Unclassified
AEA-APS-0244

THEORETICAL BACKGROUND FOR THE ACORN RANDOM NUMBER GENERATOR

Roy S Wikramaratna

AEA Petroleum Services
Winfrith
Dorchester
Dorset DT2 8DH
United Kingdom

December 1992

The information which this report contains is accurate to the best knowledge and belief of the UKAEA, but neither the UKAEA nor any person acting on behalf of the UKAEA make any warranty or representation expressed or implied with respect to the accuracy, completeness or usefulness of this information, nor assume any liabilities with respect to the use of, or with respect to any damages which may result from the use of any information, apparatus, method or process disclosed in this report.

	Name	Signature	Position	Date
Lead Author	R S Wikramaratna		Technical Manager	9th December 1992
Checked	R S Wikramaratna		Technical Manager	9th December 1992
Approved	D Wardleworth		Department Manager	9/12/92.

Abstract

The ACORN (Additive Congruential Random Number) generators have been proposed as a source of pseudo random numbers, uniformly distributed in the unit interval. Their use has been justified by empirical testing of the resulting sequences of numbers and demonstrated in practice by implementation in a number of real applications. In this paper, we derive theoretical results which prove that in a limiting case the k-th order ACORN sequences are well distributed in k dimensions. This result is contrasted with the result for the commonly used linear congruential generators, which in the corresponding limiting case are uniformly distributed (a weaker result than well distributed) in one dimension but are not uniformly distributed in any higher number of dimensions. The paper concludes that the ACORN generators merit serious consideration as an alternative source of pseudo random numbers in any application which currently uses a linear congruential generator as well as in those applications where linear congruential generators have proved inadequate because of their poor distribution properties in higher dimensions.

1 Introduction

Wikramaratna [1] has proposed the ACORN (Additive Congruential Random Number) generators as a source of uncorrelated random numbers which are uniformly distributed in the unit interval. The k-th order ACORN generator can be defined recursively from a seed X^0_0 ($0 < X^0_0 < 1$) and an arbitrary set of k initial values X^m_0, $m = 1, ..., k$ each satisfying $0 \le X^m_0 < 1$ by

$$X^0_n = X^0_{n-1} \qquad n \ge 1 \qquad (1)$$

$$X^m_n = (X^{m-1}_n + X^m_{n-1})_{\text{mod }1} \qquad n \ge 1,\ m = 1, \dots, k \qquad (2)$$

where $(X)_{\text{mod }1}$ means the fractional part of X. Alternatively, using integer arithmetic, it can be defined from a modulus M, a seed Y^0_0 ($0 < Y^0_0 < M$) and a set of k initial values Y^m_0, $m = 1, ..., k$ each satisfying $0 \le Y^m_0 < M$ by

$$Y^0_n = Y^0_{n-1} \qquad n \ge 1 \qquad (3)$$

$$Y^m_n = (Y^{m-1}_n + Y^m_{n-1})_{\text{mod }M} \qquad n \ge 1,\ m = 1, \dots, k \qquad (4)$$

$$X^m_n = Y^m_n / M \qquad n \ge 1,\ m = 1, \dots, k \qquad (5)$$

where M is a suitable large integer and where $(Y)_{\text{mod }M}$ means the remainder on dividing Y by M. It is worth noting that, for the case where all the X^m_0 are rational fractions, these two definitions are exactly equivalent (suppose, for example, that $X^m_0 = N^m / D^m$, $m = 0, ..., k$, where the N^m and D^m are integers, then choose M as the lowest common multiple of the D^m, and let $Y^m_0 = M X^m_0$, $m = 0, ..., k$).

Either definition can be used successfully as the basis for an implementation of the ACORN algorithm; the example listing in reference [1] was based on equations (1) and (2), but it is a simple matter to modify this as in [2] to implement (3) - (5). This algorithm has been implemented both for $M = 2^{30}$ and $M = 2^{60}$ and the statistical tests from [1] applied to the resulting sequences of numbers; the results obtained for the tests are very similar to those obtained with the original implementation. There are a number of practical advantages in using the second definition in implementing the generator :

(i) At each stage all of the Y^m_n are calculated exactly, so that the values of the

$Y^m{}_n$ will be the same on any machine provided only that the seed, the initial values and the modulus M are chosen to have the same values. The values of $X^m{}_n$ calculated from (5) may differ slightly due to variations in the machine representations of real numbers, but these differences will only appear in the least significant digits and there will be no cumulative buildup or growth of these differences.

(ii) By contrast, any small differences in machine representations of the seed or initial values will grow rapidly in the algorithm defined by (1) and (2), so that in general it will not be possible to generate the same sequences on different machines, even with the 'same' seed and initial values. Wikramaratna [2] has demonstrated how quickly such differences can grow. This fact does not invalidate the use of the algorithm as a source of random numbers - although the sequences may differ, they exhibit the same statistical properties - but if it desirable to repeat a computation on a different machine with the same sequence of random numbers, then the algorithm should be implemented using (3) - (5).

(iii) The theoretical results concerning the periodicity which were proven in [1] hold for the algorithm defined by (3) - (5). For the implementation of (1) and (2) using floating point arithmetic, these theoretical results can give an order of magnitude only, and no precise results exist (since the periodicity will depend on the precision as well as on the particular implementation of floating point arithmetic).

(iv) The apparent limitation of $M \leq 2^{30}$ for an implementation in integer arithmetic on a 32-bit machine can easily be overcome, by using 2 (or more) words to represent each integer $Y^m{}_n$ although this will obviously require more computational effort. An implementation using p 32-bit integers to represent each $Y^m{}_n$ permits a choice of modulus up to a maximum of 2^{30p}, and it is thus possible to generate arbitrarily long sequences by a suitable choice of p, while the computational effort per term in the sequence is approximately proportional to p. The algorithm can be implemented for example as a FORTRAN function which generates a single random number in $[0,1)$ at each call, requiring less than twenty lines of FORTRAN code.

In this paper we present a theoretical analysis of the ACORN algorithm; this analysis allows us to prove *a priori* results about the limiting behaviour of the k-th order ACORN algorithm in particular relating to the uniformity of the resulting distributions in k dimensions for any positive integer value of k. These results are contrasted with the (much weaker) results which can be obtained for the linear congruential generators in the corresponding limiting case. Our results provide both a justification for the use of the ACORN algorithm as a source of uniformly distributed pseudo random numbers and also an explanation of some of our practical experiences in using the algorithm.

2 Explicit Representation of Terms in the Sequences

The algorithm defined by (3) - (5) is very well suited to the computation of the $Y^k{}_n$. However it is useful in understanding the behaviour of the ACORN generators to derive explicit representations for the $Y^k{}_n$ (and also for the $X^k{}_n$) in terms of the modulus, seed and the initial values.

Consider first the special case of the m-th order sequence where the seed is equal to one and the initial values are all equal to zero. The resulting sequence of numbers will be denoted by $Z^m{}_n$. Wikramaratna [2] made use of a standard result

$$\sum_{i=1}^{n} i(i+1)\ldots(i+m) = \frac{n(n+1)\ldots(n+m+1)}{(m+2)} \tag{6}$$

to rewrite equations (3) and (4) in this special case as

$$Z^0{}_n = 1$$

$$Z^1{}_n = n$$

$$Z^2{}_n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2} = \frac{(n+1)!}{(n-1)!2!}$$

$$Z^m{}_n = \sum_{i=1}^{n} \frac{i(i+1)\ldots(i+m-2)}{(m-1)!} = \frac{(n+m-1)!}{(n-1)!m!} \tag{7}$$

The equations (7) hold as long as the right hand side is smaller than M. Once it exceeds this value, then the correct result is still obtained from (7) provided that the value is taken modulo M.

Making use of the additive nature of the ACORN generator, it is now straightforward to show that for the general case of $0 < Y^0{}_0 < M$ and $0 \le Y^j{}_0 < M$, $j = 1, \ldots, k$ the following equation holds for any positive integers k and n, and for any integer $h \geq 0$.

$$Y^k{}_{n+h} = \left(\sum_{j=0}^{k} Y^j{}_h Z^{k-j}{}_n\right)_{\mathrm{mod}M} \tag{8}$$

where the $Z^{k-j}{}_n$ are as defined by equation (7).

Applying a similar analysis to the sequence defined by equations (1) and (2) leads to an analogous equation which defines the $X^k{}_n$ for the general case of $0 < X^0{}_0 < 1$ and $0 \leq X^j{}_0 < 1$, $j = 1, \ldots, k$. Thus

$$X^k{}_{n+h} = (\sum_{j=0}^{k} X^j{}_h Z^{k-j}{}_n)_{\mathrm{mod}\,1} \tag{9}$$

3 Theoretical Results

In this section we will start by outlining some basic definitions and standard results. We will then prove some fundamental theoretical results in 3.2 and 3.3 which we can apply to the sequences defined by equations (1) and (2) in the limiting case where the seed $X^0{}_0$ is irrational.

3.1 Background

We follow the notation and basic definitions of Kuipers and Niederreiter [3]. Let $\mathbb{R}$ represent the real line and $\mathbb{Z}$ the set of integers. For **x** and **y** in $\mathbb{R}^k$, let <**x**,**y**> be the standard inner product. Let k be an integer; let $\mathbf{a} = (a_1, \ldots, a_k)$ and $\mathbf{b} = (b_1, \ldots, b_k)$ be two vectors with real components, thus $\mathbf{a}, \mathbf{b} \in \mathbb{R}^k$. We say that $\mathbf{a} < \mathbf{b}$ ($\mathbf{a} \leq \mathbf{b}$) if $a_j < b_j$ ($a_j \leq b_j$) for $j = 1, 2, \ldots, k$. The set of points $\mathbf{x} \in \mathbb{R}^k$ such that $\mathbf{a} \leq \mathbf{x} < \mathbf{b}$ will be denoted by $[\mathbf{a}, \mathbf{b})$. The *k-dimensional unit cube* I^k is the interval $[\mathbf{0}, \mathbf{1})$ where $\mathbf{0} = (0, \ldots, 0)$ and $\mathbf{1} = (1, \ldots, 1)$. The *integral part* of $\mathbf{x} = (x_1, \ldots, x_k)$ is $[\mathbf{x}] = ([x_1], \ldots, [x_k])$ and the *fractional part* of $\mathbf{x}$ is $\{\mathbf{x}\} = (\{x_1\}, \ldots, \{x_k\})$. Let $(\mathbf{x}_n)$, $n = 1, 2, \ldots$, be a sequence of vectors in $\mathbb{R}^k$. For a subset E of I^k, let $A(E; N)$ denote the number of points $\{\mathbf{x}_n\}$, $1 \leq n \leq N$, that lie in E; let $A(E; N, p)$ denote the number of points $\{\mathbf{x}_{p+n}\}$, $1 \leq n < N$, that lie in E. Finally, the difference operator Δ^m which operates on a sequence (x_n) is defined recursively by $\Delta x_n = x_{n+1} - x_n$ and $\Delta^m x_n = \Delta(\Delta^{m-1} x_n)$ for $m \geq 2$.

DEFINITION 1. The sequence $(\mathbf{x}_n)$, $n = 1, 2, \ldots$, is said to be *uniformly distributed mod 1 in* $\mathbb{R}^k$ (*u.d. mod 1 in* $\mathbb{R}^k$) if, for all intervals $[\mathbf{a}, \mathbf{b})$ contained in or equal to I^k, we have

$$\lim_{N \to \infty} \frac{A([\mathbf{a}, \mathbf{b}); N)}{N} = \prod_{j=1}^{k} (b_j - a_j) \tag{10}$$

The formal definition is due to Weyl [4, 5], who proved the following theorem which gives a neccesary and sufficient condition for a sequence to be u.d. mod 1.

THEOREM 1: Weyl Criterion. A sequence $(\mathbf{x}_n)$, n = 1, 2, ..., is u.d. mod 1 in $\mathbb{R}^k$ if and only if for every lattice point $\mathbf{h} \in \mathbb{Z}^k$, $\mathbf{h} \neq 0$,

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i < \mathbf{h}, \mathbf{x}_n >} = 0 \tag{11}$$

This is a standard result, which we will not prove in this paper. Weyl's original proof [4, 5] is reproduced by Kuipers and Niederreiter [3].

A special case of u.d. mod 1, which is known as w.d. mod 1, was defined by Hlawka [6] and Petersen [7]; the corresponding Weyl criterion (theorem 2), which we once again quote without proof, was also proved by these authors.

DEFINITION 2. The sequence $(\mathbf{x}_n)$, n = 1, 2, ..., is said to be *well distributed mod 1 in* $\mathbb{R}^k$ (*w.d. mod 1 in* $\mathbb{R}^k$) if, uniformly in p and for all intervals $[\mathbf{a}, \mathbf{b})$ contained in or equal to I^k, we have

$$\lim_{N \to \infty} \frac{A([\mathbf{a}, \mathbf{b}); N, p)}{N} = \prod_{j=1}^{k} (b_j - a_j) \tag{12}$$

THEOREM 2: Weyl Criterion. A sequence $(\mathbf{x}_n)$, n = 1, 2, ..., is w.d. mod 1 in $\mathbb{R}^k$ if and only if for every lattice point $\mathbf{h} \in \mathbb{Z}^k$, $\mathbf{h} \neq 0$,

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=p+1}^{p+N} e^{2\pi i < \mathbf{h}, \mathbf{x}_n >} = 0 \tag{13}$$

uniformly in p.

Finally, we quote two other standard results which gives a sufficient condition (but not a neccesary condition) for a sequence to be respectively u.d. mod 1 in $\mathbb{R}$ and w.d. mod 1 in $\mathbb{R}$; theorem 3 was due to Van der Corput [8] and a proof can also be found in Kuipers and Niederreiter [3]; theorem 4 was due to Korobov and Postnikov [9] and is in fact a special case of a subsequent more general result, due to Hlawka [6], which is also proved in [3].

THEOREM 3: Van der Corput's Difference Theorem. Let (x_n), n = 1, 2, ..., be a given sequence of real numbers. If for every positive integer h the sequence $(x_{n+h} - x_n)$, n = 1, 2, ..., is u.d. mod 1 in $\mathbb{R}$, then (x_n) is u.d. mod 1 in $\mathbb{R}$.

THEOREM 4. Let (x_n), n = 1, 2, ..., be a given sequence of real numbers. If for every positive integer h the sequence $(x_{n+h} - x_n)$, n = 1, 2, ..., is w.d. mod 1 in $\mathbb{R}$, then (x_n) is w.d. mod 1 in $\mathbb{R}$.

Note added in proof. The two theorems 5 and 6 which follow in sections 3.2 and 3.3 are the main results which are proved in this paper. It has been drawn to the author's attention that they are in fact special cases of some classical results on the uniform distribution of sequences. We observe that for fixed k the $x^k{}_n$ defined in theorem 5 is a polynomial function of n of degree k with irrational leading coefficient $(x^0{}_0/k!)$. Thus, theorem 5 is a special case of the results of Hlawka [10] and Lawton [11] which show that such sequences of polynomial values are well distributed modulo 1. Similarly, theorem 6 is a special case of an analogous result due to Cigler [12].

3.2 Uniformity in One Dimension

THEOREM 5. If a sequence $(x^k{}_n)$, n = 1, 2, ..., has the property that

$$x^k{}_n = \sum_{j=0}^{k} x^j{}_0 Z^{k-j}{}_n \tag{14}$$

for some positive integer k, where $x^0{}_0$ is an irrational number, then the sequence $(x^k{}_n)$, n = 1, 2, ..., is w.d. mod 1 in $\mathbb{R}$.

PROOF. The proof is by induction on k. We first show that the theorem holds for k = 1: this follows from the Weyl criterion for w.d. mod 1 and the inequality

$$\left|\frac{1}{N}\sum_{n=p+1}^{N+p} e^{2\pi ih(nx^0{}_0+x^1{}_0)}\right| = \left|\frac{1}{N}\sum_{n=1}^{N} e^{2\pi ih(px^0{}_0+x^1{}_0)}e^{2\pi ihnx^0{}_0}\right|$$

$$= \left|\frac{1}{N}\sum_{n=1}^{N} e^{2\pi ihnx^0{}_0}\right| = \frac{\left|e^{2\pi ihNx^0{}_0}-1\right|}{N\left|e^{2\pi ihx^0{}_0}-1\right|} \le \frac{1}{N\left|sin\ \pi hx^0{}_0\right|} \tag{15}$$

for $x^0{}_0$ irrational and for each integer $h \neq 0$.

Suppose now that the theorem holds for 1, 2, ..., k-1. Then

$$x^k{}_{n+h} - x^k{}_n = \sum_{j=0}^{k} (x^j{}_h - x^j{}_0) Z^{k-j}{}_n = \sum_{j=0}^{k} [\sum_{i=0}^{j} (x^i{}_0 Z^{j-i}{}_h) - x^j{}_0] Z^{k-j}{}_n$$
$$= \sum_{j=0}^{k} \xi^j{}_0 Z^{k-j}{}_n = \sum_{j=0}^{k-1} \psi^j{}_0 Z^{k-1-j}{}_n \tag{16}$$

where $\xi^j{}_0$ represents the term in square brackets and $\psi^j{}_0 = \xi^{j+1}{}_0$ for each j; in particular we observe that $\xi^0{}_0 = 0$ and $\xi^1{}_0 = \psi^0{}_0 = h\, x^0{}_0$. But the extreme right hand term in equation (16) is w.d. mod 1 in $\mathbb{R}$ by the induction hypothesis, and hence the theorem is true for k. ■

3.3 Uniformity in k Dimensions

THEOREM 6. If a sequence $(x^k{}_n)$, n = 1, 2, ..., is as defined by equation (14) and if we define the vector $\mathbf{x}^k{}_n \in \mathbb{R}^k$ by $\mathbf{x}^k{}_n = (x^k{}_n, x^k{}_{n+1}, ..., x^k{}_{n+k-1})$, then the sequence $(\mathbf{x}^k{}_n)$, n = 1, 2, ..., is w.d. mod 1 in $\mathbb{R}^k$.

PROOF. Observe first that

$$x^k{}_{n+i} = \sum_{j=0}^{k} x^j{}_i Z^{k-j}{}_n \tag{17}$$

If $\mathbf{h}^k = (h^k{}_0, h^k{}_1, ..., h^k{}_{k-1})$ is an arbitrary non-zero vector in $\mathbb{Z}^k$, then

$$< \mathbf{h}^k, \mathbf{x}^k{}_n >= \sum_{i=0}^{k-1} h^k{}_i (\sum_{j=0}^{k} x^j{}_i Z^{k-j}{}_n) = \sum_{j=0}^{k} (\sum_{i=0}^{k-1} h^k{}_i x^j{}_i) Z^{k-j}{}_n = \sum_{j=0}^{k} \eta^j{}_0 Z^{k-j}{}_n \tag{18}$$

where

$$\eta^j{}_0 = (\sum_{i=0}^{k-1} h^k{}_i x^j{}_i) = \sum_{i=0}^{k-1} h^k{}_i (\sum_{l=0}^{j} x^l{}_0 Z^{j-l}{}_i) = \sum_{l=0}^{j} (\sum_{i=0}^{k-1} h^k{}_i Z^{j-l}{}_i) x^l{}_0 \tag{19}$$

For each choice of $\mathbf{h}^k \neq 0$,

$$\eta^0{}_0 = x^0{}_0 \sum_{i=0}^{k-1} h^k{}_i$$

$$\eta^1{}_0 = x^0{}_0 \sum_{i=0}^{k-1} i h^k{}_i + x^1{}_0 \sum_{i=0}^{k-1} h^k{}_i$$

$$\eta^j{}_0 = \sum_{l=0}^{j} x^l{}_0 \sum_{i=0}^{k-1} \frac{i(i+1)\ldots(i+j-l-1)}{(j-l)!} h^k{}_i \qquad (20)$$

At least one of the $\eta^j{}_0$, $j = 0, 1, \ldots, (k\text{-}1)$ must be non-zero (for suppose that they are all zero, this implies that the $h^k{}_i$ must satisfy the k independant constraint equations

$$\sum_{i=0}^{k-1} h^k{}_i Z^{j-l}{}_i = 0 \qquad j = 0, \ldots, k-1 \qquad (21)$$

and this has only the trivial solution which we excluded). Suppose therefore that $\eta^j{}_0 = 0, j = 0, 1, \ldots, m\text{-}1 < k$ and $\eta^m{}_0 \neq 0$. Then we require

$$\eta^m{}_0 = x^0{}_0 \sum_{i=0}^{k-1} \frac{i\,(i+1)\ldots(i+m-1)}{m!} h^k{}_i \neq 0 \qquad (22)$$

Therefore $\eta^m{}_0$ is irrational (since $x^0{}_0$ is irrational) and if we write $\phi^j{}_0 = \eta^{j+m}{}_0$, $j = 0, \ldots, (k\text{-}m)$, then $\phi^{k\text{-}m}{}_n$ satisfies the conditions of Theorem 5 and so $\phi^{k\text{-}m}{}_n$ is w.d mod 1 in $\mathbb{R}$. By theorem 2, with $k = 1$

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=p+1}^{p+N} e^{2\pi i h \phi^{k-m}{}_n} = 0 \qquad (23)$$

uniformly in p for all $h \in \mathbb{Z}$, and in particular for $h = 1$. By construction therefore

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=p+1}^{p+N} e^{2\pi i < \mathrm{h}^k, x^k{}_n >} = 0 \qquad (24)$$

uniformly in p. But the above argument holds for every choice of $\mathrm{h}^k \neq 0$, and so the sequence $x^k{}_n$ is is w.d. mod 1 in $\mathbb{R}^k$ by theorem 2. ■

We will now prove two corollaries to the above theorem, both of which give sufficient conditions for a sequence to be w.d. mod 1 in $\mathbb{R}^k$. A special case of corollary 1 (for the case of $k = 1$,with the somewhat weaker restriction that $\Delta(x_n)$ should tend in the limit of large n to δ, and the correspondingly weaker result of u.d. mod 1 in $\mathbb{R}$), due to Van der Corput [8], is discussed together with other existing difference theorems by Kuipers and Niederreiter [3]. Corollary 2 shows that the k-th order ACORN generators also satisfy the conditions of the theorem (provided only that the seed is irrational) and so in this case the k-th order ACORN generators are w.d. mod 1 in $\mathbb{R}^k$.

COROLLARY 1. If a sequence (x_n), $n = 1, 2, \ldots$ has the property that

$$\Delta^k(x_n) = \delta \tag{25}$$

for some positive integer k, where δ is an irrational number,, and if we define the vector $\mathbf{x}_n \,\varepsilon\, \mathbb{R}^k$ by $\mathbf{x}_n = (x_n, x_{n+1}, \ldots, x_{n+k-1})$, then the sequence $(\mathbf{x}_n)$, n = 1, 2, ..., is w.d. mod 1 in $\mathbb{R}^k$.

PROOF. If (x_n) satisfies equation (25) then it can be written in the form of equation (14) with $x^0{}_0 = \delta$ and some set of constants $x^j{}_0$, $j = 1, \ldots, k$. Hence the conditions of theorem 6 are satisfied and the corollary follows immediately from the theorem. ■

COROLLARY 2. The k-th order ACORN sequence defined by equation (9) is w.d. mod 1 in $\mathbb{R}^k$, provided only that the seed $X^0{}_0$ is irrational.

PROOF. Set $x^j{}_0 = X^j{}_0$, $j = 0, \ldots, k$. Then $X^j{}_n = (x^j{}_n)_{\text{mod }1}$ for each $j = 0, \ldots, k$ and for all $n = 0, 1, 2, \ldots$; since $(x^j{}_n)$ satisfies the conditions of the theorem, both the sequences $(x^j{}_n)$ and $(X^j{}_n)$ are w.d. mod 1 in $\mathbb{R}^k$. ■

4 Corresponding Results for Linear Congruential Generators

Among the most widely used generators in common use today are the linear congruential generators (Knuth [13], Ripley [14], Anderson [15]). These generators can be defined by

$$U_n = (aU_{n-1} + c)_{\text{mod }1} \qquad n \geq 1 \tag{26}$$

where $0 \leq U_0 < 1$, $0 \leq c < 1$ and $a > 0$ is an integer, or alternatively by

$$V_n = (aV_{n-1} + d)_{\operatorname{mod} M} \qquad n \geq 1 \qquad (27)$$

$$U_n = V_n / M \qquad n \geq 1 \qquad (28)$$

where a is as before and V_0 and d are integers, $0 \leq V_0 < M$ and $0 \leq d < 1$. We note that, as in the case of the ACORN generators, the two definitions are equivalent in the case where U_0 and c are both rational fractions.

The special case $c = 0$, proposed originally by Lehmer [16] is generally known as the multiplicative congruential generator. The more general case of non-zero c, which is due independantly to Thompson [17] and Rotenberg [18] is often called the mixed congruential generator. Linear congruential generators, and the very extensive literature concerning them, are discussed in some detail in the books by Knuth [13], Ripley [14] and in the review paper by Anderson[15].

As in the case of the ACORN generators, the definition in (27) and (28) is most useful from the point of view of a practical implementation, but (26) forms a useful starting point for a theoretical analysis of distribution properties. We observe immediately that the sequence $\mathrm{U}^k{}_n$, $n = 1, 2, \ldots$ (where $\mathrm{U}^k{}_n$ means the k-tuple $(U_n, U_{n+1}, \ldots, U_{n+k-1})$) is <u>not</u> u.d. mod 1 in $\mathbb{R}^k$ for any $k > 1$. Suppose for example that $k = 2$, and let $a_1 = \varepsilon, a_2 = c - \varepsilon, b_1 = 3\varepsilon, b_2 = c + \varepsilon$ (where $\varepsilon = 1 / 4a$); then $A([\mathbf{a}, \mathbf{b}); N) = 0$ for every N, but $(b_1 - a_1)(b_2 - a_2) = 4\varepsilon^2 = 1 / 4a^2 \neq 0$. It is in fact possible to show that the sequence U_n, $n = 1, 2, \ldots$ is u.d. mod 1 in $\mathbb{R}$ (although it is <u>not</u> w.d. mod 1 in $\mathbb{R}$) provided that the seed is irrational. This contrasts with the much stronger result which has been proved in Corollary 2 and Theorem 6 above for the ACORN generators.

The set of points $\mathrm{U}^k{}_n$ generated in k-dimensional space actually fall on a lattice structure; a desirable property (which gives some approximation to uniformity in higher dimensions) is that the lattice spacing should be of a similar size in different directions. The spectral test (Coveyou and Macpherson [19]) is a theoretical test which characterises the lattice structure (and in particular the lattice spacing in different directions) for any particular linear congruential generator, taken over its entire period. By applying the spectral test to a range of generators with different choices of modulus, multiplier and additive constant it is possible to identify generators which have reasonable distribution properties in different numbers of dimensions (as well as the much larger numbers of generators which suffer from very poor distribution properties). Fishman and Moore [20] examined all possible multipliers for the modulus $(2^{31} - 1)$ (several hundreds of millions in all) and came up with a few hundred multipliers giving what they considered to be a reasonable lattice structure in up to about six dimensions. Subsequent work by Fishman [21] looked in detail at two other values of the modulus; for the case of modulus 2^{32} he performed an exhaustive search of all possible multipliers) and for the case of modulus

2^{48} he examined more than 67 million of the possible multipliers.

The spectral test provides a means of selecting those particular linear congruential generators which have adequate distribution properties in up to about six dimensions; however for larger numbers of dimensions the computational effort required to perform the spectral test for a large enough sample of multipliers becomes prohibitive. Further, if a sequence with better distribution properties or a longer period length is subsequently required, there is no alternative but to continue the search (for example, using a larger value of the modulus). Finally, the spectral test gives results which pertain only to the full period; they say nothing about the distribution properties for shorter subsequences.

5 Practical Implications for ACORN Sequences

Anderson [15] has reviewed the literature on the linear congruential generators and various other commonly used generators (shift register generators, lagged-Fibonacci generators, randomisation by shuffling, combination generators) and concludes that in spite of their drawbacks linear congruential generators are the preferred method in many applications, although they are not acceptable for higher dimensional work. He also makes some tentative suggestions concerning the use of lagged-Fibonacci and shift register generators as an alternative for applications requiring uniformity in higher dimensions, but makes no clear recommendation concerning the best approach. It should be noted that Anderson's review predated the publication of the ACORN algorithm.

Although the ACORN generators have been used in practice in geostatistical applications (for example Farmer [22], Parish et al [23], Deutsch and Journel [24]), there has not previously been any rigorous theoretical justification for their use, but only the results of empirical testing and intuitive arguments based on their observed behaviour.

The results presented in this paper have demonstrated the theoretical superiority of the ACORN generators over the linear congruential generators. When these results are taken together with other results which have previously been derived by Wikramaratna [1, 2], they provide a very strong argument for using the ACORN generators in preference to the linear congruential generators in any application.

In [1] and [2] we demonstrated the simplicity of implementing the ACORN generators. The implementation can be simply extended to allow arbitrarily large values of the modulus. Our experience [1] has shown that the execution times for the ACORN generators are comparable with those for carefully implemented linear congruential generators.

Theoretical results derived in [1] showed that the period length for the ACORN generators with a given modulus are an integer multiple of the modulus (provided the seed and modulus are relatively prime); the corresponding period length for a linear congruential generator can never exceed the modulus.

Where a longer period length is required, one can simply increase the modulus for the ACORN generators; the theoretical results proven here ensure that the resulting sequence will have good distribution properties in up to k dimensions (where k is the order of the generator being used). Indeed, by increasing the modulus one approaches even closer to the limiting case of irrational seed for which the theoretical results hold. By contrast, in the case of the linear congruential generators, any change of the modulus requires a computationally expensive search of a large number of multipliers in order to identify those multipliers which give reasonable distribution properties in more than one dimension.

Where uniformity in higher dimensions is required this can be obtained with the ACORN generators simply by increasing the order of the generator to an appropriate value, and if neccesary also increasing the modulus of the generator. For the linear congruential generators it becomes prohibitively expensive to test the distribution properties in higher dimensions using the spectral test for even a single multiplier and in practice it is difficult to perform the exhaustive testing of multipliers which is required to discover those generators which perform adequately in more than about six dimensions.

6 Conclusions

In this paper we have proved that, in the limiting case of an irrational seed, the k-th order ACORN generator is w.d. mod 1 in $\mathbb{R}^k$. In a practical implementation, with rational seed, we can approximate the first N terms of such a k-distributed sequence arbitrarily closely by choosing a sufficiently large value for the modulus and the appropriate approximation for the seed. In practice a modulus of 2^{60} and order $k \geq 10$ appears to give adequate distribution properties and sufficiently long period for most realistic applications today; if improved hardware performance results in a need for even longer sequences the algorithm can be very easily modified to use a larger modulus (say 2^{90} or 2^{120}) giving a corresponding increase in the period. The use of a larger modulus can also be expected to result in better distribution properties because of approaching the limiting case more closely.

The results which have been demonstrated for the ACORN generators have been contrasted with those which are obtained for the linear congruential generators: in the corresponding limiting case they are u.d. mod 1 (but not w.d. mod 1) in $\mathbb{R}$ and they are not u.d. mod 1 in $\mathbb{R}^k$ for any $k > 1$. A consequence of this is that in order to obtain reasonable distribution properties in more than one dimension only a minute proportion of the possible combinations of modulus and multiplier can be used. For some commonly used values of the modulus (for example (2^{31}-1), 2^{32} or 2^{48}) extensive searches (exhaustive in the first two cases) over possible multipliers have led to some hundreds of generators which have reasonable distribution properties in up to about six dimensions. Unfortunately, if a linear congruential generator with a longer period length is required (and therefore a larger modulus is selected) the computationally intensive evaluation of all the possible multipliers must be repeated for the new modulus, and a correspondingly larger number of multipliers must be evaluated each time.

The theoretical results presented in this paper suggest that there are good reasons for preferring the ACORN generators to the commonly-used linear congruential generators as a source of uniformly distributed pseudo-random numbers. We believe that the ACORN generators should be seriously considered as an alternative in any application which currently uses a linear congruential generator. The ACORN generators may also be a suitable alternative in applications where the linear congruential generators have proved inadequate (in particular those requiring good distribution properties in higher numbers of dimensions) and where other more complicated generators are currently used.

Our experience suggests that a 10-th (or higher) order ACORN generator with modulus $M = 2^{60}$, an odd seed X^0_0 chosen such that X^0_0/M lies in the approximate range [0.001,0.1] and an arbitrary set of initial values gives a sequence which will prove adequate for most applications. Note that these conditions provide a useful rule of thumb in choosing a suitable generator; we emphasise that they are not in any sense a requirement.

The performance results which were obtained in [1] suggested that the execution times for the ACORN generators are comparable with those for carefully implemented linear congruential generators. Our subsequent experience with implementations in integer arithmetic support this conclusion. The question of efficient implementation of the ACORN algorithm for use on vector and parallel hardware will be addressed in a separate paper.

We believe that the results proven in this paper can be developed further, leading eventually to quantitative discrepancy estimates for particular choices of seed, order and modulus. This is the subject of current research.

Acknowledgement

The author would like to express his thanks to the reviewer who drew his attention to the prior results of Hlawka [10], Lawton [11] and Cigler [12].

References

[1] Wikramaratna R S, 'ACORN - A New Method for Generating Sequences of Uniformly Distributed Pseudo-random Numbers', *J. Comput. Phys.*, **83**, 16-31, 1989

[2] Wikramaratna R S, 'Theoretical Analysis of the ACORN Random Number Generator', presented at the *SIAM Conference on Applied Probability in Science and Engineering*, New Orleans, Louisiana, March 1990, Unpublished (AEA Petroleum Services internal report PRTD(90)R62)

[3] Kuipers L and Niederreiter H, *Uniform Distribution of Sequences*, John Wiley and Sons, New York, 1974, 390pp

[4] Weyl H, 'Uber ein Problem aus dem Gebiete der diophantischen Approximationen', *Nachr. Ges. Wiss. Gottingen*, Math.-phys. Kl., 234-244, 1914; also in *Gesammelte Abhandlungen*, Band I, Springer-Verlag, Berlin-Heidelberg-New York, 1968, pp. 487-497

[5] Weyl H, 'Uber die Gleichverteilung von Zahlen mod. Eins', *Math. Ann.*, 77, 313-352, 1916; also in *Gesammelte Abhandlungen*, Band I, Springer-Verlag, Berlin-Heidelberg-New York, 1968, pp. 563-599; and in *Selecta Hermann Weyl*, Birkhauser Verlag, Bassel-Stuttgart, 1956, pp. 111-147

[6] Hlawka E, 'Zur formalen Theorie der Gleichverteilung in kompakten Gruppen', *Rend. Circ. Mat. Palermo (2)*, **4**, 33-47, 1955

[7] Petersen G M, 'Almost convergence and uniformly distributed sequences', *Quart. J. Math.*, 7(2), 199-191, 1956

[8] Van der Corput J G, 'Diophantische Ungleichungen I.Zur Gleichverteilung modulo Eins', *Acta Math.*, **56**, 373-456, 1931

[9] Korobov N M and Postnikov A G, 'Some general theorems on the uniform distribution of fractional parts' (Russian), *Dokl. Akad. Nauk SSSR*, **84**, 217-220, 1952

[10] Hlawka E, 'Erbliche Eigenschaften in der Theorie der Gleichverteilung', *Publ. Math. Debrecen*, **7**, 181-186, 1960

[11] Lawton B, 'A note on well distributed sequences', *Proc. Amer. Math. Soc.*, **10**, 891-893, 1959

[12] Cigler J, 'On a theorem of H Weyl', *Compositio Math.*, **21**, 151-154, 1969

[13] Knuth D, *The Art of Computer Programming, Vol. 2, Seminumerical Algorithms*, Addison-Wesley, Reading, MA, 1981, 688pp

[14] Ripley B, *Stochastic Simulation*, John Wiley and Sons, New York, 1987, 237pp

[15] Anderson S L, 'Random Number Generators on Vector Supercomputers and Other Advanced Architectures', *SIAM Review*, **32**, 221-251, 1990

[16] Lehmer D H, 'Mathematical Methods in Large-Scale Computing Units', in *Proceedings, 2nd Symposium on Large-Scale Digital Computing Machinery, Cambridge*, 141-146, Harvard University Press, Cambridge, MA, 1951

[17] Thompson W E, 'A Modified Congruence Method of Generating Pseudo-random Numbers', *Comput. J.*, **1**, 83-86, 1958

[18] Rotenberg A, 'A New Pseudo-random Number Generator', *J. Assoc. Comput. Mach.*, **7**, 75-77, 1960

[19] Coveyou R R and Macpherson R D, 'Fourier Analysis of Uniform Random Number Generators', *J. ACM*, **14**, 100-119, 1967

[20] Fishman G S and Moore L R, 'A Statistical Evaluation of Multiplicative Congruential Random Number Generators with Modulus 2^{31} - 1', *J. Amer. Statist. Assoc.*, **77**, 129-136, 1982

21] Fishman G S, 'Multiplicative Congruential Random Number Generators with Modulus 2^{β}: an Exhaustive Analysis for $\beta = 32$ and a Partial Analysis for $\beta = 48$', *Math. Comp.*, **54**, 331-344, 1990

[22] Farmer C L, 'Numerical Rocks', in *The Mathematics of Oil Recovery (based on the proceedings of a conference held at Cambridge University, July 1989)*, edited by P.R.King, Clarendon Press, Oxford,437-447, 1992.

[23] Parish R G, Wikramaratna R S, Craig P S and Seheult A H, 'GEOS - A Practical Tool for Reservoir Characterisation', presented at the *SPE Latin American Petroleum Engineering Conference*, March 1992, Unpublished (Paper number SPE 23737)

[24] Deutsch C V and Journel A J, *GSLIB: Geostatistical Software Library and User's Guide*, Oxford University Press, Oxford, 1992 (in press), 340pp