NEAVE EFFECT ALSO OCCURS WITH TAUSWORTHE SEQUENCES

Shu Tezuka

IBM Research,
Tokyo Research Laboratory
5-11 Sanbancho, Chiyoda-ku, Tokyo 102, Japan

ABSTRACT

In this paper, we show that the use of the Box-
Muller method with Tausworthe sequences for gener-
at ing normal deviates can produce pathological phe-
nomena similar to the Neave effect, which was found
to occur when linear congruential sequences and the
Box-Muller method are combined. Two examples of
the phenomena are given for Tausworthe sequences
in practical use. One of the examples demonstrates
that such phenomena possibly occur even with large-
period Tausworthe sequences. The paper also dis-
cusses the extension of the results obtained here
to Generalized Feedback Shift Register (GFSR) se-
quen ces, which are a variant of Tausworthe sequences.

1 INTRODUCTION

Most computer simulations require many random
variates from various types of distributions. Among
them, variates from normal distributions are most fre-
cently used, because of their central importance in
the field of statistics and probability theory. The Box-
Muller method is one of the most common techniques
for generating such variates. Because of its simplic-
ty, this method has recently been more and more
frequently used in computer simulations, in spite of
its use of such functions as logarithms and trigono-
metric functions.

In 1973, Neave (Neave 1973) pointed out that the
combination of the Box-Muller method and the con-
ventional linear congruential method produces unde-
irable results in some cases. To be more precise,
the tail distribution generated by this combination
differs markedly from the true distribution. This re-
result is significant, because in certain applications
such as rare event simulations the tail distribution should
be exact. One consequence is that we have to be
very careful in choosing the parameters of linear con-
gruential sequences for the Box-Muller method, or
to use alternatives, such as shift-register-type pseudo-
dorandom sequences, for the purpose. However, as
Ripley (Ripley 1987, p.59) states, “No general the-
ory has yet been developed for the sensitivity of” the
Box-Muller method to such alternatives.

Recently (Tezuka 1989, 1990), it has been shown
that Tausworthe sequences can be formulated as lin-
ear congruential sequences in terms of polynomial
arithmetic modulo two, and thereby leading to the
lattice structure of the sequences, which is theoreti-
cally similar to that of traditional linear congruential
sequences. In this paper, we will show that this de-
velopment can be used to analyze the effect of Taus-
worthe sequences on the Box-Muller method. The
result is that a similar effect to Neave’s can occur
with Tausworthe sequences. Moreover, we point out
that the effect is independent from the period size of
the sequences; in other words, the Neave effect can
occur, even if we employ long-period sequences.

The paper is organized as follows. Section 2
overviews the Neave effect for the combination of
linear congruential sequences and the Box-Muller
method. In Section 3, we show that the use of the
Box-Muller method with Tausworthe sequences pro-
duces similar phenomena to the Neave effect, and
then give some examples of the phenomena with
Tausworthe sequences in practical use. Finally, we
discuss the generalization of the theory developed
here to Generalized Feedback Shift Register (GFSR)
sequences, which are a variant of Tausworthe se-
quen ces.

2 OVERVIEW OF NEAVE EFFECT

First, we describe the definition of the Box-Muller
method, which is given as

\[ V_1 = \sqrt{-2 \ln(U_1)} \sin(2\pi U_2), \]
\[ V_2 = \sqrt{-2 \ln(U_1)} \cos(2\pi U_2), \]
where $U_1$ and $U_2$ are independent uniform random variates in $[0, 1)$ and $V_1$ and $V_2$ are independent normal random variates from $N(0, 1)$. Note that $U_1$ should not take the value of zero. For a 32-bit word-size computer, $|V_1|$ and $|V_2|$ are bounded from above by $\sqrt{-2 \ln(2^{−32})} \approx 6.600$.

Neave (Neave 1973) pointed out that some linear congruential sequences interact adversely with the popular Box-Muller method for normal random deviate generators. Let the linear congruential sequence be

$$X_i = aX_{i−1} \pmod{M}.$$  

The Box-Muller method is then given as

$$V_1 = \sqrt{-2 \ln(X_i/M)} \sin(2\pi aX_i/M),$$
$$V_2 = \sqrt{-2 \ln(X_i/M)} \cos(2\pi aX_i/M).$$

As discussed in (Bratley et al. 1987, p. 223), the plots of $(V_1, V_2)$ lie on a spiral. Hereafter, we deal only with $V_1$ unless otherwise specified, because similar results follow for $V_2$. Neave obtained the approximate range of $V_1$ with respect to the size of multipliers for linear congruential sequences; that is, the range is given as $[-\sqrt{2 \ln(4a/3)}, \sqrt{2 \ln(4a)}]$ for $V_1$. To sum up, the smaller the value of $a$, the narrower the corresponding range becomes. Specifically, when $a$ is around $\sqrt{M}$, $V_1$ takes values only in the approximate range $-4.5$ through $4.5$. Note that multipliers with a size of around $\sqrt{M}$ are very often employed due to their portability in implementation (L’Ecuyer 1988). Since the probability of the true normal deviates falling within the tails, $[-\infty, -4.5]$ and $[4.5, \infty]$, is around $6 \times 10^{-5}$, we can say that using more than $10^6$ normal deviates should not use the Box-Muller method with such generators.

In Table 1, we list examples of the tail distribution for the entire period of sequence from the most popular generator, $a = 7^5$ and $M = 2^{31} − 1$, whose range was exhaustively calculated as $[-4.476239, 4.717018]$ compared with the approximate range $[-4.475, 4.715]$. An important observation here is that a significant disparity starts from around $|V_1| = 3.6$, far ahead of the bound at which the tail disappears. Neave explained these as due to the discontinuities which occur at the zeros of the equation

$$\frac{dZ}{dX} = 0,$$

where $Z = \sqrt{-2 \ln(X)} \sin(2\pi aX)$. Note that the Neave effect occurs even when we use the sequence in reverse order, i.e.,

$$V = \sqrt{-2 \ln(X_i/M)} \sin(2\pi aX_{i−1}/M)$$
$$V = \sqrt{-2 \ln(X_i/M)} \sin(2\pi a^*X_i/M),$$

Table 1: Frequencies of $V_1$ in the tail from the Box-Muller method with linear congruential sequences, $x_i = 16807x_{i−1} \pmod{2^{31}−1}$, over the entire period

<table>
<thead>
<tr>
<th>Range</th>
<th>Observed O</th>
<th>Expected E</th>
<th>Deviation $(O - E)/\sqrt{E}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.70:3.71</td>
<td>9772</td>
<td>8955</td>
<td>8.6</td>
</tr>
<tr>
<td>3.71:3.72</td>
<td>7559</td>
<td>8632</td>
<td>-11.5</td>
</tr>
<tr>
<td>3.72:3.73</td>
<td>8887</td>
<td>8312</td>
<td>6.3</td>
</tr>
<tr>
<td>3.73:3.74</td>
<td>7566</td>
<td>8010</td>
<td>-4.9</td>
</tr>
<tr>
<td>3.74:3.75</td>
<td>7937</td>
<td>7715</td>
<td>2.5</td>
</tr>
<tr>
<td>3.75:3.76</td>
<td>7608</td>
<td>7430</td>
<td>2.0</td>
</tr>
<tr>
<td>3.76:3.77</td>
<td>6929</td>
<td>7157</td>
<td>-2.6</td>
</tr>
<tr>
<td>3.77:3.78</td>
<td>7507</td>
<td>6893</td>
<td>7.3</td>
</tr>
<tr>
<td>3.78:3.79</td>
<td>6080</td>
<td>6635</td>
<td>-6.8</td>
</tr>
<tr>
<td>3.79:3.80</td>
<td>6752</td>
<td>6390</td>
<td>4.5</td>
</tr>
</tbody>
</table>

where $a^*a = 1 \pmod{M}$, provided that the size of $a^*$ is small (even if the size of $a$ is large enough).

3 BOX-MULLER METHOD WITH TAUSWORTHY SEQUENCES

3.1 Definition of Tausworthe Sequences

A Tausworthe sequence $u_i, i = 1, 2, \ldots$, is defined as follows (Tausworthe 1965):

$$u_i = \sum_{l=1}^{L} a_{s+l}2^{-l},$$

(1)

where $a_i, i = 1, 2, \ldots$, follows the recurrence relation $a_i = c_1a_{i−1} + \cdots + c_pa_{i−p} \pmod{2}$ whose characteristic polynomial, $M(x) = x^p + c_1x^{p−1} + \cdots + c_p$, is a primitive polynomial, and $s$ is a constant representing the decimation size.

Here, we describe the following formula of Tausworthe sequences: Let $GF\{2, x\}$ denote the field of all Laurent series of the form $S(x) = \sum_{j=-\infty}^{m} c_j x^j$, where $m$ is an integer and $c_j$ is in $GF(2)$. Then we define an analogous version of linear congruential sequences in $GF\{2, x\}$. Let $\sigma$ be a mapping from $GF\{2, x\}$ to the real field, defined as

$$\sigma(S(x)) = S(2).$$
A pseudorandom sequence \( u_i, i = 1, 2, ..., \) in \([0,1]\) is then defined as
\[
f_i(x) = (g(x)f_{i-1}(x) + h(x)) \mod M(x) \\
u_i = \sigma(f_i(x)/M(x)),
\]
where \( g(x), h(x), M(x) \) and \( f_i(x) \) are polynomials in \( GF\{2, x\} \). In practical situations, \( u_i \) is expressed approximately by its truncated value, i.e., by summing from some constant \(-L\). In what follows, it is shown that a Tausworthe sequence is a special case of the above general class. Let \( M(x) = x^p + c_1x^{p-1} + \cdots + c_p \) be a primitive polynomial of degree \( p \) over \( GF(2) \), and let \( h(x) \equiv 0, g(x) = (x^s \mod M(x)), \) with \( 0 < s < 2^p - 1, \gcd(s, 2^p - 1) = 1, m = -1, \) and \( L \) be the “word-size.” Suppose \( f_0(x)/M(x) = a_1x^{-1} + a_2x^{-2} + \cdots \) then \( M(x) \cdot (a_1x^{-1} + a_2x^{-2} + \cdots) = f_0(x), \) i.e., no fractional terms exist in the LHS. Hence \( a_i, i = p + 1, p + 2, ... \) follows the recurrence relation \( a_i = c_1a_{i-1} + \cdots + c_pa_{i-p} \pmod{2} \) whose characteristic polynomial is \( M(x) \). Therefore, the sequence is written, for \( i = 1, 2, ..., \), as
\[
u_i = \sum_{l=1}^{L} a_{s+i}2^{-l}.
\]
This sequence is identical with the Tausworthe sequence defined above in (1).

Typically used Tausworthe sequences are the case of \( s = 0 \) and \( M(x) = x^p + x^q + 1 \) with \( q < p/2 \), i.e.,
\[
u_i = \sum_{l=1}^{\min(L,p)} a_{pi+l}2^{-l}.
\]
This type of Tausworthe sequence can be easily implemented in both software and hardware (Bratley et al. 1987). Some authors (Marasglia 1976) describe this generator with \( p \leq L \) by using matrix representation in the following way. Let \( S_t \) and \( S_l \) be \( p \times p \) matrices that produce right and left shifts, such as,
\[
S_l = \begin{pmatrix}
1 & 0 & \cdots & 0 \\
0 & 1 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 1 \\
0 & 0 & \cdots & 0
\end{pmatrix},
\]
and let \( I \) be the identity matrix. The p-bit typical Tausworthe sequence is then given as a sequence of binary vectors,
\[
\beta, T\beta, T^2\beta, \ldots,
\]
where \( T = (I + S_t^{-1})(I + S_l) \) and \( \beta \) is a nonzero binary vector.

### 3.2 Effect of Tausworthe Sequences on Box-Muller Method

As Ripley states (Ripley 1987, p.59), “the best way to understand the Neave effect is to note that we can be concerned with large values of \( V_1 \) and \( V_2 \), hence with small values of \( U_1 \).” Or, as Dagpunar explains in (Dagpunar 1988, p.94), “a tail deviate can be obtained only if \( U_1 \) is small, but \( U_2 \) is not so. However, for a multiplier as low as 131, a small value of \( U_1 \) always leads to a small value of \( U_2 \).”

This observation also holds for the sequence defined in (2); that is to say, when the degree of \( g(x) \) in (2) is small, the values of \( V_1 \), which is generated in the same way as above by replacing linear congruential sequences with the sequences in (2), fall within the bounded range, like the Neave effect. These assertions can be made more quantitatively. Denote \( u_i(x) = f_i(x)/M(x) \) for the equation (2), i.e., \( u_i = \sigma(u_i(x)) \). And let \( d = \deg(g(x)) \). We assume that for small \( u_i, \sqrt{2}\ln(u_i) \) is approximately flat compared with \( \sin(2\pi u_i) \). Then the value of \( u_i \) such that \( \sigma(g(x)u_i(x)) = 1/4 \) (or 3/4) gives the bound for \( V_1 \). Since \( 2^{4d}u_i < \sigma(g(x)u_i(x)) < 2^{4+1}u_i \) from the equation (2), the approximate peak of \( |V_1| \) will appear for \( u_i \) with \( 1/4(2^{2d+1}) \leq u_i \leq 1/4(2^2d) \) (or \( 3/4(2^{d+1}) \leq u_i \leq 3/4(2^d) \)). (It is worth noting that if \( d \) is greater than the word-size of a computer, the range is determined by the latter only.) These considerations can be summarized as follows:

**Proposition 1** Let \( M(x) \) be the characteristic polynomial and \( s \) be the decimation size for a Tausworthe sequence. Then the approximate range of \( V_1 \) from the Box-Muller method with the Tausworthe sequence is given as
\[
[-\sqrt{2}\ln(4 \cdot 2^3/3), \sqrt{2}\ln(4 \cdot 2^3)].
\]
Here \( d = \deg(g(x)), \) where \( g(x) = x^s \mod M(x) \).

The validity of the above approximation can be demonstrated as follows: Consider \( B(t) = \sqrt{2}\ln(2^{d-1}t)\sin(2\pi t) \) for \( t > 0 \). By using this, we can bound \( V_1 \), i.e., \( \min_{t>0} B(t) \leq \sqrt{2}\ln(u_i)\sin(2\pi u_{i+1}) \leq \max_{t>0} B(t) \) for any \( (u_i, u_{i+1}) \). Table 2 shows the minimum and maximum values of \( B(t) \), which were numerically computed, and the approximate range given in (3) for \( 1 \leq d \leq 15 \). As easily seen, the approximation is fairly good.

We should notice that the essential factor determining the approximate range is not the decimation size \( s \), but the degree of \( g(x) \) (mod \( M(x) \)). Also note that in the case of those Tausworthe sequences which are 2-distributed with \( L \)-bit resolution
Table 2: Validity of the approximate range \([LB, UB]\) of \(V_i\) given in (3), where \(LB = -\sqrt{2\ln(4 \cdot 2^d/3)}\) and \(UB = \sqrt{2\ln(4 \cdot 2^d)}\).

<table>
<thead>
<tr>
<th>(d)</th>
<th>(\min B(t))</th>
<th>(LB)</th>
<th>(UB)</th>
<th>(\max B(t))</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-1.833438</td>
<td>-1.400</td>
<td>2.039</td>
<td>2.371154</td>
</tr>
<tr>
<td>2</td>
<td>-2.178031</td>
<td>-1.829</td>
<td>2.354</td>
<td>2.644382</td>
</tr>
<tr>
<td>3</td>
<td>-2.475467</td>
<td>-2.175</td>
<td>2.632</td>
<td>2.892840</td>
</tr>
<tr>
<td>4</td>
<td>-2.740960</td>
<td>-2.473</td>
<td>2.884</td>
<td>3.122076</td>
</tr>
<tr>
<td>5</td>
<td>-2.982988</td>
<td>-2.739</td>
<td>3.115</td>
<td>3.335880</td>
</tr>
<tr>
<td>6</td>
<td>-3.206840</td>
<td>-2.982</td>
<td>3.330</td>
<td>3.536961</td>
</tr>
<tr>
<td>7</td>
<td>-3.416078</td>
<td>-3.206</td>
<td>3.532</td>
<td>3.727327</td>
</tr>
<tr>
<td>8</td>
<td>-3.613236</td>
<td>-3.415</td>
<td>3.723</td>
<td>3.908513</td>
</tr>
<tr>
<td>9</td>
<td>-3.800189</td>
<td>-3.612</td>
<td>3.905</td>
<td>4.081721</td>
</tr>
<tr>
<td>10</td>
<td>-3.978373</td>
<td>-3.799</td>
<td>4.078</td>
<td>4.247916</td>
</tr>
<tr>
<td>11</td>
<td>-4.148918</td>
<td>-3.978</td>
<td>4.245</td>
<td>4.407881</td>
</tr>
<tr>
<td>12</td>
<td>-4.312727</td>
<td>-4.148</td>
<td>4.405</td>
<td>4.562265</td>
</tr>
<tr>
<td>13</td>
<td>-4.470542</td>
<td>-4.312</td>
<td>4.560</td>
<td>4.711613</td>
</tr>
<tr>
<td>14</td>
<td>-4.622974</td>
<td>-4.470</td>
<td>4.709</td>
<td>4.856386</td>
</tr>
<tr>
<td>15</td>
<td>-4.770540</td>
<td>-4.622</td>
<td>4.854</td>
<td>4.996978</td>
</tr>
</tbody>
</table>

(Fushimi and Tezuka 1983, Tezuka 1987), the degree of \(g(x)\) is always large enough, where \(L\) is the wordsize of a computer.

Similar arguments give the other peaks approximately \(u_i\) with \(p/(4 \cdot 2^{d+1}) \leq u_i \leq p/(4 \cdot 2^d)\), where \(p\) is an odd integer with \(0 < p < 2^d\), where \(d = \text{deg}(g(x))\). These peaks might yield irregularities in the tail of \(V_i\). Theoretically, they correspond to the discontinuities which Neave found for the linear congruential case.

3.3 Practical Examples of the Effect

In this section, we give two practical examples in which a Neave-like effect occurs. Both are typical Tausworth sequences, i.e.,

\[ u_i = \sum_{l=1}^{\min(L,p)} a_{pi+l} 2^{-l} \]

Example 1 The following Tausworth sequence is a component of the combined generator, SUPER-DUPER, proposed in (Marsaglia 1976). From the discussion in Section 3.1, the generator is written as \(M(x) = x^{32} + x^{15} + 1, g(x) = x^{32} = x^{15} + 1\) (mod \(M(x)\)), \(h(x) = 0\), and \(L = 32\) in (2). Note that \(M(x)\) is not irreducible, i.e., \(M(x) = \left(x^{21} + x^{19} + x^{15} + x^{13} + x^{12} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^4 + x^2 + 1\right)\left(x^{11} + x^9 + x^7 + x^5 + 1\right)\). So, the maximum possible period is \(2^{21} - 1\)\(2^{11} - 1\) and thereby almost all initial values give the maximum period. Exhaustive calculation shows that for this generator the range into which \(V_i\) falls is \([-4.622979, 4.856391]\), while the approximate range from (3) is \([-4.622, 4.854]\), since \(\text{deg}(g(x)) = 15\). This shows that the range defined in (3) gives a good approximation. Table 3 lists examples of the tail distribution for this generator over the entire period. This shows some irregularities in the tail, which are similar to those in the case of linear congruential sequences.

Example 2 Here, we employ two Tausworth sequences, whose parameters are \(M(x) = x^{127} + x^7 + 1\), \(q = 7, 15\), with \(s = 127\) and \(L = 32\). Hence \(\text{deg}(g(x)) = 7\) or 15. The period of the sequence is equal to \(2^{127} - 1\), since \(M(x)\) above are primitive polynomials. The range for the case of \(q = 7\) is at most \([-3.417, 3.728]\) from \(\min_{t=0} B(t)\) and \(\max_{t>0} B(t)\) in Table 2. For \(q = 15\), the range is at most \([-4.771, 4.997]\) also from Table 2. Notice that the bounds given by \(\min_{t>0} B(t)\) and \(\max_{t>0} B(t)\) become tight when the period is large enough.

4 DISCUSSION

In this section, we discuss the extension of the results presented in the foregoing sections to the combination of the Box-Muller method and GFSR sequences,
which are a variant of Tausworth sequences. A GFSR sequence $u_i, i = 1, 2, \ldots$, was originally defined as follows (Lewis and Payne 1973): Let $a_i, i = 1, 2, \ldots$, be a binary sequence in $GF(2)$ whose characteristic polynomial, denoted by $M_0(x)$, is primitive. Then

$$u_i = \sum_{l=1}^{L} a_{di+l} 2^{-l},$$

where $d$ is a constant between 1 and $2^p - 1$ and $L \leq p$. Denote $b_i = a_{di}$, for $i = 1, 2, \ldots$. Let $M_b(x)$ be the characteristic polynomial of $b_i, i = 1, 2, \ldots$. Then the above sequence $u_i, i = 1, 2, \ldots$, can be written by the formulation in (2) with $M(x) = M_b(x)$, $h(x) \equiv 0$, and $g(x)$ is a primitive root modulo $M_b(x)$ such that $g^q(x) \equiv x \pmod{M_b(x)}$. Note that in this case $M_b(x)$ is always irreducible, but not primitive unless $d$ is coprime to $2^p - 1$. Therefore, we conclude that a Neave-like effect also occurs with the original GFSR sequences.

Next, we consider a more general case of GFSR sequences:

$$u_i = \sum_{l=1}^{L} a_{j_l i + 1} 2^{-l},$$

where $j_l, l = 1, \ldots, L$, are integers between 1 and $2^p - 1$. Note that $L \leq p$ (otherwise, a linear dependence relation appears between the column bits of $u_i$). For simplicity, we assume that $L = p$. As shown in (Tezuka 1987, 1990), the sequence can be written equivalently in the matrix representation as

$$\beta, T\beta, \ldots, T^j\beta, \ldots,$$

where $T$ is any nonsingular $p \times p$ matrix over $GF(2)$.

The open question is how complicated the irregularities in the tail distribution become for this general case, where unlike in the case of the original GFSR sequences discussed above we cannot make such assumptions as that the mapping $y = Tx$ is written as a linear mapping in $GF(2, x)$.

ACKNOWLEDGMENTS

The author is grateful to Prof. M. Fushimi for his careful reading of the manuscript, and to anonymous referee for his valuable comments.

REFERENCES


AUTHOR BIOGRAPHIES

SHU TEZUKA is an advisory researcher at IBM Research, Tokyo Research Laboratory. His research interests are random number generation, global optimization, and stochastic simulation. He is a member of ACM, IEEE, SIAM, and IPSJ.