STATISTICAL PROPERTIES OF FILTERED PSEUDORANDOM
DIGITAL SEQUENCES FORMED FROM THE SUM
OF MAXIMUM-LENGTH SEQUENCES

By G. R. Wallace, Glenn D. Weathers and Edward R. Graf
Astrionics Laboratory

July 9, 1973

George C. Marshall Space Flight Center
Marshall Space Flight Center, Alabama
### Technical Report

**Title:** Statistical Properties of Filtered Pseudorandom Digital Sequences Formed from the Sum of Maximum-Length Sequences

**Authors:** G. R. Wallace, *Glenn D. Weathers, and **Edward R. Graf

**Performing Organization:** George C. Marshall Space Flight Center

**Sponsoring Agency:** National Aeronautics and Space Administration

**Abstract:**

The statistics of filtered pseudorandom digital sequences called hybrid-sum sequences, formed from the modulo-two sum of several maximum-length sequences, are analyzed. The results indicate that a relation exists between the statistics of the filtered sequence and the characteristic polynomials of the component maximum-length sequences. An analysis procedure is developed for identifying a large group of sequences with good statistical properties for applications requiring the generation of analog pseudorandom noise. By use of the analysis approach, the filtering process is approximated by the convolution of the sequence with a sum of unit-step functions. The first five moments of the resulting weight tuples are used to characterize the statistics of the filtered sequence. At this point, a parameter reflecting the overall statistical properties of filtered pseudorandom sequences is derived. This parameter is called the statistical quality factor. A computer algorithm to calculate the statistical quality factor for the filtered sequences is presented, and the results for two examples of sequence combinations are included. The analysis reveals that the statistics of the signals generated with the hybrid-sum generator are potentially superior to the statistics of signals generated with maximum-length generators. Furthermore, fewer calculations are required to evaluate the statistics of a large group of hybrid-sum generators than are required to evaluate the statistics of the same size group of approximately equivalent maximum-length sequences. Pseudorandom signals generated by filtering hybrid-sum sequences have a potential application in a multichannel communications system evaluation technique. There are also applications for these sequences in areas such as coding theory and modulation format design for pseudonoise transponders.

**Key Words:**

- Communication systems testing
- Multichannel pseudonoise testing
- Filtered pseudorandom sequences
- Summed maximum-length sequences
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>FORMATION OF HYBRID-SUM SEQUENCES</td>
<td>3</td>
</tr>
<tr>
<td>MODEL OF FILTERING PROCESS</td>
<td>6</td>
</tr>
<tr>
<td>STATISTICAL PROPERTIES</td>
<td>7</td>
</tr>
<tr>
<td>TEST ALGORITHM FOR PSEUDORANDOMNESS OF DIGITAL SEQUENCES</td>
<td>26</td>
</tr>
<tr>
<td>APPLICATION TO COMMUNICATIONS SYSTEMS TESTING</td>
<td>33</td>
</tr>
<tr>
<td>CONCLUSIONS</td>
<td>38</td>
</tr>
<tr>
<td>APPENDIX A — RESULTS OF COMPUTER PROGRAM POLTE 1</td>
<td>39</td>
</tr>
<tr>
<td>APPENDIX B — FLOW DIAGRAM FOR THE PROGRAM POLTE 1</td>
<td>43</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>55</td>
</tr>
</tbody>
</table>
# LIST OF ILLUSTRATIONS

<table>
<thead>
<tr>
<th>Figure</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Hybrid-sum sequence generator</td>
<td>4</td>
</tr>
<tr>
<td>2.</td>
<td>Impulse response of assumed filter</td>
<td>6</td>
</tr>
<tr>
<td>3.</td>
<td>Autocorrelation of a random sequence, x(t)</td>
<td>8</td>
</tr>
<tr>
<td>4.</td>
<td>Examples of the autocorrelation function of sum sequences from k generators</td>
<td>12</td>
</tr>
<tr>
<td>5.</td>
<td>Computer simulation results for maximum-length sequence (11, 9, 0)</td>
<td>34</td>
</tr>
<tr>
<td>6.</td>
<td>Computer simulation results for hybrid-sum sequence (5, 2, 0) + (6, 1, 0)</td>
<td>35</td>
</tr>
<tr>
<td>7.</td>
<td>System for communications network evaluation</td>
<td>36</td>
</tr>
<tr>
<td>8.</td>
<td>Method of generating test signals</td>
<td>37</td>
</tr>
<tr>
<td>9.</td>
<td>Test configuration for a multichannel communications system</td>
<td>37</td>
</tr>
</tbody>
</table>
### LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Factorization of $L_\gamma = 2^n \gamma - 1$ into primes.</td>
<td>5</td>
</tr>
<tr>
<td>2.</td>
<td>Approximations for the first five central moments.</td>
<td>26</td>
</tr>
<tr>
<td>A-1.</td>
<td>POLTE 1 for three maximum-length sequences.</td>
<td>41</td>
</tr>
</tbody>
</table>
STATISTICAL PROPERTIES OF FILTERED PSEUDORANDOM DIGITAL SEQUENCES FORMED FROM THE SUM OF MAXIMUM-LENGTH SEQUENCES

INTRODUCTION

In 1964 Shepertycki [1] suggested the use of filtered, pseudorandom digital sequences as the test signal in a root-mean-square (rms) system evaluation configuration. The digital sequence generator suggested by Shepertycki is the maximum-length type with linear feedback.

Filtered maximum-length sequences have been used extensively for pseudorandom signal generation and similar applications [2]. The results were acceptable for low-pass filtered sequences when the ratio of the sequence digital-clock frequency to filter-cutoff frequency was approximately equal to the number of stages in the sequence-generating register. However, for higher ratio values, a definite skewing of the amplitude density function was observed by Gilson [3]. He reported that the skewing effect could be averted by using a digital sequence composed of the modulo-two sum of the outputs of two maximum-length digital-sequence generators. His paper consisted of the results of experiments with 9- and 11-stage generators. Approximately Gaussian distributed probability density functions were obtained for clock-to-filter cutoff ratios of up to 80 times the number of stages in the maximum-length sequence generator.

Recent experiments have partially confirmed Gilson's results; however, it was found experimentally and by computer simulation that sequence generation by summing two maximum-length sequences does not always result in a nonskewed amplitude probability density function [4, pp. 42-44]. The computer simulation also revealed that although the amplitude distribution of the sum of two maximum-length sequences might be symmetrical, it is still not always approximately Gaussian; it is often platykurtic\(^1\) as compared with the normal distribution.

---

1. Peaked compared with normal distribution.
Several pertinent analyses have been performed upon maximum-length sequences in the past. These include Gilson's experimental analysis, an analysis performed by Roberts and Davis [5], a computer simulation performed by White [6], and an analysis by Lindholm [7, pp. 569-576].

Gilson's paper indicated that the sum of the maximum-length sequences might provide analog noise with near Gaussian statistics when filtered but gave no analysis procedure. Roberts and Davis attempted to establish a mathematical basis for predicting the statistics of filtered maximum-length sequences, but only mean and variance tests of the distribution were considered. White performed a computer simulation basically paralleling Gilson's experimental efforts. White's results are inconclusive because of the small number of simulations attempted, but he indicated that a theoretical evaluation of the pseudorandom sequences would be of great value. Lindholm performed a theoretical evaluation of maximum-length sequences based upon the moments of weights of M-tuples from the sequence. He calculated the first three moments of several maximum-length sequences. Wainberg and Wolf [8] have used Lindholm's approach in an analysis of M-tuples from maximum-length sequences and confirmed his results.

The purpose of this study is to develop mathematical formulas to provide the basis for the design of pseudorandom signals intended for applications requiring accurate knowledge of the statistics of the signals.

The analysis approach involves generating the pseudorandom signals from a filtered hybrid-sum sequence rather than from a filtered single maximum-length sequence. The hybrid sequence is formed from the modulo-two sum of k maximum-length sequences and is an extension of the sum sequences formed from two maximum-length sequences that Gilson evaluated. The basic reason for the analysis of hybrid-sum sequences is to establish a large group of sequences with good statistical properties. It will be shown that this can be accomplished much more efficiently using the hybrid-sum approach rather than forming the group strictly from maximum-length sequences.

The need for information concerning the statistical properties of filtered pseudorandom digital sequences is critical because of the need to develop improved low-cost equipment for testing multichannel communications systems.
FORMATION OF HYBRID-SUM SEQUENCES

Figure 1 is a block diagram of a hybrid-sum-sequence generator. The sequence is formed from the sum of \( k \) maximum-length linear digital sequence generators.

The length of a hybrid-sum sequence is

\[
L = \prod_{\gamma=1}^{k} \left( 2^{n_{\gamma}} - 1 \right),
\]

(1)

where \( n_{\gamma} \) is the number of stages in the \( \gamma \)th generator.

The upper bound on the number of sequences available with \( k \)-sequence generators is

\[
U = \prod_{\gamma=1}^{k} \frac{2^{n_{\gamma}}}{n_{\gamma}}.
\]

(2)

In equation (2) it is assumed that the maximum-length generators composing the hybrid-sum generator have fixed numbers of stages. If, however, there are a total of \( N_{T} \) memory elements available which may be distributed in any "allowable" fashion among several maximum-length generators, the upper bound on the number of sequences available is

\[
U = \sum_{i=1}^{K} \prod_{\gamma=1}^{k_{i}} \frac{2^{n_{\gamma i}}}{n_{\gamma i}},
\]

(3)

where there are \( K \) "allowable" combinations of the \( N_{T} \) memory elements, and \( k_{i} \) is the number of separate generators for the \( i \)th "allowable" combination. The condition, "allowable," signifies that none of the sequence lengths of the maximum-length generators can have a common term. In other words, all the terms
Figure 1. Hybrid-sum sequence generator.
for a particular hybrid-sum generator are relatively prime. Table 1 gives the factored values of \( L_n^{\gamma} \) for values of \( n \) ranging from 3 to 34.

**TABLE 1. FACTORIZATION OF \( L_n^{\gamma} = 2^{\gamma-1} \) INTO PRIMES**

<table>
<thead>
<tr>
<th>( n )</th>
<th>( 2^{\gamma-1} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>( 2^3 - 1 = 7 )</td>
</tr>
<tr>
<td>4</td>
<td>( 2^4 - 1 = 3 \times 5 )</td>
</tr>
<tr>
<td>5</td>
<td>( 2^5 - 1 = 31 )</td>
</tr>
<tr>
<td>6</td>
<td>( 2^6 - 1 = 3 \times 3 \times 7 )</td>
</tr>
<tr>
<td>7</td>
<td>( 2^7 - 1 = 127 )</td>
</tr>
<tr>
<td>8</td>
<td>( 2^8 - 1 = 3 \times 5 \times 17 )</td>
</tr>
<tr>
<td>9</td>
<td>( 2^9 - 1 = 7 \times 73 )</td>
</tr>
<tr>
<td>10</td>
<td>( 2^{10} - 1 = 3 \times 11 \times 31 )</td>
</tr>
<tr>
<td>11</td>
<td>( 2^{11} - 1 = 23 \times 89 )</td>
</tr>
<tr>
<td>12</td>
<td>( 2^{12} - 1 = 3 \times 3 \times 5 \times 7 \times 13 )</td>
</tr>
<tr>
<td>13</td>
<td>( 2^{13} - 1 = 8191 )</td>
</tr>
<tr>
<td>14</td>
<td>( 2^{14} - 1 = 3 \times 43 \times 127 )</td>
</tr>
<tr>
<td>15</td>
<td>( 2^{15} - 1 = 7 \times 31 \times 151 )</td>
</tr>
<tr>
<td>16</td>
<td>( 2^{16} - 1 = 3 \times 5 \times 17 \times 257 )</td>
</tr>
<tr>
<td>17</td>
<td>( 2^{17} - 1 = 131071 )</td>
</tr>
<tr>
<td>18</td>
<td>( 2^{18} - 1 = 3 \times 3 \times 3 \times 7 \times 19 \times 73 )</td>
</tr>
<tr>
<td>19</td>
<td>( 2^{19} - 1 = 524287 )</td>
</tr>
<tr>
<td>20</td>
<td>( 2^{20} - 1 = 3 \times 5 \times 5 \times 11 \times 31 \times 41 )</td>
</tr>
<tr>
<td>21</td>
<td>( 2^{21} - 1 = 7 \times 7 \times 127 \times 337 )</td>
</tr>
<tr>
<td>22</td>
<td>( 2^{22} - 1 = 3 \times 23 \times 89 \times 683 )</td>
</tr>
<tr>
<td>23</td>
<td>( 2^{23} - 1 = 47 \times 178481 )</td>
</tr>
<tr>
<td>24</td>
<td>( 2^{24} - 1 = 3 \times 3 \times 5 \times 7 \times 13 \times 17 \times 241 )</td>
</tr>
<tr>
<td>25</td>
<td>( 2^{25} - 1 = 31 \times 601 \times 1801 )</td>
</tr>
<tr>
<td>26</td>
<td>( 2^{26} - 1 = 3 \times 2731 \times 8191 )</td>
</tr>
</tbody>
</table>
TABLE 1. (Concluded)

<table>
<thead>
<tr>
<th>n</th>
<th>2^n - 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>(7 \times 73 \times 262657)</td>
</tr>
<tr>
<td>28</td>
<td>(3 \times 5 \times 29 \times 43 \times 113 \times 127)</td>
</tr>
<tr>
<td>29</td>
<td>(223 \times 1103 \times 2089)</td>
</tr>
<tr>
<td>30</td>
<td>(3 \times 3 \times 7 \times 1 \times 31 \times 151 \times 331)</td>
</tr>
<tr>
<td>31</td>
<td>(2147483647)</td>
</tr>
<tr>
<td>32</td>
<td>(3 \times 5 \times 17 \times 257 \times 65537)</td>
</tr>
<tr>
<td>33</td>
<td>(7 \times 23 \times 89 \times 599479)</td>
</tr>
<tr>
<td>34</td>
<td>(3 \times 43691 \times 131071)</td>
</tr>
</tbody>
</table>

Table 1 can be used to select the number of stages \(n_y\) for each of the component maximum-length sequence generators of a hybrid-sum sequence generator.

**MODEL OF FILTERING PROCESS**

The analysis of the statistical properties of low-pass filtered hybrid-sum sequences is based upon a filter with an impulse response of the "brick-wall" type as shown in Figure 2.

![Figure 2. Impulse response of assumed filter.](image-url)
The brick-wall approximation to a filter's impulse response is equivalent to representing the impulse response as the sum of unit-step functions

\[ h(t) = u(t) - u(t - MT_b) \]  \hspace{1cm} (5)

where \( u(t) \) is the unit-step function.

The transfer function of the assumed filter is

\[ H(j\omega) = \int_{-\infty}^{\infty} h(t) e^{-j\omega t} dt = \frac{\sin\left(\frac{\omega MT_b}{2}\right)}{\frac{\omega}{2}} e^{-\frac{j\omega MT_b}{2}} \]  \hspace{1cm} (6)

This filter impulse response shown in Figure 2 serves as an approximation to the impulse response of filters commonly used in the baseband of communications systems. The primary justification for using the approximation in the analysis is the degree of correlation between the results of the analysis and experimental data obtained by filtering sequences [4, pp. 45-125].

Using the brick-wall impulse response approximation, the filtering process is equivalent to forming a signal by adding digits of the sequence when the digits are ±1. If the central-limit theorem is applied, the output signal density function tends toward a Gaussian density function if the sequence is random and the number of digits added is large. This is true because the individual digits forming the sum are independent for a random sequence [9].

The digits of a hybrid-sum sequence are not actually independent, but in many cases they approximate the random sequence well enough to approach a Gaussian distribution when filtered.

STATISTICAL PROPERTIES

An analysis of some of the statistical properties of hybrid-sum sequences is now presented. If \( x(t) \) is a digital sequence, its autocorrelation function is
\[ R_{xx}(\tau) = \lim_{T \to \infty} \frac{1}{T} \int_{-T/2}^{T/2} x(t)x(t+\tau)dt \]  

(7)

If \( x(t) \) is random, the autocorrelation function will have the form shown in Figure 3.

Figure 3. Autocorrelation of a random sequence, \( x(t) \).

If \( x(t) \) is a maximum-length sequence (sequence length equals \( L \)) an appropriate autocorrelation function is

\[ R_{xx}(\tau) = \frac{1}{T} \int_{-T/2}^{T/2} x(t)x(t+\tau)dt \]  

(8)

where \( T \) equals \( LT_b \), and \( T_b \) is a bit period.

Now assume that sequence \( x(t) \) is generated by summing (modulo-two) \( k \) maximum-length sequences.

\[ x(t) = \sum_{i=1}^{k} x_i(t) \text{ (modulo-two)} \]  

(9)
when \( x(t) \) is from \( \{1, 0\} \), or

\[
x(t) = \prod_{i=1}^{k} x_i(t)
\]

(10)

when \( x(t) \) is from \( \{-1, +1\} \).

The autocorrelation function from equation (8) becomes

\[
R_{xx}(\tau) = \frac{1}{T} \int_{-T/2}^{T/2} \prod_{\gamma=1}^{k} x_\gamma(t) \prod_{\gamma=1}^{k} x_\gamma(t+\tau) dt
\]

or

\[
R_{xx}(\tau) = \frac{1}{T} \int_{-T/2}^{T/2} \prod_{\gamma=1}^{k} x_\gamma(t) x_\gamma(t+\tau) dt
\]

(11)

(12)

When binary digits from \( \{-1, +1\} \) are used, the equivalent of the shift-and-add property becomes the shift-and-multiply property, and if

\[
\tau \neq qL_\gamma \text{ for } \gamma = 1, 2, 3, \ldots k, q \text{ is an integer, and } \tau \neq 0,
\]

then

\[
x_\gamma(t)x_\gamma(t+\tau) = x_\gamma[t+\tau_\gamma(\tau)]
\]

(13)

Substituting equation (13) into equation (12),

\[
R_{xx}(\tau) = \frac{1}{T} \int_{-T/2}^{T/2} \prod_{\gamma=1}^{k} x_\gamma(t+\tau) dt
\]

(14)
where each $\tau$ is some function of $\tau$. Since the sequence lengths have no common terms, all possible phase arrangements of the constituent sequences are cycled during the total sequence length $T$. This characteristic of the product sequence can be used to change the form of equation (14) to

$$R_{xx}(\tau \neq qL) = \frac{1}{L} \sum_{T_1=1}^{L_1} \sum_{T_2=1}^{L_2} \sum_{T_3=1}^{L_3} \cdots \sum_{T_k=1}^{L_k} \prod_{\gamma=1}^{k} x_\gamma(t)$$

$$= \frac{1}{L} \sum_{T_1=1}^{L_1} x_1(t_1) \sum_{T_2=1}^{L_2} x_2(t_2) \cdots \sum_{T_k=1}^{L_k} x_k(t_k)$$ (15)

where

$$\tau = \prod_{\gamma=1}^{k} t_\gamma$$ (16)

In each sequence there is now one more $-1$ than $+1$ and

$$R_{xx}(\tau \neq 0) = \frac{(-1)^k}{L}$$ (17)

If $\tau$ equals 0, there is no shift and

$$R_{xx}(\tau = 0) = 1$$ (18)

For the case where $\tau$ equals $qL_j$ for $1 \leq j \leq k$, and $q$ is an integer, then

$$R_{xx}(\tau = qL) = \frac{1}{T} \int_{-T/2}^{T/2} \prod_{\gamma=1}^{k} x_\gamma(t) x_\gamma(t+\tau)$$ (19)
From the shift and multiply property,

\[
R_{xx}(\tau=qL) = \frac{1}{T} \int_{-T/2}^{T/2} \prod_{\gamma=1, \gamma \neq j}^{k} x_{\gamma}(t+\tau) dt
\]

\[
= \frac{1}{L} \sum_{T_1=1}^{L_1} \sum_{T_2=1}^{L_2} \cdots \sum_{T_k=1}^{T_k} \prod_{\gamma=1, \gamma \neq j}^{k} x_{i}(\tau_{\gamma})
\]

or

\[
R_{xx}(\tau=qL) = \frac{L_j}{L} (-1)^{k-1}
\]

Figure 4 gives an example of the autocorrelation function as a function of \( \tau \) for even and odd values of \( k \). The scale is exaggerated for illustration purposes, and the figure demonstrates that the autocorrelation of a repetitive function is repetitive.

An analysis of the randomness properties of the filtered sequence can be based upon the calculation of the moments of the resulting waveform.

The filter time output, \( r(t) \), is

\[
r(t) = \int_{-\infty}^{\infty} x(\tau) h(t-\tau) d\tau
\]
With the assumed filter impulse response,

\[ r(t) \approx \sum_{i=1}^{M} x(t-iT_b) \]

where \( x(t) \) is the digital sequence. Equation (22) states that \( r(t) \) is equal to the sum of the last \( M \) digits that occurred before \( t \), and the study of the statistical properties of the filter output is based on the weights of the sequence \( M \)-tuples.

\[ R_{xx}(\tau) \]

\( k \) odd

\[ R_{xx}(\tau) \]

\( k \) even

Figure 4. Examples of the autocorrelation function of sum sequences from \( k \) generators.

The \( i^{th} \) \( M \)-tuple weight of the sum sequence is

\[ S_i = \sum_{j=0}^{M-1} b_{i+j} \]  

(23)
where

\[ b_{i+j} = \prod_{\gamma=1}^{k} x_{i+j,\gamma} \]  

Equation (24) equates the state of the \((i+j)\)th bit of the sum sequence to the product (equivalent to modulo-two addition) of the \((i+j)\)th member of the \(k\) component sequences.

The statistics of the weight functions can be investigated by calculating the moments of the weight distribution. The \(p\)th moment is

\[ s^p = \frac{1}{L} \sum_{i=0}^{L-1} s^p_i . \]  

(25)

Substituting equations (22) and (23) into equation (25) yields

\[ s^p = \frac{1}{L} \sum_{i=0}^{L-1} \left( \sum_{j=0}^{M-1} \prod_{\gamma=1}^{k} x_{i+j,\gamma} \right)^p . \]  

(26)

The first moment is

\[ s^1 = \frac{1}{L} \sum_{i=0}^{L-1} \sum_{j=0}^{M-1} \prod_{\gamma=1}^{k} x_{i+j,\gamma} \]  

(27)
The first moment does not depend on the particular sequences comprising the sum sequence, and if \( M \ll L \), then \( S^1 \) is approximately 0. The first moment indicates the mean of the weight distribution.

The second moment is

\[
S^2 = \frac{1}{L} \left[ \sum_{i=0}^{L-1} \left( \sum_{j=0}^{M-1} \sum_{\gamma=1}^{k} x_{i+j,\gamma} \right)^2 \right]
\]

\[= \frac{1}{L} \sum_{i=0}^{L-1} \left( M + 2 \sum_{j=0}^{M-2} \sum_{\zeta=j+1}^{M-1} \sum_{\gamma=1}^{k} x_{i+j,\gamma} x_{i+\zeta,\gamma} \right) \]

\[= M + 2 \sum_{j=0}^{M-2} \sum_{\zeta=j+1}^{M-1} \sum_{\gamma=1}^{k} x_{i+j,\gamma} x_{i+\zeta,\gamma} \]

Now

\[x_{i+j,\gamma} x_{i+\zeta,\gamma} = x_{i+z,\gamma} \]

if \( M < L \), for all \( \gamma \), and \( z \) is some function of \( j, \zeta \), and \( \gamma \) from the shift-and-multiply property of maximum-length sequences.
Equation (28) becomes

$$S^2 = M + \frac{2}{L} \sum_{j=0}^{M-2} \sum_{\xi=j+1}^{M-1} k \prod_{\gamma=1}^{L_{\gamma}^\gamma-1} \sum_{i=0}^{x_{i+z,\gamma}} \right) .$$

(30)

Now

$$k \prod_{\gamma=1}^{L_{\gamma}^\gamma-1} \sum_{i=0}^{x_{i+z,\gamma}} = (-1)^k ,$$

(31)

and

$$S^2 = M + \frac{(-1)^k}{L} \prod_{\gamma=1}^{L_{\gamma}^\gamma-1} \sum_{i=0}^{x_{i+z,\gamma}} \right) .$$

(32)

if $M < L$ for all $\gamma$. The second-central moment (the second moment about the mean-of-the-weight distribution) is

$$S_c^2 = S^2 - (S^1)^2$$

(33)

or

$$S_c^2 = M \left[ 1 + \frac{(-1)^k}{L} (M-1) \right] - \frac{M^2}{L^2}$$

(34)

where $M < L$ for all $\gamma$. 

15
From equation (34), the second-central moment does not depend on the particular sequences comprising the sum sequence but does depend upon the number of sequences summed.

As an example, consider the case where \( k \) equals 1, \( n_1 \) equals 5, and \( L \) equals 31:

\[
S_c^2 = M \left( 1 - \frac{M-1}{L} \right) - \frac{M^2}{L^2}.
\] (35)

The maximum second-central moment is for \( M \) approximately equal to 15, where \( S_c^2 \) is approximately 8.

As a second example, consider the sequence generated by modulo-two summing of two maximum-length sequences. The two sequences are from generators with two and three stages:

\[
n_1 = 2, n_2 = 3, L = 21
\]

and

\[
S_c^2 = M \left( 1 + \frac{M-1}{L} \right) - \frac{M^2}{L^2},
\] (36)

if \( M<3 \).

The second-central moment is a measure of central tendency. Observe from the two examples that for these particular sequence generators the second-central moment for the summed sequence is larger than the second-central moment of the single maximum-length sequence for \( 1 < M < L \) for all \( \gamma \). The generators in the two examples each require five register stages (case 1: \( n_1 \) equal to 5; case 2: \( n_1 \) equal to 2, and \( n_2 \) equal to 3), and the sequences are approximately the same length.
The third-central moment of the weight function gives an indication of the relative skewness of the graphical representation of the function probability density. The third moment is

\[ S^3 = \frac{1}{L} \sum_{i=0}^{L-1} \left( \sum_{j=0}^{M-1} \sum_{\gamma=1}^{k} x_{i+j,\gamma} \right)^3. \]  

(37)

Now

\[ \left( \sum_{j=0}^{M-1} \sum_{\gamma=1}^{k} x_{i+j,\gamma} \right)^3 = (3M-2) \sum_{j=0}^{M-1} \sum_{\gamma=1}^{k} x_{i+j,\gamma} \]

\[ + 3! \sum_{j=0}^{M-3} \sum_{v=j+1}^{M-2} \sum_{\zeta=v+1}^{M-1} \sum_{\gamma=1}^{k} x_{i+v,\gamma} x_{i+v,\gamma} x_{i+\zeta,\gamma} \]

(38)

and

\[ S^3 = \frac{(3M-2)}{L} \sum_{i=0}^{L-1} \sum_{j=0}^{M-1} \sum_{\gamma=1}^{k} x_{i+j,\gamma} \]

\[ + 3! \sum_{j=0}^{M-3} \sum_{v=j+1}^{M-2} \sum_{\zeta=v+1}^{M-1} \sum_{i=0}^{L-1} \sum_{\gamma=1}^{k} x_{i+j,\gamma} x_{i+v,\gamma} x_{i+v,\gamma} x_{i+\zeta,\gamma} \]

(39)

Using the relations

\[ \sum_{i=0}^{L-1} \sum_{\gamma=1}^{k} x_{i+j,\gamma} = \sum_{i=0}^{L-1} x_{i+j,\gamma} \]

(40)
and
\[ k \prod_{\gamma=1}^{\infty} x_{i+j, \gamma} x_{i+v, \gamma} x_{i+\xi, \gamma} = \prod_{\gamma=1}^{\infty} x_{i+j, \gamma} x_{i+\phi, \gamma}, \quad (41) \]

where \( \phi \) is a function of \( v, \xi, \) and \( \gamma \), and \( M < L \) for all \( \gamma \), equation (41) becomes

\[ S^3 = \frac{1}{L} (3M-2) (M) (-1)^k \]

\[ + \frac{3!}{L} \sum_{j=0}^{M-3} \sum_{\nu=j+1}^{M-2} \sum_{\xi=\nu+1}^{M-1} \sum_{i=0}^{L-1} \prod_{\gamma=1}^{k} x_{i+j, \gamma} x_{i+\phi, \gamma}. \quad (42) \]

If

\[ \phi = j, \quad (43) \]

\[ \sum_{i=0}^{L-1} x_{i+j, \gamma} x_{i+\phi, \gamma} = \frac{L}{y} \quad (44) \]

and if

\[ \phi \neq j, \quad (45) \]

then

18
where $M < L_{\gamma}$ for all $\gamma$.

There are $\binom{M}{3}$ combinations of $j$, $v$, and $\xi$ in the latter part of equation (42). Let $C_{\omega}$ be the number of these combinations for which the set $\omega$ (with $w$ members) of the $k$ component sequences satisfies

\[ x_{i+j,\gamma} = x_{i+v,\gamma} x_{i+\xi,\gamma} \]  

for all $i$.

The third moment becomes

\[ S^3 = \frac{1}{L} (3M-2) (M) (-1)^k + \frac{3!}{L} \sum_{\omega=1}^{2^k} \left[ C_{\omega} \prod_{\gamma=1}^{w} L_y (-1)^{k-w} \right], \]  

where $M < L_{\gamma}$ for all $\gamma$.

If equation (47) is satisfied for a particular component-maximum-length sequence, then that sequence must satisfy the trinomial equation

\[ I + A^{\xi-j} + A^{\xi-v} = 0, \]  

where $A$ is the generator $A$ matrix. The minimum polynomial that describes the sequence is
\[ A^n \gamma + \alpha_1 A^{n\gamma-1} + \ldots + \alpha_{n-1} A^1 + I = 0 \]  \hspace{1cm} \text{(50)}

and is called the characteristic equation. If the A matrix satisfies both equations (49) and (50), the polynomial on the left of equation (50) is a factor of the polynomial on the left of equation (49). If the maximum-length sequences under consideration have characteristic equations that are factors of no common trinomials of power equal to or less than M-1, then equation (48) becomes

\[ S^3 = \frac{1}{L} (3M-2) (M) (-1)^k + \frac{3!}{L} \left[ \left( \frac{M}{3} \right) - \sum_{\gamma=1}^{k} B_{\gamma} \right] (-1)^k + \sum_{\gamma+1}^{k} B_{\gamma} L_{\gamma} (-1)^{k-1} \]  \hspace{1cm} \text{(51)}

if \( M < L \) for all \( \gamma \), where \( B_{\gamma} \) is the number of trinomials of power less than or equal to M-1 that contain the \( \gamma \)-sequence characteristic polynomial as a factor. If \( M << L \), then

\[ S^3_c \approx \frac{+3!}{k} \prod_{\gamma=1}^{k} L_{\gamma} \left[ \sum_{\gamma=1}^{k} B_{\gamma} (L_{\gamma}) (-1)^{k-1} \right] \]  \hspace{1cm} \text{(52)}

where \( S^3_c \) is the third-central moment and \( M < L \) for all \( \gamma \).

From equation (52), trinomial factors tend to increase the third-central moment. To minimize the third-central moment, sequences should then be added that have characteristic equations that are factors of few trinomials of power less than or equal to M-1.

The fourth moment is
\[ S^4 = \frac{1}{L} \sum_{i=0}^{L-1} \left( \sum_{j=0}^{M-1} \prod_{\gamma=1}^{k} x_{i+j, \gamma} \right)^4 \] (53)

or

\[ S^4 = \frac{1}{L} \sum_{i=0}^{L-1} \left[ M + 12M(M-1) + 2M(3!) \sum_{j=0}^{M-2} \sum_{v=j+1}^{M-1} \prod_{\gamma=1}^{k} x_{i+j, \gamma} x_{i+v, \gamma} \right. \\
\left. + 4! \sum_{j=0}^{M-4} \sum_{v=j+1}^{M-3} \sum_{\zeta=v+1}^{M-2} \sum_{f=\zeta+1}^{M-1} \prod_{\gamma=1}^{k} x_{i+j, \gamma} x_{i+v, \gamma} x_{i+\zeta, \gamma} x_{i+f, \gamma} \right] \] (54)

Now using the shift-and-multiply property of maximum-length sequences, and assuming \( M < L \) for all \( \gamma \),

\[ S^4 = M + 12M(M-1) + \frac{(2M)3!}{L} \sum_{j=0}^{M-2} \sum_{v=j+1}^{M-1} \prod_{\gamma=1}^{k} x_{i+x, \gamma} \] (55)

\[ + \frac{4!}{L} \sum_{j=0}^{M-4} \sum_{v=j+1}^{M-3} \sum_{\zeta=v+1}^{M-2} \sum_{f=\zeta+1}^{M-1} \prod_{\gamma=1}^{k} x_{i+z_1, \gamma} x_{i+z_2, \gamma} \] (55)

There are \( \binom{M}{4} \) combinations of \( j, v, \zeta, \) and \( f \) in the latter part of equation (55). Let \( D_\omega \) be the number of these combinations for which the set \( \omega \) (with \( w \) members) of the \( k \) component sequences satisfies

\[ x_{i+j, \gamma} = x_{i+v, \gamma} x_{i+\zeta, \gamma} x_{i+f, \gamma} \] (56)

for all \( i \).
Then

\[ S^4 = M + 12M(M-1) + \frac{12M^2}{L} (M-1)(-1)^k \]

\[ + \frac{4!}{L} \sum_{\omega=1}^{2^k} \left[ D_w \prod_{y=1}^{W} L_y (-1)^{k-w} \right]. \tag{57} \]

If equation (56) holds, the particular sequence satisfies the quadrinomial equation

\[ x^{j-v} + x^{j+t} + x^{j-f} + 1 = 0, \tag{58} \]

where \( j-v \leq M-1 \).

From the properties of the characteristic equation for maximum-length sequences, if equation (56) holds, the characteristic equation will be a factor of the quadrinomial in equation (58). If none of the characteristic polynomials of the constituent maximum-length sequences are factors of common quadrinomials of powers less than or equal to \( M-1 \), then equation (57) reduces to

\[ S^4 = M + 12M(M-1) + \frac{12M^2}{L} (M-1)(-1)^k \]

\[ + \frac{4!}{L} \left[ \left( \frac{M}{4} \right) - \sum_{\gamma=1}^{k} E_{\gamma} \right] (-1)^k \]

\[ + \sum_{\gamma=1}^{k} E_{\gamma} L_{\gamma} (-1)^{k-1} \right]. \tag{59} \]
where $E$ is the number of quadrinomials of power less than or equal to $M-1$ that have the $\gamma$th characteristic equation of a factor.

If $M \ll L$,

$$S^4_c \approx M + 12M(M-1) + 4! \sum_{\gamma=1}^{k} E^\gamma L^\gamma (-1)^{k-1} \prod_{\gamma=1}^{k} L^\gamma$$

(60)

where $S^4_c$ is the fourth central moment.

The fifth moment is

$$S^5 = \frac{1}{L} \sum_{i=0}^{L-1} \left( \sum_{j=0}^{M-1} \prod_{\gamma=1}^{k} x_{i+j,\gamma} \right)^5$$

(61)

or

$$S^5 = \frac{1}{L} \sum_{i=0}^{L-1} \left\{ \left[ 1 + 5(M-1) + 30(M-1)(M-2) \right] \sum_{j=0}^{M-1} \prod_{\gamma=1}^{k} x_{i+j,\gamma} \right. \right.$$

$$+ \left. (10M)3! \sum_{j=0}^{M-3} \sum_{v=j+1}^{M-2} \sum_{\xi=v+1}^{M-1} \prod_{\gamma=1}^{k} x_{i+j,\gamma} x_{i+v,\gamma} x_{i+\xi,\gamma} \right.$$  \nonumber

$$+ \left. 5! \sum_{j=0}^{M-5} \sum_{v=j+1}^{M-4} \sum_{\xi=v+1}^{M-3} \sum_{\eta=\xi+1}^{M-2} \sum_{f=\eta+1}^{M-1} \prod_{\gamma=1}^{k} x_{i+j,\gamma} x_{i+v,\gamma} x_{i+\xi,\gamma} x_{i+f,\gamma} x_{i+g,\gamma} \right\}$$

(62)
Now distributing the sum over $i$ and simplifying,

\[
\sum_{i=0}^{L-1} \sum_{j=0}^{M-1} \sum_{\gamma=1}^{k} x_{i+j,\gamma} = \sum_{j=0}^{M-1} \sum_{\gamma=1}^{k} \sum_{i=0}^{L-1} x_{i+j,\gamma} = M(-1)^{k} \quad (63)
\]

and

\[
\sum_{i=0}^{L-1} \sum_{j=0}^{M-3} \sum_{v=j+1}^{M-2} \sum_{\xi=v+1}^{M-1} \sum_{\gamma=1}^{k} x_{i+j,\gamma} x_{i+v,\gamma} x_{i+\xi,\gamma} = \sum_{v=j+1}^{M-2} \sum_{\xi=v+1}^{M-1} \sum_{\gamma=1}^{k} x_{i+j,\gamma} x_{i+v,\gamma} x_{i+\xi,\gamma}
\]

\[
= \sum_{v=j+1}^{M-2} \sum_{\xi=v+1}^{M-1} \sum_{\gamma=1}^{k} x_{i+j,\gamma} x_{i+v,\gamma} x_{i+\xi,\gamma}
\]

\[
= \sum_{\omega=1}^{2^{k}} \left[ \sum_{w} \sum_{\gamma=1}^{L_{y}(-1)^{k-w}} \right] . \quad (64)
\]

Also,

\[
\sum_{i=0}^{L-1} \sum_{j=0}^{M-5} \sum_{v=j+1}^{M-4} \sum_{\xi=v+1}^{M-3} \sum_{f=\xi+1}^{M-2} \sum_{g=f+1}^{M-1} \sum_{\gamma=1}^{k} x_{i+j,\gamma} x_{i+v,\gamma} x_{i+f,\gamma} x_{i+g,\gamma}
\]

\[
= \sum_{v=j+1}^{M-4} \sum_{\xi=v+1}^{M-3} \sum_{f=\xi+1}^{M-2} \sum_{g=f+1}^{M-1} \sum_{\gamma=1}^{k} x_{i+j,\gamma} x_{i+v,\gamma} x_{i+f,\gamma} x_{i+g,\gamma}
\]

\[
= \sum_{\omega=1}^{2^{k}} \left[ \sum_{G} \sum_{\gamma=1}^{L_{y}(-1)^{k-w}} \right] . \quad (65)
\]
where $M < L_j$ for all $\gamma$, and $G_{\omega}$ is the number of combinations of $j$, $v$, $z$, $f$, and $g$ of the $\binom{M}{5}$ possible for which the set $\omega$ (with $w$ members) of the $k$ component sequences satisfies

$$x_{i+j,\gamma} = x_{i+v,\gamma} x_{i+z,\gamma} x_{i+g,\gamma}$$  \hspace{1cm} (66)$$

Assuming that no common trinomials or pentanomials are satisfied for the characteristic equations of the maximum-length sequences comprising the sum sequence, equation (61) becomes

$$S^5 = \frac{1 + 5 (M-1) + 30 (M-1) (M-2)}{L} M (-1)^k$$

$$+ \frac{10M3!}{L} \left\{ \left[ \frac{M}{3} \right] - \sum_{\gamma=1}^{k} B_{\gamma} \right\} (-1)^k + \sum_{\gamma=1}^{k} B_{\gamma} L_{\gamma} (-1)^{k-1}$$

$$+ \frac{5!}{L} \left\{ \left[ \frac{M}{5} \right] - \sum_{\gamma=1}^{k} F_{\gamma} \right\} (-1)^k + \sum_{\gamma=1}^{k} F_{\gamma} L_{\gamma} (-1)^{k-1}$$  \hspace{1cm} (67)$$

where $M < L_j$ for all $\gamma$, $B_{\gamma}$ is the number of trinomials of order $M-1$ or less that contains the $\gamma$th sequence characteristic polynomial as a factor, and $F_{\gamma}$ is the number of pentanomials of order $M-1$ or less that contains the $\gamma$th sequence polynomial as a factor.

If $M << L$,

$$S^5_c \approx 10M3! \frac{\sum_{\gamma=1}^{k} B_{\gamma} L_{\gamma} (-1)^{k-1}}{\prod_{\gamma=1}^{k} L_{\gamma}} + 5! \frac{\sum_{\gamma=1}^{k} F_{\gamma} L_{\gamma} (-1)^{k-1}}{\prod_{\gamma=1}^{k} L_{\gamma}}$$  \hspace{1cm} (68)$$
is an approximation for the fifth-central moment.

TEST ALGORITHM FOR PSEUDORANDOMNESS OF DIGITAL SEQUENCES

The calculations performed previously for the first five central moments are given in Table 2.

TABLE 2. APPROXIMATIONS FOR THE FIRST FIVE CENTRAL MOMENTS

<table>
<thead>
<tr>
<th>Moment (i)</th>
<th>Approximation for $S^i_c$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>$M$</td>
</tr>
<tr>
<td>3</td>
<td>$3! \sum_{\gamma=1}^{k} \left[ B_{\gamma} L_{\gamma} (-1)^{k-1} \right] / \prod_{\beta=1}^{k} L_{\beta}$</td>
</tr>
<tr>
<td>4</td>
<td>$M + 12M (M-1) + 4! \sum_{\gamma=1}^{k} \left[ E_{\gamma} L_{\gamma} (-1)^{k-1} \right] / \prod_{\beta=1}^{k} L_{\beta}$</td>
</tr>
<tr>
<td>5</td>
<td>$10M3! \sum_{\gamma=1}^{k} \left[ B_{\gamma} L_{\gamma} (-1)^{k-1} \right] / \prod_{\beta=1}^{k} L_{\beta}$ + $5! \sum_{\gamma=1}^{k} \left[ F_{\gamma} L_{\gamma} (-1)^{k-1} \right] / \prod_{\beta=1}^{k} L_{\beta}$</td>
</tr>
</tbody>
</table>

The approximations hold for the case $M < L$ for all $\gamma$, $M \ll L$ where

\[ L = \prod_{\gamma=1}^{k} L_{\gamma}, \]

and when no common trinomials, quadrinomials, and pentanomials of order $M-1$ or less contain the sequence characteristic polynomials as factors for each maximum-length sequence comprising the sum sequence.
A test involving the formation of a weighted sum of the difference in the first N moments for the sum sequence and a random sequence may be used to evaluate sequences from sum generators. This can be expressed as

$$T(M) = \sum_{i=1}^{N} W_i \left( S_i^c - S_i^{cr} \right)$$

(69)

where $S_i^c$ is the $i^{th}$ central moment for weights of $M$-tuples from a random sequence, $W_i$ is a weighting factor, and $S_i^{cr}$ is the $i^{th}$ central moment for weights of $M$-tuples from a pseudorandom sequence.

Using the results from Table 2, equation (69) becomes

$$T(M) = \frac{1}{k} \sum_{\gamma=1}^{k} \left[ \sum_{\gamma=1}^{k} \left[ W_3 B_\gamma 3! + W_4 4! \gamma \right] \right]$$

$$+ W_5 \left( 10M3! B_\gamma + 5! F_\gamma \right) L_\gamma (-1)^{k-1} \right] \right} \ .$$

(70)

For a particular selection of the weighting functions, the smaller the value of $T(M)$, the better the sequence approximates a random sequence.

The weighting values can be selected to emphasize a particular aspect of the distribution of $M$-tuple weights. For example, the term

$$W_3 \sum_{\gamma=1}^{k} \left[ B_\gamma L_\gamma (-1)^{k-1} \right] \left/ \prod_{\gamma=1}^{k} L_\gamma \right.$$ 

indicates the relative symmetry or skewing of the distribution. The term
indicates skewing of the distribution with more emphasis on the shape of the distribution of M-tuple weights beyond the variance of the distribution. The term

\[
W_5 \sum_{\gamma=1}^{k} \left[ \frac{(10M3| B_\gamma + 5| F_\gamma) \gamma (-1)^{k-1}}{\Pi_{\gamma=1}^{k} L_\gamma} \right]
\]

indicates the kurtosis of the distribution of M-tuple weights. Assuming \( W_4 > 0 \), positive values of this term indicate a leptokurtic distribution, and negative values of the term indicate a platykurtic distribution. If \( k \) is odd the distribution is leptokurtic, and if \( k \) is even the distribution is platykurtic.

A computer algorithm for evaluating the sequence test parameter, \( T(M) \), has been developed. The algorithm calculates \( B_\gamma \), the number of trinomials of order \( M-1 \) or less that contains the \( \gamma \)-sequence characteristic polynomial or a factor; \( E_\gamma \), the number of quadrinomials of order \( M-1 \) or less that contains the \( \gamma \)-sequence characteristic polynomial or a factor; and \( F_\gamma \), the number of pentanomials of order \( M-1 \) or less that contains the \( \gamma \)-sequence characteristic polynomial or a factor.

Lindholm developed an efficient algorithm for calculating \( B_\gamma \), and the algorithms developed for \( E_\gamma \) and \( F_\gamma \) are essentially extensions of Lindholm's method [7, p. 572].

---

2. The relative flatness or peakedness.

3. Flat compared with normal distribution.
If a sequence is generated by an n-stage register, and the sequence is a maximum-length type, then any 2n-1 digits of the sequence can define the particular stages that contribute to the feedback. This is equivalent to solving n-1 simultaneous equations, since for a maximum-length sequence the last stage is always fed back. If the sequence characteristic polynomial is a factor of a trinomial of the form

\[ g(x) = 1 + x^{d-c} + x^d \]  \hspace{1cm} (71)

then the sequence satisfies the recursive relation

\[ x_i = x_{i-c} \cdot x_{i-d} \]  \hspace{1cm} (72)

when the sequence is from the set \{-1, +1\}.

One particular content vector in a maximum-length sequence is \( x_0 = -1, x_1 = 1, x_2 = 1, \ldots x_{n-1} = 1, x_n = -1 \). Using this content vector as a starting point, the next M-1 content vectors are calculated using the sequence recursive relation. Then M + n digits of the sequence are known and can be represented as

\[ x_0', x_1', \ldots, x_{M+n-1} \]

\[ = -1, 1, 1, 1, \ldots -1, x_{n+1}', x_{n+2}', \ldots x_{M+n-1} \]  \hspace{1cm} (73)

Because the tuple

\[ (x_1', x_2', \ldots, x_{n-1}') = (1, 1, \ldots, 1) \]  \hspace{1cm} (74)
and if the sequence characteristic polynomial is a factor of

\[ 1 + x^{d-c} + x^d, \quad (75) \]

then the tuple

\[ (x_{d+1}, x_{d+2}, \ldots, x_{d+n-1}) (x_{c+1}, x_{c+2}, \ldots, x_{c+n-1}) = (1, 1, 1, \ldots, 1, 1) \quad (76) \]

If \( X_d \) is a vector representing the tuple \((x_{d+1}, x_{d+2}, \ldots, x_{c+n-1})\), and similarly for \( X_c \), the relation

\[ X_d^* X_c^* = I \quad (77) \]

expresses the condition of equation (71), where \( I \) is the identity matrix of order \( n-1 \), and \( X_d^* \) and \( X_c^* \) are \((n-1)\) by \((n-1)\) matrices with the elements of \( X_d \) and \( X_c \), respectively, on the main diagonal and all other elements equal to zero.

Extending this procedure to quadrinomials and pentanomials that contain the sequence characteristic polynomial as factors, the required vector relations are

\[ X_d^* X_c^* X_e^* = I \quad (78) \]

and

\[ X_d^* X_c^* X_e^* X_f^* = I \quad (79) \]
By finding tuples for which these equations hold, using the first M-1 digits after the content vector \((1, 1, 1, \ldots -1)\), all trinomials, quadrinomials, and pentanomials that contain the sequence characteristic polynomial as a factor are yielded.

The computer program POLTE 1 was written to solve for the vector relations in equations (76), (77), and (78). The results from this program can be used to evaluate \(T(M)\) from equation (69). The procedure is as follows:

1. Select \(M\), the size of the \(M\)-tuple.

2. Select \(k\) sequences to form the sum sequence.

3. Using the computerized algorithm, calculate \(B, E,\) and \(F\).

4. Select the set of weightings, \(W_i\) depending on the characteristics of the distribution of \(M\)-tuple weights that are critical.

5. Evaluate \(T(M)\) from equation (69).

This procedure can be used to evaluate candidate designs for pseudorandom sequence generators of the type shown in Figure 1.

Appendix A contains the results of the computer evaluation for a maximum-length sequence with 11 memory elements and a hybrid-sum sequence with 11 memory elements. Appendix B is a flow diagram of the program POLTE 1.

An indication of the reduction in the amount of calculations required to evaluate the statistics of a filtered hybrid-sum sequence as compared with a filtered maximum-length sequence can be determined as follows. The limit ratio of the number of pseudorandom sequences statistically evaluated compared with the amount of calculations required is

\[
R = \frac{\prod_{i=1}^{K} \frac{n_i}{2^n}}{\sum_{i=1}^{K} \frac{2^{n_i}}{2^n}}
\]

(80)
For $k=1$ the ratio is unity, but as $k$ increases the ratio tends to increase as previously illustrated. This means the hybrid-sum sequence generator configurations potentially can provide many pseudorandom digital sequences with a minimum number of calculations required.

As an example of the potential increase in computational efficiency using the hybrid-sum approach, assume that the computer algorithm was efficient enough so that each moment could be calculated in 1 second. It would then require more than 12 days of computer time to completely analyze the statistics of all possible maximum-length sequences from a 23-stage register. If, however, the sequence group is established from the hybrid sum of sequences from 11- and 12-stage registers, the analysis of sequences, which are approximately 99.9 percent as long as the maximum-length sequences from the 23-stage register, can be accomplished at a rate 120 times faster than the analysis in the maximum-length case. The more maximum-length sequences that form the hybrid-sum sequence, the greater the efficiency in forming the sequence in this manner.

As an illustration of the theory presented, a comparison is made of the statistics of a filtered maximum-length sequence from the 11-stage generator and a filtered hybrid-sum sequence from a 5- and 6-stage generator. The filter impulse-response length is assumed to be 20 digital-clock periods. The 11-stage maximum-length sequence generator is described by the polynomial $(11, 9, 0)$ and the hybrid-sum generator by the pair of polynomials $(5, 2, 0)$ and $(6, 1, 0)$.

An evaluation of equation (69) with

\[ W_3 \text{ equal to 1,} \]

\[ W_4 \text{ equal to 0,} \]

and

\[ W_5 \text{ equal to 0} \]

gives an indication of the skewing of the amplitude distribution of filtered pseudorandom sequences. Using the described method of calculation, this parameter is evaluated as follows:
For filtered maximum-length sequence \((11, 9, 0)\),

\[ T(M=20, W_3 = 1, W_4 = 0, W_5 = 0) = 54, \] (81)

indicating dominant positive skewing.

For filtered hybrid-sum sequence \((5, 2, 0) + (6, 1, 0)\),

\[ T(M=20, W_3 = 1, W_4 = 0, W_5 = 0) = -8, \] (82)

indicating slight negative skewing.

A computer program was written to evaluate the distribution of weights of the filtered sequence for both the maximum-length sequence and the hybrid-sum sequence directly. Figure 5 is the result for the maximum-length sequence. The distribution skews to the positive side and is a poor approximation to the normal distribution. Figure 6 is the result for the hybrid-sum sequence and shows very little skewing tendency.

**APPLICATION TO COMMUNICATIONS SYSTEMS TESTING**

A diagram of an arrangement for communications system evaluation is presented in Figure 7. This test configuration includes a pseudorandom signal generator that supplies the test waveforms that simulate the waveforms many communications systems are required to process in normal applications. The evaluation scheme establishes as a system quality factor the root-mean-square (rms) value of the difference between system output and input. The test configuration also includes gain- and delay-compensation facilities, which are required because the system quality factor must be minimized with respect to these two parameters. During processing by a communications system, signals may be attenuated, delayed, distorted, and random noise may be added. Of these possibilities, attenuation and uniform delay are not considered to be errors, since they represent no deterioration in the waveform's ability to convey information. Delay and gain are therefore adjusted to match the average system delay and average system attenuation. The test configuration measures waveform distortion introduced into the communications process.

The mathematical expression for the mean-square-error is [1]
Figure 5. Computer simulation results for maximum-length sequence (11, 9, 0).

\[ \bar{e}^2(t) = \lim_{T \to \infty} \frac{1}{2T} \int_{-T}^{T} [e_i(t-\tau) - Ge_o(t) - Gn_o(t)]^2 dt \quad , \quad (83) \]

where \( e_i(t-\tau) \) is the delayed system input, \( e_o(t) \) is the system output, \( G \) is the
Figure 6. Computer simulation results for hybrid-sum sequence \((5, 2, 0) + (6, 1, 0)\).

gain-compensation factor, and \(n_o(t)\) is the noise added-in system.

The value of the rms error measured as shown in Figure 7 depends upon the statistical and spectral properties of the system's input signal. Therefore, any specification relating to communications system performance as determined by the rms testing scheme must include a complete specification
of the test signal's spectral density and amplitude probability distribution. Common requirements for system test signals are an approximately Gaussian amplitude probability density function and a signal spectral envelope with the shape of common filtering functions, such as the low-pass Butterworth or Chebychev functions of a particular order.

The application of true random signals to simulate the input signals of the system is difficult because analog random signals cannot be delayed without some distortion. Also, the statistics of the noise signal must be stationary and the spectral characteristics must be well defined before the measurements can be assigned any real significance. Shepertycki's method of generating the system input signal and delayed input is shown in Figure 8. The advantage of this method is that the delay operation is performed digitally and virtually without distortion. The filters form the analog pseudorandom signal from the digital sequence. The transfer characteristics of the two filters must be closely matched to ensure proper operation.

The hybrid-sum sequence can be the source sequence for the noise signal generation scheme of Figure 8. The primary reason for the hybrid-sum sequence approach is to form large groups of pseudorandom sequences with a minimum of computer evaluation required to establish an analysis of the statistics of the filtered sequences. It has been shown that groups of hybrid-sum sequences can be evaluated much more rapidly and efficiently than groups of maximum-length sequences. The hybrid-sum approach is especially useful if a multichannel communications system is to be evaluated by establishing the mean-square error parameter as given by equation (83) for each channel.
A block diagram of the scheme for test signal generation and signal application for a multichannel communications system is shown in Figure 9. Each channel is evaluated on an rms basis, as illustrated in Figure 7. The test signals generated must be pseudoindependent in order for channel cross-talk to enter as the noise term, $[n_o(t)]$, in the error evaluation equation (83).

Figure 8. Method of generating test signals.

Figure 9. Test configuration for a multichannel communications system.
CONCLUSIONS

The purpose of this study was to establish a procedure for designing and analyzing noise-like signals from filtered, pseudorandom digital sequences. An immediate application of these filtered sequences is as test signals for performance evaluation of a multichannel communications system. The method for multichannel communications system evaluation is essentially an extension of a scheme proposed by Shepertycki; he suggested using filtered maximum-length digital sequences as the source of the data signals. Previous studies performed by Gilson [3], White [6], Lindholm [7], and Wainberg and Wolf [8] have shown that filtered maximum-length sequences do not necessarily have good statistical properties and therefore cannot be used indiscriminately in pseudorandom signal generators.

This study proposes that test signals for this performance evaluation scheme be derived from the filtered modulo-two sum of several maximum-length digital sequences. Sequences generated in this manner are called hybrid-sum sequences.

The theoretical analysis evaluates the statistics of filtered hybrid-sum sequences by calculating the higher moments of the weights of tuples from the sequence. This analysis is an extension of Lindholm's maximum-length sequences analysis to the hybrid-sum sequences.

The theory developed by this study yields a procedure for evaluating large groups of potential code sequences with a level of efficiency not previously possible; therefore, the results of the analysis may be applied not only to system testing but also to areas such as coding theory and modulation format design.
APPENDIX A
RESULTS OF COMPUTER PROGRAM POLTE 1

This appendix contains example results of the computer program POLTE 1. The program was run for three irreducible polynomials of order 11, 6, and 5. The results of POLTE 1 can be used to evaluate the statistics of filtered, pseudorandom digital sequences using equation (69).

The procedure for evaluating equation (69) using the results from POLTE 1 is as follows: For a given irreducible polynomial that generates a maximum-length sequence, the polynomial representation is printed in binary and octal form. For example,

POLYNOMIAL 110000100000
OCTAL 0103

represents the polynomial
\[ x^6 + x^5 + 1. \]

Following the polynomial octal form, the representations of the trinomials, quadrinomials, and pentanomials that contain the characteristic polynomial as a factor are printed. For example,

\((7, 5, 1, 0)\)

represents the polynomial
\[ x^7 + x^5 + x + 1. \]

This quadrinomial contains the characteristic polynomial,
\[ x^7 + x^5 + x + 1 = (x^6 + x^5 + 1) (x + 1) \pmod{2}. \] (A-1)

For a filter impulse-response period \( M \), the parameters \( B, E, \gamma \), and \( F, \gamma \) are respectively, the number of trinomials, quadrinomials, and pentanomials of order \( M-1 \) or less of the form.
\[ x^p (x^d + x^c + 1), \]
\[ x^p (x^d + x^c + x^b + 1), \]

and

\[ x^p (x^d + x^c + x^b + x^a + 1) \]

that contain the \( \gamma \)th characteristic polynomial as a factor. In the above polynomials, \( p \) can range from 0 to \( M-1-d \). Therefore, for each basic polynomial of the forms

\[ x^d + x^c + 1, \]
\[ x^d + x^c + x^b + 1, \]

or

\[ x^d + x^c + x^b + x^a + 1 \]

that contains the sequence characteristic polynomial as a factor, there are \( M-d \) product polynomials that also contain the sequence characteristic polynomial as a factor.

The algorithm in the computer program POLTE 1 detects the number of basic polynomials that contains the sequence characteristic equation as a factor. The parameters \( B_\gamma, E_\gamma, \) and \( F_\gamma \) are calculated from the results of POLTE 1 by forming the sum

\[
B_\gamma = \sum_{i=1}^{D_1} (M-d_i) \quad , \quad \text{(A-2)}
\]

\[
E_\gamma = \sum_{i=1}^{D_2} (M-d_i)_f \sum_{i=1}^{M-1} (M-i) \quad , \quad \text{(A-3)}
\]
and

\[ F_\gamma = \sum_{i=1}^{D_3} (M-d_i) \]  \hspace{1cm} (A-4)

where \(D_1, D_2, \) and \(D_3\) are the number of trinomials, quadranomials, and pentanomials of order \(M-1\) or less that are detected for the \(\gamma^{th}\)-component sequence by the program POLTE 1. If the characteristic equation of the \(\gamma^{th}\) sequence is a trinomial, \(f = 1\); \(f = 0\) otherwise.

The program POLTE 1 was used to evaluate the parameter \(B_\gamma\) for maximum-length sequences \((11, 9, 0), (6, 1, 0), \) and \((5, 2, 0),\) where \(M\) was equal to 20. The results are given in Table A-1.

<table>
<thead>
<tr>
<th>SEQUENCE</th>
<th>(B_\gamma)</th>
</tr>
</thead>
<tbody>
<tr>
<td>((11, 9, 0))</td>
<td>9</td>
</tr>
<tr>
<td>((6, 1, 0))</td>
<td>22</td>
</tr>
<tr>
<td>((5, 2, 0))</td>
<td>38</td>
</tr>
</tbody>
</table>

These values were previously used to evaluate the statistics of the maximum-length sequence \((11, 9, 0)\) and the hybrid-sum sequence \((6, 1, 0) + (5, 2, 0).\)
APPENDIX B
FLOW DIAGRAM FOR THE PROGRAM POLTE 1
1 CONTINUE

1 SET INITIAL CONTENT VECTOR

1************************************************************
1 L IS THE SEQUENCE LENGTH
1 NOSTG IS THE NUMBER OF STAGES

1 продолжающий процесс

1************************************************************
1 IF L=1139,33,34

1************************************************************
1 WRITE(6,41) NOSTG1

1************************************************************
1 ---F 61 FORMAT(///,1D1,1H 'NUMBER' 3)
1 THE STAGE = '1',13,13X 'MAXIMUM'
1 SEQUENCE LENGTH = '16',///

1************************************************************
1 I=1

1************************************************************
1 OK

1************************************************************
1 CONTINUE

1************************************************************
1 ---F WRITE OUT POLYNOMIAL CODE IN
1 [BINARY AND OCTAL FORM]

1************************************************************
1 WRITE(6,50) MMXW

1************************************************************
1 ---F 50 FORMAT(1H 'POLYNOMIAL ',2X)
1 ('1211',1H 'OCTAL',2X,911)
1 GET INITIAL CONTENT VECTOR

1************************************************************
1 STATE(NOSTG)=1
1 NOST3=NOSTG=1

1************************************************************
1 DO IN STAGE=1,NOST3

1************************************************************
1 a
1 a

1************************************************************
1 C الناتج
1 a
1 a

1************************************************************
1 NOST3=NOSTG=1

1************************************************************
1 ---F GENERATE FIRST NOSTG BITS

1************************************************************
1 INPUT=1
REFERENCES


STATISTICAL PROPERTIES OF FILTERED PSEUDORANDOM DIGITAL SEQUENCES FORMED FROM THE SUM OF MAXIMUM-LENGTH SEQUENCES

By G. R. Wallace, Glenn D. Weathers and Edward R. Graf

The information in this report has been reviewed for security classification. Review of any information concerning Department of Defense or Atomic Energy Commission programs has been made by the MSFC Security Classification Officer. This report, in its entirety, has been determined to be unclassified.

This document has also been reviewed and approved for technical accuracy.

G. SAUNDERS
Chief, Advanced Studies Office

O. T. DUGGAN
Chief, Instrumentation and Communication Division

F. B. MOORE
Director, Astrionics Laboratory
<table>
<thead>
<tr>
<th>INTERNAL</th>
<th>S&amp;E-ASTR-ZX</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIR</td>
<td>S&amp;E-ASTR-ZX</td>
</tr>
<tr>
<td>Dr. Petrone</td>
<td>A&amp;PS-MS-H</td>
</tr>
<tr>
<td>DEP-T</td>
<td>A&amp;PS-MS-IL (8)</td>
</tr>
<tr>
<td>S&amp;E-DIR</td>
<td>A&amp;PS-MS-IP (2)</td>
</tr>
<tr>
<td>S&amp;E-R-DIR</td>
<td>A&amp;PS-PAT</td>
</tr>
<tr>
<td>Dr. Johnson</td>
<td>Mr. L. D. Wofford, Jr.</td>
</tr>
<tr>
<td>S&amp;E-ASTR-DIR</td>
<td>A&amp;PS-TU (6)</td>
</tr>
<tr>
<td>Mr. Moore</td>
<td>EXTERNAL</td>
</tr>
<tr>
<td>S&amp;E-ASTR-C</td>
<td>Scientific and Technical Information Facility (25)</td>
</tr>
<tr>
<td>Mr. Swearingen</td>
<td>P. O. Box 33</td>
</tr>
<tr>
<td>S&amp;E-ASTR-G</td>
<td>College Park, Maryland 20740</td>
</tr>
<tr>
<td>Mr. Wojtalik</td>
<td>Attn: NASA Representative (S-AK/RKT)</td>
</tr>
<tr>
<td>S&amp;E-ASTR-I</td>
<td>Professor R. O. Pettus</td>
</tr>
<tr>
<td>Mr. Duggan</td>
<td>College of Engineering</td>
</tr>
<tr>
<td>Mr. Frost</td>
<td>University of South Carolina</td>
</tr>
<tr>
<td>Mr. Atherton</td>
<td>Columbia, South Carolina 29208</td>
</tr>
<tr>
<td>Mr. Eichelberger</td>
<td>Department of Electrical Engineering</td>
</tr>
<tr>
<td>Mr. G. Saunders</td>
<td>College of Engineering</td>
</tr>
<tr>
<td>Dr. Wallace (20)</td>
<td>Auburn University</td>
</tr>
<tr>
<td>Dr. Salter (Sperry)</td>
<td>Auburn, Alabama 36830</td>
</tr>
<tr>
<td>Dr. Weathers (Ala. A&amp;M) (4)</td>
<td>Attn: Professor D. Irwin (1)</td>
</tr>
<tr>
<td>Mr. Frederick (Sperry)</td>
<td>Professor E. R. Graf (4)</td>
</tr>
<tr>
<td>Mr. Gussow (Radiation, Inc.)</td>
<td></td>
</tr>
<tr>
<td>S&amp;E-ASTR-M</td>
<td>Mr. R. Watson, Director</td>
</tr>
<tr>
<td>Mr. Boehm</td>
<td>Division of Continuous Education</td>
</tr>
<tr>
<td>S&amp;E-ASTR-R</td>
<td>University of Alabama in Huntsville</td>
</tr>
<tr>
<td>Mr. Taylor</td>
<td>Huntsville, Alabama 35805</td>
</tr>
<tr>
<td>Dr. Randall</td>
<td>Hayes International Corp.</td>
</tr>
<tr>
<td></td>
<td>HIC Building</td>
</tr>
<tr>
<td></td>
<td>Huntsville, Ala. 35807</td>
</tr>
<tr>
<td></td>
<td>Attn: W. T. Weissinger</td>
</tr>
</tbody>
</table>