \mathcal{X}_1$ is the set of all $\underline{x}$ on which $\hat{f}$ takes the value 1. Let $\left|\mathcal{X}_1\right|$ denote the number of elements in $\mathcal{X}_1$. Similarly, let $\mathcal{Y}_{k1} = \left\{\underline{x} : \hat{f}(\underline{x}) = 0, x_k = 1\right\}$, $\mathcal{Y}_0 = \mathcal{X}_1^c$, and $\mathcal{Y}_{k0} = \mathcal{Y}_0 - \mathcal{Y}_{k1}$.

$$F(\underline{e}^i) = 2^{-n/2} \sum_{\underline{x}} f(\underline{x}) (-1)^{x_i}$$

$$= 2^{-n/2} \left[\left| \mathcal{X}_{i1} \right| - \left| \mathcal{X}_{i0} \right| + \left| \mathcal{Y}_{i0} \right| - \left| \mathcal{Y}_{i1} \right| \right] . \quad (7.56)$$

Let $\delta_{kl}(\underline{x})$ be the characteristic function of $\mathcal{X}_{kl}$:

$$\delta_{kl}(\underline{x}) = \begin{cases} 1 \text{ if } \underline{x} \text{ is in } \mathcal{X}_{kl} \\ 0 \text{ otherwise} , \end{cases} \quad (7.57)$$

and similarly, $\delta_{k0}(\underline{x})$ for $\mathcal{X}_{k0}$, $\delta'_{kl}(\underline{x})$ for $\mathcal{Y}_{kl}$ and $\delta'_{k0}(\underline{x})$ for $\mathcal{Y}_{k0}$. Since all $F(\underline{e}^i)$ are equal,

$$F(\underline{e}^i) = \frac{1}{n} \sum_{i=1}^{n} F(\underline{e}^i)$$

$$= \frac{1}{n} \sum_{i=1}^{n} \sum_{\underline{x}} \left[\delta_{i1}(\underline{x}) + \delta'_{i0}(\underline{x}) - \delta_{i0}(x) - \delta'_{i1}(x) \right] \quad (7.58)$$

But $\sum_{k} \delta_{kl}(\underline{x})$ is the number of different $\mathcal{X}_{kl}$ to which $\underline{x}$ belongs; when $\underline{x}$ belongs to $\mathcal{X}_1$, this sum is the number of times $x_k = 1$, *i.e.*, the number of ones in $\underline{x}$, which we denote by $\left\| \underline{x} \right\|$. If $\underline{x}$ is not in $\mathcal{X}_1$, this sum is, of course, zero. Similar results also apply to the other summands.

$$\frac{1}{n} \sum_{\underline{x}} \sum_{i=1}^{n} \delta_{i1}(\underline{x}) = \frac{1}{n} \sum_{\underline{x} \text{ in } \mathcal{X}_1} \left\| \underline{x} \right\| . \quad (7.59)$$

Similarly, for χ_{10},

$$\frac{1}{n} \sum_{\underline{x}} \sum_{i=1}^{n} \delta_{i0}(\underline{x}) = \frac{1}{n} \sum_{\underline{x} \text{ in } \chi_1} (n - \|\underline{x}\|) . \tag{7.60}$$

Inserting these into the expression for $F(\underline{e}^1)$,

$$F(\underline{e}^1) = 2^{-n/2}\left(\frac{1}{n}\right) \left\{ \sum_{\underline{x} \text{ in } \chi_1} \left[2\|\underline{x}\| - n\right] + \sum_{\underline{x} \text{ in } \gamma_{10}} \left[n - 2\|\underline{x}\|\right] \right\}. \tag{7.61}$$

In order to maximize $F(\underline{e}^1)$, it is necessary to include in χ_1 every $\underline{x}$ such that

$$\|\underline{x}\| > \frac{n}{2} \tag{7.62}$$

and exclude from χ_1 all elements $\underline{x}$ such that

$$\|\underline{x}\| < \frac{n}{2} . \tag{7.63}$$

Hence $\hat{f}$ takes on the value 0 or 1 depending on whether the strict majority of its variables are 0 or 1. When n is odd, this makes $\hat{f}$ unique. For even n, those $\underline{x}$ with $\|\underline{x}\| = n/2$ may be either excluded or included in χ_1 without changing $F(\underline{e}^i)$.

To calculate $F(\underline{e}^i)$, merely evaluate $|\chi_{k1}|$, $|\chi_{k0}|$, $|\gamma_{k0}|$ and $|\gamma_{k1}|$: Denote by $[h]$ the integer part of h. Then

$$|\gamma_{k0}| = |\chi_{kl}| = \frac{1}{n} \sum_{m=0}^{\left[\frac{n}{2}\right]} (n-m) \binom{n}{m} = \sum_{m=0}^{\left[\frac{n}{2}\right]} \binom{n-1}{m}$$

$$|\gamma_{kl}| = |\chi_{k0}| = \frac{1}{n} \sum_{m=0}^{\left[\frac{n}{2}\right]} m\binom{n}{m} = \sum_{m=0}^{\left[\frac{n}{2}\right]-1} \binom{n-1}{m} . \qquad (7.64)$$

As a result, the maximum value of $F(\underline{e}^i)$ is

$$F(\underline{e}^i) = 2^{1-n/2} \binom{n-1}{\left[\frac{n}{2}\right]} . \qquad (7.65)$$

F. Calculation of the Majority-Logic Transform

Let n be odd and let f be the unique majority logic of the previous section. We need consider only odd n, because if n were even,

$$\frac{F_n(\underline{e}^1)}{F_{n+1}(\underline{e}^1)} = \frac{2^{1-n/2} \binom{n-1}{\frac{n}{2}}}{2^{1-n/2-\frac{1}{2}} \binom{n}{\frac{n}{2}}} = 2^{-\frac{1}{2}} < 1 .$$

We could thus increase n by one to improve the correlation, thereby decreasing the correlation time, and also to decrease the ratio $\frac{\sum v_i}{\pi v_i}$.

We wish to calculate the transform of f(x). Because f is a symmetric function, if $\underline{s}$ has k ones (i.e., $\|\underline{s}\| = k$), then for some permutation π

$$F(\underline{s}) = F(\pi \underline{u}^k) = F(\underline{u}^k) , \qquad (7.66)$$

and by this symmetry of f, we need to calculate only these $F(\underline{u}^k)$.

$$F(\underline{u}^k) = 2^{-n/2} \sum_{\underline{x}} (-1)^{x_1+\ldots+x_k} f(\underline{x})$$

$$= 2^{-n/2} \left[\sum_{\underline{x},\ \|\underline{x}\|<\frac{n}{2}} (-1)^{x_1+\ldots+x_k} - \sum_{\underline{x},\ \|\underline{x}\|>\frac{n}{2}} (-1)^{x_1+\ldots+x_k} \right] \tag{7.77}$$

Define the two sums above as

$$A(k) = \sum_{\underline{x},\ \|\underline{x}\|<\frac{n}{2}} (-1)^{x_1+\ldots+x_k}$$

$$B(k) = \sum_{\underline{x},\ \|\underline{x}\|>\frac{n}{2}} (-1)^{x_1+\ldots+x_k} . \tag{7.78}$$

Suppose that a vector $\underline{x}$ has i ones in it, j of which lie in $x_1, \ldots, x_k$, and i-j in $x_{k+1}, \ldots, x_n$. There are $\binom{k}{j}\binom{n-k}{i-j}$ such vectors $\underline{x}$, and thus

$$A(k) = \sum_{i=0}^{\frac{n-1}{2}} \sum_{j=0}^{\min(k,i)} \binom{k}{j}\binom{n-k}{i-j}(-1)^j$$

$$= \sum_{i=0}^{\frac{n-1}{2}} \sum_{j=0}^{\infty} \binom{k}{j}\binom{n-k}{i-j}(-1)^j . \tag{7.79}$$

By similar reasoning,

$$B(k) = \sum_{i=\frac{n+1}{2}}^{n} \sum_{j=0}^{\infty} \binom{k}{j}\binom{n-k}{i-j}(-1)^j . \tag{7.80}$$

Let $a(t)$ be the generating function

$$a(t) = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \binom{k}{j}\binom{n-k}{i-j}(-1)^j t^i$$

$$= \sum_{j=0}^{\infty} \binom{k}{j}(-1)^j t^j \sum_{i=0}^{\infty} \binom{n-k}{i-j} t^{i-j}$$

$$= \sum_{j=0}^{\infty} \binom{k}{j}(-1t)^j \sum_{m=0}^{\infty} \binom{n-k}{m} t^m$$

$$= (1-t)^k (1+t)^{n-k} . \qquad (7.81)$$

Note that the sum of the coefficients of $t^0, t^1, \ldots, t^{\frac{n-1}{2}}$ is precisely A(k); that is,

$$\begin{aligned} A(k) &= \text{coeff. of } t^{\frac{n-1}{2}} \text{ in } (1-t)^k (1+t)^{n-k} (1+t+\ldots+t^{\frac{n-1}{2}}) \\ &= \text{coeff. of } t^{\frac{n-1}{2}} \text{ in } (1-t)^{k-1} (1+t)^{n-k} (1-t^{\frac{n+1}{2}}) \\ &= \text{coeff. of } t^{\frac{n-1}{2}} \text{ in } (1-t)^{k-1} (1+t)^{n-k} \\ &= \text{coeff. of } t^{n-1} \text{ in } (1-t^2)^{k-1} (1+t^2)^{n-k} \\ &= \text{coeff. of } t^{-1} \text{ in } \frac{(1-t^2)^{k-1} (1+t^2)^{n-k}}{t^n} . \end{aligned} \qquad (7.82)$$

By this procedure, we reduce A(k) to the residue of a rational function, to be calculated by the Cauchy residue theorem[74]:

$$A(k) = \frac{1}{2\,j} \oint \frac{(1-t^2)^{k-1} (1+t^2)^{n-k}}{t^n} \, dt, \qquad (7.83)$$

$$(j = \sqrt{-1})$$

integrating along any simple closed path containing the origin.

$$A(k) = \frac{1}{2\pi j} \oint \left(\frac{1}{t} - t\right)^{k-1} \left(\frac{1}{t} + t\right)^{n-k} \frac{dt}{t} . \tag{7.84}$$

Choose the integration path to be unit circle, $t = e^{jz}$.

$$A(k) = \frac{2^{n-2}(-j)^{k-1}}{\pi} \int_0^{2\pi} \sin^{k-1} z \cos^{n-k} z \, dz . \tag{7.85}$$

Because A(k) must be real, we may limit our attention to the real part of the equation (i.e., to odd k). This integral is one which can be reduced by a standard table of integrals (see Burrington[75], for example) to

$$A(k) = \mathrm{Re}\left\{ (-j)^{k-1} \frac{(k-1)!\left(\frac{n-k}{2}\right)!}{\left(\frac{n-1}{2}\right)!\left(\frac{k-1}{2}\right)!} \binom{n-k}{\frac{n-k}{2}} \right\} . \tag{7.86}$$

By a similar procedure, or by invoking symmetry of the majority function, we compute

$$B(k) = -A(k) . \tag{7.87}$$

The final result for $F(\underline{s})$ is, then

$$F(\underline{u}^k) = 2^{1-n/2} \, \mathrm{Re}\left\{ (-j)^{k-1} \frac{(k-1)!\left(\frac{n-k}{2}\right)!}{\left(\frac{n-1}{2}\right)!\left(\frac{k-1}{2}\right)!} \binom{n-k}{\frac{n-k}{2}} \right\} \tag{7.88}$$

which, for k = 1, gives the result obtained previously for $F(\underline{e}^1)$:

$$F(\underline{e}^1) = 2^{1-n/2} \binom{n-1}{\frac{n-1}{2}} . \tag{7.89}$$

As a function of odd k, $|F(\underline{u}^k)|$ is decreasing for $k < \frac{n-1}{2}$ and increasing for $k > \frac{n-1}{2}$, as shown by

$$\left| \frac{F(\underline{u}^k)}{F(\underline{u}^{k+2})} \right| = \frac{(k-1)!(\frac{n-k}{2})!}{(\frac{n-1}{2})!(\frac{k-1}{2})!} \binom{n-k}{\frac{n-k}{2}} \frac{(\frac{n-1}{2})!(\frac{k-1}{2}+1)!}{(k+1)!(\frac{n-k}{2}-1)!} \binom{n-k-2}{\frac{n-k}{2}+1}^{-1}$$

$$= \frac{n-k-1}{k} \quad . \tag{7.90}$$

A certain symmetry is also present in the fact that $|F(\underline{u}^k)| = |F(\underline{u}^{n-k+1})|$.

G. Optimizing the Value of n

Now, let us go back and compute the coefficients of $C\,\xi_i(m)$ in $C_\alpha \xi_i(m)$ more closely; this coefficient is $F(\underline{e}^i) + F$ where

$$F = \sum_{\substack{\underline{s}, s_i = 1 \\ \underline{s} \neq \underline{e}^i}} F(s) \prod_{j \neq i} (D_j/v_j)^{s_j} \quad . \tag{7.91}$$

Again, by the triangle inequality and symmetry

$$|F| \leq \sum_{\substack{\underline{s}, s_1 = 1 \\ \underline{s} \neq \underline{e}^1}} |F(s)| \left| \prod_{j \neq 1} (D'/p')^{s_j} \right|$$

$$\leq \sum_{k=3}^{n} \binom{n-1}{k-1} |F(\underline{u}^k)| \, (D'/p')^{k-1} \quad . \tag{7.92}$$

The first term in the bound is

$$\binom{n-1}{2} \left|F(\underline{e}^2)\right| (D'/v')^2 = \frac{3}{2} \left|F(\underline{e}^1)\right| \frac{(n-1)(n-2)}{(n-4)} (D'/v')^2 . \tag{7.93}$$

The next terms involve quantities $(D'/v')^{k-1}$ with $k \geq 5$, which we can safely omit. Hence, if

$$D'/v' << \sqrt{\frac{2}{3}\left(\frac{1}{n-1}\right)} < \sqrt{\frac{2}{3}\left(\frac{n-4}{(n-1)(n-2)}\right)} , \tag{7.94}$$

we may assume that the coefficient of $C_{\xi_i}(m)$ in $C_{\alpha\xi_i}(m)$ is merely $2^{-n/2} F(\underline{e}^i)$.

Into the expression for T'/T in Chapter 2, we insert the distinguishability for the cross-correlations $C_{\alpha\xi_i}(m)$ and the distinguishability of $C_{\alpha'}$ if α' were an optimal sequence. Whenever the v_i are much larger than unity, both $\Delta C_{\alpha\xi_i}$ and $\Delta C_{\alpha'}$ are approximately one. Hence,

$$\frac{T'}{T} = \left[2^{1-n} \binom{n-1}{\frac{n-1}{2}} \right]^{-2} . \tag{7.95}$$

The acquisition ratio to be minimized is, then, approximately given by

$$\frac{T'_{acq}(n)}{T_{acq}} \approx n\, p^{\frac{1-n}{n}} \left[2^{1-n} \binom{n-1}{\frac{n-1}{2}} \right]^{-2} . \tag{7.96}$$

For any given p, there is some n which minimizes this ratio. As an indication of the behavior, we approximate the binomial coefficient using Sterling's formula[76].

$$k! \approx (2\pi)^{\frac{1}{2}}\, k^{k+\frac{1}{2}}\, e^{-k} . \tag{7.97}$$

When this is done,

$$\binom{n-1}{\frac{n-1}{2}} = 2^{n-1} \left(\frac{\pi}{2} (n-1) \right)^{-\frac{1}{2}}, \tag{7.98}$$

reducing the approximate acquisition ratio to

$$\frac{T'_{acq}}{T_{acq}} = \left(\frac{\pi}{2p} \right) n(n-1) \; p^{1/n} . \tag{7.99}$$

To find the optimum value of n, take the derivative of T'_{acq}/T_{acq}:

$$\frac{d(T'_{acq}/T_{acq})}{dn} = \left(\frac{\pi}{2p} \right) \left(\frac{p^{1/n}}{n} \right) \left[2n^2 - n - (n-1) \ln p \right] \tag{7.100}$$

This goes to zero only when the term in brackets is zero; this occurs at those values of n, such that

$$\ln p = \frac{(2n-1)n}{n-1}$$

$$p = e^{\frac{n(2n-1)}{n-1}}$$

$$v_i \approx \sqrt[n]{p} = e^2 \; e^{\frac{1}{n+1}} . \tag{7.101}$$

Upon insertion of this value into the acquisition ratio, we find the optimal ratio:

$$\left(\frac{T'_{acq}}{T_{acq}} \right)_{opt} \approx \frac{n\left(\frac{e}{4} \right) \left((2/e)^2 \right)^n}{\binom{n-1}{\left[\frac{n}{2}\right]}^2}$$

$$\frac{\pi}{2} \; n(n-1) \; e^{-2n+1} . \tag{7.102}$$

This ratio above is tabulated in Table 7.1. Note that the ratio is less than unity, and hence the minimal acquisition-time receiver is better than matched filters.

Hence, the minimal acquisition-time receiver would, ideally, given an α-period p, combine n optimal binary sequences with

$$p \approx e^{\frac{n(2n-1)}{n-1}}, \tag{7.103}$$

using component sequences ξ_i of periods v_i relatively prime in pairs and near to $v_i \approx 9$.

TABLE 7.1

Optimal Acquisition Ratio
and Periods for Given n
Single Correlator Case

n	p	$\left(\frac{T'_{acq}}{T_{acq}}\right)$
1	any	1.0×10^{0}
3	1.8×10^{3}	8.1×10^{-2}
5	7.6×10^{4}	4.4×10^{-3}
7	3.8×10^{6}	2.4×10^{-5}
9	2.0×10^{8}	5.0×10^{-6}
11	1.0×10^{10}	1.4×10^{-8}
13	5.7×10^{11}	3.5×10^{-9}
15	3.1×10^{13}	8.7×10^{-11}
17	1.6×10^{15}	2.1×10^{-12}
19	9.1×10^{16}	4.7×10^{-14}

H. Modified Component-Correlator Receivers

Suppose, as a third alternative, we are willing to make a receiver which has one correlator for each of the components ξ_i of α. What is the best receiver? Just as in the constant-equipment case, we define an acquisition ratio:

$$\frac{T'_{acq}}{T_{acq}} = \frac{\text{time for n-component acquisition}}{\text{time for 1-component acquisition}} . \tag{7.104}$$

The time for a 1-component code α to be acquired is merely its period p times the integration time T per phase, or pT. On the other hand, with n correlators working simultaneously, the time to acquire is the new integration time per step T' times the number of phases, or $\max_i \{v_i\} T'$,

$$\frac{T'_{acq}}{T_{acq}} = \frac{\max \{v_i\}}{[v_1, v_2, \ldots, v_n]} \frac{T'}{T} . \tag{7.105}$$

To minimize this ratio, we may argue as before: the v_i must be relatively prime for if they were not, we could pick a relatively prime set with the same least common multiple but having a smaller maximum component. Next, to further minimize the ratio, we want to make $(v_i)_{max}$ as close to the average v_i as possible

$$(v_i)_{max} \approx \frac{v_1 + \ldots + v_n}{n} . \tag{7.106}$$

The best acquisition ratio is thus given by

$$\frac{T'_{acq}}{T_{acq}} = \frac{v_1 + \cdots + v_n}{n\, v_1 v_2 \cdots v_n} \cdot \frac{T'}{T} \quad . \tag{7.107}$$

This equation is exactly the same form as that for the minimum-equipment receiver described previously, except for a factor of $\frac{1}{n}$. The same technique for obtaining α from the components ξ_i (which must be optimum binary sequences) must be applied in both cases; that is, $\hat{\alpha} = \text{maj}(\hat{\xi})$. Further,

$$v_i \approx \sqrt[n]{p} \quad . \tag{7.108}$$

With a majority logic, optimum components, and $v_i \approx \sqrt[n]{p}$, the acquisition ratio is approximately $\frac{1}{n}$ times that found in Section E.

$$\frac{T'_{acq}}{T_{acq}} \approx p^{-1+1/n} \left[2^{-n+1} \binom{n-1}{\frac{n-1}{2}} \right]^{-2} \tag{7.109}$$

Upon setting the derivative of this ratio to zero, we find

$$p = e^{\frac{n^2}{n-1}}$$

$$v_i \approx e^{\frac{n}{n-1}} \approx e$$

$$\frac{T'_{acq}}{T_{acq}} \approx \frac{2^{2n}}{4e^n \binom{n-1}{\left[\frac{n}{2}\right]}^2}$$

$$\approx \frac{\pi}{2} (n-1)\, e^{-n} \quad . \tag{7.110}$$

This is tabulated in Table 7.2. Although if each v_i were about $3(\approx e)$ in length, the analysis above, based upon the assumptions that the D_i/v_i are small and n is large, may not be strictly valid, because the relative prime condition on $\{v_i\}$ may carry $(v_i)_{max}$ far from e. But the analysis is indicative of the action to be taken in the design of such a receiver: after an approximate choice of p, choose n such that

$$p = e^{\frac{n^2}{(n-1)}} . \tag{7.111}$$

Having this n, choose n relatively prime optimal components ξ_i whose periods are as <u>small</u> (but not greater than one) as possible. Then modify the choice of p to

$$p = v_1 v_2 \cdots v_n . \tag{7.112}$$

The approximations certainly establish a lower bound on the acquisition ratio, in any case, since optimal conditions were assumed at all times.

TABLE 7.2

Optimal Acquisition Ratio
and Periods for Given n
n-correlator case

n	p	$\left(\frac{T'_{acq}}{T_{acq}}\right)$
1	any	1.0×10^{0}
3	9.0×10	2.0×10^{-1}
5	5.2×10^{2}	4.8×10^{-2}
7	3.5×10^{3}	9.3×10^{-3}
9	2.5×10^{4}	1.7×10^{-3}
11	1.8×10^{5}	2.8×10^{-4}
13	1.3×10^{6}	4.4×10^{-5}
15	9.5×10^{6}	7.0×10^{-6}
17	7.0×10^{7}	1.1×10^{-6}
19	5.1×10^{8}	1.6×10^{-7}

APPENDIX OF MINIMAX SEQUENCES

This appendix lists the known optimal and minimax sequences up to length 63 and their corresponding correlation functions. In the tables, "+" stands for +1 and "-" stands for -1. The number at the top is the period, and both the sequences α_m and its correlation function $R_\alpha(m)$ are listed, starting with m = 1:

p	
sgn α_1	$R_\alpha(1)$
sgn α_2	$R_\alpha(2)$
.	.
.	.
.	.
sgn α_p	$R_\alpha(p)$.

Only the best sequence found for each specified period is given, and the method used to find it is also given. There is a minimax sequence for every period from 3 to 63 listed, except for p = 40, 48, 52 and 56, all of which are divisible by 4. Note that in some cases (e.g., p = 13), there exist more than one type of optimal sequence.

In the comments to the side, s refers to the 2sth loss function about r(m) = -2 first used to find the sequence, D the absolute value of the imbalance and N the number of out-of-phase maxima. All sequences are minimal loss for each of the criteria s = 1, 2 and 4, and maximum correlation of Chapter 5.

APPENDIX (continued)

Table A.1
SUMMARY OF
MINIMAX SEQUENCES

p	R_M	R_{min}	D	N	Number Levels	Method
3	-1	-1	1	0	2	l.s.r (opt)
4	0	-4	0	2	3	2 ⊠ 2 (opt)
5	1	-3	1	2	3	q.r (opt)
6	2	-2	0	1	3	3 ⊠ 2 (opt)
7	-1	-1	1	0	2	l.s.r. (opt)
8	0	-4	0	5	3	s = 1 (opt)
9	1	-3	1	4	3	s = 1 (opt)
10	2	-2	0	4	3	s = 1 (opt)
11	-1	-1	1	0	2	q.r. (opt)
12	0	-4	0	8	3	s = 1 (opt)
13	1	-3	1	6	3	s = 1 (opt)
14	2	-2	2	4	3	s = 1 (opt)
15	-1	-1	1	0	2	l.s.r (opt)
16	0	-4	0	11	3	s = 1 (opt)
17	1	-3	1	8	3	s = 1 (opt)
18	2	-2	0	4	3	s = 1 (opt)
19	-1	-1	1	0	2	q.r. (opt)
20	0	-4	0	14	3	s = 1 (opt)
21	1	-3	1	10	3	s = 1 (opt)
22	2	-2	0	5	3	s = 1 (opt)

APPENDIX (continued)

p	R_M	R_{min}	D	N	Number Levels	Method
23	-1	-1	1	0	2	q.r. (opt)
24	0	-4	4	21	3	s = 1 (opt?)
25	1	-3	1	12	3	s = 1 (opt)
26	2	-2	0	6	3	s = 1 (opt)
27	3	-5	1	2	4	s = 1 (opt)
28	0	-4	2	21	3	4 * 7 (opt?)
29	1	-3	1	14	3	q.r. (opt)
30	2	-2	2	8	3	s = 4 (opt?)
31	-1	-1	1	0	2	l.s.r. (opt)
32	0	-8	0	24	4	s = 1 (opt?)
33	1	-3	3	18	3	s = 2 (opt?)
34	2	-6	0	10	4	s = 4
35	-1	-1	1	0	2	Jacobi (opt)
36	0	-4	4	27	3	backtrack (opt?)
37	1	-3	1	18	3	s = 1 (opt)
38	2	-6	0	11	4	s = 4
39	3	-5	3	6	4	s = 2
40						
41	1	-3	1	20	3	q.r. (opt)
42	2	-6	0	14	4	s = 4
43	-1	-1	1	0	2	q.r. (opt)
44	0	-4	3	33	3	11 * 4 (opt?)
45	1	-7	1	24	4	s = 4

APPENDIX (continued)

p	R_M	R_{min}	D	N	Number Levels	Method
46	2	-6	2	18	4	s = 2
47	-1	-1	1	0	2	q.r. (opt)
48						
49	1	-7	1	36	3	7 ⊠ 7
50	2	-6	2	16	4	s = 4
51	3	-5	3	12	4	s = 2
52						
53	1	-3	1	26	3	q.r. (opt)
54	2	-6	4	21	4	s = 2
55	3	-5	5	10	4	Jacobi (opt?)
56						
57	1	-19	1	36	4	19 ⊠ 3
58	2	-6	0	20	4	s = 4
59	-1	-1	1	0	2	q.r. (opt)
60	0	-4	2	45	3	15 * 4 (opt?)
61	1	-3	1	30	3	q.r. (opt)
62	2	-6	0	25	4	s = 4
63	-1	-1	1	0	2	l.s.r. (opt)

APPENDIX (continued)

Table A.2

TABULATED MINIMAX SEQUENCES

	3	D = 1, N = 0, 2-level, minimax.
+	-1	optimal
-	-1	(linear shift register)
-	3	
	4	D = 0, N = 2, 3-level, minimax.
+	0	optimal
-	-4	(2 ⊠ 2)
-	0	
+	4	
	5	D = 1, N = 2, 3-level, minimax.
+	1	optimal
-	-3	(quadratic residue)
-	-3	
+	1	
+	5	
	6	D = 0, N = 1, 3-level, minimax.
+	-2	optimal
-	-2	(3 ⊠ 2)
-	2	
+	-2	
-	-2	
+	6	
	7	D = 1, N = 0, 2-level, minimax.
+	-1	optimal
-	-1	(linear shift register)
-	-1	
+	-1	
-	-1	
+	-1	
+	7	

APPENDIX (continued)

8 s = 1, D = 1, N = 0, 3-level, minimax

-	0
-	0
-	-4
+	0
-	-4
+	0
+	0
+	8

optimal

9 s = 1, D = 1, N = 4, 3-level, minimax.

-	1
-	1
-	-3
+	-3
-	-3
+	-3
+	1
+	1
+	9

optimal

10 s = 1, D = 1, N = 4, 3-level, minimax

-	2
-	-2
-	-2
+	-2
-	-2
-	-2
+	-2
+	-2
+	2
+	10

optimal

11 s = 1, D = 1, N = 0, 2-level, minimax.

-	-1
-	-1
-	-1
+	-1
-	-1
-	-1
+	-1
-	-1
+	-1
+	-1
+	11

optimal
(quadratic residue)

APPENDIX (continued)

	12	s = 1, D = 0, N = 8, 3-level, minimax.
−	0	optimal
−	0	
−	0	
+	-4	
−	0	
−	-4	
+	0	
−	-4	
+	0	
+	0	
+	0	
+	12	
	13	s = 1, D = 1, N = 6, 3-level, minimax.
−	1	optimal
−	1	(<u>not</u> quadratic residue sequence)
−	1	
+	-3	
−	-3	
−	-3	
+	-3	
−	-3	
+	-3	
+	1	
+	1	
+	1	
+	13	
	14	s = 1, D = 2, N = 4, 3-level, minimax.
+	-2	optimal
+	2	(exhaustive search showed no balanced 3-level sequence)
−	-2	
+	-2	
+	2	
−	-2	
+	-2	
−	-2	
+	2	
−	-2	
−	-2	
−	2	
+	-2	
+	14	

APPENDIX (continued)

	15	D = 1, N = 0, 2-level, minimax.
-	-1	optimal
-	-1	(linear sequence)
-	-1	
+	-1	
-	-1	
-	-1	
+	-1	
+	-1	
-	-1	
+	-1	
-	-1	
+	-1	
+	-1	
+	-1	
+	15	
	16	s = 1, D = 0, N = 11, 3-level, minimax.
-	0	optimum
-	0	
-	0	
+	-4	
-	0	
-	0	
+	-4	
+	0	
-	-4	
+	0	
-	0	
+	-4	
+	0	
+	0	
+	0	
-	16	

APPENDIX (continued)

17 s = 1, D = 1, N = 8, 3-level, minimax.

-	-3
-	1
-	1
+	1
-	-3
-	-3
+	1
+	-3
-	-3
+	1
-	-3
+	-3
+	1
+	1
+	1
-	-3
+	17

optimal

(not quadratic residue)

18 s = 1, D = 0, N = 4, 3-level, minimax

-	2
-	-2
+	-2
+	-2
-	-2
-	-2
+	2
+	-2
-	-2
+	-2
-	2
+	-2
+	-2
+	-2
+	-2
-	-2
-	2
-	18

optimal

APPENDIX (continued)

	19	s = 1, D = 1, N = 0, 2-level, minimax.
-	-1	optimal
-	-1	(quadratic residue)
-	-1	
-	-1	
+	-1	
-	-1	
+	-1	
-	-1	
+	-1	
+	-1	
+	-1	
+	-1	
-	-1	
-	-1	
+	-1	
-	-1	
-	-1	
+	-1	
+	19	
	20	s = 1, D = 0, N = 14, 3-level, minimax.
-	0	optimal
-	0	
-	0	
-	0	
-	-4	
+	0	
+	0	
-	-4	
+	0	
-	-4	
-	0	
+	-4	
+	0	
+	0	
-	-4	
+	0	
+	0	
+	0	
-	0	
+	20	

APPENDIX (continued)

21 s = 1, D = 1, N = 10, 3-level, minimax.

-	-3	optimal
-	1	
-	1	
-	-3	
-	-3	
+	-3	
+	1	
-	-3	
+	1	
-	1	
-	1	
+	1	
-	-3	
+	1	
-	-3	
+	-3	
+	-3	
+	1	
-	1	
+	-3	
+	21	

22 s = 1, D = 0, N = 5, 3-level, minimax.

-	-2	optimal
-	2	
-	-2	
-	-2	
-	-2	
+	-2	
+	-2	
-	2	
+	-2	
-	-2	
-	2	
+	-2	
-	-2	
+	2	
-	-2	
+	-2	
+	-2	
+	-2	
-	-2	
+	2	
+	-2	
+	22	

APPENDIX (continued)

	23	s = 2, D = 1, N = 0, 2-level, minimax.
-	-1	optimal
-	-1	(quadratic residue)
+	-1	
+	-1	
-	-1	
-	-1	
+	-1	
+	-1	
-	-1	
+	-1	
-	-1	
+	-1	
+	-1	
+	-1	
+	-1	
-	-1	
-	-1	
-	-1	
-	-1	
-	-1	
+	-1	
-	-1	
+	23	
	24	s = 1, D = 4, N = 21, 3-level, minimax.
-	0	optimal (?)
-	0	
+	0	
-	0	
-	0	
-	0	
+	0	
+	0	
+	0	
+	-4	
-	0	
+	0	
+	0	
+	-4	
+	0	
+	0	
-	0	
-	0	
+	0	
-	0	
+	0	
-	0	
+	0	
+	24	

APPENDIX (continued)

25 s = 1, D = 1, N = 12, 3-level, minimax.

-	-3	optimal	
-	-3		
+	1		
+	1		
-	1		
-	-3		
-	-3		
+	1		
-	1		
+	-3		
-	1	+	-3
-	-3	+	-3
+	-3	-	1
-	1	+	1
-	1	-	1
+	-3	-	-3
+	1	+	-3
+	1	+	25

26 s = 1, D = 0, N = 6, 3-level, minimax

-	-2	optimal
-	-2	
-	-2	
-	2	
-	2	
+	-2	
+	-2	
-	2	
+	-2	
-	-2	
-	-2	
+	-2	
-	-2	
+	-2	
-	-2	
+	-2	
+	-2	
+	2	
-	-2	
+	-2	
+	2	
+	2	
-	-2	
-	-2	
+	-2	
+	26	

APPENDIX (continued)

27 — s = 1, D = 1, N = 4, 4-level, minimax.

optimal?

-	-1
+	-1
-	3
-	-1
+	-1
-	-5
+	-1
+	-1
+	-1
-	-1
-	-1
-	-1
-	-1
+	-1
-	-1
-	-1

+	-1
+	-1
+	-1
-	-5
+	-1
+	-1
+	3
-	-1
+	-1
+	27

28 — D = 2, N = 21, 3-level, minimax.

optimal?
(4 * 7)

+	0
-	0
-	0
+	-4
-	0
-	0
+	0
-	-4
-	0
+	0
-	0
+	-4
-	0
+	0
-	0
-	-4
+	0
+	0
+	0
-	-4
-	0
-	0
+	0
+	-4
+	0
+	0
+	0
+	28

APPENDIX (continued)

29 s = 4, D = 1, N = 14, 3-level, minimax.

+	-3
-	1
-	-3
+	1
+	1
-	1
+	-3
+	1
+	-3
+	-3
-	1
+	-3
+	-3
-	1
+	1
-	-3
+	-3
-	1
+	-3
-	-3
-	1
-	-3
+	1
+	1
+	1
-	-3
-	1
-	-3
-	29

optimal
(not quadratic residue sequence)

APPENDIX (continued)

30 s = 4, D = 2, N = 8, 3-level, minimax.

optimal?

−	−2
−	−2
−	−2
+	−2
+	−2
−	−2
+	2
−	−2
+	2
+	2
−	2
+	−2
+	−2
−	−2
+	−2
+	−2
+	−2
−	−2
+	2
−	2
−	2
−	−2
+	2
+	−2
+	−2
+	−2
−	−2
−	−2
−	−2
+	30

APPENDIX (continued)

31		D = 1, N = 0, 2-level, minimax.
+	-1	optimal
+	-1	(linear sequence)
+	-1	
+	-1	
-	-1	
+	-1	
-	-1	
+	-1	
-	-1	
-	-1	
-	-1	
+	-1	
-	-1	
-	-1	
+	-1	
+	-1	
+	-1	
-	-1	
-	-1	
-	-1	
-	-1	
-	-1	
+	-1	
+	-1	
-	-1	
-	-1	
+	-1	
-	-1	
+	-1	
+	-1	
-	31	

APPENDIX (continued)

32 s = 1, D = 0, N = 24, 4-level, minimax.

-	-4	optimal?
+	0	
-	0	
+	-4	
-	0	
+	0	
-	0	
+	-4	
+	0	
-	0	
-	0	
-	0	
-	0	
+	0	
+	0	
+	-8	
+	0	
+	0	
-	0	
+	0	
+	0	
-	0	
+	0	
-	-4	
-	0	
+	0	
+	0	
-	-4	
-	0	
-	0	
+	-4	
-	32	

APPENDIX (continued)

33

s = 2, D = 3. N = 18, 3-level, minimax.

optimal?

-	-3
+	-3
-	1
+	1
-	-3
+	1
+	1
+	-3
+	1
-	1
+	-3
-	-3
-	1
+	-3
+	1
+	1
+	1
-	1
-	-3
+	1
+	-3
-	-3
+	1
+	1
-	-3
+	1
+	1
-	-3
-	1
-	1
+	-3
-	-3
-	33

APPENDIX (continued)

34 s = 1, D = 0, N = 10, 4-level, minimax.

-	-6
-	-2
+	-2
-	2
-	-2
+	-2
+	-2
+	-2
+	2
+	-2
-	2
+	-2
-	2
-	-2
+	-2
-	2
+	-2
-	2
+	-2
-	-2
-	2
-	-2
+	2
-	-2
+	2
-	-2
-	-2
+	-2
+	-2
+	2
-	-2
-	-2
+	-6
+	34

APPENDIX (continued)

35 D = 1, N = 0, 3-level, minimax.

+	-1	optimal
+	-1	(twin-prime sequence)
+	-1	
-	-1	
-	-1	
-	-1	
+	-1	
+	-1	
+	-1	
+	-1	
+	-1	
-	-1	
+	-1	
+	-1	
+	-1	
-	-1	
-	-1	
+	-1	
-	-1	
-	-1	
-	-1	
-	-1	
-	-1	
+	-1	
-	-1	
+	-1	
-	-1	
+	-1	
+	-1	
-	-1	
-	-1	
+	-1	
-	-1	
-	-1	
+	-1	
-	35	

APPENDIX (continued)

	36	s = 2, D = 2, N = 27, 3-level, minimax.
-	0	optimal?
-	0	found by backtrack
-	0	
+	0	
+	0	
+	0	
-	0	
+	0	
-	-4	
+	-4	
-	0	
-	-4	
+	0	
+	0	
-	-4	
+	0	
+	0	
-	0	
-	0	
-	0	
+	-4	
-	0	
-	0	
-	-4	
-	0	
-	-4	
-	-4	
+	0	
-	0	
+	0	
+	0	
-	0	
+	0	
+	0	
+	0	
+	36	

APPENDIX (continued)

37 s = 2, D = 1, N = 18, 3-level, minimax.

-	-3	optimum
-	1	(<u>not</u> quadratic residue sequence)
-	-3	
-	-3	
+	1	
-	-3	
+	1	
-	-3	
-	1	
+	1	
-	-3	
+	1	
+	1	
-	1	
+	-3	
+	-3	
+	-3	
-	1	
+	1	
-	-3	
+	-3	
+	-3	
+	1	
-	1	
+	1	
+	-3	
-	1	
-	1	
-	-3	
+	1	
-	-3	
-	1	
-	-3	
+	-3	
+	1	
+	-3	
+	37	

APPENDIX (continued)

38 s = 1, D = 0, N = 11, 4-level, minimax.

-	-2
-	-2
-	-6
-	-2
-	2
+	-2
-	-2
-	2
+	-2
+	-2
+	2
+	-2
-	-2
+	2
-	-2
+	-2
+	2
-	-2
-	2
+	-2
+	2
+	-2
-	-2
+	2
-	-2
-	-2
-	2
+	-2
+	-2
+	2
-	-2
-	-2
+	2
-	-2
+	-6
-	-2
+	-2
+	38

APPENDIX (continued)

39 s = 4, D = 3, N = 6, 4-level, minimax.

-	-1
-	-1
-	-1
-	-1
+	-5
-	-1
+	-1
-	3
-	3
+	-1
-	-5
+	-1
+	-1
-	3
+	-1
+	-1
+	-1
-	-1
+	-1
-	-1
+	-1
+	-1
+	-1
-	-1
+	3
+	-1
+	-1
-	-5
+	-1
+	3
-	3
-	-1
-	-1
+	-5
+	-1
+	-1
+	-1
+	-1
-	39

APPENDIX (continued)

41		D = 1, N = 20, 3-level, minimax
+	1	optimal
+	1	(quadratic residue sequence)
+	-3	
-	1	
+	1	
+	-3	
-	-3	
-	1	
+	1	
+	1	
+	-3	
-	-3	
-	-3	
-	-3	
-	-3	
-	1	
+	-3	
-	1	
+	-3	
-	1	
+	1	
+	-3	
-	1	
+	-3	
-	1	
+	-3	
-	-3	
-	-3	
-	-3	
-	-3	
-	1	
+	1	
+	1	
+	-3	
-	-3	
-	1	
+	1	
+	-3	
-	1	
+	1	
+	41	

APPENDIX (continued)

42 s = 4, D = 0, N = 14, 4-level, minimax.

-	2
-	2
-	2
-	2
+	-2
-	-2
+	-2
-	-2
-	2
+	-2
-	-2
+	2
+	2
-	-2
+	-6
+	-6
+	-2
-	-2
+	-2
-	-2
+	-2
+	-2
+	-2
-	-2
+	-2
+	-6
-	-6
-	-2
+	2
+	2
-	-2
-	-2
-	2
+	-2
+	-2
+	-2
+	-2
+	2
-	2
-	2
-	2
-	42

APPENDIX (continued)

43		D = 0, N = 0, 2-level, minimax
+	-1	optimum
+	-1	(quadratic residue)
-	-1	
-	-1	
+	-1	
-	-1	
+	-1	
-	-1	
-	-1	
+	-1	
+	-1	
+	-1	
-	-1	
+	-1	
+	-1	
+	-1	
+	-1	
+	-1	
-	-1	
-	-1	
-	-1	
+	-1	
-	-1	
+	-1	
+	-1	
+	-1	
-	-1	
-	-1	
-	-1	
-	-1	
-	-1	
+	-1	
-	-1	
-	-1	
-	-1	
+	-1	
+	-1	
-	-1	
+	-1	
-	-1	
+	-1	
+	-1	
-	43	

APPENDIX (continued)

	44	D = 3, N = 33, 3-level, minimax.
+	0	optimal?
+	0	(11 * 4 sequence)
-	0	
-	-4	
+	0	
+	0	
-	0	
+	-4	
-	0	
+	0	
-	0	
-	-4	
+	0	
-	0	
+	0	
-	-4	
+	0	
-	0	
-	0	
+	-4	
+	0	
-	0	
+	0	
-	-4	
-	0	
+	0	
+	0	
-	-4	
-	0	
-	0	
-	0	
-	-4	
-	0	
+	0	
+	0	
+	-4	
+	0	
+	0	
+	0	
+	-4	
-	0	
-	0	
+	0	
+	44	

APPENDIX (continued)

45 s = 4, D = 1, N = 24, 4-level, minimax.

-	1
+	-3
+	1
-	-3
-	1
-	-3
+	1
+	1
+	-3
+	-3
-	-3
-	-3
-	-3
-	1
+	1
+	1
-	1
-	1
+	1
-	-3
-	-7
+	1
-	1
+	-7
+	-3
-	1
+	1
-	1
+	1
-	1
-	1
-	-3
+	-3
-	-3
-	-3
-	-3
+	1
+	1
-	-3
+	1
+	-3
+	1
+	-3
+	1
+	45

APPENDIX (continued)

46 s = 1, D = 2, N = 18, 4-level, minimax.

-	2
+	2
-	2
+	-2
-	2
-	-2
+	-2
+	2
+	2
+	-2
-	-6
-	-2
-	-2
-	-2
+	2
+	-2
-	2
-	-6
+	-6
-	-2
-	2
+	-2
-	-2
+	-2
+	2
-	-2
-	-6
-	-6
+	2
-	-2
-	2
-	-2
+	-2
-	-2
-	-6
-	-2
-	2
+	2
-	-2
+	-2
+	2
+	-2
+	2
+	2
+	2
+	46

APPENDIX (continued)

47 D = 1, N = 0, 2-level, minimax optimal (quadratic residue sequence)

-	-1
+	-1
+	-1
+	-1
+	-1
-	-1
+	-1
+	-1
+	-1
+	-1
-	-1
-	-1
+	-1
-	-1
+	-1
-	-1
+	-1
+	-1
+	-1
-	-1
-	-1
+	-1
-	-1
-	-1
+	-1
+	-1
-	-1
+	-1
+	-1
-	-1
-	-1
-	-1
+	-1
-	-1
+	-1
-	-1
+	-1
+	-1
-	-1
-	-1
-	-1
-	-1
+	-1
-	-1
-	-1
-	-1
-	47

APPENDIX (continued)

49		D = 1, N = 36, 3-level, minimax.
+	1	(7 ⊠ 7)
+	-7	
+	1	Note that the two out-of-phase levels are not adjacent (separation 8)
-	-7	
-	1	
+	-7	
-	-7	
+	1	
+	1	
+	1	
-	1	
-	1	
+	1	
-	-7	
+	1	
+	1	
+	1	
-	1	
-	1	
+	1	
-	-7	
-	1	
-	1	
-	1	
+	1	
+	1	
-	1	
+	-7	
-	1	
-	1	
-	1	
+	1	
+	1	
-	1	
+	-7	
+	1	
+	1	
+	1	
-	1	
-	1	
+	1	
-	-7	
-	-7	
-	1	
-	-7	
+	1	
+	-7	
-	1	
+	49	

APPENDIX (continued)

50 s = 4, D = 2, N = 16, 4-level, minimax.

−	−2
−	2
+	−2
−	2
+	2
+	−2
−	−2
+	−2
−	−2
+	−2
−	2
−	2
−	−2
−	−6
+	−2
+	2
−	−2
+	2
−	−2
+	−2
−	2
−	−2
−	−2
+	−2
−	−6
+	−2
+	−2
−	−2
−	2
−	−2
−	−2
−	2
+	−2
−	2
−	−2
−	−6
+	−2
+	2
+	2
+	−2
+	−2
+	−2
−	−2
+	−2
+	2
+	2
−	−2
−	2
+	−2
+	50

APPENDIX (continued)

51 s = 2, D = 3, N = 12, 4-level, minimax.

-	3
+	-1
+	3
-	-1
-	-1
+	-1
-	-1
-	-1
-	-1
-	-5
-	-1
-	-5
-	-5
+	-1
-	-1
-	-5
+	3
-	-1
-	3
+	-1
+	-5
+	-1
+	-1
+	3
-	3
-	3
-	3
-	-1
+	-1
+	-5
+	-1
-	3
+	-1
+	3
-	-5
+	-1
-	-1
+	-5
-	-5
-	-1
-	-5
+	-1
+	-1
-	-1
-	-1
+	-1
+	-1
+	3
+	-1
-	3
+	51

APPENDIX (continued)

53 D = 1, N = 26, 3-level, minimax.

+	1
+	-3
-	-3
-	1
+	-3
-	1
+	1
+	-3
-	1
+	1
+	1
+	-3
-	1
+	-3
-	1
+	1
+	1
+	-3
-	-3
-	-3
-	-3
-	-3
-	-3
-	1
+	1
+	-3
-	-3
-	1
+	1
+	-3
-	-3
-	-3
-	-3
-	-3
-	-3
-	1
+	1
+	1
+	-3
-	1

optimum
(quadratic residue sequence)

+	-3
-	1
+	1
+	1
+	-3
-	1
+	1
+	-3
-	-3
-	1
+	-3
-	1
+	53

APPENDIX (continued)

54 s = 2, D = 0, N = 23, 5-level, minimax.

-	2		
+	2		
-	-2		
-	-2		
-	2		
+	2		
-	2		
-	2		
+	2		
+	-2		
-	2		
-	-2		
-	-2		
+	-10		
+	-2		
-	-10		
+	2		
-	2		
-	-2		
+	-2		
-	2	-	-10
+	-2	+	-2
+	-6	-	-10
-	-2	+	-2
-	-2	+	-2
-	-2	+	2
+	2	-	-2
-	-2	+	2
-	-2	-	2
-	-2	+	2
-	-6	+	2
+	-2	+	2
+	2	+	-2
+	-2	+	-2
-	-2	+	2
-	2	+	2
-	2	+	54

APPENDIX (continued)

55 D = 5, N = 10, 4-level, minimax.

+	-1	optimal?
+	-1	(Jacobi sequence)
+	-1	
-	-1	
+	3	
-	-1	
-	-1	
+	-1	
+	-1	
+	3	
-	-5	
+	-1	
-	-1	
+	-1	
+	3	
-	-1	
+	-1	
+	-1	
+	-1	
-	3	
-	-1	
-	-5	
+	-1	
-	-1	
-	3	
-	-1	
+	-1	
-	-1	
+	-1	
-	3	
-	-1	
+	-1	+ -5
+	-5	+ 3
+	-1	- -1
+	3	- -1
-	-1	- -1
+	-1	- -1
-	-1	+ 3
-	-1	- -1
-	3	- -1
-	-1	+ -1
-	-1	- -1
-	-1	- 55

APPENDIX (continued)

57 D = 1, N = 36, 4-level, minimax.

(19 ⊠ 3 sequence)

Note non-adjacent levels

+	1		
+	-19		
-	-3		
+	1		
+	1		
-	-3		
-	1		
-	1		
+	-3		
-	1		
-	1		
+	-3		
+	1		
+	1		
-	-3		
+	1		
+	1		
-	-3		
+	1		
+	1		
-	-3	-	1
-	1	+	-3
-	1	-	1
+	-3	-	1
+	1	+	-3
+	1	-	1
-	-3	-	1
-	1	+	-3
-	1	+	1
+	-3	+	1
+	1	-	-3
+	1	+	1
-	-3	+	1
-	1	-	-3
-	1	-	-19
+	-3	-	1
-	1	+	57

APPENDIX (continued)

58 s = 4, D = 0, N = 20, 4-level, minimax.

+	-2		
+	2		
+	-2		
+	-2		
-	-2		
-	2		
-	-2		
+	-2		
-	2		
+	2		
-	-2		
+	2		
-	2		
+	-6		
-	-2		
-	-6		
+	-2		
-	-6		
+	2		
+	-2		
-	2		
+	-2		
-	-2		
-	2		
+	-2	-	-6
+	-2	-	-2
+	2	-	-6
-	-2	-	2
-	-2	+	2
-	-2	-	-2
+	2	-	2
-	-2	+	2
-	-2	+	-2
-	2	+	-2
+	-2	+	2
-	-2	+	-2
-	2	-	-2
+	-2	+	-2
+	2	+	2
+	-6	-	-2
-	-2	+	58

APPENDIX (continued)

59 D = 1, N = 0, 2-level, minimax.

-	-1	optimal
+	-1	(quadratic residue)
-	-1	
+	-1	
+	-1	
+	-1	
-	-1	
+	-1	
-	-1	
+	-1	
-	-1	
-	-1	
+	-1	
-	-1	
-	-1	
+	-1	
+	-1	
+	-1	
-	-1	
+	-1	- -1
+	-1	- -1
+	-1	+ -1
+	-1	- -1
-	-1	- -1
-	-1	- -1
+	-1	+ -1
+	-1	+ -1
+	-1	- -1
+	-1	+ -1
+	-1	+ -1
-	-1	- -1
-	-1	+ -1
-	-1	- -1
-	-1	+ -1
-	-1	- -1
+	-1	- -1
+	-1	- -1
-	-1	+ -1
-	-1	- 59

APPENDIX (continued)

60

D = 2, N = 45, 3-level, minimax.

optimal?
(15 * 4 sequence)

-	0		
-	0		
-	0		
-	-4		
+	0		
+	0		
+	0		
+	-4		
+	0		
-	0		
+	0		
-	-4		
-	0		
-	0		
+	0		
+	-4		
-	0		
-	0		
+	0		
-	-4		
+	0		
+	0		
-	0		
-	-4		
-	0		
+	0		
+	0		
+	-4		
-	0	+	0
+	0	-	0
-	0	-	0
+	-4	+	-4
-	0	+	0
+	0	+	0
+	0	+	0
-	-4	-	-4
+	0	-	0
-	0	+	0
+	0	-	0
+	-4	-	-4
+	0	+	0
+	0	-	0
-	0	-	0
+	-4	-	60

APPENDIX (continued)

61 D = 1, N = 30, 3-level, minimax.

+	1
+	-3
-	1
+	1
+	1
+	-3
-	-3
-	-3
-	1
+	-3
-	-3
-	1
+	1
+	1
+	1
+	1
+	-3
-	-3
-	1
+	1
+	-3
-	1
+	-3
-	-3
-	1
+	-3
-	1
+	-3
-	-3
-	-3
-	-3
-	-3
-	-3
-	1
+	-3
-	1
+	-3
-	-3
-	1
+	-3
-	1
+	1
+	-3
-	-3
-	1
+	1
+	1
+	1
+	1
+	1

optimal
(quadratic residue sequence)

+	-3
-	-3
-	1
+	-3
-	-3
-	-3
-	1
+	1
+	1
+	-3
-	1
+	61

APPENDIX (continued)

62 s = 4, D = 0, N = 25, 4-level, minimax.

+	-2
-	-2
+	-6
-	-2
-	-2
-	2
+	-2
-	2
-	2
-	-2
-	2
-	-6
-	-2
+	-2
+	2
+	2
-	2
+	2
-	2
-	-2
+	-2
+	2
-	-6
+	2
-	-6
-	2
+	-6
-	-2
-	-2
+	-2
-	2
+	-2
-	-2
+	-2
+	-6
+	2
+	-6
-	2
-	-6
+	2
+	-2

-	-2
-	2
+	2
+	2
+	2
-	2
-	-2
-	-2
+	-6
+	2
+	-2
+	2
+	2
-	-2
+	2
-	-2
+	-2
+	62

APPENDIX (continued)

63 D = 1, N = 0, 2-level, minimax.

-	-1	optimal
-	-1	(linear sequence)
-	-1	
-	-1	
-	-1	
+	-1	
+	-1	
+	-1	
+	-1	
+	-1	
+	-1	
-	-1	
+	-1	
-	-1	
+	-1	
-	-1	
+	-1	
+	-1	
-	-1	
-	-1	
+	-1	
+	-1	
-	-1	
+	-1	- -1
+	-1	+ -1
+	-1	+ -1
-	-1	+ -1
+	-1	+ -1
+	-1	- -1
-	-1	- -1
+	-1	+ -1
-	-1	- -1
-	-1	+ -1
+	-1	- -1
-	-1	- -1
-	-1	- -1
+	-1	+ -1
+	-1	+ -1
+	-1	- -1
-	-1	- -1
-	-1	- -1
-	-1	- -1
+	-1	+ 63

REFERENCES

1. Golomb, S. W., Sequences with Randomness Properties, Terminal Progress Report (1955), Contract No. 639498, The Martin Company, Baltimore, Maryland, pp. 5 - 39.

2. Hall, M., Jr., Proc. Am. Math. Soc. (1956), Vol. 7, pp. 975 - 986.

3. Zierler, Neal, Jour. Soc. Indust. Applied Math. (1959), Vol. 7, pp. 31 - 48.

4. Hall, M., Jr., Projective Planes and Related Topics (1954) lecture notes, pp. 67 - 74.

5. Easterling, M., Long Range Precision Ranging System (1961), Jet Propulsion Laboratory Report #32-80, pp. 1 - 7.

6. Easterling, M., et. al., Jet Propulsion Laboratory Research Summary (1961), No. 36-7, Vol. I, pp. 62 - 65.

7. Viterbi, A. J., Systematic Coding for the Continuous Gaussian Channel (1962), Doctorate Thesis, University of Southern California, pp. 70 - 79.

8. Titsworth, R. C., and Welch, L. R., Modulation by Random and Pseudo-random Sequences (1959), Jet Propulsion Laboratory Report #20-387, pp. 4 - 28.

9. Titsworth, R. C., and Welch, L. R., Power Spectra of Signals Modulated by Random and Pseudorandom Sequences (1961), Jet Propulsion Laboratory Report #32-140, pp. 5 - 45.

10. Davenport, W. B., and Root, W. L., Random Signals and Noise (1958), McGraw-Hill Publishing Company, pp. 175-178.

11. Ibid, pp. 183 - 185.

12. Feller, W., An Introduction to Probability Theory and Its Applications (1950), Vol. I, John Wiley and Sons, Inc., pp. 388 - 395.

13. Gantmacher, F. R., Applications of the Theory of Matrices (1959), Interscience Pub. Inc., pp. 99 - 106.

14. Fréchet, M., Recherches Theoriques Modernes Sur le Calcul des Probabilites (1938), Paris, pp. 14 - 60.

15. Feller, op. cit., pp. 380 - 384.

16. Titsworth, R. C., Calculation of Matrix Functions (1961), Jet Propulsion Laboratory Research Summary, No. 36-7, Vol. I, pp. 47 - 48.

17. Goldman, S., Frequency Analysis, Modulation, and Noise (1948), McGraw-Hill, pp. 53 - 56.

18. Zierler, loc. cit.

19. Golomb, op. cit., pp. 5 - 48.

20. Golomb, S. W., Structural Properties of Pseudonoise Sequences (1958), Jet Propulsion Laboratory Section Report 8-574, pp. 16 - 18.

21. Jaffe, R. M., and Rechtin, E., Transactions of the IRE (1955), Vol. IT-1, pp. 66 - 76.

22. Gilchriest, C., Jet Propulsion Laboratory Research Summary (1961), No. 36-10, Vol. I, pp. 54 - 63.

23. Grenander, U., Arkiv fur Matematik (1950), Vol. I(17), pp. 195 - 277.

24. Woodward, P. M., Probability and Information Theory with Applications to Radar (1953), McGraw-Hill, pp. 62 - 67.

25. Loève, M., Probability Theory (1955), Van Nostrand, Inc., p. 24.

26. Woodward, op. cit., pp. 65 - 66.

27. Balakrishnan, A. V., Jour. Math. Anal. and Applications (1961), Vol. 3, pp. 485 - 506.

28. Ibid.

29. Viterbi, A. J., op. cit., pp. 39 - 44.

30. Kotel'nikov, V. A., The Theory of Optimum Noise Immunity (1947), McGraw-Hill, pp. 53 - 56.

31. Viterbi, op. cit., pp. 39 - 44.

32. Apostol, R. M., Mathematical Analysis (1957), Addison-Wesley, p. 160.

33. Fine, N. J., Illinois Jour. Math. (1958), Vol. 2, pp. 285 - 302.

34. Gilbert, E.N., and Riordan, J., Illinois Jour. Math. (1961), Vol. 5(4), pp. 657 - 665.

35. Riordan, J., An Introduction to Combinatorial Analysis (1958), John Wiley, p. 162.

36. Golomb, S. W., Mathematical Theory of Discrete Classification (1960), Proc. London Symposium on Information Theory, pp. 404 - 425.

37. Pólya, G., Acta Math. (1937), Vol. 68, pp. 145 - 253.

38. Nagell, T., Introduction to Number Theory (1951), John Wiley, pp. 23 - 26.

39. Birkhoff, G., and MacLane, S., A Survey of Modern Algebra (1953 Rev.), MacMillan, pp. 252 - 254.

40. Nagell, T., op. cit., pp. 28 - 29.

41. Nagell, op. cit., pp. 19 - 23.

42. Golomb, loc. cit., Ref. 1.

43. Feller, loc. cit.

44. Zierler, op. cit., p. 40.

45. Golomb, S. W., Sequences with the Cycle-and-Add Property (1957), Jet Propulsion Laboratory Section Report 8-573, pp. 1 - 8.

46. Golomb, loc. cit., Ref. 1.

47. Hall, loc. cit., Ref. 2.

48. Hall, loc. cit., Ref. 4.

49. Golomb, loc. cit., Ref. 20.

50. Zierler, N., Proc. Am. Math. Soc. (1956), Vol. 7(4), pp. 675 - 681.

51. Bruck, R., and Ryser, H., Canadian Jour. Math. (1949), Vol. I, pp. 83 - 93.

52. Van Der Waerden, B. L., Modern Algebra (1949), Vol. I, Frederick Anger, pp. 42 - 45.

53. Hall, M., Jr., The Theory of Groups (1959), MacMillan, pp. 255 - 261.

54. Ibid.

55. Bruck and Ryser, loc. cit.

56. Hall, loc. cit., Ref. 2.

57. Baumert, L., Easterling, M., Golomb, S., and Viterbi, A., Coding Theory and Its Applications to Communications Systems (1961), Jet Propulsion Laboratory Report #32-67, pp. 2 - 18.

58. Golomb, loc. cit., Ref. 1.

59. Baumert, et al, loc. cit.

60. Nagell, op. cit., pp. 141 - 145.

61. Hall, op. cit., Ref. 53, pp. 267 - 285.

62. Nagell, op. cit., pp. 145 - 149.

63. Brauer, A., Mathematische Zertischrift (1953), Vol. 58, pp. 219 - 225.

64. Turyn, R. J., Optimal Code Study (final report) (1960), Sylvania Electronics Systems Report, pp. V-1 - V-6.

65. Barker, R. H., Communications Theory (1953), London, pp. 273 - 287.

66. Turyn, R. J., and Storer, J., Proc. Am. Math. Soc. (1961), Vol. 12(3), pp. 394 - 399.

67. Coll, D. C., Proc. IRE (1961), Vol. 49(7), p. 1230.

68. Zygmund, A., Trigonometric Series (1955), Diver, pp. 122 - 130.

69. Ibid., pp. 9 - 10.

70. Golomb, S. W., Transactions of the IRE (1959), Symposium on Circuit and Information Theory, pp. 176 - 186.

71. Ninomiya, I., Memoirs of the Faculty, Nagoya University (1958), Vol. 10(2), pp. 175 - 190.

72. Calingaert, P., Switching Function Canonical Forms (1960), AIEE Fall General Meeting, pp. 1 - 18.

73. Birkhoff and MacLane, op. cit., p. 25.

74. Apostol, op. cit., pp. 510 - 514.

75. Burington, R. S., Mathematical Tables and Formulas (1933), Handbook Pub., Inc., p. 88.

76. Feller, op. cit., pp. 50 - 53.