IDENTIFICATION OF NONLINEAR AND MULTIVARIABLE SYSTEMS
BY MEANS OF PERIODIC STEP SEQUENCES

by

Noel REAM

Thesis submitted for the degree of Doctor of Philosophy
of the University of London
in the Faculty of Science

1969
Abstract

The thesis deals with theoretical aspects of the measurement, by correlation, of the kernels of time-invariant multivariable and nonlinear dynamical systems, using periodic-step-sequence inputs of the pseudorandom type.

The crosscorrelation of equal-length pairs of binary maximum-length sequences is examined in detail. The frequency distributions of the correlation coefficients are listed for all such pairs of period \( \leq 255 \), and formulae are derived for the first four moments of the distribution. A limited amount of information about the correlation sequences is obtained from a study of the generating polynomials. The sampling property of maximum-length sequences is used, in an alternative approach, to classify the frequency distributions. Finally, recent work by Gold (1968) is related to the author's work on ternary correlation sequences, and suggestions are made for extending this.

The problem of calculating the linear kernels of a multi-input system, from input/output crosscorrelations evaluated at sample time intervals, is found to reduce to the solution of a finite set of linear algebraic equations in the system 'weights'. Two cases of practical importance are found to yield exactly \( N \) independent equations, where \( N \) is the period of the output signal. From this result, and a review of other work, a suggestion is made as to the best type of input for any multiple linear identification.

The same reduction to \( N \) equations is found to hold for a single-input nonlinear system, defined by a Volterra series of any order, when the test signal is a binary or inverted-binary maximum-length sequence, or a ternary maximum-length sequence. A non-rigorous argument is adduced to show why this reduction to \( N \) equations may hold for any form of identification by sample-interval correlation using synchronized periodic step sequences.

It is proved that all binary maximum-length sequences, but not all ternary sequences, can be started at such a point that the first moment vanishes.
Acknowledgements

I wish to thank Mr P. H. Hammond, formerly of the National Physical Laboratory and now at Warren Spring Laboratory, for suggesting the field of study, and I am grateful to Mr P. A. N. Briggs and Dr K. R. Godfrey of the same group for their advice and criticism throughout the course of the work. During the period covered by this thesis I have held a Readership at Battersea College of Technology, and its successor the University of Surrey, and I am indebted to Professors D. R. Chick and W. F. Lovering, of the Electrical and Control Engineering Department, for the facilities for doing the work. Professor F. M. Arscott, of the Department of Mathematics, read the thesis in draft and made valuable suggestions for improving the presentation.

The thesis is dedicated to my wife, Margaret Lorna, for her patience and help towards its completion.

University of Surrey
Guildford, Surrey
30 January 1969.
## CONTENTS

<table>
<thead>
<tr>
<th>List of Symbols</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6</td>
</tr>
</tbody>
</table>

1. Introduction and conclusions  
1.1 Statement of the problem  
1.2 Outline of the research  
1.3 Conclusions; suggestions for further work  

2. Pseudorandom sequences  
2.1 The use of pseudorandom sequences in system identification  
2.2 Pseudorandom binary sequences  
2.3 Binary maximum-length sequences (m-sequences)  
2.4 Quadratic-residue sequences  
2.5 Some nonbinary pseudorandom sequences  
2.6 Conclusions  

3. Crosscorrelation of equal-length pairs of binary m-sequences  
3.1 Introduction. Frequency distributions for $N \leq 255$  
3.2 Moments of the frequency distribution  
3.3 Generating-polynomial approach to the determination of the structure of crosscorrelation sequences  
3.4 Example to illustrate the generating-polynomial analysis  
3.5 Ternary crosscorrelation sequences  
3.6 Values of $N_1$ and $N_2$ for Type 0 distributions  
3.7 Classification of crosscorrelation sequences by means of the sampling property  
3.8 Gold sequences: a class of ternary crosscorrelation sequences  
3.9 Conclusions  
3.10 A note on computing time  

4. Identifying multi-input linear systems by crosscorrelation of periodic sequences  
4.1 General remarks  
4.2 A survey of work on crosscorrelation of periodic sequences  
4.3 Redundancy of the system equations
5. Identifying nonlinear systems by means of pseudorandom inputs

5.1 The approximation problem 55
5.2 Weight equations arising from a periodic-step-sequence input 57
5.3 Second-order weight equations for two types of binary input:
   1. Binary m-sequence 60
   2. Binary m-sequence with alternate terms inverted 61
   3. Discussion 63
5.4 Correlation functions \( X_1 \) and \( X_3 \) for ternary-m-sequence input 64
5.5 Second-order weight equations for ternary-m-sequence input 67
5.6 Correlation equations arising from particular input sequences:
   1. Ternary m-sequence, \( N = 8 \) 69
   2. Binary m-sequence, \( N = 31 \) 70
   3. Inverted binary m-sequence, \( N = 30 \) 71
   4. Ternary m-sequence, \( N = 26 \) 71
   5. Comparison of the inverted-binary and the ternary input 74
5.7 Higher-order correlation equations with ternary input
   1. The general identity 75
   2. Correlation function of order \( 2n - 1 \) 76
   3. Reduction of the correlation equations 78
5.8 Discussion on nonlinear correlation 79

Appendixes

1. Effect of drift on linear identification by means of binary or ternary m-sequences 81
2. Further data for ternary m-sequences 88

References 90

Annex 1. 'Testing a 2-input linear system with periodic binary sequences' 92
LIST OF SYMBOLS

The equation and page numbers refer to the first appearance of a symbol. In Chapters 2 and 3, equations are numbered section by section, e.g. 2.1(1); in Chapter 5, the numbering is continuous, starting with 5(1).

The notation used in Annex 1 is different, and is defined there.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>( {a_i} ) or ( a )</td>
<td>Periodic sequences with general term ( a_i, b_i )</td>
</tr>
<tr>
<td>( {b_i} ) or ( b )</td>
<td>In Chapter 2, ( a_i ) has values (1,-1) and ( b_i ) has values (0,1); in Chapter 3, ( a ) and ( b ) denote different sequences whose terms may be from either field</td>
</tr>
<tr>
<td>( f^{a,r}_r )</td>
<td>( r ) th translate of ( a, b )</td>
</tr>
<tr>
<td>( a )</td>
<td>Sampled sequence ( {a_{ri}} )</td>
</tr>
<tr>
<td>( a^\prime )</td>
<td>Reversed sequence ( {a_{-i}} )</td>
</tr>
<tr>
<td>( a_0 )</td>
<td>'Base' sequence</td>
</tr>
<tr>
<td>( a^+, a^- )</td>
<td>Levels of binary m-sequence with zero mean</td>
</tr>
<tr>
<td>( a(X), b(X) )</td>
<td>Polynomial representation of sequences, 3.3(1)</td>
</tr>
<tr>
<td>([a, b])</td>
<td>Correlation sequence from ( a ) and ( b )</td>
</tr>
<tr>
<td>( A, B, \ldots )</td>
<td>Translation sets</td>
</tr>
<tr>
<td>( \hat{A} )</td>
<td>'Reverse' of set ( A ) for binary sequence</td>
</tr>
<tr>
<td>( \hat{A} )</td>
<td>'Half-cycle shift' of set ( A ) for ternary sequence</td>
</tr>
<tr>
<td>( C_S, c_S )</td>
<td>Forms of the crosscorrelation, 3.1(1),(2)</td>
</tr>
<tr>
<td>( C(t) )</td>
<td>Crosscorrelation sequence from ( a ) and ( a(t) )</td>
</tr>
<tr>
<td>( d_S )</td>
<td>Form of the crosscorrelation, 3.8(3)</td>
</tr>
<tr>
<td>( D )</td>
<td>Value of ( c_S ) in ternary crosscorrelation sequence</td>
</tr>
<tr>
<td>( E )</td>
<td>Quantity defined in 3.5(3)</td>
</tr>
<tr>
<td>( e_i(t) )</td>
<td>Error in ( i ) th approximation to ( y(t) )</td>
</tr>
<tr>
<td>( e(t) )</td>
<td>Noise term, A(1)</td>
</tr>
<tr>
<td>( e, f, g, h )</td>
<td>Order of translation set</td>
</tr>
<tr>
<td>( f_0(x), f_c(x) )</td>
<td>Frequency distributions of ( C_S, c_S )</td>
</tr>
<tr>
<td>( g(X), g_i )</td>
<td>Generating polynomial and coefficients, 2.3(1),(2)</td>
</tr>
<tr>
<td>( h(X), h_i )</td>
<td>Generator etc. for sequence ( b )</td>
</tr>
<tr>
<td>( h(t) )</td>
<td>Linear kernel</td>
</tr>
<tr>
<td>( h_i(u,v,\ldots) )</td>
<td>Kernel of order ( i ), 5(1)</td>
</tr>
<tr>
<td>( h_i(j) )</td>
<td>( j ) th approximation to ( h_i )</td>
</tr>
<tr>
<td>([j_1,j_2,\ldots] )</td>
<td>General autocorrelation function, 5(82)</td>
</tr>
<tr>
<td>Symbol</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>k</td>
<td>'Off-peak' value of two-level correlation</td>
</tr>
<tr>
<td>$k_i$</td>
<td>Coefficients in $e(t)$, $A(5)$</td>
</tr>
<tr>
<td>$l, L$</td>
<td>Integers defined in $3.8(6)$</td>
</tr>
<tr>
<td>m</td>
<td>Number of positive terms in sequence $a$</td>
</tr>
<tr>
<td>$m_k$</td>
<td>Number of 'ones' in binary number $h$</td>
</tr>
<tr>
<td>M</td>
<td>$= \frac{3}{2}N$ for ternary or inverted-binary sequence</td>
</tr>
<tr>
<td>$M_r, m_r$</td>
<td>$r^{th}$ moments of $f_c(x), f_c(x)$, $3.2(1), (25)$</td>
</tr>
<tr>
<td>n</td>
<td>Degree of generator</td>
</tr>
<tr>
<td>n</td>
<td>Integer associated with ternary identity</td>
</tr>
<tr>
<td>N</td>
<td>Period of $y(t)$</td>
</tr>
<tr>
<td>$N, N_+$</td>
<td>Numbers of upper and lower terms in ternary ${c_s}$</td>
</tr>
<tr>
<td>$N_1, N_2$</td>
<td>Numbers of 'correspondences', $3.2(12), (22)$</td>
</tr>
<tr>
<td>$P_n, Q_n$</td>
<td>Expressions in ternary identity, $5(73), (74)$</td>
</tr>
<tr>
<td>p(X), $p_s$</td>
<td>Product polynomial etc., $3.3(3), (4)$</td>
</tr>
<tr>
<td>$p^*(x)$</td>
<td>'Binary' form of $p(X)$, $3.3(6)$</td>
</tr>
<tr>
<td>$p_1(x)$</td>
<td>Halved product, $3.3(16)$</td>
</tr>
<tr>
<td>$p_2(x)$</td>
<td>Quartered product, $3.3(26)$</td>
</tr>
<tr>
<td>q(X), r(X)</td>
<td>Polynomials defined in $3.3(18), (19)$</td>
</tr>
<tr>
<td>$q$</td>
<td>Base of $m$-sequence</td>
</tr>
<tr>
<td>r</td>
<td>Sampling interval of $m$-sequence</td>
</tr>
<tr>
<td>r, s</td>
<td>Integer values of time</td>
</tr>
<tr>
<td>${T_n}$</td>
<td>Correlation sequence, $2.2(1)$</td>
</tr>
<tr>
<td>R($\pi$)</td>
<td>Correlation function</td>
</tr>
<tr>
<td>$R_j$</td>
<td>First moment of $q$-ary sequence, $A(21)$</td>
</tr>
<tr>
<td>$S_j$</td>
<td>First moment of binary sequence, $A(12)$</td>
</tr>
<tr>
<td>$S(i_1, i_2, \ldots)$</td>
<td>Sum defined in $3.2(2)$</td>
</tr>
<tr>
<td>s(X)</td>
<td>Polynomial defined in $3.3(30)$</td>
</tr>
<tr>
<td>t</td>
<td>Current time</td>
</tr>
<tr>
<td>T(x)</td>
<td>Trace of $x$ in $GF(2^n)$, $3.8(1)$</td>
</tr>
<tr>
<td>$T_k$</td>
<td>Translation set with the leading element $b_k$</td>
</tr>
<tr>
<td>$t_k$</td>
<td>Sum of suffixes of elements of $T_k$</td>
</tr>
<tr>
<td>t</td>
<td>Integer such that $b = a(t)$</td>
</tr>
<tr>
<td>u</td>
<td>Modulo-$N$ reciprocal of $t$</td>
</tr>
<tr>
<td>u(X), v(X)</td>
<td>Polynomials defined in $3.3(24), (25)$</td>
</tr>
<tr>
<td>w</td>
<td>Number of nonzero coefficients in $g(X)$</td>
</tr>
<tr>
<td>Symbol</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>( w_i )</td>
<td>Weight of order ( i ), 5(8)</td>
</tr>
<tr>
<td>( W_i )</td>
<td>Modified ( w_i ) for 'half-cycle inversion', 5(34),(39)</td>
</tr>
<tr>
<td>( x, y, z )</td>
<td>Elements from field ((0,1,-1))</td>
</tr>
<tr>
<td>( x, y, z )</td>
<td>Integers defined in 5(67),(70)</td>
</tr>
<tr>
<td>( x(t), y(t) )</td>
<td>System input, output</td>
</tr>
<tr>
<td>( \bar{x}(t) )</td>
<td>Time-average of ( x(t) )</td>
</tr>
<tr>
<td>( X_i, Y_i )</td>
<td>Autocorrelation, crosscorrelation of order ( i )</td>
</tr>
<tr>
<td>( y )</td>
<td>Value of coefficient in ( q(X) )</td>
</tr>
<tr>
<td>( Z_r )</td>
<td>'Off-diagonal weight' expression 5(63)</td>
</tr>
<tr>
<td>( \alpha )</td>
<td>Primitive ( N^{th} ) root of unity in ( GF(2^n) )</td>
</tr>
<tr>
<td>( \varepsilon )</td>
<td>Kronecker-like symbol, defined in 3.2(2) as ( \varepsilon(i,j) ); 25 ( \varepsilon_j )</td>
</tr>
<tr>
<td>( \lambda )</td>
<td>Difference-set parameter, 2.2(6)</td>
</tr>
<tr>
<td>( \mu )</td>
<td>Mean of ( { a_i } )</td>
</tr>
<tr>
<td>( \rho_s )</td>
<td>Normalized correlation coefficient, 2.2(4)</td>
</tr>
<tr>
<td>( \sigma, \tau )</td>
<td>Delay in correlation functions</td>
</tr>
</tbody>
</table>

**Suffixes**

The following are used as integer suffixes throughout:

\( i,j,k,l,m,n,r,s,t,u,v \). The usual meanings assigned to them are:

- \( i \) varies from 1 to \( N \) over one cycle of the input 14
- \( l, u \) shift-and-add suffixes, 5(25),(29),(48) 60
- \( m, v \) shift-and-subtract suffixes, 5(48) 65
- \( s \) separation between terms in correlation, 2.1(1) 14

In Section 3.2, suffixes and brackets are used interchangeably.

**Operations**

- \( +, \odot \) Modulo-\( q \) addition, subtraction 17
- \( a(X) \cdot b(X) \) 'Binary' multiplication of polynomials 3.3(7) 29
1. INTRODUCTION AND CONCLUSIONS

1.1. Statement of the problem

Identification of a system S implies constructing a model M of S which can represent S for a particular purpose. In the words of Eykhoff (1966), M is 'A representation of the essential aspects of a planned or an existing system, which provides the information about that system in a usable form'. In practice, M will normally be a set of equations of a chosen form, containing a limited number of parameters whose values are to be adjusted so that the behaviour of M is acceptably close to that of S over a selected set of conditions.

The systems envisaged here are dynamical, i.e. they can be described by integrodifferential equations with time as the independent variable. We restrict our study to systems which are time-invariant, i.e. their parameters do not change with time; and for convenience we generally assume that noise is absent, i.e. that the output is due solely to the input or inputs, with no contribution from disturbances or errors of measurement.

Periodic digital step sequences are a comparatively new form of input for identifying dynamical systems; they are periodic signals, having two or more discrete levels, and with no change in level occurring except at equally-spaced time instants. These sequences have the advantage over the traditional 'sinewave' input of containing a spectrum of discrete frequencies, and hence giving more information per test; and they are superior to the traditional 'step' or 'impulse' input in the presence of random noise, whose effect can be reduced by averaging over a number of cycles of the periodic sequence.

As explained in Section 2.1, sequences with the so-called 'pseudorandom' property have certain advantages of convenience over other periodic sequences in identifying the linear kernel or 'impulse response' of a system. In 1964, when this work was begun, several types of pseudorandom sequence were known, notably the maximum-length or m-sequences and the quadratic-residue sequences. These had been successfully used to find the linear kernel of a single-input system; the main object of the present study has been to look into the correlation equations for multi-input linear, and nonlinear, systems, using either pseudorandom sequences or sequences derived from these.
1.2. Outline of the research

The theory of pseudorandom sequences is in much the same state now (1969) as in 1964; it has been well summarized by Everett (1966) who himself discovered a number of pseudorandom sequences. No new sequences have been found in the course of the present work, but Chapter 2 gives a survey of the existing theory.

Original work begins in Chapter 3. Before the limitations on the independence of the correlation equations were understood, the work described in Sections 3.1 to 3.6 had been undertaken, with the intention of applying it to the identification of multi-input linear systems. Later, the results were systematized by the study of sampled m-sequences (Section 3.7), and by an appreciation of work by Gold (1968) on three-level crosscorrelation sequences. Gold's proof of the existence of such sequences for all odd $n$ is the first significant result in this field.

The central result in Chapter 4 is believed to be new: two or more pseudorandom binary sequences of period $N$, when applied simultaneously to a multi-input linear system, reduce in a defined way to exactly $N$ independent equations for the locally-averaged values of the kernels, which we call the 'weights' of the system; it is assumed, both here and in the nonlinear case, that the input/output correlations are available only for integer values of the 'delay'. This result has been published (Ream 1967), and the publication is attached as Annex 1.

Original work on nonlinear correlation is described in Sections 5.2 to 5.7. It is there shown that three types of pseudorandom sequence all give exactly $N$ independent equations for the kernels in the Volterra functional-power-series expansion of the output, to whatever order of approximation we may take this expansion. Although the theory of the approximation, based on the minimum-mean-square-error criterion, is known, the derivation of the exact form of the equations for a periodic-step-sequence input is new, and so is the discovery and proof of the redundancy of these equations.

Appendix 1 gives the first known proof of an important property of binary m-sequences noticed by Barker (1967), that the starting-point of a cycle can always be chosen so as to make the first moment vanish; this proof has been published (Ream 1968). Counter-examples are given for some ternary m-sequences.
1.3. Conclusions; suggestions for further work

The main conclusion is that, perhaps for all periodic step sequences, certainly for all those we have studied, the correlation equations reduce to exactly \( N \) independent equations for identifying the system weights; this applies to the multivariable and to the nonlinear types of system, as well as to the single-input linear systems. Here, \( N \) is the overall period of the response of the system - the l.c.m. of the input periods - and the conditions under which the result holds are that the response has become periodic, the inputs change in synchronism, and the delay times of the input/output crosscorrelations are the integers 1 to \( N \).

A non-rigorous argument in support of this conclusion is as follows: the effect of restricting delay times to integer values is equivalent to sampling the output at the rate of one sample per unit time; hence, components of the output signal having frequency \( f \) (in cyclic measure) such that \(|f| > \frac{1}{2}\) cannot be separated from those with \(|f| < \frac{1}{2}\). If the input and output have period \( N \), they contain only components having frequency \( f = (r/N) \), \( r = 0, \pm 1, \pm 2, \ldots \). If \( N \) is odd, the range \(|f| < \frac{1}{2}\) corresponds to \(-\frac{1}{2}(N-1) < r < \frac{1}{2}(N-1)\), comprising \( N \) values of \( r \). Hence at most \( N \) independent equations can be obtained by correlation. This argument needs sharpening and extending to \( N \) even; moreover, since correlation takes no account of the phase of the frequency components, it might be expected that only positive frequencies should be considered.

Even when such a result is established, however, it is another matter to show the manner in which the reduction is effected.

The fact that this result was not discovered earlier is perhaps due to the practice of using large values of \( N \). This is done so as to make the period long compared to the 'settling time' of the system, but it means that, unless conditions are stationary to an unusual degree, correlation can extend over only a few cycles. The measured values will then be poor estimates under noisy conditions.

The following are suggestions for further work:

1. Crosscorrelation of pairs of binary \( m \)-sequences with \( n = 9, 11, \ldots \), to check the conjectural principle stated in Section 3.9 and to extend Gold's approach;

2. The detailed study, for nonlinear identification, of the reduction of the correlation equations for sequences other than binary or ternary \( m \)-sequences;
3. A closer comparison of the merits of binary and ternary input sequences for nonlinear identification; binary inputs are generally simpler to apply to real systems;

4. If ternary inputs have the advantage, it may be worth while to look for some class of ternary sequences which may be derived from quadratic-residue sequences, in order to fill the gaps caused by the 3:1 ratio between the periods of successive orders of ternary m-sequences.
2. PSEUDORANDOM SEQUENCES

2.1. The use of pseudorandom sequences in system identification

For a linear system whose output $y(t)$ is due solely to the input $x(t)$, the following equation holds:

$$y(t) = \int_{0}^{\infty} h(u) x(t-u) \, du$$  \hspace{1cm} (1)

where $h(t)$ is the kernel or 'weighting function' of the system.

Given a complete record of $x(t)$ and $y(t)$ we can in principle solve (1) for $h(t)$ and thus identify the system. In particular, by using as input an acceptable approximation to the unit impulse or Dirac function $\delta(t)$, we get the convenient form

$$h(t) = y(t) .$$  \hspace{1cm} (2)

The correlation approach is used instead of (1) when the relationship between input and output is not sufficiently linear, or when the output is affected by additive disturbances or 'noise'. We are then interested in the 'best linear approximation' to the observed $y(t)$ for given $x(t)$, and we seek the function $h(t)$ which minimizes the meansquare error

$$\frac{1}{T} \left[ \int_{t}^{t+T} \left( y(t) - \int_{0}^{\infty} h(u) x(t-u) \, du \right)^2 \right] .$$

In Section 5.1 we show that this approach leads to the correlation equation

$$R_{xy}(\tau) = \int_{0}^{\infty} h(u) R_{xx}(\tau-u) \, du$$  \hspace{1cm} (3)

where

$$R_{xx}(\tau) = \overline{x(t) x(t+\tau)}$$  \hspace{1cm} (4)

is the 'input autocorrelation function' (the bar denotes time-averaging), and

$$R_{xy}(\tau) = \overline{x(t) y(t+\tau)}$$  \hspace{1cm} (5)

is the 'input/output crosscorrelation function'. Again, by using as input an acceptable approximation to 'white noise'

$$R_{xx}(\tau) = \delta(\tau)$$, we get the convenient form

$$h(t) = R_{xy}(t) .$$  \hspace{1cm} (6)
Because no random input is repeatable, however, and since extraneous noise is not known a priori but only through its effect on the output, it proves difficult to distinguish one from the other and to assign confidence limits to the calculated $h(t)$. Moreover, the correlation operations in (4) and (5) are not easy to mechanize. For these reasons, and others connected with the nature of the physical input in many systems, it is advantageous to use an input with the following properties:

(a) Periodic, so that the disappearance of the initial transient can be recognized, and the correlations can be computed over a whole number of cycles

(b) Discrete-level, to simplify the delay and multiplication in (4) and (5)

(c) Time-quantized, i.e. changing only at discrete instants - these are normally made equally-spaced, in which case (3) becomes a set of linear simultaneous algebraic equations in a set of averaged 'weights' - see Chapters 4 and 5.

The final simplification, which introduces the property of 'pseudorandomness', is to seek classes of such 'periodic step sequences' which resemble white noise insofar as they lead to an equation similar to (6). The rest of this chapter contains a review of some types of pseudorandom sequence, with a brief account of those properties which are relevant to system identification.

2.2. Pseudorandom binary sequences

Let $\{a_i\}$, $i = 0, \pm 1, \pm 2, \ldots$, be a periodic binary sequence, of period $N$, with levels $\pm 1$. Define the correlation sequence $\{r_s\}$ as

$$r_s = \sum_{i=1}^{N} a_i a_{i+s}, \quad s = 0, \pm 1, \pm 2, \ldots.$$  

(1)

This too is periodic with period $N$; and $r_0 = N$. The sequence $\{a_i\}$ is pseudorandom, in the sense of Section 2.1, if $r_s \ll N$ for all $s \neq 0 \mod N$.

From (1) and the periodicity of $\{a_i\}$ we have

$$\sum_{s=0}^{N-1} r_s = \sum_{i=1}^{N} a_i \sum_{s=0}^{N-1} a_{i+s} = (\sum_{i=1}^{N} a_i)^2.$$  

(2)
The sequence \( \{a_i\} \) is said to have 'two-level correlation' if \( r_s = k, \) say, for all \( s \not\equiv 0 \mod N. \) In this case (2) gives

\[
N + (N-1)k = N^2 \mu^2 \tag{3}
\]

where \( \mu \) is the mean of the sequence. The normalized correlation coefficient \( \rho_s \) defined as

\[
\rho_s = \frac{\sum_{i=1}^{N} (a_i - \mu)(a_{i+s} - \mu)}{\sum_{i=1}^{N} (a_i - \mu)^2} \tag{4}
\]

has \( \rho_0 = 1; \) and for \( s \not\equiv 0 \mod N, \) equations (1) to (4) give

\[
\rho_s = \frac{k - N\mu^2}{N(1 - \mu^2)} = \frac{1}{N - 1}. \tag{5}
\]

This analysis has been included to show that, as might be expected but contrary to some opinion, a binary sequence with two-level correlation has a correlation which is independent of the mean. Moreover, as we show in Section 4.3, equations can be derived for the linear system 'weights' in terms of \( \rho_s \) alone; hence we may regard a binary sequence with two-level correlation as pseudorandom if \( N \gg 1. \)

Useful sources of information on sequences with two-level correlation are Golomb (1964) and Everett (1966). Everett, in particular, explores the following interesting connection between such sequences and the theory of difference sets.

A set \( S_1, \ldots, S_m \) of distinct elements of an Abelian group \( G \) of \( N \) elements is called a difference set (Hall 1956, Mann 1965) with parameters \( (N, m, \lambda), \) if every nonzero element of \( G \) can be written as the difference of two elements in exactly \( \lambda \) ways. It follows, by counting the total number of such differences, that

\[
\lambda(N - 1) = m(m - 1). \tag{6}
\]

Now suppose the binary sequence \( \{a_i\} \) has correlation levels \( N \) and \( k, \) and let \( m \) be the number of positive elements in one cycle of the sequence; then (2) gives

\[
N + k(N - 1) = (2m - N)^2. \tag{7}
\]
Let the consecutive pair \((1,-1)\) occur \(m-\lambda\) times in one cycle, then \((-1,1)\) also occurs as a consecutive pair \(m-\lambda\) times, so from (1) we have

\[
 r_A = (-1) \cdot 2(m - \lambda) + 1 \cdot (N - 2m + 2\lambda).
\]

Since \(r_A = k\) by hypothesis, this gives

\[
k = N + 4(\lambda - m).
\]  

(8)

Eliminating \(k\) from (7) and (8) yields (6); hence (6) is a necessary condition for the existence of a binary sequence with two-level correlation, as well as for the existence of a difference set. It is not, however, a sufficient condition for either; Everett gives a list of solutions of (6) up to \(\lambda = 49\), \(m-\lambda = 50\), and he finds the two-level-correlation solutions to be a small subset of the class of difference sets in this range. It is probable, but it has not been proved, that all two-level-correlation solutions correspond to difference sets.

The more important types of pseudorandom binary sequence—the maximum-length and the quadratic-residue sequences—are described in the next two sections. We conclude this section with a brief account of two further types of binary sequence with two-level correlation, and another two types which are pseudorandom in a looser sense.

1. An \(e^{th}\)-power-residue sequence of period \(N\) is defined as:

\[
a_i = 1 \text{ if } i \text{ is an } e^{th}\text{-power residue mod } N; \text{ otherwise } a_i = -1.
\]

For some values of \(e\), such residues are associated with difference sets (Mann 1965), and Everett (1966) has used this relationship to find a number of such sequences with two-level correlation, for \(e \leq 14\).

2. Everett shows that a binary sequence derived from a non-binary \(m\)-sequence (Section 2.5) by replacing all the nonzero elements by ones, has two-level correlation. Neither these, nor the \(e^{th}\)-power-residue sequences with \(e > 2\), appear to have any
advantage as system inputs over the sequences to be described in the next sections; and they have the disadvantage of having many more elements of one level than of the other.

3. By inverting certain elements of a two-level-correlation sequence of period \( N \), one may obtain a sequence of period \( N = 2^N \) whose autocorrelation \( \rho_s \) takes values 1 or -1 for \( s \equiv 0 \mod N \), but is otherwise small; such behaviour may be termed 'weakly pseudorandom'. The reason for this inversion is to obtain pairs of sequences with negligible crosscorrelation, in order to identify multivariable systems, and a fuller account of them is given in Section 4.2.

4. Brown and Goodwin (1967) found some 'maximally orthogonal sequences' having \( N \) even and

\[
\begin{align*}
 r_s &= N, \ s \equiv 0 \mod N; \\
 4 - N, \ s \equiv 2N \mod N; \\
 0 \text{ otherwise.}
\end{align*}
\]

These weakly pseudorandom sequences have not been related to any other type; particular sequences were found with the aid of a computer. No application to system identification has been reported.

2.3. Binary maximum-length sequences (m-sequences)

In this section we define m-sequences and show they have two-level correlation. These sequences have many interesting properties; the best account of them is by Zierler (1959).

Let \( \{b_i\} \) be a binary sequence with elements from the \((0,1)\) field, and let these elements satisfy the linear recurrence equation

\[
g_0 b_i \oplus g_1 b_{i-1} \oplus \cdots \oplus g_n b_{i-n} = 0, \quad i = 0, \pm 1, \pm 2, \ldots \quad (1)
\]

The \( g \)'s are elements of the \((0,1)\) field, and all operations are in that field, e.g. \( 1 \oplus 1 = 0 \). Then if the polynomial

\[
g(x) = g_0 + g_1 x + \cdots + g_n x^n
\]

(2)
is primitive and irreducible, i.e. it has no factors in this field and it divides $X^p - 1$ for $p = 2^n - 1$ but for no smaller value of $p$, then the sequence $\{b_i\}$ has period $N = 2^n - 1$. No greater period is possible, since this is the number of nonzero $n$-digit binary numbers, and by (1) no such binary number can appear more than once per period as a set of $n$ consecutive $b_i$, nor can the zero set occur. The sequence generated by a primitive irreducible $g(X)$ is therefore called a maximum-length or m-sequence.

An m-sequence is completely specified, except for its starting point, by its generating polynomial; for example, $1 + X + X^3$ generates $\{b_i\} = 0011101, 0011101, \ldots$, or any translate of this.

To prove two-level correlation we need the following properties of binary m-sequences:

A. Each cycle contains $2^n - 1$ zeros and $2^n - 1$ ones, from a count of the $n$-digit binary numbers

B. Every translate of $\{b_i\}$ satisfies (1), and any sequence satisfying (1) is a translate of any other such sequence. The sum of any two translates also satisfies (1), and is thus either a translate or the zero sequence.

If $\{a_i\}$ is derived from $\{b_i\}$ by mapping $(0,1)$ onto $(1,-1)$, then addition in the $b$-field corresponds to multiplication in the $a$-field.

The property corresponding to A above is therefore:

$$\sum_{i=1}^{N} a_i = (2^{n-1} - 1) - 2^{n-1} = -1 \quad (3)$$

Property B states that for all $i$ and for $s \not\equiv 0 \mod N$, there exists $t = t(s) \not\equiv 0 \mod N$ such that

$$b_i \oplus b_{i+s} = b_{i+t} \quad (4)$$

In the $a$-field this gives:

$$a_i \cdot a_{i+s} = a_{i+t} \quad (5)$$

From (3), (5) and 2.2(1) we have

$$r_s = \sum_{i=1}^{N} a_{i+t} = -1 \quad (6)$$

This establishes the two-level correlation.
2.4. Quadratic-residue sequences

A quadratic-residue sequence of period \( N \) is defined by

\[
    a_i = \left( \frac{i}{N} \right), \text{ i prime to } N, \tag{1}
\]

where the Legendre symbol \( (\frac{i}{N}) \) has the value 1 when \( i \) is a quadratic residue mod \( N \), and -1 when \( i \) is a quadratic nonresidue mod \( N \).

We now show that the sequence has two-level correlation if \( N \) is an odd prime and \( a_0 = 0 \), or if \( N \) is a prime of the form \( 4r - 1 \) and \( a_0 \) has any value. The proof follows Vinogradov (1955: see p71 problem 8a); Everett (1966) gives a similar proof.

Let \( N \) be an odd prime, then (1) defines all \( a_i \) with \( i \not\equiv 0 \mod N \).

From Fermat's theorem \( i^{N-1} \equiv 1 \mod N \), we have \( (\frac{i}{N}) \equiv i^{\frac{N-1}{2}} \mod N \).

Hence

\[
    \left( \frac{ik}{N} \right) \equiv \left( \frac{i}{N} \right) \left( \frac{j^2}{N} \right) \left( \frac{k}{N} \right) \equiv \left( \frac{i}{N} \right) \left( \frac{j}{N} \right) \left( \frac{k}{N} \right) \tag{2}
\]

where \( i, j, k \) are any integers prime to \( N \). From (1) and (2) we have

\[
    a_i a_{i+s} = \left( \frac{i}{N} \right) \left( \frac{i+s}{N} \right). \tag{3}
\]

For each \( i \) there is just one \( j \) such that \( ij \equiv 1 \mod N \). As \( i \) goes through values 1 to \( N-1 \), \( j \) goes through the same set in another order, and so therefore does \( sj \) provided \( s \) is prime to \( N \). For such an \( s \), choose \( j \) in (3) so that \( ij \equiv 1 \mod N \), and sum over \( i \), then

\[
    \sum_{i=1}^{N} a_i a_{i+s} = (a_0 a_s + a_{-s} a_0) + \sum_{i} \left( \frac{1+s}{N} \right). \tag{4}
\]

In this equation, the terms omitted in the final summation are:

- \( i = N \) for which \( j \) is not defined;
- \( i = N-s \) for which \( ij + sj \equiv 0 \mod N \); or \( 1+sj \equiv 1-ij \equiv 0 \mod N \). Hence \( 1+sj \) goes through all residues mod \( N \) except \( 0 \) and \( 1 \), and (4) gives

\[
    r_s = a_0 (a_s + a_{-s}) + \sum_{k=2}^{N-1} a_k = a_0 (a_s + a_{-s}) - 1. \tag{5}
\]

The second equality follows from the fact that \( \sum_{k=1}^{N-1} a_k = 0 \) (equal numbers of residues and nonresidues) and that \( a_1 = 1 \) by Fermat's theorem.
From (5), the sequence \( \{a_n\} \) has two-level correlation if \( a_0 = 0 \) - in which case the sequence is no longer binary - or if \( a_s + a_{-s} = 0 \), for all \( s \) prime to \( N \). Now from (1) and (2) we have

\[
a_{-s} = \left( \frac{-s}{N} \right) = \left( \frac{-1}{N} \right) \left( \frac{s}{N} \right) = a_{-1} a_s
\]

\[
= (-1)^{\frac{1}{2}(N-1)} a_s \quad \text{by Fermat's theorem.}
\]

Hence \( a_s + a_{-s} = 0 \) if \( \frac{1}{2}(N-1) \) is odd, i.e. if \( N = 4r - 1 \). In this case the sequence has two-level correlation whatever the value of \( a_0 \), but this value is usually taken as \( \pm 1 \) to preserve the binary form of the sequence. Note that this condition on \( N \) is equivalent to 2.2(8).

2.5. Some nonbinary pseudorandom sequences

Nonbinary sequences do not have two-level correlation, and so at best they are 'weakly pseudorandom' in the sense of Section 2.2.

1. The most important type are \( m \)-sequences; to obtain nonbinary \( m \)-sequences one merely substitutes for the binary field the field of \( q = p^m \) elements where \( p \) is any prime (Zierler 1959).

A nonbinary \( m \)-sequence is not necessarily pseudorandom, since for \( q > 2 \) it is not possible to choose the elements of the \( a \)-field and the \( b \)-field so that multiplication in the one corresponds to addition in the other (unless complex values are allowed, in which case the \( a \)-elements can be the \( q \)th roots of unity). However, if \( q \) is a small prime, and the field elements are taken as the integers centred on zero, Zierler shows that the \( m \)-sequences are in fact pseudorandom; the correlations being zero except for the following:

<table>
<thead>
<tr>
<th>( q )</th>
<th>( \text{elements} )</th>
<th>( r_0 = -r_{\frac{1}{2}N} )</th>
<th>( r_{N/6} = r_{5N/6} = -r_{\frac{3}{2}N} = -r_{\frac{5}{2}N} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0, ±1</td>
<td>( 2 \cdot 3^{n-1} )</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0, ±1, ±2</td>
<td>( 2 \cdot 5^n )</td>
<td>( 4 \cdot 7^n )</td>
</tr>
<tr>
<td>7</td>
<td>0, ±1, ±2, ±3</td>
<td></td>
<td>( 2 \cdot 7^n )</td>
</tr>
</tbody>
</table>

where \( N = q^n - 1 \).
As before, each nonzero n-digit q-ary number occurs exactly once per cycle of the q-ary m-sequence. A feature which only appears for $q > 2$ is that the cycle comprises $q - 1$ blocks, each of $(q^n - 1)/(q - 1)$ elements, such that the elements of one block are $\gamma$ times the elements of another, where $\gamma$ is some $(q - 1)^{th}$ root of unity in the q-element field. In particular, if $q$ is an odd prime and the element field is taken as in the above table, then one half-cycle of the sequence is the negative of the other half; this property is valuable in the correlation analysis of nonlinear systems, and is dealt with in detail in Section 5.4.

2. Certain pairs of binary m-sequences yield three-level crosscorrelation or 'product' sequences. As shown in Section 3.8, Gold (1968) has proved their existence for all odd $n$, and since the 'zero' elements of such a product sequence or 'Gold sequence' coincide with the zero elements $b_i$ of a binary m-sequence, Briggs and Godfrey (1968) suggest using them for system-identification; but so far no results have been reported.

2.6. Conclusions

Of the binary sequences with two-level correlation, none but the maximum-length and the quadratic-residue sequences seem worth considering for system identification. The only advantage of the quadratic-residue type appears to be that primes of the form $4r - 1$ are more numerous than values of $2^n - 1$; otherwise, m-sequences are simpler to generate and have a simpler algebraic structure.

Of the other binary and nonbinary sequences mentioned in this chapter, the advantages lie in the identification of nonlinear systems (Chapter 5).
3. CROSSCORRELATION OF EQUAL-LENGTH PAIRS OF BINARY M-SEQUENCES

3.1. Introduction. Frequency distributions for \( N \leq 255 \)

In this chapter we examine some features of the crosscorrelation or 'product' sequences formed from two binary m-sequences of period \( N \). The original aim was to find pairs of sequences with negligible crosscorrelation, for use as inputs in identifying multivariable linear systems. No such pairs were found, and it is likely that none exist, since according to Briggs and Godfrey (1966), a pair of two-level-correlation sequences can only have zero crosscorrelation if their periods are coprime. Moreover, the author's work on multivariable systems (Ream 1967 and Chapter 4) indicates that the degree of crosscorrelation is not relevant there.

Sections 3.1 to 3.7, which are believed to be new, are therefore presented as a contribution to the theory of binary m-sequences. Section 3.8 gives an account of work by Gold (1968) proving the existence of ternary product sequences for all odd \( n \), which had been suspected from the formulae for the first four moments (Sections 3.2 and 3.5).

We denote the pair of binary m-sequences by \( \{a_i\}, \{b_i\} \); the element field will be taken to be either \((0,1)\) or \((1,-1)\) as convenient. Using the \((1,-1)\) field we define the crosscorrelation sequences as \( \{C_s\} \) with

\[
C_s = \sum_{i=1}^{N} a_i b_{i+s} ;
\]

the corresponding sequence for the \((0,1)\) field will be used in Section 3.3 and written \( \{p_s\} \).

Property A of Section 2.3 implies that, in the \((1,-1)\) field, if the pair \( a_i = b_{i+s} = -1 \) occurs \( 2^{n-2} - c_s \) times, say, in the sum (1), then the frequency of the other pairs is as follows:

\[
\begin{align*}
  a_i = 1, b_{i+s} = -1 & : 2^{n-2} - c_s \\
  a_i = -1, b_{i+s} = 1 & : 2^{n-2} - c_s \\
  a_i = b_{i+s} = 1 & : 2^{n-2} + c_s + 1 .
\end{align*}
\]
Substituting these values in (1) gives
\[ C_s = 4c_s - 1; \]  
(2)

c_s is an alternative, and in some respects more convenient, 
crosscorrelation parameter to replace C_s.

Frequency distributions of c_s for all pairs of binary m-sequences 
with n \leq 8 (N \leq 255) were found by computation. They were found to 
belong to one of three types as shown by the list in Table 3.1:

Type 0 distributions contain both odd and even values of c_s
Type 1 distributions contain odd and even multiples of 2, only
Type 2 distributions contain odd and even multiples of 4, only.

This classification will be discussed in Section 3.3.

3.2. Moments of the frequency distribution

Let \( f_c(x) \) be the number of values of s, in one cycle of the 
crosscorrelation sequence, for which \( C_s = x \). The \( r \)th moment of 
\( f_c(x) \), \( M_r \), is defined as
\[ M_r = \sum_s \left( \sum_i a_i b_{i+s} \right)^r. \]  
(1)

In this section, summations are over the range 1 to N unless 
otherwise shown, and we may write \( a(i) \) for \( a_{i1} \), etc., to avoid 
clumsy suffixes. The analysis is based on changing the order of 
summation in (1) to give
\[ M_r = \sum_{i_1, i_2, \ldots, i_r} a(i_1) \ldots a(i_r) S(i_1, i_2, \ldots, i_r) \]  
(2)

where
\[ S(i_1, \ldots, i_r) = \sum_s b(i_1 + s) \ldots b(i_r + s). \]

We proceed to obtain formulae for the moments up to \( M_4 \).

1. From (1), \( M_0 = N \). From 2.3(3) we have \( S(i) = -1 \), so for the 
first moment (2) gives
\[ M_1 = \sum_i a_i S(i) = -\sum_i a_i = 1. \]  
(3)

2. For the second moment, we note that \( S(i, j) \) is the 
autocorrelation \( r_{i-j} \) of the sequence \( \{b_i\} \) (see 2.2(1)). We have 
\( r_0 = N \), and by 2.3(6), \( r_s = -1 \) for \( s \neq 0 \) mod \( N \); we may therefore
Table 3.1. Frequency distributions of $c_s$  
Values of $f(x)$ for sequences with $3 \leq n \leq 8$

**Type 0 distributions**

<table>
<thead>
<tr>
<th>x</th>
<th>-7</th>
<th>-6</th>
<th>-5</th>
<th>-4</th>
<th>-3</th>
<th>-2</th>
<th>-1</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>n = 3</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>10</td>
<td>5</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>7</td>
<td>12</td>
<td>12</td>
<td>6</td>
<td>9</td>
<td>8</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>7</td>
<td>8</td>
<td>21</td>
<td>7</td>
<td>14</td>
<td>21</td>
<td>7</td>
<td>14</td>
<td>14</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td>8</td>
<td>18</td>
<td>24</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>20</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>20</td>
<td>8</td>
<td>5</td>
</tr>
</tbody>
</table>

**Type 1 distributions**

<table>
<thead>
<tr>
<th>x</th>
<th>-10</th>
<th>-8</th>
<th>-6</th>
<th>-4</th>
<th>-2</th>
<th>0</th>
<th>2</th>
<th>4</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>n = 3</td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>15</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>18</td>
<td>27</td>
<td>12</td>
<td>4</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>14</td>
<td>28</td>
<td>35</td>
<td>28</td>
<td>14</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Type 2 distributions**

<table>
<thead>
<tr>
<th>x</th>
<th>-16</th>
<th>-12</th>
<th>-8</th>
<th>-4</th>
<th>0</th>
<th>4</th>
<th>8</th>
<th>12</th>
<th>16</th>
<th>20</th>
<th>24</th>
</tr>
</thead>
<tbody>
<tr>
<td>n = 3</td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>47</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>28</td>
<td>63</td>
<td>36</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8a</td>
<td>96</td>
<td>59</td>
<td>96</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b</td>
<td>88</td>
<td>87</td>
<td>64</td>
<td>8</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c</td>
<td>88</td>
<td>89</td>
<td>56</td>
<td>20</td>
<td>0</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d</td>
<td>18</td>
<td>48</td>
<td>100</td>
<td>84</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e</td>
<td>1</td>
<td>0</td>
<td>8</td>
<td>64</td>
<td>100</td>
<td>68</td>
<td>10</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>f</td>
<td>16</td>
<td>52</td>
<td>104</td>
<td>68</td>
<td>14</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g</td>
<td>8</td>
<td>60</td>
<td>108</td>
<td>76</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>h</td>
<td>80</td>
<td>119</td>
<td>16</td>
<td>40</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
write $S(i,j) = (N + 1) \epsilon(i,j) - 1$, where

$$\epsilon(i,j) = \begin{cases} 1 & \text{if } i - j \equiv 0 \mod N \\ 0 & \text{otherwise} \end{cases}$$

(4)

Then with $r = 2$, (2) becomes

$$M_2 = (N + 1) \sum a_i^2 - (\sum a_i)^2 = N(N + 1) - 1 \text{ by 2.3(3).}$$

(5)

3. The above moments depend only on $N$, but higher moments bring in Property B of Section 2.3, and they can be different for different pairs of sequences. Denote the $i$th translate of \{b_i\} by $i^b$; then in the $(0,1)$ field there will be some $i,j,k$ for which, by 2.3(4),

$$ib + jb + kb \equiv 0 \mod N \tag{6}$$

Values of $k$ satisfying (6) may be written

$$k = k(i,j) = i + t' \text{ where } t' = t'(j-i) \tag{7}$$

A similar relationship holds when $i,j,k$ satisfy

$$ia + ja + ka \equiv 0 \tag{8}$$

let the corresponding values of $k$ be

$$k = i + t \text{ where } t = t(j-i) \tag{9}$$

4. For the third moment, we need to evaluate

$$S(i,j,k) = \sum s b_{i+s} b_{j+s} b_{k+s} .$$

The following cases arise:

Two or three suffixes equal; then $S(i,j,k) = -1$

The suffixes satisfy (6); then each term in the sum is 1, so $S(i,j,k) = N$

Otherwise, the terms are a translate of \{b_i\}, so $S(i,j,k) = -1$.

Substituting these values into (2) with $r = 3$ gives

$$M_3 = (N + 1) \sum' a_i a_j a_k - (\sum a_i)^3$$

$$= (N + 1) \sum' a_i a_j a_k + 1 \tag{10}$$

where the summation $\sum'$ is over all sets of suffixes satisfying (6).

In the notation of (7) and (9), we can write this sum as
\[ \sum' a_i a_j a_k = \sum_{i=1}^{N} \sum_{j=1}^{N-1} a_{i+j} a(i+t_j'). \]

Its value thus depends on the number, \( N_1 \) say, of 'correspondences' between \( t_j \) and \( t_j' \) as \( j \) runs through all values; in the notation of (4) we have

\[ N_1 = \sum_{j=1}^{N-1} \mathcal{E}(t_j, t_j'). \]

Substituting (12) into (11) gives

\[ \sum' a_i a_j a_k = NN_1 - (N - 1 - N_1), \]

and substituting (13) into (10) gives

\[ M_3 = (N + 1)^2 N_1 - N^2 + 2. \]

5. The same approach is used in deriving the fourth moment. We have

\[ S(i,j,k,l) = \sum b_{i+s} b_{j+s} b_{k+s} b_{l+s} \]

and so

\[ M_4 = (N + 1) \sum'' i,j,k,l a_i a_j a_k a_l - 1, \]

where the summation \( \sum'' \) is over all sets of suffixes satisfying

\[ i^b + j^b + k^b + l^b = 0. \]

Three such sets of suffixes may be distinguished: (a) all equal, (b) equal in pairs (three ways), (c) unequal. Let

\[ \sum'' i,j,k,l a_i a_j a_k a_l = S_a + S_b + S_c, \]

where the three terms correspond to categories (a) to (c) above.

The first two terms are given by

\[ S_a = N; \quad S_b = 3 \sum a_i^2 \sum_{j=1}^{N-1} a_j^2 = 3N(N - 1). \]

In (c), there is just one \( l \) satisfying (16) for each triad \( i,j,k \), except when the triad satisfies (6) in which case there is no such \( l \). Write the value of \( l \) satisfying (16) as

\[ l = l(i,j,k) = i + u' \quad \text{where} \quad u' = u'(j-i,k-i); \]

then (17) gives

\[ S_c = \sum' i,j,k a_i a_j a_k a(i+u'_j k), \]

where the summation \( \sum' \) extends over all \( i, j \neq i \), and all \( k \) except the values \( i, j, \) and \( i + t' \) as given by (7).
As in (11), we write (20) as

\[ S_c = \sum_{j,k} \sum_i a(i + u_{jk}) a(i + u'_{jk}) \]  \( (21) \)

where \( u \) is defined for the sequence \( \{a_i\} \) in the same way as \( u' \) was defined for \( \{b_i\} \) in (19). Let \( N_2 \) be the number of correspondences between \( u_{jk} \) and \( u'_{jk} \) as \( j,k \) run through all the values included in (21), i.e.,

\[ N_2 = \sum_{j,k} \varepsilon(u_{jk}, u'_{jk}) \]  \( (22) \)

there are \( N - 1 \) values of \( j \) and \( N - 3 \) values of \( k \) in this summation, so from (21) and (22) we have

\[ S_c = (N + 1) N_2 - (N - 1)(N - 3) \]  \( (23) \)

Substituting (18) and (23) into (17), the resulting equation into (15), and this in turn into (45), gives finally

\[ N_4 = (N + 1) \left\{ (N + 1) N_2 + (2N^2 + 2N - 3) \right\} - 1 \]  \( (24) \)

6. The moments \( m_r \) of the frequency distribution of \( c \), \( f_c(x) \), whose values are set out in Table 3.1, are obtained from 3.1(2) and the equations (3), (5), (14) and (24) of this section. They are conveniently expressed in terms of \( 2^n = N + 1 \), and are found to be

\[
\begin{align*}
    m_1 &= 2^{n-2} \\
    m_2 &= 2^{2n-4} \\
    m_3 &= 2^{2n-6}(2 + N_1) \\
    m_4 &= 2^{2n-8}(2^{n+1} + 4N_4 + N_2^n).
\end{align*}
\]

\( (25) \)

Values of \( N_1 \) and \( N_2 \), computed from the data in Table 3.1 by means of (25), are given in Table 3.2.

<table>
<thead>
<tr>
<th>Type 0:</th>
<th>( N_1 ) = 0 for ( n ) odd; ( N_1 = 2 ) for ( n ) even; ( N_2 = 0 ).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type 1:</td>
<td>( n = 5 )</td>
</tr>
<tr>
<td>( \frac{1}{2}N_4 )</td>
<td>0</td>
</tr>
<tr>
<td>( \frac{1}{24}N_2 )</td>
<td>0</td>
</tr>
<tr>
<td>Type 2:</td>
<td>( n = 6 )</td>
</tr>
<tr>
<td>( \frac{1}{2}N_4 )</td>
<td>1</td>
</tr>
<tr>
<td>( \frac{1}{24}N_2 )</td>
<td>5</td>
</tr>
</tbody>
</table>
7. Discussion of the moment analysis. In principle, the above method can be used to derive moments of any order, but for \( r > 4 \) the algebra becomes excessively complicated and brings in higher-order 'correspondences'. Hence the value of the approach depends on the use we can make of the first four moments.

Even the third- and fourth-moment formulae, however, are of doubtful utility, since in general the values of \( N_1 \) and \( N_2 \) are best obtained from the frequency distribution. Only in two cases is more known about their values: (a) for Type 0 distributions the values given in Table 3.2 hold for all \( n \) (Section 3.5); (b) for three-level distributions the values are restricted (Sections 3.5 and 3.8) - but in this case the first and second moments fix the distribution.

Since the frequency distribution gives no clue to the structure of the sequence \( \{c_i\} \), the next step is to try an algebraic approach based on the generating polynomials of the \( m \)-sequences. This is described in the next section.

3.3. Generating-polynomial approach to the determination of the structure of crosscorrelation sequences

In this section the \((0,1)\) field is used exclusively. A generating polynomial for the crosscorrelation sequence may be found as follows: define polynomials

\[
a(X) \equiv \sum_{i=1}^{N} a_i X^{N-i}, \quad b(X) \equiv \sum_{i=0}^{N-1} b_i X^i
\]  

(1)

in terms of the elements of one cycle of the sequences \( \{a_i\} \) and \( \{b_i\} \). Let \( p(X) \) be the polynomial of degree \( N - 1 \) (at most) formed by multiplying \( a(X) \) and \( b(X) \), and then adding the coefficient of \( X^{N+S} \) to that of \( X^S \), i.e.

\[
a(X) b(X) \equiv p(X) \mod (X^N - 1).
\]  

(2)
Then if
\[ p(X) = \sum_{s=0}^{N-1} p_s X^s \quad (3) \]
we have, taking into account the periodicity of the sequences,
\[ p_s = \sum_{i=1}^{N} a_i b_{i+s} \quad (4) \]
Since \( a_i \) and \( b_{i+s} \) are in the \((0,1)\) field, \( p_s \) is the number of pairs \( a_i = b_{i+s} = 1 \), i.e. from Section 3.1
\[ p_s = 2^{n-2} + c_s \quad (5) \]
p(\( X \)) may be called the 'product polynomial' of \( a(\( X \)) \) and \( b(\( X \)) \), and \( \{p_s\} \) the 'product sequence'.

Let \( p^*(\( X \)) \) be the polynomial with binary coefficients \( p^*_s \) derived from \( p_s \) as follows:
\[ p_s \equiv p^*_s \mod 2 \quad p^*(\( X \)) = \sum_{s=0}^{N-1} p^*_s X^s \quad (6) \]
p\(^*(\( X \)) \) may be obtained from \( a(\( X \)) \) and \( b(\( X \)) \) by a form of multiplication analogous to (2), which we call 'binary multiplication' and denote by a dot, i.e.
\[ p^*(\( X \)) = a(\( X \)).b(\( X \)) \quad (7) \]

1. We first examine the case where \( \{a_i\} \) is the reverse of \( \{b_i\} \); we shall call such sequences a 'reversed pair'. No generality is lost by translating one sequence so as to make \( a_i = b_{N-i} \) for all \( i \); then from (1) we have \( a(\( X \)) \equiv b(\( X \)) \). (7) now becomes
\[ p^*(\( X \)) \equiv b(\( X \)).b(\( X \)) \quad (8) \]
In terms of real multiplication we have, since \( b_i^2 = b_i \),
\[ b^2(\( X \)) = \sum_{i=0}^{N-1} b_i X^{2i} + 2 c(\( X \)) \]
where \( c(\( X \)) \) is some polynomial with coefficients 0 or 1. From this equation, together with (2), (6) and (8) we have
\[ p^*_s = b_i \quad \text{where} \quad 2s \equiv i \mod N , \quad (9) \]
i.e. \( \{p_s\} \) is derived from \( \{b_i\} \) by taking every other term. This is called 'sampling' and will be discussed in Section 3.7; here we merely note that the basic equation 2.3(1) can be written using binary multiplication as
\[ g(X) \cdot b(X) = 0 \quad (10) \]

Binary multiplication is associative, so from (8) and (10) we have
\[ g(X) \cdot p^*(X) = \{g(X) \cdot b(X)\} \cdot b(X) = 0 \quad (11) \]

\( g(X) \) is thus a generator of \( p^*(X) \), which, being nonzero by (9),
must accordingly be a translate of \( b(X) \) in the sense that \( \{p_s^*\} \)
is a translate of \( \{b_s\} \). It follows that the even/odd values of \( p_s \)
coincide with the zero/nonzero values of some translate of \( \{b_s\} \).
All the Type 0 distributions of Table 3.1 arise in this way.

2. If the two sequences are not a reversed pair, let their
generating equations be
\[ g_0 a_i + g_1 a_{i+1} + \ldots + g_n a_{i+n} = 0 \quad (12) \]
\[ h_0 b_i + h_1 b_{i-1} + \ldots + h_n b_{i-n} = 0 \quad (13) \]

In terms of the binary multiplication of polynomials, these
equations may be written
\[ g(X) \cdot a(X) = 0 \quad (12) \]
\[ h(X) \cdot b(X) = 0 \quad (13) \]

From (7) and (12) we have, by associativity,
\[ g(X) \cdot p^*(X) = \{g(X) \cdot a(X)\} \cdot b(X) = 0 \quad \text{(14)} \]
and from (7) and (13),
\[ h(X) \cdot p^*(X) = \{h(X) \cdot b(X)\} \cdot a(X) = 0 \quad \text{(15)} \]

(14) implies that \( \{p_s^*\} \) is either a translate of \( \{a_s\} \) reversed, or
the zero sequence; and (15) implies that it is either a translate
of \( \{b_s\} \) or zero. Since \( \{a_s\} \) and \( \{b_s\} \) are not a reversed pair, it
follows that \( p_s^* = 0 \) for all \( s \). Thus all the \( p_s \) are even, and we
can write
\[ p(X) \equiv 2 p_1(X) \quad p_1(X) \equiv \sum_{s=0}^{N-1} \langle p_s^* \rangle X^s \quad (16) \]

where \( p_1(X) \) has integer coefficients. As in (6), we define the
'binary form' of \( p_1(X) \), written \( p_1^*(X) \), by
\[ \langle p_1 \rangle_s \equiv \langle p_1^* \rangle_s \mod 2 \quad p_1^*(X) \equiv \sum_{s=0}^{N-1} \langle p_1^* \rangle_s X^s \quad (17) \]
3. We have now shown that Type 0 distributions arise solely from the crosscorrelation of reversed pairs. To proceed further, we return to (12) and (13), and write the corresponding equations involving 'real' multiplication as

\[ g(X) a(X) = X^N - 1 + 2q(X), \]
\[ h(X) b(X) = X^N - 1 + 2r(X), \]

(18)

(19)

where the coefficients of \( q(X) \) and \( r(X) \) are integers. Now, each binary \( m \)-sequence contains one run of \( n - 1 \) zeros, from the fact that every nonzero \( n \)-digit binary number appears in the sequence; it follows from (1) that by a suitable translation of \( \{a_i\} \) and \( \{b_i\} \) the degree of \( a(X) \) and of \( b(X) \) can be made \( N - n \). Then in (18) and (19), \( q(X) \) and \( r(X) \) have degree \( N - 1 \) at most. No generality is lost by these translations, and from now on they will be assumed to have been effected.

From (2), (16) and (18) we have

\[ \frac{1}{2} g(X) a(X) b(X) \equiv g(X) p_1(X) \mod(X^N - 1) \]
\[ \equiv q(X) b(X) \mod(X^N - 1), \]

whence

\[ g(X) p_1(X) \equiv q(X) b(X) \mod(X^N - 1). \]

(20)

Similarly, (2), (16) and (19) give

\[ h(X) p_1(X) \equiv r(X) a(X) \mod(X^N - 1). \]

(21)

Let \( q^*(X), r^*(X) \) be the binary forms of \( q(X), r(X) \), defined as usual by taking residues mod 2 of the coefficients. Then the binary-multiplication equations corresponding to (20) and (21) are

\[ g(X) p_1^*(X) = q^*(X) b(X), \]
\[ h(X) p_1^*(X) = r^*(X) a(X). \]

(22)

(23)

By Property B of Section 2.3, the right-hand side of (22) is either zero or some translate of \( \{b_i\} \), and the right-hand side of (23) is either zero or some translate of \( \{a_i\} \) reversed. Since the sequences are not a reversed pair, one at least of these right-hand sides must be zero, and so the possibilities are:
(a) Both (22) and (23) zero: then, by a previous argument, 
p^*(X) = 0 and so the p are multiples of 4. The Type 2 distributions of Table 3.1 correspond to this case.

(b) (22) zero, (23) nonzero: here, p^*(X) cannot be zero, so by (22) the sequence \( \{p^*_i\} \) must be a translate of \( \{a_i\} \) reversed, such as to satisfy (23). This case yields a Type 1 distribution.

(c) (22) nonzero, (23) zero: here, \( \{p^*_i\} \) is a translate of \( \{b_i\} \) such as to satisfy (22). Type 1 distribution.

If (22) is zero then q^*(X) must be 'divisible' by h(X) in the sense that a polynomial u(X) exists, of degree less than N, such that
\[
q^*(X) = h(X).u(X). \quad (24)
\]
Similarly, if (23) is zero there exists v(X) such that
\[
r^*(X) = g(X).v(X). \quad (25)
\]
It is shown below that neither q^*(X) nor r^*(X) can be identically zero, so u(X) and v(X) are both nonzero.

4. In case (a) above, write
\[
p(X) = 4p_2(X) \quad (26)
\]
where the coefficients of \( p_2(X) \) are integers, and form the binary polynomial \( p^*_2(X) \) by taking coefficients as mod-2 residues. From (2), (18), (19) and (26) we have
\[
\frac{1}{2} g(X) h(X) a(X) b(X) \equiv g(X) h(X) p_2(X) \mod(X^N - 1)
\]
\[
\equiv q(X) r(X) \mod(X^N - 1),
\]
whence
\[
g(X) h(X) p^*_2(X) \equiv q(X) r(X) \mod(X^N - 1). \quad (27)
\]
The binary form of (27) is
\[
g(X).h(X).p^*_2(X) \equiv q^*(X).r^*(X). \quad (28)
\]
From (24), (25), and (28) we have
\[
g(X).h(X).s(X) \equiv 0, \quad (29)
\]
where
\[
s(X) \equiv p^*_2(X) - u(X).v(X). \quad (30)
\]
To satisfy (29), the sequence \( \{s_i\} \) represented by s(X) must be
(a) zero, (b) a translate of \( \{a_i\} \) reversed, (c) a translate of \( \{b_i\} \), or (d) the sum of (b) and (c).
We now examine the frequency distribution of the coefficients of the polynomials \( q(X) \) and \( r(X) \) defined in (18) and (19); it is sufficient to consider \( q(X) \).

Let \( w \) be the 'weight' of \( g(X) \), i.e. the number of nonzero \( g_i \). \( w \) is odd, since \( g(X) \) is irreducible; if \( w \) were even, \( g(X) \) would be divisible by \( 1 + X \).

Coefficients of value \( y \) in \( q(X) \) are generated by exactly \( 2y \) of the \( w \) 'ones' of \( g_0 \ldots g_n \) pairing with ones of \( \{a_i\} \). Since \( g_0 = 1 \), this occurs whenever either \( 2y \) or \( 2y - 1 \) of \( g_0 \ldots g_n \) are ones pairing with ones of \( \{a_i\} \).

First suppose \( y > 0 \), and consider a particular set of \( 2y \) out of the \( w - 1 \) ones in \( g_1 \ldots g_n \). Since the set of \( n \)-digit subsequences of \( \{a_i\} \) is the set of all \( n \)-digit binary numbers except zero, the number of coefficients \( q_i \) of \( q(X) \) in which just these \( 2y \) digits are paired with ones of \( \{a_i\} \), and the remaining \( w - 2y - 1 \) ones in \( g_1 \ldots g_n \) are paired with zeros, is \( 2^{n-w+1} \). Multiplying by the number of ways of distributing \( 2y \) things among \( w - 1 \) places, and adding the corresponding term for the case when \( 2y - 1 \) ones of 
\( g_1 \ldots g_n \) are paired with ones of \( \{a_i\} \), gives the following formula for the number of \( q_i \) with value \( y > 0 \):

\[
f_q(y) = 2^{n-w+1} \left( \binom{w-1}{2y} + \binom{w-1}{2y-1} \right) = 2^{n-w+1} \binom{w}{2y} . \tag{31}\]

When \( y = 0 \), the number is decreased by one because of the absence of the zero subsequence; hence

\[
f_q(0) = 2^{n-w+1} - 1 . \tag{32}\]

(31) and (32) show that all coefficient values are present in \( q(X) \) up to \( y = \frac{1}{2}(w - 1) \); it follows that \( q^*(X) \) is not identically zero. They also show that the odd and even values are not present in the right numbers for \( \{q_i^*\} \) to be an \( m \)-sequence.

The same analysis and conclusions apply also to \( r(X) \).
6. **Discussion of the generating-polynomial analysis.** The Type 0 distributions have been accounted for; they arise from the cross-correlation of reversed pairs of sequences. In Section 3.7 we show why there is only one Type 0 distribution for each \( n \).

If the sequences are not a reversed pair, we have only shown in general that their product elements \( p_s \) are even. If the distribution is Type 1, then the analysis shows why the even/odd multiples of 2 in \( \{ p_s \} \) form an m-sequence, and it predicts this sequence to be either \( \{ b_1 \} \) or \( \{ a_1 \} \) reversed, but it does not predict which.

If the distribution is neither Type 0 or 1, equations (26) to (30) apply; these do not, however, appear to throw much light on the structure of the product sequence. In the example given in the next section to illustrate the analysis, the distribution is Type 2 and the even/odd multiples of 4 in \( \{ p_s \} \) form an m-sequence. This m-sequence is not a translate of \( \{ b_1 \} \) or \( \{ a_1 \} \) reversed, and the analysis does not predict its occurrence.

The method, then, is of limited value, and further work on such lines is not considered to be of interest.

### 3.4. Example to illustrate the generating-polynomial analysis

All equation numbers in this section refer to Section 3.3.

The pair of sequences to be crosscorrelated have \( N = 127 \), \( n = 7 \). One cycle of each is given below, starting with \( a_1 \) and \( b_0 \). The run of 6 zeros has been put at the beginning of the cycle for \( \{ a_1 \} \) and at the end for \( \{ b_1 \} \), so as to give \( a(X) \) and \( b(X) \) the lowest possible degree of 120. As defined in (1), these polynomials are

\[
\begin{align*}
    a(X) & = X^{120} + X^{117} + \ldots + X^6 + 1 \\
    b(X) & = 1 + X + \ldots + X^{114} + X^{120}.
\end{align*}
\]

The sequences are as follows:
Calculating $p_s$ for these sequences, according to (4), is found to give a three-level sequence with element values 36, 32, 28.

Writing $x$ for 36, $\Theta$ for 32 and $y$ for 28, and starting the cycle at $P_0$, we find:

$$p_s = \overline{000yy} \overline{x00x0} \overline{000y0} \overline{yxx00} \overline{0y000} \overline{0y000} \overline{yxy00} \overline{xy000} \overline{0y000} \overline{x00y0} \overline{0xx0} \overline{x00x0} \overline{000y0} \overline{000yy} \overline{xy000} \overline{xy000} \overline{0x00y} \overline{x0y00} \overline{0xx0} \overline{x00x0} \overline{x00x0} \overline{yxx}$$

Since this is Type 2, the next step is to form the binary sequence $\{p^*_s\}$ by writing 0 for $\Theta$ and 1 for $x$ and $y$. The resulting sequence is in fact an m-sequence generated by $x^7 + x^5 + x^4 + x^3 + 1$.

To find $\{q^*_i\}$ and $\{r^*_i\}$ we need to know the generators of $\{a^*_i\}$ and $\{b^*_i\}$, as defined by (12) and (13). They are:

$$g(X) = 1 + X^4 + X^7, \quad h(X) = X^7 + X + 1.$$  

Then from (18) and (19), by polynomial operation with coefficients in the real-number field, we get

$$q(X) = X^{124} + X^{121} + \ldots + X^4 + 1,$$

$$r(X) = 1 + X + \ldots + X^{120} + X^{121}.$$  

Since $g(X)$ and $h(X)$ are of weight 3, it follows from (31) and (32) that in each cycle of $\{q^*_i\}$ and $\{r^*_i\}$ there are 31 zeros and 96 ones.

The sequences are found to be as follows, starting with $q_0$ and $r_0$:

$$\{q^*_i\} = \overline{10001} \overline{00110} \overline{01101} \overline{11111} \overline{11011} \overline{10110} \overline{11001} \overline{10111} \overline{01111} \overline{01111} \overline{11111} \overline{11111} \overline{11011} \overline{11101} \overline{01110} \overline{11111} \overline{11111} \overline{11111} \overline{11111} \overline{11111} \overline{11011} \overline{11101} \overline{11110} \overline{11110}$$

$$\{r^*_i\} = \overline{11111} \overline{11111} \overline{11110} \overline{11101} \overline{11111} \overline{11110} \overline{11111} \overline{11111} \overline{00111} \overline{11111} \overline{11111} \overline{11111} \overline{11111} \overline{11111} \overline{11110} \overline{10110} \overline{01111} \overline{01110} \overline{11110} \overline{11110} \overline{11110} \overline{10000} \overline{11000} \overline{00}$$

In this example, $q^*_i = q^*_i$ and $r^*_i = r^*_i$. Dividing $q^*(X)$ by $h(X)$, and $r^*(X)$ by $g(X)$, according to (24) and (25), with coefficients in the binary field, gives
\[ u(X) = X^{117} + X^{114} + \ldots + X + 1, \]
\[ v(X) = 1 + X + \ldots + X^{113} + X^{114}. \]

The corresponding sequences, starting with \( u_0 \) and \( v_0 \), are:

\[ \{u_i\} = 11110 \ 00001 \ 01001 \ 00001 \ 00101 \ 01010 \ 11101 \ 11111 \ 11111 \ 00000 \ 00101 \ 01000 \ 10101 \ 10011 \ 00010 \ 00110 \ 10111 \ 10100 \ 00011 \ 01010 \ 01111 \ 00010 \ 00100 \ 00000 \ 00 \]

\[ \{v_i\} = 11110 \ 00100 \ 00111 \ 10011 \ 00101 \ 01101 \ 01110 \ 10001 \ 01001 \ 00111 \ 11001 \ 11011 \ 00001 \ 00110 \ 01010 \ 11001 \ 11010 \ 00111 \ 00001 \ 01011 \ 00000 \ 00 \]

The product \( u(X) \cdot v(X) = z(X) \), say, yields the sequence:

\[ \{z_i\} = 01000 \ 10100 \ 01100 \ 10111 \ 10111 \ 00101 \ 10001 \ 11000 \ 11010 \ 00110 \ 01001 \ 00000 \ 01011 \ 01111 \ 01100 \ 11100 \ 00011 \ 10100 \ 00011 \ 01011 \ 00101 \ 10011 \ 00100 \ 11111 \ 11000 \ 01001 \ 01110 \ 00010 \ 00111 \ 01 \]

Subtracting this from \( \{(p_i)\} \) to form \( \{s_i\} \) according to (30), we get

\[ \{s_i\} = 01011 \ 00110 \ 01100 \ 01011 \ 10100 \ 01101 \ 10011 \ 10111 \ 00110 \ 01100 \ 11110 \ 11011 \ 01101 \ 11111 \ 11000 \ 01001 \ 01110 \ 00010 \ 10011 \ 11101 \ 11001 \ 11000 \ 01111 \ 01 \]

\( \{s_i\} \) is not an \( m \)-sequence, so it must be a sum of a translate of \( \{b_i\} \) and a translate of \( \{a_i\} \) reversed. One way of finding these is to obtain \( g(X) \cdot s(X) \), which equals \( g(X) \cdot b'(X) \) say where \( b'(X) \) is the polynomial representing the translated \( b \)-sequence. This in turn equals \( b''(X) \) say, representing another translate, and we can now find \( b'(X) \) by comparing \( b''(X) \) with \( g(X) \cdot b(X) \). Calculation shows that the sequence corresponding to \( b''(X) \) is \( \{b_i\} \) shifted 87 places to the right, i.e. \( \{b_{i-87}\} \), and that \( g(X) \cdot b(X) \) gives \( \{b_{i-64}\} \); hence the sequence corresponding to \( b'(X) \) is \( \{b_{i-23}\} \). Subtracting the latter from \( \{s_i\} \) is found to give \( s_i = a_{44-i} + b_{i-23} \).

3.5. Ternary crosscorrelation sequences

A feature of Table 3.1 is the presence of distributions having only the values \( c_0 = 0, D, -D \), where \( D \) is some power of 2. We call the corresponding sequences 'ternary' sequences. The 'Gold sequences' described in Section 3.8 are of this form, and they occur for all odd \( n \). In this section we show, from the moment
analysis given in Section 3.2, the possible values of $D$.

Suppose a cycle of the sequence contains $N_0$ terms $c_s = 0$, $N_+$ terms $c_s = D$, and $N_-$ terms $c_s = -D$; then the $r$th moment of $f_c(x)$ is

$$m_r = \sum x^r f_c(x) = D^r \{ N_+ + (-1)^r N_- \}.$$  

From (1) we have

$$N_+ = \frac{1}{2}(D^{-2}m_2 + D^{-1}m_1) = \frac{1}{2}E(E+1),$$  

where from 3.2(25),

$$E = 2^{n-2}D^{-1}.$$  

From (2) we have

$$N_0 = N - N_+ - N_- = N - E^2.$$  

Again, from (1) and 3.2(25) we have

$$16 m_2/m_1 = 16 D^2 = 2^n(2 + N_0);$$  

and

$$16 m_4/m_2 = 16 D^2 = 2^{n+1} + 4N_0 + N_1.$$  

Eliminating $D$ from (5) and (6) gives

$$N_2 = (2^n - 4)N_1.$$  

1. For $n$ odd, the general solution of (5) is

$$D = 2^{\frac{3}{2}(n-3)} + j, \quad N_1 = 2(2^j - 1); \quad j = 0, 1, 2, \ldots.$$  

Then from (3) we have

$$E = 2^{\frac{3}{2}(n-1)} - j,$$  

and since $E$ is an integer, $j$ cannot exceed $\frac{1}{2}(n-1)$. It is found that Gold sequences, and all other ternary sequences with odd $n \leq 7$, have $j = 0$. In this case, from (2), (4), (5), (7), (8), and (9),

$$N_1 = N_2 = 0; \quad D = 2^{\frac{3}{2}(n-3)};$$

$$N_+ = 2^{n-2} + 2^{\frac{3}{2}(n-3)}; \quad N_0 = 2^{n-1} - 1.$$  

The above value of $N_0$ suggests that the zero/nonzero terms in $\{c_s\}$ may form an $m$-sequence; they do so for all Gold sequences and for all other ternary sequences with odd $n \leq 7$.

2. For $n$ even, the general solution of (4) is

$$D = 2^{\frac{3}{2}n} + j \cdot \frac{1}{2}, \quad N_1 = 2(2^j + 1) - 1; \quad j = 0, 1, \ldots.$$  


From (3) and (11) we have
\[ E = 2^{\frac{3}{2}n - j - 1} ; \quad j \leq \frac{3}{2}n - 1 . \tag{12} \]

The only ternary sequence for even \( n \leq 8 \) occurs for \( n = 6 \) and has \( j = 0 \) (see Table 3.1). It is not known whether ternary sequences exist for even \( n > 8 \).

3. Discussion. The existence of ternary crosscorrelation sequences is compatible, for any \( n \), with the equations 3.2(25) for the first four moments. Except for the isolated case \( n = 6 \), all those found so far have \( n \) odd, and all have \( j = 0 \).

From (4), (9) and (12) we have
\[ N_0 = \begin{cases} N - 2^n - 2j - 1, & n \text{ odd} ; \\ N - 2^n - 2j - 2, & n \text{ even} . \end{cases} \]

Since \( N \sim 2^n \) for \( N \) large, the proportion of nonzero terms in \( \{ c_s \} \) is roughly \( 2^{-2j - 1} \) or \( 2^{-2j - 2} \) as the case may be. Hence, any sequence with \( j > 0 \) would have a preponderance of zero terms; but there is no reason to suppose such a sequence exists.

3.6. Values of \( n_1 \) and \( n_2 \) for Type O distributions

We showed in Section 3.3 that a distribution is Type O if and only if the sequences are a reversed pair. The object of this section is to prove that for all Type O distributions:
- For \( n \) odd, \( n_1 = n_2 = 0 \);
- For \( n \) even, \( n_1 = 2, n_2 = 0 \).

1. As in Section 3.2, we denote sequence \( \{ a_i \} \) by \( a \), and its \( i \)th translate by \( _i a \). Then, using the \((0,1)\) element field, \( N_1 \) has been defined as the number of values of \( i, 1 \leq i \leq N - 1, \) for which there exists \( j = j(i), 1 \leq j \leq N - 1, \) such that the following equations are satisfied:
   \[ a + _i a + _j a \equiv 0 ; \tag{1} \]
   \[ b + _i b + _j b \equiv 0 . \tag{2} \]
If \( b \) is the reverse of \( a \), (2) is equivalent to
\[
a + (-i)a + (-j)a \equiv 0 \, ,
\]
or
\[
j^a + (-i)a + a \equiv 0 \, .
\]
(3)
From (1) and (3), we have \( i.a \equiv j-i.a \), and since translation leaves an m-sequence unaltered only if translation is by a multiple of \( N \), it follows that
\[
i \equiv (j-i) \mod N , \text{ or } 2i \equiv j \mod N . \quad (4)
\]
In the definition of \( N_1 \), \( i \) and \( j \) are interchangeable; hence we also have
\[
2j \equiv i \mod N . \quad (5)
\]
From (4) and (5) we have
\[
3i \equiv 0 \mod N . \quad (6)
\]
Since \( N = 2^n - 1 \), \( N \) is divisible by 3 if and only if \( n \) is even. If \( n \) is odd, (6) has no solution \( 1 \leq i \leq N-1 \), and so \( N_1 = 0 \). If \( n \) is even, there are two solutions: \( i = \frac{3}{2}N \), \( j = \frac{3}{2}N \); and \( i = \frac{3}{2}N \), \( j = \frac{3}{2}N \).
Thus \( N_1 = 2 \).

2. From Section 3.2, \( N_2 \) is defined as the number of ordered pairs \((i,j), 1 \leq i,j \leq N-1\), for which there exists \( k=k(i,j) \) such that the following equations are satisfied:
\[
a + i^a + j^a + k^a \equiv 0 \, ;
\]
\[
b + i^b + j^b + k^b \equiv 0 .
\]
(8)
If \( b \) is the reverse of \( a \), (8) is equivalent to
\[
k^a + k-i^a + k-j^a + a \equiv 0 \, ,
\]
and from (7) and (9) we have
\[
i^a + j^a \equiv k-i^a + k-j^a . \quad (10)
\]
For \( k \) to exist we must have \( i \neq j \), and so there exists \( l = l(i,j) \) such that
\[
i^a + j^a \equiv i^a \, .
\]
(11)
From (10) and (11) we have
\[
l^a \equiv k-i^a + k-j^a \equiv k-i-j(j^a + i^a) \equiv k-i-j+l^a ,
\]
whence
\[
i + j \equiv k \mod N . \quad (12)
\]
In the definition of $N$, $i$, $j$, $k$ are interchangeable; hence we also have
\[ i + k = j \pmod{N}. \]  
(13)

From (12) and (13) we have
\[ 2i \equiv 0 \pmod{N}, \]
and this has no solution since $N$ is odd. Hence $N_2 = 0$.

3.7. Classification of crosscorrelation sequences by means of the sampling property

The sampling property of m-sequences (Zierler 1959) is as follows: if $\{a_i\}$ is an m-sequence, of period $N$, and $r$ is prime to $N$, then $\{a_{ri}\}$ is an m-sequence. The proof comes directly from the definitions 2.3(1) and (2); if $g(X)$ generates $\{a_i\}$ then $g(X^r)$ generates $\{a_{ri}\}$. Since $g(X)$ is primitive, any zero $\alpha$ of $g(X)$ is such that $\alpha^N = 1$ but $\alpha^p \neq 1$ for $p < N$. Hence for any $r$ prime to $N$, $\alpha^{rN} = 1$ but $\alpha^{rp} \neq 1$ for $p < N$. Thus $\alpha^r$ is a zero of a primitive polynomial of degree $n$; this polynomial, however, generates $\{a_{ri}\}$, which is therefore an m-sequence.

A special case of sampling, of binary m-sequences, was given in Section 3.3, where it was shown that $\{a_{2i}\}$ is a translate of $\{a_i\}$. In terms of the above argument, this follows from the fact that all the zeros of $g(X)$ are $\alpha, \alpha^2, \alpha^4, \ldots, \alpha^{2^{n-1}}$.

In this section we use the sampling property to classify crosscorrelation sequences. We denote $\{a_i\}$ by $a$, as usual, and we shall denote the sampled sequence $\{a_{ri}\}$ by $a^{(r)}$, and the reversed sequence $\{a_{-i}\}$ by $\bar{a}$. Any two sequences differing only by a translation will be regarded as equivalent.

1. We deal first with the crosscorrelation of a reversed pair of sequences. Suppose the pair $a, \bar{a}$ yield the sequence $\{c_s\}$ where
\[ c_s = \sum_{i=1}^{N} a_i a_{-i-s}, \]  
(1)
and that the pair \( a^{(r)} , \bar{a}^{(r)} \) give \( \{ C'_s \} \) where
\[
C'_s = \sum_{i=1}^{N} a_i a_{i-ri+rs} \tag{2}
\]
For \( r \) prime to \( N \), \( \{ a_i \} \) is a rearrangement of \( \{ a_i \} \), so from (1) and (2) we have
\[
C'_s = \sum_{j=1}^{N} a_j a_{j+rs} = C_{rs} \tag{3}
\]
i.e. \( \{ C'_s \} \) is derived from \( \{ C_s \} \) by sampling. Hence, for given \( N \), all reversed pairs yield the same (Type 0) distribution.

We shall denote the crosscorrelation sequence derived from sequences \( a \) and \( b \) by \( [a, b] \); then the above result may be written
\[
[a, \bar{a}]^{(r)} = [a^{(r)}, \bar{a}^{(r)}] .
\]

2. An immediate generalization of (3), proved in the same way, is
\[
[a, b]^{(r)} = [a^{(r)}, b^{(r)}] \tag{4}
\]
where \( a \) and \( b \) are any two sequences of period \( N \), and \( r \) is prime to \( N \). Now it can be shown (Zierler 1959) that for any such \( a, b \), there exists \( t \) prime to \( N \) such that
\[
b = a^{(t)} , \text{ or } a = b^{(u)} \tag{5}
\]
where \( u \) is the reciprocal of \( t \) defined by
\[
tu \equiv 1 \mod N \tag{6}
\]
Putting \( r = u \) in (4), and using (5), gives
\[
[a, a^{(t)}]^{(u)} = [a^{(u)}, a] \tag{7}
\]
We may further simplify the notation by taking a particular sequence \( a_0 \) as a 'base' and denoting \( [a_0, a_0^{(t)}] \) by \( C(t) \). Then from (4), all crosscorrelation sequences of period \( N \) are represented by the set of \( C(r)(t) \), where \( r \) and \( t \) are prime to \( N \). In particular, \( C(1) \) is the autocorrelation sequence and so, by Section 2.3, \( C(r)(1) = C(1) \) for all such \( r \). \( C(-1) \) is the correlation sequence for the pair \( a, \bar{a} \). Since \( [b, a] \) is the reverse of \( [a, b] \), (7) may be written
\[
C^{(u)}(t) = \bar{C}(u) , \text{ or } C(t) = \bar{C}(t)(u) . \tag{8}
\]
3. Given a base sequence \( a_0 \), all the \( \varphi(N) \) values of \( r \) prime to \( N \) yield \( m \)-sequences \( a_0^{(r)} \), but not all these are translation-distinct; the \( n \) values \( t, 2t, 4t, \ldots, 2^{n-1}t \) all give translates of \( a_0^{(t)} \). There are therefore \( n \varphi(N) \) translation-distinct sequences of period \( N \).

For \( n = 5 \), for instance, all the integers 1-30 are prime to \( N \), and they form 'translation sets' \( A - \bar{A} \) as shown in Table 3.3. The notation \( \bar{A} \) is used to indicate that the sequences corresponding to the values of \( r \) in \( \bar{A} \) are the reverse of those corresponding to the values of \( r \) in \( A \).

<table>
<thead>
<tr>
<th>Set:</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>( \bar{A} )</th>
<th>( \bar{E} )</th>
<th>( \bar{C} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Values of ( r ):</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>15</td>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>6</td>
<td>10</td>
<td>30</td>
<td>14</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>12</td>
<td>20</td>
<td>29</td>
<td>28</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>24</td>
<td>9</td>
<td>27</td>
<td>25</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>23</td>
<td>19</td>
<td>21</td>
</tr>
</tbody>
</table>

We take as the generator of the base sequence for each \( n \), the first entry in Petersen's (1961) table of primitive polynomials. Table 3.4 lists these generators for \( n = 3 - 8 \). The generator of \( a_0^{(r)} \), for those values of \( r \) in the top row of the translation-set table, may be found from Peterson's table.

<table>
<thead>
<tr>
<th>( n )</th>
<th>( g(X) = x^n + \ldots )</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>( x^2 + X + 1 )</td>
</tr>
<tr>
<td>4</td>
<td>( x^4 + X + 1 )</td>
</tr>
<tr>
<td>5</td>
<td>( x^5 + x^2 + 1 )</td>
</tr>
<tr>
<td>6</td>
<td>( x^6 + X + 1 )</td>
</tr>
<tr>
<td>7</td>
<td>( x^7 + x^3 + 1 )</td>
</tr>
<tr>
<td>8</td>
<td>( x^8 + x^4 + x^3 + x^2 + 1 )</td>
</tr>
</tbody>
</table>

(Note: the sequences are understood to be generated according to 2.3(1), i.e., in the same sense as the \( b \)-sequences of Section 3.3, and not in the 'reverse' sense as the \( a \)-sequences of that section.)
4. We proceed to classify the correlation sequences for $n = 5 - 8$. 
(For $n = 3, 4$ the only translation-distinct $m$-sequences form a reversed pair.) We begin by calculating the 'composition table' of $rxt$: this lists, for given $n$, $r$, $t$, the translation set which contains $rt$ or its residue mod $N$. (For reasons given below, the set is labelled; not by its letter, but by its leading element.) Since the type of correlation sequence depends on $t$ and not on $r$, we then list the distribution type, and any other known feature of the sequence, under $t$. To use the table to classify the correlation $[a, b]$ given $a$ and $b$, we must know the generators of $a$ and $b$, and thus obtain the values of $r$ and $rt$ from Peterson's table; the value of $t$ can now be read directly from our table.

As an illustration, consider the example of Section 3.4. The generator of $a$ is $x^7 + x^3 + 1$ (not $x^7 + x^4 + 1$; see note to Table 3.4), and the generator of $b$ is $x^7 + x + 1$. Thus $r = 1$, and $rt = 13$ (Peterson), giving $t = 13$. Had we formed $[\bar{a}, b]$ the values would have been $r = 63$ and $rt = 23$; from Table 3.7, below, $t = 13$ so the new correlation sequence would be a sampled version of the former; in fact, it is clearly the reverse of it.

For $n = 5$, the composition table and sequence types are given in Table 3.5. All the information can be accounted for by using the results of Section 3.8, where it is shown that $u = 3$ and 5 give the ternary 'Gold sequences' which are here of Type 1 and are translates of $b$. It follows from (8) that the sequences for $u = 11$ and 7 are translates of $\bar{a}$, since, for example, if $C(t)$ is a translate of $a^{(t)}$, and $u'$ is a member of the translation set containing the reciprocal $u$ of $t$, and $t'$ is the reciprocal of $u'$, then (8) gives

$$C(u') = C(u')^{(t')}$$

the right-hand side is thus a translate of $a^{(tu)}$, which is in turn a translate of $a^{(tu)}$ i.e. $a$. If $t = 3$ then one value of $u'$ is 11, and likewise 7 is in the 'reciprocal set' of 5.
Table 3.5. Composition table for $n = 5$

<table>
<thead>
<tr>
<th>$r$</th>
<th>1</th>
<th>3</th>
<th>5</th>
<th>11</th>
<th>7</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>11</td>
<td>7</td>
<td>15</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>5</td>
<td>15</td>
<td>1</td>
<td>11</td>
<td>7</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>15</td>
<td>7</td>
<td>3</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>1</td>
<td>3</td>
<td>7</td>
<td>15</td>
<td>5</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>15</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>15</td>
<td>15</td>
<td>7</td>
<td>11</td>
<td>5</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Translate of</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto</td>
<td>$\bar{a}$ $\bar{a}$ $\bar{b}$ $\bar{b}$</td>
</tr>
</tbody>
</table>

For $n = 6$, the composition table appears as Table 3.6. By calculation it is found that $t = 5$ gives a Type 2 sequence; hence, by (8), so does $t = 13$, being in the reciprocal set of 5. Also by calculation, it is found that $t = 23$ gives a Type 1 translate of $b$, and so $t = 11$ (reciprocal set) gives a Type 1 translate of $\bar{a}$.

Table 3.6. Composition table for $n = 6$

<table>
<thead>
<tr>
<th>$r$</th>
<th>1</th>
<th>5</th>
<th>11</th>
<th>13</th>
<th>23</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>5</td>
<td>11</td>
<td>13</td>
<td>23</td>
<td>31</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>11</td>
<td>31</td>
<td>1</td>
<td>13</td>
<td>23</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>31</td>
<td>23</td>
<td>5</td>
<td>1</td>
<td>13</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
<td>1</td>
<td>5</td>
<td>23</td>
<td>31</td>
<td>11</td>
</tr>
<tr>
<td>23</td>
<td>23</td>
<td>13</td>
<td>1</td>
<td>31</td>
<td>11</td>
<td>5</td>
</tr>
<tr>
<td>31</td>
<td>31</td>
<td>23</td>
<td>13</td>
<td>11</td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Translate of</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto</td>
<td>2 1 2 1 0</td>
</tr>
<tr>
<td>$\bar{a}$ $\bar{b}$</td>
<td></td>
</tr>
</tbody>
</table>

For $n = 7$, see Table 3.7. The Gold sequences are here of Type 2, and occur for $u = 3, 5$ and 9; these are translates of $b$. The Type 2 sequences for the 'reciprocal-set' $u = 43, 27, 15$ are therefore translates of $\bar{a}$. The Type 1 sequences were found by calculation to occur, as translates of $b$, for $t = 31, 47$ and 55; the reciprocal-set values therefore give Type 1 translates of $\bar{a}$ for $t = 21, 19$ and 7. The remaining values of $t$ were found, by calculation, to give Type 2 translates of sequences other than $b$ or $\bar{a}$. Reciprocal-set values
enable the translates for \( t = 13 \) and 29 to be derived from those for \( t = 11 \) and 23, as follows: \( C(11) \) is found to give a translate of \( a^{(9)} \), and from (8) we have \( C(13) = C(13)(11) \) which is a translate of \( a^{(9 \times 13)} \) or \( a^{(47)} \) or \( a^{(5)} \). Similarly, \( C(23) \) is found to give a translate of \( a^{(5)} \), so \( C(29) \) gives a translate of \( a^{(55)} \).

To conclude the discussion of the case \( n = 7 \), consider again the example of Section 3.4. According to Table 3.7, \( C(13) \) gives a translate of \( a^{(5)} \), and from Peterson's table, the generator corresponding to \( r = 5 \) is \( x^7 + x^4 + x^3 + x^2 + 1 \); this was given as the generator of \( \mathbb{Z}_2(X) \) in Section 3.4.

**Table 3.7. Composition table for \( n = 7 \)**

| \( r \) | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 19 | 21 | 43 | 27 | 23 | 29 | 55 | 15 | 47 | 31 | 63 |
| 1 | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 19 | 21 | 43 | 27 | 23 | 29 | 55 | 15 | 47 | 31 | 63 |
| 3 | 3 | 9 | 15 | 21 | 27 | 5 | 29 | 23 | 63 | 1 | 13 | 11 | 47 | 19 | 43 | 7 | 55 | 31 |
| 5 | 5 | 15 | 19 | 13 | 43 | 55 | 3 | 63 | 29 | 11 | 1 | 31 | 9 | 21 | 23 | 27 | 7 | 47 |
| 7 | 7 | 21 | 13 | 11 | 63 | 27 | 55 | 3 | 5 | 47 | 31 | 9 | 19 | 1 | 29 | 23 | 43 | 15 |
| 9 | 9 | 27 | 43 | 63 | 13 | 15 | 47 | 11 | 31 | 3 | 29 | 5 | 7 | 23 | 1 | 21 | 19 | 55 |
| 11 | 11 | 5 | 55 | 27 | 15 | 31 | 1 | 21 | 13 | 23 | 43 | 63 | 3 | 7 | 19 | 9 | 47 | 29 |
| 13 | 13 | 29 | 3 | 55 | 47 | 1 | 21 | 15 | 19 | 27 | 7 | 43 | 63 | 5 | 9 | 31 | 11 | 23 |
| 19 | 19 | 23 | 63 | 3 | 11 | 21 | 15 | 47 | 9 | 55 | 5 | 7 | 43 | 29 | 31 | 1 | 13 | 27 |
| 21 | 21 | 63 | 29 | 5 | 31 | 13 | 19 | 9 | 15 | 7 | 55 | 27 | 23 | 3 | 47 | 11 | 1 | 43 |
| 43 | 43 | 1 | 11 | 47 | 3 | 23 | 27 | 55 | 7 | 15 | 9 | 19 | 13 | 31 | 5 | 29 | 63 | 21 |
| 27 | 27 | 13 | 1 | 31 | 29 | 43 | 7 | 5 | 55 | 9 | 47 | 15 | 21 | 11 | 3 | 63 | 23 | 19 |
| 23 | 23 | 11 | 31 | 9 | 5 | 63 | 43 | 7 | 27 | 19 | 15 | 21 | 1 | 47 | 55 | 3 | 29 | 15 |
| 29 | 29 | 47 | 9 | 19 | 7 | 3 | 63 | 43 | 23 | 13 | 21 | 1 | 31 | 15 | 27 | 55 | 5 | 11 |
| 55 | 55 | 19 | 21 | 1 | 23 | 7 | 5 | 29 | 3 | 31 | 11 | 47 | 15 | 13 | 63 | 43 | 27 | 9 |
| 15 | 15 | 43 | 23 | 29 | 1 | 19 | 9 | 31 | 47 | 5 | 3 | 55 | 27 | 63 | 11 | 13 | 21 | 7 |
| 47 | 47 | 7 | 27 | 23 | 21 | 9 | 31 | 1 | 11 | 29 | 63 | 3 | 55 | 43 | 13 | 19 | 15 | 5 |
| 31 | 31 | 55 | 7 | 43 | 19 | 47 | 11 | 13 | 1 | 63 | 23 | 29 | 5 | 27 | 21 | 15 | 9 | 3 |
| 63 | 63 | 31 | 47 | 15 | 55 | 29 | 23 | 27 | 43 | 21 | 19 | 13 | 11 | 9 | 7 | 5 | 3 | 1 |

**Type** | \( A^u \) | 2 | 2 | 1 | 2 | 2 | 1 | 1 | 2 | 2 | 2 | 1 | 2 | 2 | 1 | 1 | 0 |

**Translate of** | \( \overline{a} \) | \( a \) | \( \overline{a} \) | \( a \) | \( \overline{a} \) | \( a \) | \( \overline{a} \) | \( b \) | \( a \) | \( \overline{a} \) | \( b \) | \( b \) | \( b \) | \( b \) | \( b \) | \( b \) |
For \( n = 8 \), see Table 3.8. The 14 values of \( t \) other than \( t = 1 \) and 127 all give Type 2 correlation sequences. There are 8 distinct reciprocal-set pairs among these values, since \( t = 43 \) and 53 are self-reciprocal; these 8 pairs yield the different distributions labelled a–h (in arbitrary order) in Table 3.1. The Type 2 sequences do not give rise to m-sequences.

Table 3.8. Composition table for \( n = 8 \)

<table>
<thead>
<tr>
<th>r</th>
<th>1</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>19</th>
<th>23</th>
<th>37</th>
<th>43</th>
<th>53</th>
<th>91</th>
<th>29</th>
<th>59</th>
<th>47</th>
<th>61</th>
<th>31</th>
<th>127</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>7</td>
<td>11</td>
<td>13</td>
<td>19</td>
<td>23</td>
<td>37</td>
<td>43</td>
<td>53</td>
<td>91</td>
<td>29</td>
<td>59</td>
<td>47</td>
<td>61</td>
<td>31</td>
<td>127</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>19</td>
<td>53</td>
<td>91</td>
<td>11</td>
<td>13</td>
<td>1</td>
<td>23</td>
<td>29</td>
<td>127</td>
<td>47</td>
<td>61</td>
<td>37</td>
<td>43</td>
<td>59</td>
<td>31</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>53</td>
<td>47</td>
<td>31</td>
<td>29</td>
<td>127</td>
<td>19</td>
<td>91</td>
<td>37</td>
<td>59</td>
<td>.1</td>
<td>23</td>
<td>7</td>
<td>13</td>
<td>43</td>
<td>61</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
<td>91</td>
<td>31</td>
<td>53</td>
<td>127</td>
<td>11</td>
<td>23</td>
<td>19</td>
<td>59</td>
<td>29</td>
<td>61</td>
<td>1</td>
<td>43</td>
<td>7</td>
<td>37</td>
<td>47</td>
</tr>
<tr>
<td>19</td>
<td>19</td>
<td>11</td>
<td>29</td>
<td>127</td>
<td>53</td>
<td>91</td>
<td>7</td>
<td>13</td>
<td>47</td>
<td>31</td>
<td>37</td>
<td>43</td>
<td>1</td>
<td>23</td>
<td>61</td>
<td>59</td>
</tr>
<tr>
<td>23</td>
<td>23</td>
<td>13</td>
<td>127</td>
<td>11</td>
<td>91</td>
<td>19</td>
<td>43</td>
<td>7</td>
<td>61</td>
<td>1</td>
<td>127</td>
<td>11</td>
<td>31</td>
<td>47</td>
<td>59</td>
<td>37</td>
</tr>
<tr>
<td>37</td>
<td>37</td>
<td>1</td>
<td>19</td>
<td>23</td>
<td>7</td>
<td>43</td>
<td>47</td>
<td>61</td>
<td>11</td>
<td>13</td>
<td>53</td>
<td>31</td>
<td>29</td>
<td>59</td>
<td>127</td>
<td>91</td>
</tr>
<tr>
<td>43</td>
<td>43</td>
<td>23</td>
<td>91</td>
<td>19</td>
<td>13</td>
<td>7</td>
<td>61</td>
<td>1</td>
<td>127</td>
<td>11</td>
<td>31</td>
<td>47</td>
<td>59</td>
<td>37</td>
<td>29</td>
<td>53</td>
</tr>
<tr>
<td>53</td>
<td>53</td>
<td>29</td>
<td>37</td>
<td>59</td>
<td>47</td>
<td>31</td>
<td>11</td>
<td>127</td>
<td>1</td>
<td>61</td>
<td>7</td>
<td>13</td>
<td>19</td>
<td>91</td>
<td>23</td>
<td>43</td>
</tr>
<tr>
<td>91</td>
<td>91</td>
<td>127</td>
<td>59</td>
<td>29</td>
<td>31</td>
<td>53</td>
<td>13</td>
<td>11</td>
<td>61</td>
<td>47</td>
<td>43</td>
<td>7</td>
<td>23</td>
<td>19</td>
<td>1</td>
<td>37</td>
</tr>
<tr>
<td>29</td>
<td>29</td>
<td>47</td>
<td>1</td>
<td>61</td>
<td>37</td>
<td>59</td>
<td>53</td>
<td>31</td>
<td>7</td>
<td>43</td>
<td>19</td>
<td>91</td>
<td>11</td>
<td>127</td>
<td>13</td>
<td>23</td>
</tr>
<tr>
<td>59</td>
<td>59</td>
<td>61</td>
<td>23</td>
<td>1</td>
<td>43</td>
<td>37</td>
<td>31</td>
<td>47</td>
<td>13</td>
<td>7</td>
<td>91</td>
<td>53</td>
<td>127</td>
<td>29</td>
<td>11</td>
<td>19</td>
</tr>
<tr>
<td>47</td>
<td>47</td>
<td>37</td>
<td>7</td>
<td>43</td>
<td>1</td>
<td>61</td>
<td>29</td>
<td>59</td>
<td>19</td>
<td>23</td>
<td>11</td>
<td>127</td>
<td>55</td>
<td>31</td>
<td>91</td>
<td>13</td>
</tr>
<tr>
<td>61</td>
<td>61</td>
<td>43</td>
<td>13</td>
<td>7</td>
<td>23</td>
<td>1</td>
<td>59</td>
<td>37</td>
<td>91</td>
<td>19</td>
<td>127</td>
<td>29</td>
<td>31</td>
<td>47</td>
<td>53</td>
<td>11</td>
</tr>
<tr>
<td>31</td>
<td>31</td>
<td>59</td>
<td>43</td>
<td>37</td>
<td>61</td>
<td>47</td>
<td>127</td>
<td>29</td>
<td>23</td>
<td>1</td>
<td>13</td>
<td>11</td>
<td>91</td>
<td>53</td>
<td>19</td>
<td>7</td>
</tr>
<tr>
<td>127</td>
<td>127</td>
<td>31</td>
<td>61</td>
<td>47</td>
<td>59</td>
<td>29</td>
<td>91</td>
<td>53</td>
<td>43</td>
<td>37</td>
<td>23</td>
<td>19</td>
<td>13</td>
<td>11</td>
<td>7</td>
<td>1</td>
</tr>
</tbody>
</table>

**Type Au f e d b c f g a h e d b c h • .**

3.8. Gold sequences: a class of ternary crosscorrelation sequences

After the bulk of the work described in Sections 3.1–3.7 had been done, Gold (1968) published a proof of the existence of ternary crosscorrelation sequences \( \{c_s\} \) for all odd \( n \). His sequences have element-values given by 3.5(10), and their zero/nonzero terms form a translate of the zero/one terms of sequence \( b \). Since his approach seems more promising than those we have used so far, we give Gold's
proof in some detail. A novel application of his method is given in Appendix 1, where we show that the first moment of any binary m-sequence can be made to vanish by starting the sequence at the appropriate point.

Instead of defining the sequence \{b_i\} by the recurrence equation 2.3(1), one may, using the (0,1) element field, define

$$b_i = T(\alpha^i) \quad (1)$$

where \(\alpha\) is a primitive Nth root of unity in the Galois field of \(2^n\) elements, and the 'trace' \(T(x)\) is defined as

$$T(x) = \sum_{j=0}^{n-1} x^j \quad (2)$$

The sum in (2) is modulo 2; in this section we shall denote mod-2 addition by \(\oplus\). From (2) we have

$$T^2(\alpha) = (\alpha \oplus \alpha^2 \oplus \alpha^4 \oplus \ldots \oplus \alpha^{2^{n-1}})^2$$

$$= \alpha^2 \oplus \alpha^4 \oplus \alpha^8 \oplus \ldots \oplus \alpha^{2^n}$$

$$= T(\alpha) \text{ since } \alpha^{2^n} = \alpha \text{ for a primitive root}.$$  

This confirms that \(b_i\) given by (1) can take only values 0 and 1.

The sampling property (Section 3.7) follows from the fact that, if \(\alpha\) is a primitive root, so is \(\alpha^r\) for \(r\) prime to \(N\); replacing \(\alpha\) by \(\alpha^r\) in (1) yields the sampled sequence \(\{b_{ri}\}\), which is thus an m-sequence.

As an example, take \(n = 5\) and denote the translation sets by A - C as in Table 3.3. Then the sequence according to (1) is:

$$i = 0 \quad 5 \quad 10 \quad 15 \quad 20 \quad 25 \quad 30$$

$$b_i = 1AABA \quad CBAC \quad CCBCB \quad AABCDE \quad CCBAB \quad BCBAB \quad A$$

The values to be assigned to the sets depend on the choice of the generating polynomial; for instance, the generator \(x^5 + x^2 + 1\) produces a sequence with terms as follows:

$$A = 0, B = 0, C = 1, \bar{C} = 1, \bar{B} = 1, \bar{A} = 0.$$  

2. The pair of sequences to be crosscorrelated, \(\{a_i\}\) and \(\{b_i\}\), will be taken to have elements \((0,1)\). A modified form of
correlation will be used, defined by the coefficient
\[ d_s = \sum_{i=0}^{N-1} (a_i \oplus b_{i+s}) = 2^{n-1} - 2c_s . \] (3)
Suppose \( a_i = b_{ui} \) for all \( i \), where \( u \) is prime to \( N \), and let \( b_i \) be
given by (1). Then from (1) and (3) we have
\[ d_s = \sum_i \{ T(\alpha^{ui}) \oplus T(\alpha^{i+s}) \} = \sum_i T(\alpha^{ui} \oplus \alpha^{i+s}) , \text{ by (2)}. \] (4)
As \( i \) varies, \( \alpha^i \) goes through all the elements of \( \text{GF}(2^N) \) except 0.
By definition \( T(0) = 0 \); hence (4) can be written as
\[ d_s = \sum_x T\{(x^{i-1} \oplus \alpha^s)x\} , \] (5)
summed over all \( x \) in \( \text{GF}(2^N) \).

3. To proceed further, Gold assumes that \( n \) is odd and that
\[ u = 2^l + 1 = L + 1 , \text{ say, where } l \text{ is prime to } n . \] (6)
He observes that since, for any \( y \) in \( \text{GF}(2^N) \), the set \( \{x \oplus y\} \) is a
permutation of \( \{x\} \), (5) and (6) give
\[ d_s = \sum_x T\{(x \oplus y)^L \oplus \alpha^s\}(x \oplus y) \]
\[ = \sum_x T\{(x^L \oplus y^L \oplus \alpha^s)(x \oplus y)\} \]
\[ = \sum_x T\{x^{L+1} \oplus x(y^L \oplus \alpha^s \oplus y^{L-1}) \oplus y^{L+1} \oplus \alpha^s y\} ; \] (7)
the last line follows since \( T(x^L y) = T(xy^{L-1}) \). He then shows,
first, that if \( b_s = T(\alpha^s) = 0 \), there is a value \( y = y_0 \), say, such that
\[ T(y_0^L \oplus \alpha^s \oplus y_0^{L-1}) = 0 . \] (8)
Putting \( y = y_0 \) in (7), and using (8), gives
\[ d_s = \sum_x T(x^{L+1} \oplus y_0^{L+1} \oplus \alpha^s y_0) \]
\[ = \sum_x \{ T(x^{L+1} \oplus T(y_0^{L+1} \oplus \alpha^s y_0) \} . \] (9)
Since the set \( \{T(x^{L+1})\} \), for all \( x \) in \( \text{GF}(2^N) \), is a permutation of
\( \{T(x)\} \), it contains \( 2^{n-1} \) zeros and \( 2^{n-1} \) ones. Thus, from (9), the
value of \( d_s \) is \( 2^{n-1} \) whether the second trace is 0 or 1. It follows
from (3) that \( c_s = 0 \) whenever \( b_s = 0 \).
Secondly, if \( b_s = 1 \), then since \( n \) is odd, \( T(1) = 1 \) and so
\[ T(\alpha^s \oplus 1) = 0 . \] By the argument leading to (8), there is a value
\[ y = y_1 \text{ say, such that } \]
\[ T\{ y_1^L \oplus (\alpha^S \oplus 1) \oplus y_1^{-L-1} \} = 0 \]  \hspace{1cm} (10)

Putting \( y = y_1 \) in (7), and using (10), gives
\[ d_s = \sum_x T(x \oplus x^{L+1} \oplus y_1^{L+1} \oplus \alpha^S y_1) \]  \hspace{1cm} (11).

If \( T(y_1^{L+1} \oplus \alpha^S y_1) = k \), say (value 0 or 1), we have from (11):
\[ d_s = \sum_x \{ T(x \oplus x^{L+1} \oplus k) \} = \sum_{i=0}^{N-1} (b_i \oplus a_i \oplus k) \oplus k^S, \text{ from (6)}, \]
\[ = d_0 \text{ if } k = 0; = 2^n - d_0 \text{ if } k = 1. \]

Since \( n \) is odd, \( b_0 = 1 \). \( c_s \) thus equals \( \pm c_0 \) according as \( k = 0 \) or 1.

By analysing the frequency of zero and nonzero \( k \), Gold finally obtains the required result 3.5(10).

The occurrence of Gold sequences for \( n = 5 \) and 7 has been discussed in Section 3.7. For \( n = 9 \), Gold sequences occur for \( u = 3, 5 \) and 17, the reciprocal-set values being \( t = 171, 103 \) and 31.

They may be termed 'Type 3' with the frequency distribution
\[ f_c(0) = 255, f_c(8) = 136, f_c(-8) = 120. \]

Examples of Gold sequences for \( n = 5 \) and 7 are given by Briggs and Godfrey (1968).

3.9. Conclusions

Neither moment-analysis nor generating-polynomial analysis give much information about the crosscorrelation sequences. In any case, the distributions in Table 3.1 are too irregular for moments to have much meaning. The 'correspondences' \( N_1 \) and \( N_2 \) which enter into the moment formulae are an interesting concept, but they do not assist the calculation.

The generating-polynomial approach suffers from the fact that, whereas \( m \)-sequences obey a binary algebra, correlation introduces the algebra of real numbers. It does not seem to be a worthwhile way of studying correlation sequences.
The 'sampling' approach is a useful classification technique for relating any correlation sequence to one of a few basic sequences.

The most promising approach is that of Gold, using the algebra of finite fields and the relation between such fields and m-sequences. The next step might be to compute the correlation sequences for, say, \( n = 9 \) and \( 11 \), to see whether they are all related to m-sequences in the same way as those for \( n = 5 \) and 7. Again, a study of the elements of \( \text{GF}(128) \) might show whether there is any algebraic significance in the fact that, in Table 3.7, the Type 1 sequences occur for just those values of \( t \) which are in the 'reverse sets' to the values corresponding to the Gold sequences. It might be possible to account for the different sequence types in this way, both for \( n = 7 \) and higher values.

3.10. A note on computing time

The data in Table 3.1 were calculated on a Ferranti Hermes computer, programmed in machine code. The computing time per sequence-pair was about 4.5s for \( n = 8 \), and this should roughly quadruple for each unit increase in \( n \).

For \( n = 9 \), there are 48 translation-distinct m-sequences. Without taking into account self-reciprocal values of \( t \), there are 24 basic sequences to be calculated, of which 3 are Gold sequences. The total computing time is about one hour.

For \( n = 11 \), there are 178 translation-distinct sequences. Since each sequence-pair should take one hour, the complete calculation could require a considerable amount of Hermes time.

This program does not print out the correlation sequences. For \( n = 7 \), these were generated on a special 'shift-register' device built in the Electrical Engineering Department of Surrey University. An improved version might be a better way of investigating the case \( n = 11 \) than a general-purpose computer.
4. IDENTIFYING MULTI-INPUT LINEAR SYSTEMS BY CROSSCORRELATION OF PERIODIC SEQUENCES

4.1. General remarks

Once pseudorandom sequences had become established as test inputs for single-input systems, it was natural to consider their possible use in identifying the dynamics of systems with more than one input. Unlike the control problem for multivariable systems, the linear identification problem differs in degree, rather than in kind, from the single-input problem; the main difference is that no practically-useful way has been found of choosing sets of sequences which approach the ideal, as regards both auto- and crosscorrelation.

This chapter is brief, since it is my opinion that despite various attempts, no-one has improved on the elementary idea of making each input a translate of the same pseudorandom sequence. Cummins (1965) ascribes this to A. Fekete of Imperial College, London; I had it from Professor J. H. Westcott in 1964. Cummins, however, dismisses it on the grounds that 'There appears to be no advantage with this arrangement over that where a number of independent experiments are performed over correspondingly shorter periods of time. This arrangement (i.e. the latter) then solves the noninteraction problem at the expense of experimental time. Independent experiments have an advantage in that the noise level due to cross-coupling will be lower'. Though he does not point out that with independent experiments one has to wait for the system to settle down to a periodic response to each input in turn, it seems clear that only rarely will the simultaneous testing via several inputs be justified.
4.2. A survey of work on crosscorrelation of periodic sequences

Most of the work on crosscorrelation has been aimed at finding sequences whose crosscorrelation is negligible for all, or most, relative shifts. This was the original purpose behind the work reported in Chapter 3.

Cummins (1965) correlated quadratic-residue sequences of periods 7 and 11, and found a uniform $C_s = -1$; he conjectured this to be the case for all pairs of pseudorandom binary sequences whose periods are coprime, but remarked that the product of the periods would constitute an unacceptable length of time for system testing. He looked into, but rejected, the idea of using unequal step-lengths for the pair, so as to produce the same duration for each period; the resulting crosscorrelation of the 7- and 11-term sequences was neither constant nor uniformly small. He concluded that it would be better to go for zero crosscorrelation with non-ideal autocorrelation, e.g. by using Walsh functions (Henderson 1964).

Briggs and Godfrey (1966) proved, by moment analysis, that the crosscorrelation of two pseudorandom binary sequences can only be constant if the periods are coprime. Instead of using two or more such sequences simultaneously, they suggested taking a single pseudorandom binary sequence $\{a_i\}$ and forming the $r^{th}$ input $x^{(r)}$ where $x_{i+jN}^{(r)} = k_{rj} a_i$, $k_{rj}$ being the ($r,j$) element of a Hadamard matrix. (A Hadamard matrix has elements $\pm 1$ and its rows are mutually orthogonal; if the order is a power of 2, then the rows may be taken as Walsh functions.) The effect is to make the crosscorrelation, as well as the autocorrelation, small except for 'spikes' where the shift is a multiple of $N$; the crosscorrelation, indeed, may be identically zero. The simplest case is $r = 2$, when $[k_{rj}] = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, i.e. the first input is the unmodified sequence, and alternate terms of it are inverted to form the other input.
Various other possibilities are discussed in the above paper or in a companion report (Godfrey and Briggs 1966): ternary m-sequences with levels (0, 1, -1) or (-1, 1, 1); quadratic-residue and Hall sequences, particularly those which share a value of N with one another or with a binary m-sequence; 'slowed-down' sequences where one input has twice the step length of the other; and sequences derived from pseudorandom binary sequences by various means. By theory or calculation, the authors conclude that none of these ideas is as good as the Hadamard-matrix scheme already referred to.

The latter was tried out by Williams (1966) on a computer model with four inputs, in the presence of computer-generated noise added to the output; but the results were not conclusive.

4.3. Redundancy of the correlation equations

Since the crosscorrelation of different types of sequence had been so extensively surveyed, I approached the problem from another angle. It has so far been assumed that multi-input systems can be effectively identified only if the input crosscorrelation is virtually zero. I proceeded to check this by taking the exact correlation equations for a two-input linear system and reducing them to a set of linear algebraic equations. I took into account the step-sequence form of the inputs, their periodicity, and the effect of subtracting the mean values of the input and output functions so as to give the true correlations.

The detailed analysis has appeared in a published paper (Ream 1967), which is reproduced as an Annex to this thesis. The result of the analysis was unexpected; if each input is a two-level-autocorrelation sequence of period N, then there are only N independent equations altogether, whatever the number of inputs, for determining the dynamics of the system. This being so, there
seems to be little point in using any but the simplest scheme for
a set of input sequences of period N, namely the translation of
one sequence to form all the input sequences.

This result has not been shown to apply for sequences other than
two-level-autocorrelation sequences, but the above paper produces
the same effect (reduction to N equations) in the case of the
simplest form of Hadamard modification.

More work would be needed to examine the other possible schemes
mentioned in this chapter, unless it is possible to derive a
general result for all step-sequence inputs of the same period. In
view of the similar results obtained in Chapter 5 for nonlinear
systems, the existence of such a general result seems probable.

Since the detailed analysis of a single-input nonlinear system
yields the same type of equations as the multi-input linear case,
and since the multi-input linear equations are set out in the Annex
(though in a somewhat different notation), the latter will not be
repeated here.
5. IDENTIFYING NONLINEAR SYSTEMS BY MEANS OF PSEUDORANDOM INPUTS

5.1. The approximation problem

We shall approach the nonlinear identification problem by assuming that the output $y(t)$ can be expanded in a functional (Volterra) power series in the input $x(t)$:

$$y(t) = \int_0^\infty h_1(u) x(t-u) \, du + \int_0^\infty \int_0^\infty h_2(u,v) x(t-u) x(t-v) \, du \, dv + \ldots$$

(1)

where $h_1, h_2, \ldots$ are the kernels which describe the system and are to be determined.

One advantage of this approach is that it reduces to the linear identification problem when $h_2$ and higher kernels are ignored. A disadvantage is the lack of direct connexion with the differential equation relating $x(t)$ and $y(t)$; the same objection applies to the linear case, but users have become familiar with the linear kernels corresponding to the linear differential equations which are commonly met. Barrett (1963) gives a useful survey of the integral-equation approach to nonlinear systems.

It is safe to assume that in practice, only a few terms of (1) can be identified from experimental data, and that the right-hand side will be an approximation, only, to the observed $y(t)$. Then, whether the desired description is linear or nonlinear, there exists a regular method of approximation by minimizing the mean-square error, which leads in the linear case to the correlation equation of Section 2.1, and in the nonlinear case to a set of simultaneous equations involving higher-order correlations. A standard variational technique is used to derive these, and they appear to have been first used by Schetzen and Lee (1961). In this section we give an outline derivation of the equations for the linear and the second-order approximations.
1. The best linear approximation to $y(t)$, in the minimum-mean-square-error sense, is obtained by minimizing $e_1^2(t)$ where

$$e_1(t) = y(t) - \int_0^\infty h_1(u) x(t-u) \, du$$

(2)

Let the best-linear-approximation kernel be $h_1(t)$. The standard technique involves setting $h_1(t) = h_1(t) + \varepsilon_1 f_1(t)$ where $f_1(t)$ is an arbitrary function, zero for $t<0$; expanding $e_1^2(t)$ in powers of $\varepsilon_1$; and choosing $h_1(t)$ to make the multiplier of $\varepsilon_1 f_1(t)$ zero in this expansion. The resulting equation for $h_1(t)$ is the correlation equation $2.1(3)$, which we now write in the form

$$Y_1(\sigma) = \int_0^\infty h_1(u) X_1(\sigma-u) \, du$$

(3)

where

$$X_1(u) = \frac{x(t-u)x(t)}{}, \quad Y_1(\sigma) = \frac{x(t-\sigma)y(t)}{}$$

(4)

2. Let the kernels corresponding to the best second-order approximation be $h_1^{(2)}(t), h_2^{(2)}(u,v)$. The quantity to be minimized is the mean square of

$$e_2(t) = e_1(t) - \int_0^\infty \int_0^\infty h_2(u,v) x(t-u) x(t-v) \, du \, dv$$

(5)

Write $h_1(t) = h_1^{(2)}(t) + \varepsilon_1 f_1(t)$, $h_2(u,v) = h_2^{(2)}(u,v) + \varepsilon_2 f_2(u,v)$ where $f_1$ and $f_2$ are arbitrary functions, zero for negative values of each argument; expand $e_2^2(t)$ in powers of $\varepsilon_1$ and $\varepsilon_2$; and choose $h_1^{(2)}$ and $h_2^{(2)}$ to make the multipliers of $\varepsilon_1 f_1$ and $\varepsilon_2 f_2$ zero in this expansion. The resulting equations for $h_1^{(2)}$ and $h_2^{(2)}$ are:

$$Y_1(\sigma) = \int_0^\infty h_1^{(2)}(u) X_1(\sigma-u) \, du + \int_0^\infty \int_0^\infty h_2^{(2)}(u,v) X_2(u-\sigma,v-\sigma) \, du \, dv$$

(6)

$$Y_2(\sigma,\tau) = \int_0^\infty h_2^{(2)}(u) X_2(\tau-\sigma,u-\sigma) \, du$$

$$+ \int_0^\infty \int_0^\infty h_2^{(2)}(u,v) X_3(\tau-\sigma,u-\sigma,v-\sigma) \, du \, dv$$

(7)

where $Y_1$ and $X_1$ are as defined in (4), and

$$X_2(u,v) = \frac{x(t-u)x(t-v)x(t)}{}$$

$$X_3(u,v,w) = \frac{x(t-u)x(t-v)x(t-w)x(t)}{}$$

$$Y_2(\sigma,\tau) = \frac{x(t-\sigma)x(t-\tau)y(t)}{}$$

(8)
3. The same method applied to the \( n \)-th order approximation (1) results in a set of \( n \) equations for the kernels \( h_1^{(n)} \cdots h_n^{(n)} \), whose form can be seen from (5), (6) and (7). They involve autocorrelation functions \( X_1 \cdots X_{2n-1} \) and crosscorrelation functions \( Y_1 \cdots Y_n \). This general set of equations will be discussed in Section 5.7, in connexion with the ternary-m-sequence type of input.

We conclude this section by mentioning a property of the correlation equations which does not appear to have been explicitly stated elsewhere: namely, that averaging any equation with respect to one independent variable gives one of the equations of the next order below. For instance, averaging (7) with respect to \( \tau \) gives (6) multiplied by \( X_0 = \overline{x(t)} \); again, averaging (6) with respect to \( \sigma \), and dividing by \( X_0 \), gives the 'zero-order' equation

\[
Y_0 = \overline{y(t)} = X_0 \int_{0}^{\infty} h_1^{(2)}(u) \, du + \int_{0}^{\infty} \int_{0}^{\infty} h_2^{(2)}(u,v) X_1(u-v) \, du \, dv .
\]

This effect of averaging is not important with continuously-varying inputs, but it is relevant to the analysis for step-sequence inputs as we show in the next section.

5.2. Weight equations arising from a periodic-step-sequence input

In this section we derive the equations corresponding to (6) and (7) for the case when \( x(t) \) changes only at integer values of \( t \), and is periodic with period \( N \).

1. Each \( X_i \) \((i = 1, 2, \ldots)\) then varies linearly, with respect to each of its arguments, between successive integer values of the argument. This result for \( X_1 \) has already been used in the multi-input analysis (see Annex 1); the derivation for \( X_1 \) is as follows.

Let \( u = r + \theta \), where \( 0 \leq \theta < 1 \). Then the step-sequence property implies that

\[
x(t-u)x(t) = x(t-r)x(t) \quad \text{when} \quad t-[t]\geq\theta;
\]

\[
x(t-r-1)x(t) \quad \text{when} \quad t-[t]<\theta,
\]

where \([t]\) is the integer part of \( t \). Averaging over \( t \), and using (4),
gives
\[ X_1(r + \theta) = (1 - \theta)X_1(r) + \theta X_1(r + 1), \quad (10) \]
i.e. linear interpolation with respect to \( \theta \) between 0 and 1.

In the same way, we find for \( 0 < \theta, \varphi < 1 \):
\[ X_2(r + \theta, s + \varphi) = (1 - \theta)(1 - \varphi)X_2(r, s) + \theta(1 - \varphi)X_2(r + 1, s) + \theta \varphi X_2(r + 1, s + 1). \quad (11) \]

From (10) we obtain, after some reduction,
\[ \int_{0}^{\infty} h_1^{(2)}(u)X_1(u - r)\, du = \sum_{j=0}^{\infty} H_1(j)X_1(j - r), \quad (12) \]
where \( H_1(j) = \int_{0}^{1} \{(1 - \theta)\{h_1^{(2)}(j + \theta) + h_1^{(2)}(j - \theta)\}\} d\theta , \quad (13) \)
and \( h_1^{(2)}(u) = 0 \) for \( u < 0 \). Similarly, (11) gives after reduction:
\[ \int_{0}^{\infty} h_2^{(2)}(u,v)X_2(u - r, v - s)\, du\, dv = \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} H_2(j, k)X_2(j - r, k - s), \quad (14) \]
where
\[ H_2(j, k) = \int_{0}^{1} \int_{0}^{1} \{(1 - \theta)(1 - \varphi)\{h_2^{(2)}(j + \theta, k + \varphi) + h_2^{(2)}(j - \theta, k + \varphi) + h_2^{(2)}(j + \theta, k - \varphi) + h_2^{(2)}(j - \theta, k - \varphi)\}\} d\theta\, d\varphi \quad (15) \]
and \( h_2^{(2)}(u,v) \) is zero for negative \( u \) or \( v \).

2. Now suppose \( x(t) \) has period \( N \). Then each \( X_1 \) is periodic, with period \( N \), in each of its arguments, and we have
\[ \sum_{j=0}^{\infty} H_1(j)X_1(j - r) = \sum_{j=0}^{N} X_1(j - r) \sum_{l=-\infty}^{\infty} H_1(j + lN); \quad (16) \]
\[ \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} H_2(j, k)X_2(j - r, k - s) = \sum_{j=1}^{N} \sum_{k=1}^{N} X_2(j - r, k - s) \sum_{l=-\infty}^{\infty} \sum_{m=-\infty}^{\infty} H_2(j + lN, k + mN). \quad (17) \]
We write
\[ \sum_{l=-\infty}^{\infty} H_1(j + lN) = w_1(j); \quad \sum_{l=-\infty}^{\infty} \sum_{m=-\infty}^{\infty} H_2(j + lN, k + mN) = w_2(j, k). \quad (18) \]
Then putting \( \sigma = r \) in (6), and using (12), (14), (16), (17) and (18), we get
\[ X_1(r) = \sum_{j} w_1(j)X_1(j - r) + \sum_{j} w_2(j, k)X_2(j - r, k - r), \quad (19) \]
all summations being from 1 to \( N \). Again, putting \( \sigma = r \) and \( \tau = s \) in (7), and using equations analogous to (16) and (17), gives
\[ Y_2(r,s) = \sum_j w_1(j) X_2(s-r,j-r) + \sum_{jk} w_2(j,k) X_3(s-r,j-r,k-r). \]  

(20)

3. We have now obtained equations, in the case of a periodic-step-sequence input, which may be solved for the unknown system 'weights' \( w_1 \) and \( w_2 \). By considering only integer values of \( \sigma \) and \( \tau \), we have thrown away information about the kernels \( h_1 \) and \( h_2 \), whose behaviour can now only be inferred from the weights which are their locally-averaged values. In this section we have discussed the second-order approximation to \( y(t) \); the linear-approximation case has been dealt with in similar fashion in Annex 1; the extension to higher orders is straightforward. The equations in their exact form are believed to be new; previous investigators have merely replaced summation by integration, without averaging. The distinction only becomes important when \( N \) is not large, and the kernels vary appreciably within the unit time-interval.

The above analysis has assumed all necessary convergence properties to hold; this is probably, though not certainly, the case for any stable system. In practice, the system must be more than merely stable - its transients must decay fast enough for correlation to be possible after one or two cycles of the input. It is thought that any system stable enough to be tested in this way will present no convergence difficulties.

4. We conclude this section by referring to the reduction of order by averaging, described in Section 5.1. Averaging (20) over \( s = 1 \) to \( N \) gives (19) multiplied by \( X_0 \), and averaging (19) over \( r = 1 \) to \( N \) gives the zero-order equation corresponding to (9):

\[ Y_0 = X_0 \sum_j w_1(j) + \sum_{jk} w_2(j,k) X_1(j-k). \]  

(21)

Hence all the information available for determining the weights is in (20); there are at most \( \frac{1}{2} N(N+1) \) equations in this set, since \( Y_2(r,s) = Y_2(s,r) \), to determine both the \( \frac{1}{2} N(N+1) \) weights \( w_2 \) and the \( N \) weights \( w_1 \). Thus, at best, the weights are underdetermined.
5.3. Second-order weight equations for two types of binary input

The next few sections are devoted to a detailed examination of the correlation equations (19) and (20), for various types of pseudorandom input. We begin with binary inputs, because these have been the best-studied in connexion with linear identification; and we consider the two types of binary input already discussed in Annex 1 for the multi-input linear case.

1. Binary m-sequence. Take the levels as \((1,-1)\), then from 2.3(3) and (6) we have

\[
X_0 = -N^{-1}; \quad X_1(j) = (1 + N^{-1})E_j - N^{-1},
\]

where 
\[
E_j = 1, \quad j \equiv 0 \mod N; \quad E_j = 0 \text{ otherwise}.
\]

(Compare the definition 3.2(4).) Hence the binary-m-sequence form of (21) is:

\[
Y_0 = -N^{-1} \sum_j w_1(j) + (1 + N^{-1}) \sum_j w_2(j,j) - N^{-1} \sum_{jk} w_2(j,k).
\]

To evaluate \(X_2\) we use Property B' of Section 2.3, which we now write as

\[
a_{i-1} = a_{i-j} a_{i-k}, \quad \text{all } i.
\]

(25) defines a unique 1 in \(1 \leq 1 \leq N\), for any values \(j,k\) in this range such that \(j \neq k\). From (8) and (25), together with (22) and (23), we have

\[
X_2(j-r,k-r) = N^{-1} \sum_{i} a_{i-r} a_{i-j} a_{i-k}
\]

\[
= N^{-1} \sum_{i} a_{i-r} a_{i-1} = (1 + N^{-1})E_{1-r} - N^{-1}.
\]

Hence (19) becomes

\[
Y_1(r) = \sum_j w_1(j) \left\{ (1 + N^{-1})E_{j-r} - N^{-1} \right\}
\]

\[
+ \sum_{jk} w_2(j,k) \left\{ (1 + N^{-1})E_{1-r} - N^{-1} \right\}.
\]

By subtracting (24) from (27) we obtain the neater form

\[
Y_1(r) - Y_0 = (1 + N^{-1}) \left\{ w_1(r) + \sum'_{jk} w_2(j,k) - \sum_{j} w_2(j,j) \right\},
\]

where the sum \(\sum'_{jk}\) is over those values of \((j,k)\) for which (25) gives \(l = r\).
From the uniqueness property of \( l \), it follows that each equation of the set (28), \( r = 1 \) to \( N \), contains exactly \( N - 1 \) elements \( w_2(j,k) \) with \( j \neq k \), and that in the set of \( N \) equations each such element occurs exactly once. We have therefore achieved as good a separation of the unknowns as may be obtained using the correlation equations (39) and (21); and we have a total of \( N \) equations to determine both the \( N \) linear weights \( w_1 \) and the \( \frac{1}{2}N(N+1) \) second-order weights \( w_2 \).

We now show that no additional information is provided by the correlation equations (20), for the binary-\( m \)-sequence input. Let

\[
a_i = a_i - a_i - s , \quad \text{all } i ,
\]

where \( u, r \) and \( s \) are in the range \( 1 \) to \( N \) and \( r \neq s \); this defines a unique \( u \) for given \( r, s \). From (4), (8) and (29) we have

\[
Y_2(r,s) = Y_1(u) ;
\]

also, since \( a_i^2 = 1 \) for all \( i \), we have

\[
Y_2(r,r) = Y_0 .
\]

It follows from (30) and (31) that the left-hand side of any equation of the set (20) equals the corresponding term in one of (28), and the same may be shown to hold for the equation as a whole. Hence with this input, equations (20) give redundant information.

In the same way, it can be shown that the higher-order correlation equations, obtained for the higher-order approximations to \( y(t) \), all reduce to a set of \( N \) independent equations.

2. Binary \( m \)-sequence with alternate terms inverted. The \( i \)th term of this sequence is \((-1)^i a_i \) where \( \{a_i\} \) is a binary \( m \)-sequence. We denote the overall period by \( N \), as usual, so that the period of \( \{a_i\} \) is \( M = \frac{1}{2}N \).

Since the second half-cycle is the negative of the first half, all \( X_i \) are zero for even \( i \). Defining now \( \xi_j = 1 \) when \( j \equiv 0 \mod M \), and \( \xi_j = 0 \) otherwise, we have
\[ X_1(j) = (-1)^j \{ (1 + M^{-1}) E_j - M^{-1} \} . \quad (32) \]

From (19) and (32) we have
\[ Y_1(r) = (1 + M^{-1}) \left\{ w_1(r) - w_1(r + M) \right\} - (-1)^r M^{-1} \sum_j (-1)^j w_1(j) , \quad (33) \]
where the summation is over \( j = 1 \) to \( N \) as before. It is convenient to introduce the modified weights \( W_1(j) \), \( j = 1 \) to \( M \), defined as
\[ W_1(j) = w_1(j) - w_1(j + M) . \quad (34) \]
then (33) becomes
\[ Y_1(r) = (1 + M^{-1}) W_1(r) - (-1)^r M^{-1} \sum_{j=1}^M (-1)^j W_1(j) . \quad (35) \]

From (35) we have
\[ \sum_{r=1}^M (-1)^r Y_1(r) = \sum_{j=1}^M (-1)^j W_1(j) ; \]
the solution of (35) for the modified linear weights is thus
\[ (1 + M^{-1}) W_1(r) = Y_1(r) + (-1)^r M^{-1} \sum_{j=1}^M (-1)^j Y_1(j) . \quad (36) \]

Now consider the second-order weights, and suppose first that \( r - s \neq 0 \) mod \( M \), and \( j - k \neq 0 \) mod \( M \). Then from (8), (25) and (29) we have
\[ X_3(s-r,j-r,k-r) = N^{-1} (-1)^{r+s+j+k} \sum_{i} a_{i-r} a_{i-s} a_{i-j} a_{i-k} \]
\[ = N^{-1} (-1)^{r+s+j+k} \sum_{i} a_{i-u} a_{i-l} \]
\[ = (-1)^{r+s+j+k} \left\{ (1 + M^{-1}) E_{u-l} - M^{-1} \right\} . \quad (37) \]

Further,
\[ Y_2(r,s) = (-1)^{r+s+u} Y_1(u) . \quad (38) \]
It is again convenient to use the inverted-half-cycle property of the input by introducing the modified weights \( W_2(j,k) \), \( 1 \leq j, k \leq M \):
\[ W_2(j,k) = w_2(j,k) - w_2(j + M,k) - w_2(j,k + M) + w_2(j + M,k + M) . \quad (39) \]

From (20), (37), (38) and (39) we have
\[ (-1)^u Y_1(u) = \sum_{j=1}^M \sum_{k=1}^M (-1)^{j+k} W_2(j,k) \left\{ (1 + M^{-1}) E_{u-l} - M^{-1} \right\} \]
\[ = (1 + M^{-1}) \sum_{j,k} (-1)^{j+k} W_2(j,k) - M^{-1} \sum_{j=1}^M \sum_{k=1}^M (-1)^{j+k} W_2(j,k) \quad (40) \]
where the summation \( \sum' \) is over those \( (j,k) \) in the range 1 to \( M \) for which \( l = u \).
Now let \( r = s \), then since \( X_0 = 0 \) for this input, we have from (21) and (32):
\[
Y_2(r,r) = Y_0 = \sum_{j=1}^{M} \sum_{k=1}^{M} w_2(j,k) \cdot (-1)^{j+k} \left\{ (1 + M^{-1}) \sum_{j=1}^{M} \sum_{k=1}^{M} w_2(j,k) \right\}
\]
\[
= (1 + M^{-1}) \sum_{j=1}^{M} w_2(j,j) - M^{-1} \sum_{j=1}^{M} \sum_{k=1}^{M} (-1)^{j+k} w_2(j,k). \quad (41)
\]

Putting \( u = r \) in (40), and combining this equation with (41), gives
\[
(-1)^r Y_1(r) - Y_0 = (1 + M^{-1}) \left\{ \sum_{j=1}^{M} (-1)^{j+k} w_2(j,k) - \sum_{j=1}^{M} w_2(j,j) \right\}. \quad (42)
\]

Owing to the half-cycle symmetry of the input, \( y(t + M) = -y(t) \); hence (42) is unchanged if \( r \) is replaced by \( r + M \). Thus there are just \( M \) equations (42) for the second-order weights, and another \( M \) equations (36) for the linear weights.

By extending the 'shift-and-add' process defined in (25) or (29), we can show that higher-order approximations yield correlation equations which are linearly dependent on those for \( Y_1(r) \), so that there remain only \( N \) independent equations for determining all the weights.

3. Discussion. There is little to choose between these two types of input, except that the 'inverted binary' input separates the equations for the \( w_1 \) from those for the \( w_2 \). Each type yields exactly \( N \) equations.

It is conjectured that no other type of binary input sequence will yield more information; but since the other main class of pseudorandom binary sequence, the quadratic-residue class, do not possess the 'shift-and-add' property, no general method has been found for obtaining expressions for the higher-order correlation functions.

Section 5.6 gives examples of second-order correlation equations derived from the above two types of binary input. The next two sections are concerned with ternary-m-sequence inputs.
5.4. Correlation functions $X_1$ and $X_3$ for a ternary m-sequence

Let the ternary element field be $(0,1,-1)$ and let $M = \frac{1}{2} N$. Then, as stated in Section 2.5, we have $a_{i+M} = -a_i$, all $i$. Hence all the even $X_i$ are zero; it follows, as in the case of the 'inverted binary' input of Section 5.3, that the odd-order and the even-order weights $w_i$ appear in separate sets of equations.

This was the reason why Hooper and Gyftopoulos (1967) selected ternary m-sequences, out of the class of pseudorandom sequences, for nonlinear correlation. These authors, however, were unable to derive an expression for $X_3(i,j,k)$ when no two of $i,j,k$ are equal, and they obtained such values by computation. In this section we give the required expression for $X_3$; this result is believed to be new, and it is extended in Section 5.7 to give $X_i$ of any odd order.

Zierler (1959) derives $X_1$ from his Theorem 12, which when applied to a ternary sequence states that in the set of ordered pairs $\{(a_{i-j}, a_i)\}$, $i=1$ to $N$, $j \neq 0 \mod M$, the pair $(0,0)$ appears $3^{n-2} - 1$ times, and each other pair appears $3^{n-2}$ times; where $N = 3^n - 1$. From this result and the property $a_{i+M} = -a_i$, we have from (4),

$$X_1(j) = N^{-1} \sum_{i=1}^{N} a_{i-j} a_i = N^{-1} (2 \cdot 3^{n-1}) (-1)^{j/M} \varepsilon_j,$$  \hspace{1cm} (43)

where $\varepsilon_j = 1$ if $j \equiv 0 \mod M$, and $\varepsilon_j = 0$ otherwise.

We shall now derive (43) by using the following identity, which will also be used to derive $X_3$: let $x$, $y$ be any elements from the field $(0,1,-1)$ and let $\oplus$, $\ominus$ denote addition and subtraction modulo 3. Then

$$(x \oplus y)^2 - (x \ominus y)^2 \equiv x y \mod 3.$$  \hspace{1cm} (44)

Now put $x = a_i$, $y = a_{i-j}$, and suppose $j \neq 0 \mod M$. Then by the 'shift-and-add' property there exist $p$, $q$ such that, for all $i$,

$$a_{i-p} = a_i \ominus a_{i-j}, \quad a_{i-q} = a_i \oplus a_{i-j}.$$  \hspace{1cm} (45)
From (44) and (45) we have
\[ a_{i-j} a_i = a_{i-p}^2 - a_{i-q}^2. \]  
(46)

Summed over \( i = 1 \) to \( N \), we have \[ \sum_i a_{i-p}^2 = \sum_i a_{i-q}^2 = 2 N \gamma^{-1}; \] hence \( X_i(j) = 0 \) for \( j \neq 0 \mod M \). The nonzero values of \( X_i(j) \) follow directly from the property \( a_{i+M} = -a_i \), but we may note here that if \( j = 0 \) then \( a_{i-p} = -a_i \) and \( a_{i-q} \) is replaced by zero in (45); and if \( j = M \) then \( a_{i-q} = a_i \) and \( a_{i-p} \) is replaced by zero.

2. Now consider \( X_j \); from (8) we have, summing from \( i = 1 \) to \( N \),
\[ X_j(s-r,j-r,k-r) = N^{-1} \sum_i a_{i-r} a_{i-s} a_{i-j} a_{i-k}. \]  
(47)

Suppose that neither \( j - k \) nor \( r - s \) is a multiple of \( M \), then there exist \( l, m, u, v \) such that
\[ a_{i-l} = a_{i-j} \oplus a_{i-k}, \quad a_{i-m} = a_{i-j} \oplus a_{i-k}; \]
\[ a_{i-u} = a_{i-r} \oplus a_{i-s}, \quad a_{i-v} = a_{i-r} \oplus a_{i-s}. \]  
(48)

From (44), (47) and (48) we have
\[ X_j(s-r,j-r,k-r) = N^{-1} \sum_i (a_{i-l}^2 - a_{i-m}^2)(a_{i-u}^2 - a_{i-v}^2). \]  
(49)

To evaluate expressions such as \( \sum_i a_{i-l}^2 a_{i-u}^2 \), we may either use Zierler's theorem, or an identity derived from (44). The latter approach, though longer, leads on to a general theorem which we shall derive and use in Section 5.7; we therefore adopt this method of evaluating \( X_j \).

Squaring both sides of the identity (44) gives
\[ (x \oplus y)^4 - 2(x^2 - y^2)^2 + (x \odot y)^4 \equiv x^2 y^2 \].

Since \( z^4 = z^2 \) for any element \( z \) of the ternary field, this gives
\[ (x \oplus y)^2 - 2(x^2 - 2x^2 y^2 + y^2) + (x \odot y)^2 \equiv x^2 y^2 \],
or \[ (x \oplus y)^2 - 2(x^2 + y^2) + (x \odot y)^2 \equiv -3x^2 y^2 \],
(50)
which is the required identity.

Putting \( x = a_{i-l}, y = a_{i-u} \) in (50), and summing over \( i = 1 \) to \( N \), gives
\[ 3 \sum_i a_{i-l}^2 a_{i-u}^2 = \sum_i 2(a_{i-l}^2 + a_{i-u}^2) - \sum_i (a_{i-l} \oplus a_{i-u})^2 \]
\[ - \sum_i (a_{i-l} \oplus a_{i-u})^2. \]  
(51)
The first sum on the right-hand side of (51) equals $2 \cdot 3^{n-1}$; the second sum is zero if $l - u \equiv M \mod N$, and equals $2 \cdot 3^{n-1}$ otherwise; the third sum is zero if $l - u \equiv 0 \mod N$, and equals $2 \cdot 3^{n-1}$ otherwise. Hence (51) can be written as

$$\sum_{i} a_{i-1}^2 a_{i-u}^2 = 2 \cdot 3^{n-2}(2 + \epsilon_{l-u})$$  \hspace{1cm} (52)

From (49) and (52) we get the required expression

$$X_3(s-r,j-r,k-r) = N^{-1}(2 \cdot 3^{n-2})(\epsilon_{l-u} - \epsilon_{m-u} - \epsilon_{1-v} + \epsilon_{m-v})$$  \hspace{1cm} (53)

By forming the modulo-3 sum and difference of $a_{i-1}$ and $a_{i-m}$, and using (48), we find that $l - m \not\equiv 0 \mod M$; similarly, $u - v \not\equiv 0 \mod M$.

Hence if $\epsilon_{l-u} = 1$, then $\epsilon_{m-u} = \epsilon_{1-v} = 0$. Again, we have from (48):

$$a_{i-1} \oplus a_{i-u} = a_{i-m} \oplus a_{i-v}$$  \hspace{1cm} (54)

If $l = u$, the left-hand side of (54) equals $-a_{i-1} = a_{i-1+M}$. In this case the relation $m - v \equiv 0 \mod N$ would imply $l - m \equiv 0 \mod N$ which is false; and $m - v \equiv M \mod N$ would imply that the right-hand side of (54) is zero, which is false. Hence $m - v \not\equiv 0 \mod M$, and this result also holds, by a similar argument, when $l = u + M$. Thus, if $\epsilon_{l-u} = 1$, then $\epsilon_{m-v} = 0$.

By the same reasoning applied to the other three terms in (53), it follows that the only values possible for $\epsilon_{l-u} - \epsilon_{m-u} - \epsilon_{1-v} + \epsilon_{m-v}$ are $0, 1, -1$.

Finally we consider the cases where either or both of $j - k$ and $r - s$ are multiples of $M$. If $r = s$ then (44), (47) and (52) give

$$X_3(0,j-r,k-r) = N^{-1} \sum_{i} (a_{i-1}^2 - a_{i-m}^2) = N^{-1}(2 \cdot 3^{n-2})(\epsilon_{1-r} - \epsilon_{m-r})$$  \hspace{1cm} (55)

If $r = s + M$, the sign of $X_3$ is reversed. Similar results hold when $j = k$ or $j = k + M$. If both $r = s$ and $j = k$, then (47) and (52) give

$$X_3(0,j-r,j-r) = N^{-1} \sum_{i} a_{i-1}^2 a_{j-i}^2 = N^{-1}(2 \cdot 3^{n-2})(2 + \epsilon_{r-j})$$  \hspace{1cm} (56)

This completes the determination of $X_3$ for a ternary $m$-sequence.

Tables of values of $X_3$ for some specific sequences are given in Section 5.6.
5.5. Second-order weight equations for ternary-m-sequence input

In this section we derive explicit solutions for the weights $w_1$ and $w_2$, from the second-order-approximation equations (19) and (20), using the results of Section 5.4.

1. Since $a_{1+M} = -a_1$, and thus $X_2 = 0$, we introduce the modified linear weights $W_1$ defined in (34). Then from (19) and (43) we have the solution:

$$W_1(r) = M \cdot 3^{1-n} X_1(r) \quad r = 1 \text{ to } M. \quad (57)$$

2. Since $X_2 = 0$, the equations (20) for the weights $w_2$ become

$$Y_2(r,s) = \sum_{j,k} w_2(j,k) X_3(s-r,j-r,k-r). \quad (58)$$

If neither $r-s$ nor $j-k$ is a multiple of $M$, we have from (53) and (55):

$$X_3(s-r,j-r,k-r) = X_3(0,j-u,k-u) - X_3(0,j-v,k-v), \quad (59)$$

where $u$ and $v$ are defined in (48). (59) may be shown to hold also when $j-k \equiv 0 \pmod{M}$, by using (56) and equations similar to (55).

(58) and (59) therefore give

$$Y_2(r,s) = Y_2(u,u) - Y_2(v,v). \quad (60)$$

From (60), and the fact that $Y_2(r+M,s) = -Y_2(r,s)$ etc., it follows that all those equations of the set (58) which have $r \neq s$ are redundant, and the complete set reduces to the $M$ equations with $r = s = 1 \text{ to } M$.

As in Section 5.3, $j$ and $k$ can be restricted to the range 1 to $M$ by using the modified weights $W_2$ defined in (39). Then the $M$ independent equations of the set (58) are:

$$Y_2(r,r) = \sum_{j=1}^{M} \sum_{k=1}^{M} W_2(j,k) X_3(0,j-r,k-r). \quad (61)$$

From (55), (56) and (61) we have

$$Y_2(r,r) = M^{1} \cdot 3^{n-2} \left\{ W_2(r,r) + 2 \sum_{j=1}^{M} W_2(j,j) + Z_r \right\}, \quad (62)$$

where

$$Z_r = \sum_{j,k} W_2(j,k) \cdot (\epsilon_{1-r} - \epsilon_{m-r}) \quad \quad (63)$$

in (63), $\sum^*$ denotes summation over $j,k = 1 \text{ to } M$ with $j \neq k$, and $1,m$ are defined in (48).
Since \(1\) and \(m\) are functions of \((j,k)\), there is just one \(r\) in the range \([1, M]\) for which \(1 - r \equiv 0 \mod M\), and similarly for \(m\); hence (63) implies
\[
\sum_{r=1}^{M} Z_r = 0. \tag{64}
\]
Using (64), we can write (62) as
\[
Y_2(r,r) = M^{-1}3^{n-2}\left[\sum_{j=1}^{M} W_2(j,j) + Z_j\right],
\]
which has the solution
\[
W_2(r,r) + Z_r = M^{-2-n}\left(Y_2(r,r) - 2 \cdot 3^{-n} \sum_{j=1}^{M} Y_2(j,j)\right). \tag{65}
\]

3. Discussion. This completes the determination of the second-order weights, so far as they can be identified by means of a ternary-m-sequence input. Compared with the 'inverted-binary' equations (42), we see that (65) entails the calculation of the \(Y_2(r,r)\) as well as the \(Y_1(r)\) required by (42) or (57). Whether this additional calculation, and the extra 'hardware' needed to apply a three-level rather than a two-level input, are worthwhile in terms of improved identification, remains to be seen in practice.

It is difficult to compare our results with those of Hooper and Gyftopoulos (1967), whose work seems to be the only published account of nonlinear identification by means of ternary m-sequences. These authors, as we have stated, did not elucidate the behaviour of \(X_2\), hence they did not discover the redundancy of the equations. They did not distinguish between the weights \(w_i\) and the kernels \(h_i\), but they appear to have made a partial application of (56) to (58), and to have written the latter as
\[
Y_2(r,s) = M^{-1}3^{n-2}(2 + \varepsilon_{r-s})w_2(r,s).
\]
Nevertheless, in a computer simulation they succeeded in identifying a second-order, negative-exponential kernel to within a few percent of the true peak value, though to achieve this they had to use selected ternary sequences of period 2186 or 6560.
5.6. Correlation equations arising from particular input sequences

In this section we consider, first, a ternary m-sequence of period 8, to show how the correlation equations reduce to the set (58) or (65). This is followed by an examination of a binary m-sequence of period 31; an inverted binary m-sequence of period 30; and a ternary m-sequence of period 26.

1. Ternary m-sequence, N = 8. The sequence, starting with $a_0$, is

$$a_1 = -1, 1, -1, 0, 1, 0, 1, 1$$

We take the suffixes $r, s, j, k$ over the range 0 to 3 instead of 1 to 4, for convenience in calculating the $X^3_2$; and we use the symmetry $W_2(r,s) = W_2(s,r)$ to reduce the number of 'unknowns'.

Then (58) is as follows:

<table>
<thead>
<tr>
<th>Row</th>
<th>$W_2(0,0)$</th>
<th>$Y_2(0,0)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3, 2, 2, 2, 0, 1, -1, 0, 1, 0</td>
<td>1, 1</td>
</tr>
<tr>
<td>2</td>
<td>2, 3, 3, 2, 0, 0, 1, -1, 0, 1</td>
<td>2, 2</td>
</tr>
<tr>
<td>3</td>
<td>2, 2, 2, 3, 1, -1, 0, 1, 0, 0</td>
<td>3, 3</td>
</tr>
<tr>
<td>4</td>
<td>2, 0, 0, -1, 1, 2, -1, 0, 1, 1</td>
<td>2W_2(1,0)</td>
</tr>
<tr>
<td>5</td>
<td>2, 1, 0, 0, -1, 1, 2, -1, 1, 1, 0</td>
<td>1, 0</td>
</tr>
<tr>
<td>6</td>
<td>3, 2, -1, 0, 0, 1, 2, -1, -1, 2, -1</td>
<td>2, 1</td>
</tr>
<tr>
<td>7</td>
<td>3, 2, 0, 0, -1, 1, 1, -1, 2, 0, -1</td>
<td>3, 2</td>
</tr>
<tr>
<td>8</td>
<td>3, 1, 0, 0, -1, 1, 1, -1, 2, 0, 1</td>
<td>2, 1</td>
</tr>
<tr>
<td>9</td>
<td>3, 1, 0, 0, -1, 1, 1, -1, 2, 0, 0</td>
<td>3, 2</td>
</tr>
<tr>
<td>10</td>
<td>3, 0, 0, -1, 1, 1, -1, 2, 0, 1</td>
<td>3, 0</td>
</tr>
</tbody>
</table>

By inspection, the dependence of the last six equations on the first four is given by: row $i = $ row $j - $ row $k$ where

$$i = 5, 6, 7, 8, 9, 10$$

$$j = 4, 1, 2, 4, 1, 2$$

$$k = 3, 4, 1, 2, 3, 3$$

The quantities $Z_0$ to $Z_3$ defined by (63) are the terms of the first four equations involving the 'off-diagonal' $W_2$:

$$Z_0 = 2\{W_2(2,1) - W_2(3,2) + W_2(3,1)\}$$
$$Z_1 = 2\{W_2(3,2) - W_2(2,0) + W_2(3,0)\}$$
$$Z_2 = 2\{W_2(1,0) + W_2(3,1) + W_2(3,0)\}$$
$$Z_3 = 2\{W_2(1,0) - W_2(2,1) + W_2(2,0)\}$$
2. Binary m-sequence, \( N = 31 \). The determination of the correlation terms for a binary or ternary m-sequence is essentially the determination of the shift-and-add table for that sequence. For large \( N \), this can be done using polynomial multiplication (Davies 1965) or transition-matrix methods (Ireland and Marshall 1968), but for the values of \( N \) we shall use, it is easy to recognize the shifted form of the sequence.

We choose the sequence generated by \( X^5 + X^2 + 1 \), and write it in the form shown in Section 3.8. The construction of the table of \( l(j,k) \) defined by (25) is helped by using the translation-set approach. We may start directly from the generating polynomial, which gives

\[
a_i a_{i-2} = a_{i-5}, \quad \text{or} \quad l(j,j+2) = j + 5.
\]

(66)

By doubling each suffix we derive

\[
a_{2i} a_{2i-4} = a_{2i-10}, \quad \text{or} \quad l(j,j+4) = j + 10.
\]

Three more relations are obtained by successive doubling; the values may be obtained from Table 3.3, Section 3.7:

\[
l(j,j+8) = j + 20; \quad l(j,j+16) = j + 9; \quad l(j,j+1) = j + 18.
\]

We have so far 'paired' sets \( A \) and \( C \). By rearranging (66) we get

\[
a_i a_{i-3} = a_{i-29}, \quad \text{or} \quad l(j,j+3) = j + 29.
\]

This pairs sets \( B \) and \( \bar{A} \). The final rearrangement

\[
a_i a_{i-28} = a_{i-26}, \quad \text{or} \quad l(j,j+28) = j + 26
\]

pairs sets \( \bar{B} \) and \( \bar{C} \), and completes the table of \( l(j,k) \).

It is convenient to present the values in the form

\[
l(j,j+x) = j + y; \quad y = y(x),
\]

(67)

and to note that (67) implies \( l(j,j+y) = j + x \). See Table 5.1.

To use the table, write (28) as

\[
Y_1(r) - Y_0 = (1 + N^{-1}) \left[ w_1(r) + \sum_{i=1}^{N} w_2(r+i,r+i+y(N-i)) \right] = \sum_{j=1}^{N} w_2(j,j).
\]

(68)
Table 5.1. Values of \((x,y)\) in (67), for sequence generated by \(x^5 + x^2 + 1\)

<table>
<thead>
<tr>
<th>Set A</th>
<th>(x) or (y)</th>
<th>1</th>
<th>2</th>
<th>4</th>
<th>8</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>(y) or (x)</td>
<td>18</td>
<td>5</td>
<td>10</td>
<td>20</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>(x) or (y)</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>24</td>
<td>17</td>
</tr>
<tr>
<td>(\tilde{A})</td>
<td>(y) or (x)</td>
<td>29</td>
<td>27</td>
<td>23</td>
<td>15</td>
<td>30</td>
</tr>
<tr>
<td>(\tilde{B})</td>
<td>(x) or (y)</td>
<td>7</td>
<td>14</td>
<td>28</td>
<td>25</td>
<td>19</td>
</tr>
<tr>
<td>(\tilde{C})</td>
<td>(y) or (x)</td>
<td>22</td>
<td>13</td>
<td>26</td>
<td>21</td>
<td>11</td>
</tr>
</tbody>
</table>

3. Inverted binary \(m\)-sequence, \(N = 30\) (\(M = 15\)). We choose the generator \(X^4 + X + 1\). Table 5.2 gives the translation sets, the element values, and the \((x,y)\) table. To use the table to obtain the equations for the second-order weights, write (42) as

\[
(-1)^r Y_0(r) - Y_0 = (1 + M^{-1}) \left[ \sum_{i=1}^{M} (-1)^{y(M-i)} W_2(x+i, r+i+y(M-i)) \right] - \sum_{j=1}^{M} W_2(j, j). \tag{69}
\]

Table 5.2. Data for inverted-binary sequence generated by \(X^4 + X + 1\)

<table>
<thead>
<tr>
<th>Set A</th>
<th>(x) or (y)</th>
<th>1</th>
<th>2</th>
<th>4</th>
<th>8</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>(y) or (x)</td>
<td>4</td>
<td>8</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>(x) or (y)</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>(\tilde{A})</td>
<td>(y) or (x)</td>
<td>14</td>
<td>13</td>
<td>11</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>(x) or (y)</td>
<td>10</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4. Ternary \(m\)-sequence, \(N = 26\). For ternary sequences we shall adopt the convention that the translation set \(\tilde{A}\) contains elements which are those of set \(A\) shifted by half a cycle; we shall not use the same letter to denote 'reversed pairs'.

We choose the generator \(X^3 - X^2 + 1\); Table 5.3 gives the translation sets, and the element-values for this generator. The 'shift-and-add' table must now give \(1\) and \(m\) as defined by (48).

Table 5.3 gives this information as the values of \(y(x)\) and \(z(x)\) in the equations:

\[
l(j, j+x) = j + y; \quad m(j, j+x) = j + z. \tag{70}
\]
Given the first equation of (70), we can derive the following seven variants by using (48) and the half-cycle symmetry of the m-sequence:

\[ l(j, j-x) = j + y - x; \]
\[ m(j, j+x-y) = j-y, \quad m(j, j-y) = j + x - y; \]
\[ m(j, j+x+M) = j+y, \quad m(j, j-x+M) = j+y-x; \]
\[ l(j, j+x-y+M) = j-y, \quad l(j, j-y+M) = j+x-y. \]

From the generator we have, immediately, the pair \( x = 3, y = 2 \). The seven variants of this give a further seven translation-distinct pairs. The remaining values of \( (x,y) \) were found by searching for other three-term recurrence relations in the sequence; it was found that \( a_i \otimes a_{i+2} \otimes a_{i+8} = 0 \), giving \( x = 2, y = 7 \); and that \( a_i \otimes a_{i-4} \otimes a_{i-12} = 0 \), giving \( x = 4, y = 12 \).

Each of these relations provided three distinct variants.

To use the \( (x, y, z) \) table, we write (63) as

\[ z_r = \sum_{x=1}^{M-1} W_2(j_1, k_1) - W_2(j_2, k_2) \tag{71} \]

and determine the arguments from the equations:

\[ r - y = j_1 \mod M, \quad r + x - y = k_1 \mod M; \]
\[ r - z = j_2 \mod M, \quad r + x - y = k_2 \mod M. \tag{72} \]

The values of these arguments, for given \( r \), may be found from Table 5.4. In this table, a '+1' entry at \( (j-r,k-r) \) corresponds to \( j = j_1, k = k_1 \), and a '-1' entry to \( j = j_2, k = k_2 \).

Table 5.3. Data for ternary sequence generated by \( x^3 - x^2 + 1 \)

<table>
<thead>
<tr>
<th>Set</th>
<th>( \Theta )</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>( \bar{A} )</th>
<th>( \bar{B} )</th>
<th>( \bar{C} )</th>
<th>( \bar{D} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elements</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>7</td>
<td>13</td>
<td>14</td>
<td>5</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>21</td>
<td>16</td>
<td>15</td>
<td>25</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>18</td>
<td>10</td>
<td>11</td>
<td>22</td>
<td>19</td>
<td>23</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Value</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>-1</td>
<td>-1</td>
</tr>
</tbody>
</table>

**x = 1** 2 4 7 14 5 17 8
**y = 18B 7D 12C 3A 24B 14A 23B 19B**
**z = 24B 16A 23B 15B 18B 11D 12C 9B**

**To obtain other values, multiply these by 3 and 9, and read the residue mod 26 from the table, using the set-letter.**
Table 5.4. Values of arguments in (71) for sequence $x^5 - x^2 + 1$

See previous page for meaning of entries. The table is symmetrical, and only the half for $j < k$ is given.

| k - r | \hline | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 | 21 | 23 | 25 |
|-------|------|---|---|---|---|----|----|----|----|----|----|----|----|
| j - r | 1    | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| 2     | -1   | 1  | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| 3     | 1    | -1 | 1  | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| 4     | 1    | 1  | -1 | 1  | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| 5     | -1   | 1  | -1 | 1  | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| 6     | 1    | -1 | 1  | -1 | 1  | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| 7     | 1    | 1  | -1 | 1  | -1 | 1  | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| 8     | -1   | 1  | -1 | 1  | -1 | 1  | -1 | 1  | -1 | -1 | -1 | -1 | -1 |
| 9     | 1    | -1 | 1  | -1 | 1  | -1 | 1  | -1 | 1  | -1 | -1 | -1 | -1 |
| 10    | 1    | 1  | -1 | 1  | -1 | 1  | -1 | 1  | -1 | 1  | -1 | -1 | -1 |
| 11    | -1   | 1  | -1 | 1  | -1 | 1  | -1 | 1  | -1 | 1  | -1 | 1  | -1 |
| 12    | 1    | -1 | 1  | -1 | 1  | -1 | 1  | -1 | 1  | -1 | 1  | -1 | 1  |
| 13    | -1   | 1  | -1 | 1  | -1 | 1  | -1 | 1  | -1 | 1  | -1 | 1  | 1  |
| 14    | 1    | -1 | 1  | -1 | 1  | -1 | 1  | -1 | 1  | -1 | 1  | 1  | 1  |
| 15    | -1   | 1  | -1 | 1  | -1 | 1  | -1 | 1  | -1 | 1  | 1  | 1  | 1  |
| 16    | 1    | -1 | 1  | -1 | 1  | -1 | 1  | -1 | 1  | 1  | 1  | 1  | -1 |
| 17    | -1   | 1  | -1 | 1  | -1 | 1  | -1 | 1  | 1  | 1  | 1  | -1 | 1  |
| 18    | 1    | -1 | 1  | -1 | 1  | -1 | 1  | 1  | 1  | 1 | 1  | -1 | -1 |
| 19    | -1   | 1  | -1 | 1  | -1 | 1  | 1  | 1 | 1  | 1 | 1  | -1 | -1 |
| 20    | 1    | -1 | 1  | -1 | 1  | 1  | 1  | 1  | 1 | 1 | 1  | -1 | -1 |
| 21    | -1   | 1  | -1 | 1  | 1  | 1  | 1 | 1  | 1 | 1 | 1 | 1 | 1  |
| 22    | 1    | -1 | 1  | 1  | 1  | 1 | 1  | 1 | 1 | 1 | 1 | 1 | -1 |
| 23    | -1   | 1  | -1 | 1  | 1  | 1 | 1  | 1 | 1 | 1 | 1 | 1 | 1  |
| 24    | 1    | -1 | 1  | 1  | 1 | 1  | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 25    | -1   | 1  | -1 | 1  | 1 | 1  | 1 | 1 | 1 | 1 | 1 | 1 | 1|

For example, put $r = 4$ in (71) and use the property $W_2(j,k) = W_2(k,j)$; then Table 5.4 gives, from the entries with $1 \leq j - r, k - r \leq 12$:

$$Z_r = 2\{W_2(5,9) - W_2(5,15) - W_2(6,7) - W_2(6,11) - W_2(7,11)$$
$$- W_2(8,14) - W_2(8,16) + W_2(9,15) + W_2(10,12) - W_2(10,13)$$
$$+ W_2(12,13) - W_2(14,16)\}.$$

To bring all the arguments into the range 1 to 12, we then use the property $W_2(j,k) = W_2(j + M, k + M) = -W_2(j + M, k) = -W_2(j, k + M)$.

Thus, only the 'first quadrant' of Table 5.4 is needed in order to determine all the values of $Z_r$. 


5. Comparison of the inverted-binary and the ternary input. To help to assess the relative merits of these two types of input in determining the second-order weights, we give, in Table 5.5, the coefficients of $W_2(j,k)$ in the following equations: (a) (69) with $r \neq 0$; (b) (6$\sharp$) with $r \neq 0$, using (71). The data are taken from Tables 5.2 and 5.4 respectively, and to reduce the number of terms we have arbitrarily ignored $W_2(j,k)$ for $j + k > 8$.

Table 5.5. Coefficients of $W_2(j,k)$ in (a) inverted-binary, (b) ternary correlation equations

<table>
<thead>
<tr>
<th></th>
<th>j</th>
<th>k</th>
<th>r = 1 2 3 4 5</th>
<th>6 7 8 9 10</th>
<th>11 12 13 14 15</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>-1 -1 ...</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>3</td>
<td>-1 -1 ...</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>4</td>
<td>-1 -1 ...</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>3</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>4</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>4</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>5</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>6</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>7</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>3</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>3</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>6</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>7</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>4</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>4</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>5</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>5</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>6</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>6</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>7</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>4</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>4</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>5</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>5</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>6</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>6</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>7</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
</tbody>
</table>
5.7. Higher-order correlation equations with ternary input

In this section we first extend the identity (44) to a product of 2n ternary elements, and then use this result to express any correlation function of order 2n - 1 in terms of correlation functions of order 2n - 3, when the input is a ternary m-sequence. We thereby achieve the complete reduction of the correlation equations, for any order of approximation to the expansion (1).

1. The general identity. Let \( x_1, x_2, \ldots, x_{2n} \) be any 2n elements from the field \((0, 1, -1)\), and write

\[
P_n = (-3)^{n-1} x_1 x_2 \cdots x_{2n}.
\]

Let \( \oplus^i \) denote \( \oplus \) if \( i \) is even, and \( \ominus \) if \( i \) is odd; and write

\[
Q_n = \sum_{i=0}^{2n-1} \left( \sum_{i_1=0}^{2} \sum_{i_2=0}^{2} \cdots \sum_{i_{2n-1}=0}^{2} (-1)^{i_1+i_2+\cdots+i_{2n-1}} (x_1 \oplus^{i_1} x_2 \oplus^{i_2} \cdots \oplus^{i_{2n-1}} x_{2n})^2 \right).
\]

We prove, by induction on \( n \), that \( P_n = Q_n \).

Suppose \( P_{n-1} = Q_{n-1} \), then from (73), and from (44) with

\[
x = x_{2n-1}, \quad y = x_{2n},
\]

we have

\[
P_n = -3Q_{n-1} x_{2n-1} x_{2n} = -3Q_{n-1} \left\{ (x_{2n-1} \oplus x_{2n})^2 - (x_{2n-1} \ominus x_{2n})^2 \right\}.
\]

Now use (50) twice: first with

\[
x = x_1 \oplus^{i_1} x_2 \ominus^{i_2} \cdots \ominus^{2n-3} x_{2n-2}, \quad y = x_{2n-1} \ominus x_{2n} = y_1 \text{ say};
\]

and again with the same \( x \) and with

\[
y = x_{2n-1} \oplus x_{2n} = y_2 \text{ say}.
\]

Then, substituting for \( Q_{n-1} \) in (75) the expression obtained by replacing \( n \) by \( n-1 \) in (74), and using (50) in the manner described, we have

\[
P_n = \sum \cdots \sum (-1)^{i_1+i_2+\cdots+i_{2n-3}} (-3x^2 y_1^2 + 3x^2 y_2^2)
\]

\[
= \sum \cdots \sum (-1)^{i_1+i_2+\cdots+i_{2n-3}} \left\{ (x \ominus y_1)^2 + (x \oplus y_1)^2 \right. - (x \ominus y_2)^2 - (x \oplus y_2)^2 - 2(y_1^2 - y_2^2) \right\}.
\]
In (76), the term \((y_1^2 - y_2^2)\) is independent of \(i_1 \cdots i_{2n-3}\), and so the sum of such terms is zero. The remaining terms give \(Q_n\) as defined in (74). To complete the induction we note that (44) is in fact the identity \(P_1 = Q_1\); hence

\[
P_n \equiv Q_n.
\]

Note that, by defining \(z = z(i_{2n-2}, i_{2n-1})\) such that

\[
z = x_{2n-2} \oplus i_{2n-2} x_{2n-1} \oplus i_{2n-1} x_{2n},
\]

we can write (74) in the form

\[
Q_n \equiv Q_n(x_1, \ldots, x_{2n}) = \sum_{i_{2n-2}=0}^{1} \sum_{i_{2n-1}=0}^{1} (-1)^{i_{2n-1}+i_{2n-2}} Q_{n-1}(x_1, \ldots, x_{2n-3}, z).
\]

This form will be found useful in the correlation analysis.

2. Correlation function of order \(2n-1\). The basic approach is to apply the identity (77) with elements taken as:

\[
x_k = x_k(i) = a_{i-j_k}, \quad k = 1 \text{ to } 2n,
\]

where \(\{a_i\}\) is the ternary m-sequence. We write the resulting \(P_n\), defined in (73), as \(P_n(i)\), and use the following contracted notation for the correlation coefficient of order \(2n-1\):

\[
X_{2n-1}(j_2 - j_1, j_3 - j_1, \ldots, j_{2n} - j_1) \equiv [j_1, j_2, \ldots, j_{2n}].
\]

Then from (73), (80) and (81) we have

\[
\sum_{i=1}^{N} P_n(i) = (-3)^{n-1} N[j_1, \ldots, j_{2n}].
\]

Similarly, write \(Q_n = Q_n(i)\) with elements (80); then from (74) we have

\[
\sum_{i=1}^{N} Q_n(i) = \sum_{i_1}^{i_2} \cdots \sum_{i_{2n-1}}^{i_n} (-1)^{i_1 + \cdots + i_{2n-1}} \sum_{i=1}^{N} a_{i-i-1},
\]

where \(l = l(i_1, \ldots, i_{2n-1})\) is given by

\[
a_{i-1} = a_{i-j_1} \oplus a_{i-j_2} \oplus \cdots \oplus a_{i-j_{2n}}.
\]

From (77), (82) and (83) we have

\[
[j_1, \ldots, j_{2n}] = N^{-1}(-3)^{1-n} \sum_{i_1}^{i_2} \cdots \sum_{i_{2n-1}}^{N} (-1)^{i_1 + \cdots + i_{2n-1}} \sum_{i=1}^{N} a_{i-i-1}.
\]
Since $\sum_{i=1}^{N} a_{i-1}^2$ is independent of $1$, the right-hand side of (85) is zero, except when the values of $j_1, \ldots, j_{2n}$ are such that the right-hand side of (84) is zero for some set $(i_1, \ldots, i_{2n-1})$. In this event, the right-hand side of (83) has the value $\pm K$ say, where $K$ depends only on $N$ and $n$. (Compare (53) for the third-order correlation function; but note that we have changed the meaning of $n$).

The evaluation of $X_{2n-1}$ thus reduces to the determination of sets of parameters for which the right-hand side of (84) is zero. It is not necessary, however, to do this in order to reduce the correlation equations; instead, we shall use (79) to express $X_{2n-1}$ in terms of values of $X_{2n-3}$.

From (79) and (80) we have, in a straightforward extension of the previous notation:

$$
\sum_{i=1}^{N} Q_n(i; x_1, \ldots, x_{2n}) = \sum_{i=2n-2}^{i=2n-1} (-1)^{i_{2n-2}+i_{2n-1}} \sum_{i_{2n-2}}^{i_{2n-1}} (-1)^{i_{2n-2}+i_{2n-1}} Q_{n-1}(i; x_1, \ldots, x_{2n-3}, z).
$$

Multiplying (86) by $(-3)^{n-1}N$, and using (77), (78) and (82), gives

$$
-3 \sum_{j_1, \ldots, j_{2n}} [j_1, \ldots, j_{2n}] = \sum_{i=2n-2}^{i=2n-1} (-1)^{i_{2n-2}+i_{2n-1}} [j_1, \ldots, j_{2n-3}, j_{2n-2}+m],
$$

where $m = m(i_{2n-2}, i_{2n-1})$ is given by

$$
a_{i-j_{2n-2}-m} = a_{i-j_{2n-2}} \otimes a_{i-j_{2n-1}} \otimes a_{i-j_{2n}}
$$

Note that $m$ depends on the differences $j_{2n-1} - j_{2n-2}$ and $j_{2n} - j_{2n-2}$, but is otherwise independent of the $j$'s.

From (87) it follows that each $X_{2n-1}$ can be expressed as the sum (or difference) of four values of $X_{2n-3}$. It remains to be shown that this operation reduces each correlation equation to a sum or difference of equations of lower order.
3. Reduction of the correlation equations. By a straightforward extension of the analysis given in Sections 5.1 and 5.2, we can generalize equations such as (19) and (20) into:

\[ Y_k(r_1, r_2, \ldots, r_k) = \sum_{j_1} w_1(j_1) [j_1, r_1, \ldots, r_k] + \sum_{j_1, j_2} w_2(j_1, j_2) [j_1, j_2, r_1, \ldots, r_k] + \text{terms in } w_3, w_4, \ldots, \] (89)

where all summations are over 1 to \( N \). If terms up to order \( n \) are retained in the expansion (1), i.e. weights beyond \( w_n \) are ignored, then \( k \) ranges from 1 to \( n \).

For the ternary-\( m \)-sequence input, bracketed quantities \([\ldots]\) containing an odd number of terms are zero. Suppose first that \( k \) is odd, and consider the term in (89) containing \( w_1(j_1) \). In (87) and (88), replace \( j_2, \ldots, j_{2n} \) by \( r_1, \ldots, r_k \) and \( i_{2n-1} \) by \( i \). Then we have

\[ -3 [j_1, r_1; \ldots, r_k] = \sum_{i=0}^{k} \sum_{j=0}^{t} (-1)^{i+j} [j_1, r_1; \ldots, r_{k-3}, r_{k-2} + m(i,j)] \] (90)

\( m \) is independent of \( j_1 \), and a similar equation holds for each term in (89) containing \( w_2 \), each term containing \( w_3 \), and so on. Hence from (89) and (90) we have

\[ -3 Y_k(r_1, \ldots, r_k) = \sum_{i=0}^{k} \sum_{j=0}^{t} (-1)^{i+j} Y_{k-2}(r_1, \ldots, r_{k-2} + m) \] (91)

If \( k \) is even, the same result holds by consideration of the terms in (89) containing \( w_2, w_4, \ldots \).

By successive application of (91), we can reduce any correlation equation such as (89) to the equations for \( Y_2 \) if \( k \) is even, or to \( Y_1 \) if \( k \) is odd. It can be shown that (60) still holds for the higher-order approximations; hence the complete set (89) reduces to \( M \) equations in \( Y_1(r) \) and another \( M \) equations in \( Y_2(r,r) ; r = 1 \) to \( M \).
5.8. Discussion on nonlinear correlation

There is little to add to what we have stated in Section 5.5; the choice of input sequences for nonlinear identification seems to lie between the 'inverted-binary' and the ternary m-sequences. The superficial comparison between these, given in Section 5.6, Table 5.5, is of small value in the absence of practical experience.

Such experience will be of particular interest in revealing any advantage of a three-level over a two-level input. Common sense suggests that the former should provide a much more precise identification of the nonlinear weights, but this is not readily seen from our analysis. To take the point further: I have briefly studied quinary m-sequences, with levels 0, ±1, ±2, but I have not succeeded in finding an identity corresponding to the result (44) which gave the key to the higher-order correlations of ternary m-sequences.

We have not tried to compare pseudorandom sequences with other kinds of input as regards nonlinear identification. Hooper and Gyftopoulos (1967) claim that their test input achieved the same precision as that reported in a similar experiment using 'white' Gaussian noise as input, but needed only one-quarter as much input/output data; indeed, their reason for using ternary m-sequences was the imagined resemblance to white Gaussian noise.

In passing, we may note that the idea of using Gaussian noise to test nonlinear systems goes back to Wiener (1928), in whose hands it became a powerful analytical tool for use with an expansion of the nonlinearity in a series of orthogonal functions of time and amplitude. Wiener's work has found few direct applications, though it has done much to stimulate analytical thought. A survey by Harris and Lapidus (1967) describes some possible simplifications, notably the use of two-level inputs. However, once the strict
Wiener approach is abandoned, the connexion between random input and orthogonality of system description disappears; one can keep either a simple input, or an orthogonal-series model, but not both. For example, Lubbock and Barker (1964) used an adaptive orthogonal model with naturally-occurring disturbances as input; whereas Roy, Miller and deRusso (1964) used a nonperiodic binary input, and an unstructured model which was merely the set of stored values of the transient response to that input.

To conclude: periodic step sequences are one of many possible types of test input, and the expansion (1) is one of many possible nonlinear models. As a systematic approach which leads to a known set (probably N) independent equations, exact in the absence of noise, it should be worth exploiting on actual systems. In practice, the distinction between the weights \( w_i \) and the kernels \( h_i \) is probably unimportant, and indeed a discrete model may well be superior, computationally, to a continuous one. The distinction should be kept in mind; however; it is essential to use as short a period as is compatible with the 'settling time' of the system, in order that the scatter of experimental results due to external disturbances may be reduced by correlating over a number of cycles.
Appendix 1. Effect of drift on linear identification by means of binary or ternary m-sequences

1. Suppose equation 2.1(1) for the output of a linear system is replaced by

\[ y(t) = \int_0^\infty h(u)x(t-u)\,du + e(t) \]  

(1)

where \( e(t) \) is an unknown 'noise' term, occurring independently of the input \( x(t) \). Suppose also that, because \( e(t) \) is unknown, we compute a kernel \( h^*(t) \) from the correlation equation 2.1(3):

\[ R_{xy}(\tau) = \int_0^\infty h^*(u)R_{xx}(\tau-u)\,du \]  

(2)

using the definitions 2.1(4) and (5) of \( R_{xx} \) and \( R_{xy} \). This compares with the 'true' equation for \( h(t) \) obtained from (1) by multiplying by \( x(t-\tau) \) and averaging over \( t \):

\[ R_{xy}(\tau) = \int_0^\infty h(u)R_{xx}(\tau-u)\,du + R_{xe}(\tau) \]  

(3)

where \( R_{xe}(\tau) = \frac{1}{
\int_0^\infty x(t)e(t+\tau)\,dt \).  

(4)

From (2) and (3) it follows that \( h^*(t) = h(t) \) only if \( R_{xe}(\tau) \equiv 0 \); the noise is then said to be 'uncorrelated' with the input.

2. We consider here the case where the noise is a secular variation or 'drift' of the form:

\[ e(t) = k_0 + k_1 t + \ldots + k_r t^r \]  

(5)

the values of the constants \( k_0 \ldots k_r \) being unknown. If all the \( k \)'s are zero except \( k_0 \) and \( k_1 \), we speak of 'linear drift'; if \( k_2 \) also is nonzero, we speak of 'quadratic drift'.

The fact that significant errors, due to drift, occur in identifying \( h(t) \) by means of pseudorandom inputs, has been known experimentally for some time. Douce, Ng and Walker (1966) performed experiments on a linear system, subjected to linear drift and with a binary-m-sequence input; they found that the error could be materially decreased by starting the correlation averaging at the right point in the input cycle. Subsequently, it was shown empirically by Barker (1967) that linear-drift error could be
removed altogether, by the appropriate choice of starting-point, for any binary m-sequence of period $N \leq 255$; he also examined the dependence of the quadratic-drift error on the choice of sequence.

Meanwhile, Davies and Douce (1967) had developed a method of removing the error due to drift of the form (5), by computing the correlations cycle-by-cycle and solving a set of $r$ simultaneous equations in the input moments.

The object of the work reported here is to prove Barker's result for binary m-sequences, and to show that it does not hold for all ternary m-sequences.

3. Let the input sequence be $\{a_i\}$, with levels as yet undefined. The input is then

$$x(t) = a_i, \quad i \leq t < i + 1; \quad i = 0, \pm 1, \pm 2, \ldots \quad (6)$$

From (4), (5) and (6) we have

$$R_{xe}(\tau) = \frac{\text{av}}{i} \left[ a_i \right]_i^{-i+1} e(t) dt$$

$$= \frac{\text{av}}{i} \left[ a_i [k_0 + (i+\tau+\frac{1}{2})k_1 + \{(i+\tau)^2 + (i+\tau)+\frac{1}{2}\}k_2 + \ldots] \right]$$

From (7), the condition for zero error, i.e. $R_{xe}(\tau) = 0$, in the presence of drift of the form (5) is:

$$\frac{\text{av}}{i} \left[ i^j a_i \right] = 0, \quad j = 0, 1, \ldots, r \quad (8)$$

Since the sequence is periodic, the averaging operation in (8) may be replaced by summation, with respect to $i$, over any cycle or whole number of cycles.

4. Now suppose $\{a_i\}$ is a binary m-sequence; let $\{b_i\}$ be the mapping of this sequence onto the $(0,1)$ field; and suppose $b_i = 0$ corresponds to $a_i = a_-$, and $b_i = 1$ to $a_i = a_+$. Also let

$$M = \frac{1}{2}(N + 1) = 2^{n-1}.$$  

Then putting $j = 0$ in (8) gives

$$0 = \frac{\text{av}}{i} \left[ a_i \right] = a_+ - (a_+ - a_-) \frac{\text{av}}{i} \left[ b_i \right]$$

$$= a_+ - (a_+ - a_-) \frac{M}{N}, \quad (9)$$

by Property A of Section 2.3. This is the condition for the removal of the 'bias' error in the correlation equation. Again,
putting $j = 1$ in (8) gives

$$0 = a_i v[i a_i] = a_i v[i] - (a_+ - a_-) a_i v[i b_i].$$

(10)

To remove the effect of linear drift, both (9) and (10) must hold.

It is convenient to take the average over a single cycle starting with $i = 1$. Since $\sum_{i=1}^{N} i = N M$, (9) and (10) then give:

$$\sum_{i=1}^{N} i b_i = M N a_+/(a_+ - a_-) = M^2.$$ 

(11)

This equation is equivalent to the one obtained by Barker.

5. We proceed to show that (11) can be satisfied by any binary $m$-sequence, with appropriate translation. The proof has been published (Ream 1968), and the result is believed to be new.

The sequence will be defined by equation 3.8(1), and since this definition fixes the point $i = 0$, we retain the freedom to translate the sequence by rewriting (11) as

$$\sum_{i=1}^{N} i b_i + j = M^2.$$ 

(12)

The problem is now to choose $j$ so that $0 \leq j \leq N - 1$ and (12) holds.

Denote the left-hand side of (12) by $S_j$, then we have

$$S_j - S_{j-1} = N b_j - \sum_{i=0}^{N-1} b_{i+j} = N b_j - M.$$ 

(13)

By repeated use of (13) we obtain

$$S_j - S_0 = N \sum_{i=1}^{N} b_i - jM.$$ 

(14)

From (14) it follows that, to satisfy (12), we must choose $j$ so that

$$S_0 = M^2 + jM - N \sum_{i=1}^{j} b_i.$$ 

(15)

6. $S_0$ will be evaluated by examining the translation sets such as those shown in Table 3.3. We denote by $T_k$ the translation set whose leading element is $b_k$.

The number of elements in $T_k$ is the least integer $e$ for which $k(2^e - 1)$ is a multiple of $N$. We write

$$f = 2^e - 1, \ g = N/f, \ h = k/g.$$ 

(16)

$f$, $g$ and $h$ are integers dependent on $k$. By definition, we have

$$1 \leq h \leq f,$$ 

and so $h$ has an $e$-digit binary representation. The values
of the suffix \( i \) for every \( b_i \) in the set \( T_k \) are obtained by successive cyclic shifts of the binary number \( h \); let these shifts produce in turn the numbers \( h, h', h'', \ldots \), then from (16) the suffixes of the elements of \( T_k \) are:

\[
k = gh, \quad k' = gh', \quad k'' = gh'', \quad \ldots
\]  

(17)

If \( h \) contains a 'one' in the most-significant-digit place, then from (16), \( k \) lies in the range \( M \leq k \leq N \); and similarly for \( k' \) etc. Hence the number of elements of \( T_k \) whose suffixes lie in the above range is the number of ones in the binary number \( h \); let this number of ones be \( m_k \).

Let \( t_k = \sum_i, \) summed over the values of \( i \) which occur as suffixes in \( T_k \). Then from (16) and (17) we have

\[
t_k = g(h + h' + h'' + \ldots) = g m_k f = N m_k.
\]  

(18)

Hence \( t_k / N \) is the number of elements of \( T_k \) whose suffixes lie in the range \( M \leq i \leq N \). Summing (18) over those values of \( k \) for which \( b_k = 1 \) (these values depend on the choice of sequence generator), we get

\[
t_k = S_0 = N \sum_{i=M}^{N} b_i.
\]  

(19)

Since \( M \) and \( N \) are coprime, the fact that (19) and (15) together give

\[
n(\sum_{i=1}^{j} b_i + \sum_{i=M}^{N} b_i) = M^2 + j M
\]  

(20)

implies that the unique value of \( j = M - 1 \) exists satisfying the condition for removal of linear-drift error, since in this case, either side of (20) has the value \( NM \). We must therefore start a cycle, for correlation purposes, with the term \( b_M \) as defined by 3.8(1).

As an illustration, Table A.1 shows the translation sets and the other quantities mentioned above, for the case \( n = 6, N = 63 \).
7. We now attempt to extend the result to nonbinary m-sequences; we shall consider the case where the base q is an odd prime, and the mapping is from the q-ary field 0, 1, ..., q - 1 onto the levels 0, 1, ..., \( \frac{q}{2}(q - 1) \), \( -\frac{q}{2}(q - 1) \), ..., \(-1\). Then, since one cycle contains \( q^{n-1} \) of each nonzero element, and these are balanced about zero, condition (8) with \( j = 0 \) is satisfied. To remove linear-drift error, therefore, it is sufficient to satisfy (8) with \( j = 1 \).

Proceeding as in the binary case, we define

\[
R_j = \sum_{i=1}^{N} a_{i+j},
\]

and seek a value of \( j \) in the range 0 \( \leq j \leq N - 1 \) such that \( R_j = 0 \). We have

\[
R_j = R_{j-1} + Na_j - \sum_{i=0}^{N-1} a_{i+j} = R_{j-1} + Na_j, \text{ by the 'zero-mean' property },
\]

\[
= \ldots = R_0 + N \sum_{i=1}^{j} a_i .
\]
e is again the number of elements in the set $T_k$, and now the integers $f, g$ and $h$ are defined as

$$f = q^e - 1, \quad g = N/f, \quad h = k/g.$$  \hfill (23)

The suffixes of the elements of $T_k$ are $gh, gh', \ldots$, where $h, h', \ldots$ are successive cyclic shifts of the q-ary number $h$.

If the most-significant digit of $h$ has the value $r$, then from (23),

$$r q^{n-1} \leq g h \leq (r+1)q^{n-1} - 1.$$  \hfill (24)

Hence the number of $r$'s in the q-ary number $h$, $m^{(r)}_k$ say, is the number of elements of $T_k$ whose suffixes lie in the range (24).

Summing the values $i$ of the suffixes in $T_k$, by summing a geometric series and using (23), gives

$$t_k = g\{h + h' + \ldots + h^{(e-1)}\}$$

$$= g\{(q^e - 1)/(q - 1)\} \sum_{r=1}^{q-1} r m_k^{(r)}$$

$$= \left\{N/(q - 1)\right\} \sum_{r=1}^{q-1} r m_k^{(r)}.$$  \hfill (25)

Denote by $\sum_i^{(r)}$ summation over those values of $i$ lying in the range (24); then from (25) we have

$$R_0 = \left\{N/(q - 1)\right\} \sum_{r=1}^{q-1} r \sum_i^{(r)} a_i.$$  \hfill (26)

From (22) and (26), the condition for zero linear-drift error is

$$\sum_{r=1}^{q-1} r \sum_i^{(r)} a_i + (q - 1) \sum_{i=1}^j a_i = 0.$$  \hfill (27)

8. A necessary condition for (27) to hold for some $j$ is that the first term be divisible by $q - 1$; we now show that no ternary m-sequence with $n = 3$ or 4 has this property.

For $n=3$, we require $\sum_{i=1}^{17} a_i$ to be even. In the notation of Table 5.3, the middle third of the cycle is represented by the sequence of sets $A C D C \overline{A} \overline{B} \overline{A} \overline{C}$. Each letter appears here an odd number of times, and so the sum of the $a_i$ is even only if the element-values corresponding to an odd number of the letters are zero. Now, the value for $\overline{A}$ is 0 for any 26-digit sequence, and
since one complete cycle contains 8 zeros, it follows that just one of the four pairs \((A, \overline{A})\) ... \((D, \overline{D})\) has zero element-value. Hence (27) is not satisfied for any value of \(j\).

For \(n=4\) we require \(\sum_{i=27}^{53} a_i\) to be even. In the notation of Appendix 2, the middle third of the cycle is represented by the sequence of sets

\[
A \ C \ E \ G \ I, \ F \ H \ K \ D \ C, I \ K \ I \ \Theta, \ A \ B \ A \ C \ D \ B, \ E \ F \ A \ G \ H, \ C \ I.
\]

Each letter appears an even number of times except \(\Theta\), whose value is always \(-1\) for \(n=4\). Hence the sum of the \(a_i\) is necessarily odd, and (27) cannot be satisfied for any \(j\).

9. Discussion. It appears that the immunity to linear drift, which has been proved for all binary m-sequences, does not extend, in general, to nonbinary m-sequences. The difficulty of proving whether such sequences do exist satisfying (27) seems severe; for instance, the range (24) does not coincide with one or more of the 'blocks' mentioned in Section 2.5. We may note in passing that the derivation of (27) only assumes the average level over a cycle to be zero; it is not necessary, though it is generally convenient, to assume the \(q\) element-values to be equally-spaced.

As Barker (1967) has shown, no binary m-sequence with \(N \leq 255\) gives immunity to quadratic drift. To find the effect of such drift entails evaluating \(\sum_{i=1}^{N} i^2 b_{i+j}\), and no way has been found of relating this quantity to the translation-set parameters. However, the likelihood of it being zero for any binary m-sequence seems too small to make the point worth pursuing.
Appendix 2. Further data for ternary m-sequences

We refer to equation 5(71) and Table 5.4, and consider sequences of periods 26 and 80.

1. The four translation-distinct sequences of period 26. These may be obtained from the data in Table 5.3 by sampling (Section 3.7) with \( r = 5, 7 \) or 17 (these are the leading elements of the translation sets prime to 26). The sequence for \( r = 7 \) is the reverse of that for \( r = 5 \), and \( r = 17 \) gives the reverse of the original sequence. Table A.2 gives the values of the arguments in 5(71) for the four sequences; for the reasons previously described, it is only necessary to show the principal octant of the complete table.

Table A.2. First-octant values of arguments in 5(71) for \( N = 26 \)

\[
\begin{array}{cccccccccc}
\text{k} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\
\hline
\text{j} \backslash \text{k} & \text{r=1} & \text{r=5} & \text{r=7} & \text{r=17} \\
1 & 1 & 1 & 1 & 1 \\
2 & -1 & -1 & -1 & -1 \\
3 & 1 & 1 & 1 & 1 \\
4 & -1 & -1 & -1 & -1 \\
5 & 1 & 1 & 1 & 1 \\
6 & -1 & -1 & -1 & -1 \\
7 & 1 & 1 & 1 & 1 \\
8 & -1 & -1 & -1 & -1 \\
9 & 1 & 1 & 1 & 1 \\
10 & -1 & -1 & -1 & -1 \\
11 & 1 & 1 & 1 & 1 \\
12 & -1 & -1 & -1 & -1 \\
\end{array}
\]
2. The eight translation-distinct sequences of period 86. The base sequence will be taken to be the one generated by $x^4 - x^3 - 1$.

The translation sets, and the element-values for this sequence, are shown in Table A.3.

Translation-distinct sequences are obtained by using the following values of $r$, given in 'reversed pairs':

$1, 53; 7, 17; 11, 23; 13, 41$.

Table A.4 lists the values of $j-r$ and $k-r$ in the 'first octant', which lead to positive or negative values of the argument in $5(71)$, for the base sequence.

<table>
<thead>
<tr>
<th>Set</th>
<th>$\emptyset$</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elements</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>7</td>
<td>8</td>
<td>10</td>
<td>11</td>
<td>13</td>
<td>20</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>15</td>
<td>21</td>
<td>24</td>
<td>30</td>
<td>35</td>
<td>39</td>
<td>60</td>
<td>66</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>18</td>
<td>36</td>
<td>45</td>
<td>63</td>
<td>72</td>
<td>19</td>
<td>37</td>
<td>38</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>27</td>
<td>54</td>
<td>28</td>
<td>55</td>
<td>29</td>
<td>56</td>
<td>57</td>
<td>31</td>
<td>34</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Value</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>-1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>-1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Set</th>
<th>$\emptyset$</th>
<th>$\bar{A}$</th>
<th>$\bar{B}$</th>
<th>$\bar{C}$</th>
<th>$\bar{D}$</th>
<th>$\bar{E}$</th>
<th>$\bar{F}$</th>
<th>$\bar{G}$</th>
<th>$\bar{H}$</th>
<th>$\bar{I}$</th>
<th>$\bar{J}$</th>
<th>$\bar{K}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elements</td>
<td>40</td>
<td>41</td>
<td>14</td>
<td>44</td>
<td>25</td>
<td>23</td>
<td>16</td>
<td>50</td>
<td>17</td>
<td>53</td>
<td>26</td>
<td></td>
</tr>
<tr>
<td></td>
<td>43</td>
<td>42</td>
<td>52</td>
<td>75</td>
<td>69</td>
<td>48</td>
<td>70</td>
<td>51</td>
<td>79</td>
<td>78</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>49</td>
<td>46</td>
<td>76</td>
<td>65</td>
<td>47</td>
<td>64</td>
<td>73</td>
<td>77</td>
<td>74</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>67</td>
<td>58</td>
<td>68</td>
<td>35</td>
<td>61</td>
<td>32</td>
<td>59</td>
<td>71</td>
<td>62</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Value</td>
<td>-1</td>
<td>0</td>
<td>0</td>
<td>-1</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Positive values:</th>
<th>j - r =</th>
<th>1</th>
<th>1</th>
<th>3</th>
<th>3</th>
<th>5</th>
<th>5</th>
<th>6</th>
<th>6</th>
<th>8</th>
<th>8</th>
<th>9</th>
<th>9</th>
<th>10</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>k - r =</td>
<td>4</td>
<td>13</td>
<td>12</td>
<td>39</td>
<td>26</td>
<td>34</td>
<td>11</td>
<td>12</td>
<td>14</td>
<td>19</td>
<td>36</td>
<td>37</td>
<td>20</td>
<td>30</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Negative values:</th>
<th>j - r =</th>
<th>2</th>
<th>2</th>
<th>4</th>
<th>7</th>
<th>7</th>
<th>11</th>
<th>12</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>20</th>
<th>23</th>
<th>26</th>
</tr>
</thead>
<tbody>
<tr>
<td>k - r =</td>
<td>17</td>
<td>24</td>
<td>13</td>
<td>23</td>
<td>25</td>
<td>32</td>
<td>39</td>
<td>19</td>
<td>38</td>
<td>33</td>
<td>34</td>
<td>30</td>
<td>25</td>
<td>34</td>
<td>31</td>
</tr>
</tbody>
</table>
REFERENCES


Cummins, J.D., 1965: 'The simultaneous use of several pseudorandom binary sequences in the identification of linear multivariable dynamical systems', UKAEA Repart AEEW-M507

Davies, A.C., 1965: 'Delayed versions of maximal-length linear binary sequences', Electronics Letters, 1, 61-62


Gold, R., 1968: 'Maximal recursive sequences with 3-valued recursive crosscorrelation functions', IEEE Trans. IT-14, 154-156
Golomb, S.W., 1964: 'Digital communications' (Prentice-Hall)


Mann, H.B., 1965: 'Addition theorems' (Wiley)

Peterson, W.W., 1961: 'Error-correcting codes' (MIT/Wiley)


———, 1968: 'Proof of the drift-resistant property of binary m-sequences' Electronics Letters, 4, 380-381


Vinogradov, I.M., 1955: 'An introduction to the theory of numbers' (Pergamon)

Wiener, N., 1958: 'Nonlinear problems in random theory' (Chapman and Hall)


MATERIAL REDACTED AT REQUEST OF UNIVERSITY