Proceedings of the 1991 Winter Simulation Conference
Barry L. Nelson, W. David Kelton, Gordon M. Clark (eds.)

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 generating normal deviates can produce pathological phenomena 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 discusses the extension of the results obtained here to Generalized Feedback Shift Register (GFSR) sequences, 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 frequently 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 simplicity, this method has recently been more and more frequently used in computer simulations, in spite of its use of such functions as logarithms and trigonometric functions.

In 1973, Neave (Neave 1973) pointed out that the combination of the Box-Muller method and the conventional linear congruential method produces undesirable results in some cases. To be more precise, the tail distribution generated by this combination differs markedly from the true distribution. This 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 congruential sequences for the Box-Muller method, or to use alternatives, such as shift-register-type pseudorandom sequences, for the purpose. However, as Ripley (Ripley 1987, p.59) states, "No general theory 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 linear congruential sequences in terms of polynomial arithmetic modulo two, and thereby leading to the lattice structure of the sequences, which is theoretically similar to that of traditional linear congruential sequences. In this paper, we will show that this development can be used to analyze the effect of Tausworthe 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 produces 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 sequences.

2 OVERVIEW OF NEAVE EFFECT

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

$$\begin{aligned} V_1 &= \sqrt{-2\ln(U_1)}\sin(2\pi U_2), \\ V_2 &= \sqrt{-2\ln(U_1)}\cos(2\pi U_2), \end{aligned}$$

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 $\sqrt{-2\ln(2^{-32})} \approx 6.660$.

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

$$\begin{aligned} V_1 &= \sqrt{-2\ln(X_i/M)}\sin(2\pi a X_i/M), \\ V_2 &= \sqrt{-2\ln(X_i/M)}\cos(2\pi a X_i/M). \end{aligned}$$

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 6×10^{-6}, we can say that simulation 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 $[-4.476239, 4.717016]$ 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 $Z = \sqrt{-2\ln(X)}\sin(2\pi a X)$. Note that the Neave effect occurs even when we use the sequence in reverse order, i.e.,

$$\begin{aligned} V &= \sqrt{-2\ln(X_i/M)}\sin(2\pi X_{i-1}/M) \\ &= \sqrt{-2\ln(X_i/M)}\sin(2\pi a^* X_i/M), \end{aligned}$$

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

Range	Observed O	Expected E	Deviation $(O-E)/\sqrt{E}$
3.70:3.71	9772	8955	8.6
3.71:3.72	7559	8632	-11.5
3.72:3.73	8887	8312	6.3
3.73:3.74	7566	8010	-4.9
3.74:3.75	7937	7715	2.5
3.75:3.76	7608	7430	2.0
3.76:3.77	6929	7157	-2.6
3.77:3.78	7507	6893	7.3
3.78:3.79	6080	6635	-6.8
3.79:3.80	6752	6390	4.5
-3.60:-3.61	12552	12906	-3.1
-3.61:-3.62	12278	12455	-1.5
-3.62:-3.63	11974	12004	-0.2
-3.63:-3.64	11692	11574	1.0
-3.64:-3.65	11447	11166	2.6
-3.65:-3.66	11244	10758	4.6
-3.66:-3.67	9357	10372	-9.9
-3.67:-3.68	10089	10007	0.8
-3.68:-3.69	10126	9642	4.9
-3.69:-3.70	8729	9298	-5.9

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 TAUSWORTHE SEQUENCES

3.1 Definition of Tausworthe Sequences

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

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

where $a_i, i = 1, 2, \ldots$, follows the recurrence relation $a_i = c_1 a_{i-1} + \cdots + c_p a_{i-p} \pmod{2}$ whose characteristic polynomial, $M(x) = x^p + c_1 x^{p-1} + \cdots + c_p$, is a primitive polynomial, and s is a constant representing the decimation size.

Here, we describe the following formulation 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 σ be a mapping from $GF\{2, x\}$ to the real field, defined as

$$\sigma(S(x)) = S(2).$$

A pseudorandom sequence u_i, $i = 1, 2, \ldots$, in [0,1) is then defined as

$$\begin{aligned} f_i(x) &= (g(x)f_{i-1}(x) + h(x)) \bmod M(x) \\ u_i &= \sigma(f_i(x)/M(x)), \end{aligned} \qquad (2)$$

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 $h(x) \equiv 0$, $g(x) = (x^s \bmod M(x))$, 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 $M(x) \times (a_1x^{-1} + a_2x^{-2} + \cdots) = f_0(x)$, i.e., no fractional terms exist in the LHS. Hence $a_i, i = p+1, p+2, \ldots$ 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 $i = 1, 2, \ldots$, as

$$u_i = \sum_{l=1}^{L} a_{si+l}2^{-l}.$$

This sequence is identical with the Tausworthe sequence defined above in (1).

Typically used Tausworthe sequences are the case of $s = p$ 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 (Marsaglia 1976) describe this generator with $p \le L$ by using matrix representation in the following way. Let S_r and S_l be $p \times p$ matrices that produce right and left shifts, such as,

$$S_l = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & \cdots & \cdots & \cdots & \\ & \cdots & \cdots & \cdots & \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

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 $T = (I + S_l^{p-q})(I + S_r^q)$ and β 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_i." 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 $\sin(2\pi u_{i+1})$. 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 $2^d u_i \le \sigma(g(x)u_i(x)) < 2^{d+1}u_i$ from the equation (2), the approximate peak of $|V_1|$ will appear for u_i with $1/(4\cdot 2^{d+1}) \le u_i \le 1/(4\cdot 2^d)$ (or $3/(4\cdot 2^{d+1}) \le u_i \le 3/(4\cdot 2^d)$). (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*

$$[-\sqrt{2\ln(4\cdot 2^d/3)}, \sqrt{2\ln(4\cdot 2^d)}]. \qquad (3)$$

Here $d = \deg(g(x))$, where $g(x) = x^s \pmod{M(x)}$.

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., $\min_{t>0} B(t) \le \sqrt{-2\ln(u_i)}\sin(2\pi u_{i+1}) \le \max_{t>0} B(t)$ 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 $1 \le d \le 15$. 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 $g(x)(= x^s \pmod{M(x)})$. 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_1 given in (3), where LB$= -\sqrt{2\ln(4\cdot 2^d/3)}$ and UB$= \sqrt{2\ln(4\cdot 2^d)}$.

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

(Fushimi and Tezuka 1983, Tezuka 1987), the degree of $g(x)$ is always large enough, where L is the word-size of a computer.

Similar arguments give the other peaks approximately for u_i with $p/(4\cdot 2^{d+1}) \le u_i \le p/(4\cdot 2^d)$, where p is an odd integer with $0 < p < 2^d$, where $d = \deg(g(x))$. These peaks might yield irregularities in the tail of V_1. 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 Tausworthe sequences, i.e.,

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

Example 1 *The following Tausworthe 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* $M(x) = x^{32} + x^{15} + 1, g(x) = x^{32} = x^{15} + 1 \pmod{M(x)}, h(x) = 0$, *and* $L = 32$ *in (2). Note that* $M(x)$ *is not irreducible, i.e.,* $M(x) = (x^{21} + x^{19} + x^{15} + x^{13} + x^{12} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^4 + x^2 + 1)(x^{11} + x^9 + x^7 + x^2 + 1)$. *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_1 *falls is* $[-4.622979, 4.856391]$, *while the approximate range from (3) is* $[-4.622, 4.854]$, *since* $\deg(g(x)) = 15$. *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.*

Table 3: Frequencies of V_1 in the tail from the Box-Muller method with the Tausworthe sequence, SUPER-DUPER, over the entire period

Range	Observed O	Expected E	Deviation $(O-E)/\sqrt{E}$
3.65:3.66	21345	21517	-1.1
3.66:3.67	21053	20757	2.0
3.67:3.68	19716	20014	-2.1
3.68:3.69	20025	19284	5.3
3.69:3.70	18138	18622	-3.5
3.70:3.71	17716	17910	-1.4
3.71:3.72	17372	17265	0.8
3.72:3.73	17336	16625	5.5
3.73:3.74	15791	16020	-1.8
3.74:3.75	15295	15431	-1.0
-3.85:-3.86	9757	10157	-3.9
-3.86:-3.87	9952	9775	1.7
-3.87:-3.88	9959	9405	5.7
-3.88:-3.89	8238	9045	-8.4
-3.89:-3.90	8832	8718	1.2
-3.90:-3.91	9117	8349	8.4
-3.91:-3.92	7026	8048	-11.3
-3.92:-3.93	8265	7735	6.0
-3.93:-3.94	6880	7438	-6.4
-3.94:-3.95	7451	7151	3.5

Example 2 *Here, we employ two Tausworthe sequences, whose parameters are* $M(x) = x^{127} + x^q + 1$, $q = 7, 15$, *with* $s = 127$ *and* $L = 32$. *Hence* $\deg(g(x)) = 7$ *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 Tausworthe sequences. A GFSR sequence $u_i, i = 1,2,...$, was originally defined as follows (Lewis and Payne 1973): Let $a_i, i = 1,2,...$, be a binary sequence in $GF(2)$ whose characteristic polynomial, denoted by $M_a(x)$, is primitive. Then

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

where d is a constant between 1 and $2^p - 1$ and $L \leq p$. Denote $b_i = a_{di}$, for $i = 1,2,....$ Let $M_b(x)$ be the characteristic polynomial of $b_i, i = 1,2,....$ Then the above sequence $u_i, i = 1,2,...$, 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 $g^d(x) \equiv x \pmod{M_b(x)}$. 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:

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

where $j_l, l = 1,...L$, 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

$$\beta, T\beta, ..., T^i\beta, ...,$$

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

Bratley, P., B.L. Fox, and L.E. Schrage. 1987. *A Guide to Simulation*, 2nd ed., Springer-Verlag.

Dagpunar J. 1988. *Principles of Random Variate Generation*, Oxford Univ. Press.

Fushimi, M. and S. Tezuka. 1983. The k-distribution of generalized feedback shift register pseudorandom numbers. *Comm. ACM.* **26**: 516-523.

L'Ecuyer P. 1988. Efficient and portable combined random number generators. *Comm. ACM.* **31**: 742-749,774.

Lewis, J.G. and W.H. Payne. 1973. Generalized feedback shift register pseudorandom number algorithm. *J. ACM.* **20**: 456-468.

Marsaglia, G. 1976. Random number generation. In: *Encyclopedia of Computer Science*, eds. A. Ralston and C.L. Meek, 1192-1197. New York: Petrocelli/Charter.

Neave, H.R. 1973. On using the Box-Muller transformation with multiplicative congruential pseudorandom number generators. *Appl. Stat.* **22**: 92-97.

Ripley, B.D. 1987. *Stochastic Simulation*, Wiley.

Tausworthe, R.C. 1965. Random numbers generated by linear recurrence modulo two. *Math. Comp.* **19**: 201-209.

Tezuka, S. 1987. Walsh-spectral test for GFSR pseudorandom number generators. *Comm. ACM.* **30**: 731-735.

Tezuka, S. 1989. Random number generation based on polynomial arithmetic modulo two. Research Report, RT-0017, IBM Tokyo Research Laboratory.

Tezuka, S. 1990. Lattice structure of pseudorandom sequences from shift register generators. In *Proceedings of the 1990 Winter Simulation Conference*, eds. O. Balci, R.P. Sadowski, and R.E. Nance, 266-269. Institute of Electrical and Electronics Engineers, New Orleans, Louisiana.

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.