Technical Report CS74012-R

THE RELATIONSHIP BETWEEN THE MULTIPLICATIVE AND MIXED GENERATORS MODULO 2^b . †

Claude Overstreet, Jr.*

July 1974

†Research conducted through a summer grant by the Department of Computer Science, V.P.I. & S.U.

*Department of Computer Science, Bowling Green State University, Bowling Green, Ohio.

INTRODUCTION

In 1951, D. H. Lehmer [1] first proposed the linear congruential technique,

$$X_{n+1} \equiv aX_n + c \pmod{M}$$

as a source of random numbers. This technique has since become known as the multiplicative random number generator for $c = 0$ and as the mixed random number generator for $c \neq 0$.

These two forms of the linear congruential technique have been studied in depth, particularly when M is of the form 2^b. Although Hull and Dobell [2] have shown the mixed generator to have a longer period than the multiplicative generator, the question has persisted concerning which of the two techniques gives rise to better statistical behavior. Hull and Dobell [3] in a subsequent paper, while comparing the mixed and multiplicative generators, state that the statistical behavior of mixed generators is not as good as that of multiplicative generators. MacLaren and Marsaglia [4] comment that their test results suggest that the multiplicative generator performs better than the mixed generator.

We attempt to answer the above question by showing that for any sequence of real values in (0,1) produced by the multiplicative generator modulo 2^b a corresponding mixed generator exists which, for practical purposes, produces the same sequence of real values.

Mathematical Development of the Relationship between the Multiplicative and Mixed Generators Modulo 2^b

The multiplicative generator is defined as

$$X_{n+1} \equiv aX_n \pmod{2^b}.$$

Hull and Dobell [2] show that the multiplicative generator obtains a maximum period of 2^{b-2} when $b > 3$, $a \equiv 3$ and $5 \pmod 8$ and X_o is odd. Jansson [5] presents results that are summarized in the following lemma.

Lemma 1

1. When $a \equiv 5 \pmod 8$ and $X_o \equiv 1 \pmod 4$ the sequences generated contain the numbers $4v + 1$ $(v = 0,1,\ldots 2^{b-2}-1)$
2. When $a \equiv 5 \pmod 8$ and $X_o \equiv 3 \pmod 4$ the sequences generated contain the numbers $4v + 3$ $(v = 0,1,\ldots,2^{b-2}-1)$
3. When $a \equiv 3 \pmod 8$ and $X_o \equiv 1 \pmod 2$ the sequences generated contain the numbers $2v + 1$ $(v = 0,1,\ldots,2^{b-1}-1)$

Let us first consider the sequences generated by the multiplicative generator when $a \equiv 5 \pmod 8$ and $X_o \equiv 1 \pmod 4$.

Theorem 1

Given a multiplicative generator

$$X_{n+1} \equiv aX_n \pmod{2^b}$$

with $a \equiv 5 \pmod 8$ and $X_o \equiv 1 \pmod 4$ then there exists a mixed generator

$$Y_{n+1} \equiv aY_n + a' \pmod{2^{b-2}}$$

for $Y_i = \lfloor X_i/4 \rfloor$ and $a' = \lfloor a/4 \rfloor$ such that for all corresponding values X_n and Y_n, the multiplicative generator produces real values $Xn/2^b$ and the mixed generator produces real values $\frac{Yn}{2^{b-2}} = \frac{Xn}{2^b} - \frac{1}{2^b}$.

Proof:

Given,

1) $X_{n+1} \equiv aX_n \pmod{2^b}$ with $a \equiv 5 \pmod 8$
and $X_o \equiv 1 \pmod 4$.

From lemma 1, we have $X_i = 4 \cdot \lfloor X_i/4 \rfloor + 1$
and letting $Y_i = \lfloor X_i/4 \rfloor$ we have $X_i = 4Y_i + 1$.

$4Y_{n+1} + 1 \equiv a(4Y_i+1) \pmod{2^b}$
$4Y_{n+1} + 1 \equiv 4aY_i + a \pmod{2^b}$
given $a \equiv 1 \pmod 4$
implies $a = 4\lfloor a/4 \rfloor + 1$
$= 4a' + 1$
where $a' = \lfloor a/4 \rfloor$
$4Y_{n+1} + 1 \equiv 4aY_i + 4a' + 1 \pmod{2^b}$
$4Y_{n+1} \equiv 4aY_i + 4a' \pmod{2^b}$

2) $Y_{n+1} \equiv aY_i + a' \pmod{2^{b-2}}$.

The real values produced by the multiplicative generator (1) is $\frac{Xn}{2^b}$. The real values produced by the mixed generator (2) is $\frac{Yn}{2^{b-2}} = \frac{4Yn}{2^b} = \frac{Xn-1}{2^b} = \frac{Xn}{2^b} - \frac{1}{2^b}$.

Corollary 1

Given a multiplicative generator

$$X_{n+1} \equiv aX_n \pmod{2^b}$$

with $a \equiv 5 \pmod 8$ and $X_o \equiv 3 \pmod 4$ then there exist a mixed generator

$$Y_{n+1} \equiv aY_n + 3a' \pmod{2^{b-2}}$$

for $Y_i = \lfloor X_i/4 \rfloor$ and $a' = \lfloor a/4 \rfloor$ such that for all corresponding values X_n and Y_n, the multiplicative generator produces real values $X_n/2^b$ and the mixed generator produces real values $\frac{Yn}{2^{b-2}} = \frac{Xn}{2^b} - \frac{3}{2^b}$.

Corollary 2

Given a multiplicative generator $X_{n+1} \equiv aX_n \pmod{2^b}$ with $a \equiv 3 \pmod 8$ and $X_o \equiv 1 \pmod 2$ then there exist a mixed generator

$$Y_{n+1} \equiv aY_n + a' \pmod{2^{b-1}}$$

for $Y_i = \lfloor X_i/2 \rfloor$ and $a' = \lfloor a/2 \rfloor$ such that for all corresponding values X_n and Y_n, the multiplicative generator produces real values $X_n/2^b$ and the mixed generator produces real values $\frac{Yn}{2^{b-1}} = \frac{Xn}{2^b} - \frac{1}{2^b}$.

Illustration of the Relationship between a Multiplicative Generator and a Mixed Generator

The values presented in Table 1 are generated from the following two generators chosen to illustrate Theorem 1.

Multiplicative generator:

$$X_{n+1} \equiv 189\ X_n \pmod{2^{31}}$$
$$X_o = 4000003$$

Mixed generator:

$$Y_{n+1} \equiv 189\ Y_n + 141 \pmod{2^{29}}$$
$$Y_o = 1000000$$

Note that for all values $X_n = 4Y_n + 3$.

Multiplicative Generator		Mixed Generator		
X_n	$\frac{X_n}{2^{31}}$	Y_n	$4 \cdot Y_n$	$\frac{Yn}{2^{29}}$
4000003	0.0018626465	1000000	4000000	0.0018626451
756000567	0.3520401972	189000141	756000564	0.3520401958
1150186395	0.5355972773	287546598	1150186392	0.5355972759
489380207	0.2278854171	122345051	489380204	0.2278854157
151062259	0.0703438459	37765564	151062256	0.0703438445
633479527	0.2949868920	158369881	633479524	0.2949868906
1616029963	0.7525225928	404007490	1616029960	0.7525225915
486984991	0.2267700578	121746247	486984988	0.2267700564
1845850083	0.8595409258	461462520	1845850080	0.8595409244
973314711	0.4532349812	243328677	973314708	0.4532349798

Table 1. Comparison of a Multiplicative and Mixed Generator.

Conclusion:

We have shown that for any sequence of real values X_i, in the interval (0,1) produced by a multiplicative generator of maximum period modulo 2^b, there exists some corresponding sequence of real values Y_i, produced by a mixed generator such that the maximum difference between X_i and Y_i is $\frac{3}{2^b}$. For all practical purposes the generators produce the same sequence of real values. Thus the question of which type of generator to use reduces to consideration of a larger period length for the mixed generator compared to a faster execution time for the multiplicative generator. The statistical behavior of the two should produce imperceptible differences.

References

1. Lehmer, D. H., "Mathematical Methods in Large-Scale Computing Units", Proceedings of the 2nd Symposium on Large-Scale Digital Computing Machinery, Harvard University Press, 1951, 141-145.

2. Hull, T. E., A. R. Dobel, "Random Number Generators", Society for Industrial and Applied Mathematics Review, July 1962, 230-254.

3. Hull, T.E., A.R. Dobel, "Mixed Congruential Random Number Generators for Binary Machines; JACM, January 1964, 31-40.

4. MacLaren M.D., G. Marsaglia, "Uniform Random Number Generators", JACM, January 1965, 83-89.

5. Jansson, B., Random Number Generators, Stockholm, Almgvist and Wiksell, 1966.