AN EMPIRICAL STUDY OF LOCALLY PSEUDO-RANDOM SEQUENCES

by

Alan Rodney Dobell

B.A., The University of British Columbia, 1959

A Thesis Submitted in Partial Fulfilment of

The Requirements for the Degree of

Master of Arts

in the Department of

Mathematics

We accept this thesis as conforming

to the required standard

The University of British Columbia

April, 1961

In presenting this thesis in partial fulfilment of the requirements for an advanced degree at the University of British Columbia, I agree that the Library shall make it freely available for reference and study. I further agree that permission for extensive copying of this thesis for scholarly purposes may be granted by the Head of my Department or by his representatives. It is understood that copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Department of Mathematics

The University of British Columbia,
Vancouver 8, Canada.

Date April 12, 1961.

Abstract

In Monte Carlo calculations performed on electronic computers it is advantageous to use an arithmetic scheme to generate sets of numbers with "approximately" the properties of a random sequence. For many applications the local characteristics of the resulting sequence are of interest.

In this thesis the concept of a pseudo-random sequence is set out, and arithmetic methods for their generation are discussed. A brief survey of some standard statistical tests of randomness is offered, and the results of empirical tests for local randomness performed on the ALWAC III-E computer at the University of British Columbia are recorded. It is demonstrated that many of the standard generating schemes do not yield sequences with suitable local properties, and could therefore be responsible for misleading results in some applications. A method appropriate for the generation of short blocks of numbers with approximately the properties of a randomly selected set is proposed and tested, with satisfactory results.

TABLE OF CONTENTS

Chapter 1.	Introduction	Page 1
Chapter 2.	Statistical Tests	9
Chapter 3.	Methods of Generation	18
Chapter 4.	Locally Pseudo-Random Sequences	29
Chapter 5.	Summary and Conclusions	37
Bibliography		38

Tables.	Table I	To Follow Page 31
	Table II	To Follow Page 33
	Table III	To Follow Page 34
	Table IV	To Follow Page 34

Acknowledgements

I wish to acknowledge the assistance extended to me by Dr. L. Schwartz, who read and criticized this thesis in draft form, by the staff of the Computing Centre at the University of British Columbia, with whom I have had the privilege of working, and in particular by its director, Professor Thos. E. Hull. For any merits this thesis may finally claim, his enthusiasm and ready counsel are primarily responsible.

Introduction

Solutions to many problems require random numbers. Simulation techniques and Monte Carlo methods often depend in an essential way on the fact that if F is a probability distribution function, with inverse F^{-1}, and X is a random variable uniformly distributed on $[0, 1]$, then $F^{-1}(X)$ is a random variable with distribution function F. (See, e.g.[5], [7].) Applications in mathematical statistics often depend in an essential way on theoretical properties of random numbers. (See, e.g.,[8]) A concern basic to both applications, and of importance in other problems of applied analysis, is that of guaranteeing adequate supplies of numbers apparently independently drawn from a population uniformly distributed on the unit interval. That is, the problem is to provide numbers x drawn in such a way that

$$\text{Prob. } (x \leq a) = a \qquad \text{for } 0 \leq a \leq 1$$

independently of all preceding or succeeding numbers. The purpose of this essay is to describe and examine some methods by which numbers with "approximately" this property may be supplied in a practical way using electronic computers.

Let us establish at the outset that a <u>number</u> is to be interpreted as a point on the real line. This understanding will serve to distinguish the following study from work dealing with random sampling digits.

Random digits have long been of concern to the statistician interested in actual sampling procedures, or in the theoretical

procedure known as distribution sampling. Discussion of the problem of supplying suitable random sampling digits seems to have begun with Kendall and Babington-Smith [24] [25], although Tippett's tables were published earlier [36] and some theoretical sampling techniques had been used earlier yet.[35] This work on random digits is naturally very closely related to the problem of random number generation; the two problems are not, however, equivalent. Thus, although we shall refer to articles on random sampling digits, and shall use modified forms of tests proposed for random digits, we shall retain the distinction, and phrase our discussion entirely in terms of points on the real line.

In terms of points x, the theoretical requirements imposed on a random set of numbers may be summarized in the following standard definitions.

Defn. 1: The set of numbers $x_1, x_2, \ldots, x_n$ will be said to be random if it represents an observation on a vector random variable

$$X^{(n)} = (X_1, X_2, \ldots, X_n)$$

with a joint cumulative distribution function

$$F^n = F^n(x_1, x_2, \ldots, x_n) = \prod_{i=1}^{n} F^1(x_i)$$

where F^1 is some univariate distribution function.

Defn. 2: The set of numbers $x_1, x_2, \ldots, x_n$ will be said to be perfectly random if the distribution function F^1 of Definition 1 is the distribution function

$$F^1(x) = \begin{cases} 0 \text{ if } x \leq 0 \\ x \text{ if } 0 \leq x \leq 1 \\ 1 \text{ if } x \geq 1 \end{cases}$$

and $x_i \in [0, 1]$.

This definition sets out the properties required in analytical work; we must modify it somewhat for our purposes.

We must recognize initially that the numbers with which we are concerned will be represented in a finite word length computer by a finite number of digits. Thus only a finite number (depending on the computer) of distinct configurations is possible; if the radix is denoted r, and the word length k, then the number of distinct elements in the set S of distinguishable numbers is just r^k. We can deal only with discrete approximations, uniform over the set S, to the distribution functions mentioned in Definition 2.

It will be the definition in terms of these discrete approximations which is meant when reference is made in the following to properties of randomness.

But in any case one has in general no prior knowledge of the distribution function F -- the only procedure which can determine whether an observed set of numbers may be said to satisfy Definitions 1 or 2 is a statistical testing procedure. And any finite testing procedure is imperfect: sets of numbers which actually satisfy Definition 2 may not satisfy standard tests; sets of numbers passing any given class of tests may yet not be random in the sense of the definition.

This difficulty will not concern us in the following. Because the requirements in application are for sets of numbers with certain specified properties, our objective will be simply

to construct methods which pass tests for these properties. Because applications are set up generally to mirror the condition of theoretical randomness, a set of numbers will be suitable in application if specific properties it displays do not deviate "too markedly" from those expected of a random set. Therefore we may apply the machinery of statistical tests of randomness to determine whether a particular set of numbers will be suitable in a given application. These considerations lead to the following definition of a pseudo-random sequence.

Defn.: A pseudo-random sequence is a set of numbers which passes the tests in a class C of tests of randomness.

Our objective is to construct pseudo-random sequences.

The choice of a particular class C of tests is a problem to which satisfactory answers cannot be given in general. No finite set of numbers can satisfy all plausible tests of randomness; on examination, every finite sequence will display some peculiarities which would cause it to be rejected as a randomly generated set. The choice of tests can be finally determined only by the use to which the sequence is to be put, and the properties which are essential in that use. An initial discussion of this question, and of the way in which the tests will be used, is given in Chapt. 2.

Having in hand a procedure for determining whether an observed sequence is pseudo-random, the problem is to construct methods which yield sequences likely to satisfy the test criteria.

The first suggestion may be to make use of mechanical

processes which are believed a priori to satisfy the conditions of Definition 2 -- processes such as the drawing of cards from a "properly shuffled deck" of numbered cards, the flipping of "true" coins, the rolling of "fair" dice. Tables of random digits have been constructed by such means, and the methods are still proposed. (See the review by Tompkins [121] of icosahedral dice.) They are, however, both too slow and too limited in scope to be of use in computer applications. In the same spirit is the suggestion that tables could be constructed from numbers appearing on census returns, waybills, etc. The tables of Tippett [36], and Horton and Smith [104] used this method, with a randomizing transformation described in [104]. For more extensive tables, some methods utilize physical processes which are expected, on the basis of physical theory, to yield completely random output. It was by this means that the tables of Kendall and Babington-Smith [26] and the RAND Corporation [33] were constructed.

It might be expected that if electronic equipment can be constructed to produce random output, such equipment could easily be wired into a computer, yielding random numbers on demand. Apart from the important fact that such equipment would be expensive, there are major disadvantages.

i) The equipment has a tendency to degenerate to a systematic output; (see [3] on the RAND experience) and would therefore be expensive to maintain in the 'random' condition.

ii) A calculation could not be checked or re-run. The output cannot be duplicated.

iii) No attempt can be made in the calculation to avoid the deviations from mean behaviour which inevitably occur in a random sequence. That is, although the sequence may be random, it need not be pseudo-random. Not all random sequences would be suitable in application; the deviations mentioned above may be responsible for misleading or anomalous results.

Rather than incorporating special equipment into the computer, we might utilize existing tables to input random numbers as required. This, even with the most efficient input equipment, is too slow to be feasible. Alternatively, to attempt to store tables in the computer memory would require a prohibitively large amount of memory, and in many cases would still be unduly slow. Both measures have the additional disadvantage that the volume of numbers required for some calculations could well exceed the size of the largest existing tables. Thus, neither published tables nor external procedures are satisfactory for standard computer applications.

Recognizing the disadvantages of the above proposals, it has been suggested that suitable pseudo-random sequences could be supplied by an arithmetic method of generation. Of course, such methods do not satisfy the conditions of a random method of generation; they are, in fact, completely determined by one or two previous elements of the sequence. As John von Neumann says ([124] page 36) "any one who considers using arithmetical methods of producing random digits is, of course, in a state of sin." But the point is that we are not concerned with the conditions of randomness -- we require only a pseudo-random

sequence. Which means that we look no farther than the sequence itself for our criteria of suitability; we care not how it was produced.

In Chapter 3 we outline several proposed methods for generating arithmetically a pseudo-random sequence, and relate the results of statistical tests performed on these. In that discussion it will be noted that the number sequences so generated are periodic; the problem of assuring a sufficiently long period is successfully treated by methods of number theory, and all the methods proposed are such as yield a maximal period for a given computer.

Applications arise, however, in which a shorter block of random numbers appears as an integral part of the calculations. This situation suggested the present study; it appeared not at all obvious that a sequence which suitably passed a class of tests would yield short subblocks which in themselves would pass the same class of tests. In Chapter 4 we outline empirical work which was undertaken to test whether a sequence with maximal period is most suitable for use in such a situation. Our conclusion, based on this experimental work, is that it is not. It seems rather that a sequence with shorter period displays more suitable properties over short blocks of numbers. This result again points up the fact that the choice of a method for generating a sequence must be made with the requirements and characteristics of the particular application in mind.

These then are the main themes of this thesis: that there is in practice no definition of randomness for finite sets apart from a class of specific tests; that this class of tests

must be selected with reference to the intended application of the random sequence; and that for some applications the choice of a suitable method of generation will lead to sequences with less than maximal period.

In the next chapter we begin our discussion by determining an adequate procedure for testing sequences.

Chapter 2. Tests of Randomness

Tests of randomness are unlimited in number. Many are extensively studied in the statistical literature, and references to much of this work are included in our bibliography. The general problem is described by Levene [63] as follows:

"Let the vector random variable

$$X^{(n)} = (X_1, X_2, \ldots, X_n)$$

have the joint cumulative distribution function

$$F^n = F^n(x_1, x_2, \ldots, x_n).$$

.... Let Ω_n be the class of all continuous F^n, and let ω_n be the class of all F^n of the form $F^n = \prod_{i=1}^{n} F^1(x_i)$ where F^1 is some continuous univariate distribution function. By the hypothesis of randomness, H_o, we mean the hypothesis that F^n, known to belong to Ω_n, actually belongs to ω_n. The statistical problem is to test H_o on the basis of one observation x^n on X^n. .... The most usual procedure has been for the statistician to devise some statistic whose distribution could be obtained without too much trouble. Then if extreme values of this statistic were observed, the hypothesis of randomness was rejected."

Likewise, to test the hypothesis that an observed set $x^{(n)}$ is perfectly random is to test the hypothesis that $F^n \in \omega_n'$, where ω_n' is the class of all F^n of the form $F^n = \prod F^1(x_i)$ and $F^1(x) = \begin{cases} 0 & x \leq 0 \\ x & 0 \leq x \leq 1 \\ 1 & x \geq 1 \end{cases}$

i.e. -- where F^1 is the uniform distribution on $[0, 1]$.

A difficulty mentioned in the introduction arises at this point. As Levene [63] points out:

"... if we look long enough we will find something very peculiar and non-random about any given sequence and can prove that the probability of this peculiarity arising by chance is very small. The difficulty is that randomness is not a property of a sequence of numbers, but of the process that produced them, that is, of F^n ."

Consequently there is no test with a high probability of rejecting H_o whenever $F_n \in \omega_n$.

"In fact, given any critical region of size α, there exists $F^n \in \omega_n$ for which the probability of the critical set is zero." [63]

The theoretical alternative proposed is to restrict the class F^n to a class of alternatives especially feared, and to choose statistics with good power against these. In practice this means we must stipulate ahead of time specific properties essential in a given application, and test the sequence for these properties. Because we wish only to determine whether an observed sequence is pseudo-random, we test the hypothesis of randomness only against alternatives which would represent sets unsuitable in application. That is, the class of alternatives will contain only distributions which are non-random in such a way as to render samples drawn from them unsatisfactory for the intended application. In particular, the alternatives will not include distributions associated with the type of arithmetic dependence we describe later.

These considerations then suggest the correct interpretation to be assigned to certain extreme values of the test statistics. In general an observed value Z_o for a test statistic Z is considered to give cause for the rejection of the null hypothesis at a level of significance α if Z_o falls in a

critical region w where

$$\text{Probability}\,[w] \approx \alpha$$

when the null hypothesis is true.

In the tests which we will describe and use in the following, Z is a "distance" statistic and the critical region w is of the form

$w = \{Z_o: \ Z_o \geq c\}$ where c is a constant and

Prob $[Z \geq c] \approx \alpha$ when the null hypothesis is true.

Following the lead of Kendall and Babington-Smith [24] several writers have used a "two-tailed" test for testing pseudo-random sequences. (See, e.g. [67] on the tests of the digits of π and e, and the comment of Taussky and Todd [117] that the digits of e are "apparently bad" (P. 26).)

But, by virtue of the way in which we restrict the class of alternatives to be considered, there is no alternative which justifies the rejection of the null hypothesis on the basis of extremely low values of the test statistics we shall use. For the purpose of assessing a pseudo-random sequence, a "two-tailed" test procedure is not appropriate. (On this question, see also [40] [51].)

The tests outlined below fall in the class known as non-parametric or distribution free tests. We shall describe some which have been extensively used, and offer references to several others.

Uniformity -- The Chi-square Test

The basic requirement on pseudo-random sequences is that they be "approximately" uniformly distributed -- i.e. -- that

$$\text{Probability}\,[X \leq a] = a \qquad 0 \leq a \leq 1 \ .$$

The standard way to test whether this property can be said to hold for an observed sequence is to subdivide the unit interval into k disjoint intervals I_j of length L_j and calculate the value of the statistic

$$X_1^2 = \sum_{j=1}^{k} (f_j - nL_j)^2/nL_j;$$

if the intervals are of equal length

$$X_1^2 = \sum_{j=1}^{k} (f_j - n/k)^2/(n/k) ,$$

where f_j denotes the number of elements of the sequence falling in interval j, and n denotes the total number of elements. The limiting distribution of this well-known statistic was developed by Pearson [72], and is tabulated as the χ^2 statistic with $k-1$ degrees of freedom. We reject the hypothesis of randomness at the level of significance α if

$$X_1^2 \geq C \quad \text{where} \quad \text{Prob.}\left[\chi^2_{[k-1]} \geq C\right] \approx \alpha$$

when the null hypothesis is true, and $\chi^2_{[k-1]}$ is the tabulated χ^2 distribution with $k-1$ degrees of freedom.

Such χ^2 goodness of fit tests are used in many different tests of randomness. The question of optimal choice of k has been studied [83], but is frequently settled by considerations of programming convenience. Further studies discuss the applicability of χ^2 tests in general, and discuss possible modifications. [43] [57]

Other possible "distance" measures used as tests of goodness of fit involve the evaluation of expressions like

$$\sup_x \left| F_n(x) - G(x) \right|$$

where F_n is the empirical distribution to be tested, G the hypothesized "true" distribution. Such expressions are extremely awkward to program, and we therefore have made no use of them in this initial experimental work.

No application seems to have been made of such statistics in any published tests of pseudo-random sequences.

Independence -- The Serial Matrix Test

Consider a set of n digits $a_1, a_2, \ldots, a_n$ where each a_i is drawn from a set of t digits in a random manner. Then it is to be expected that no digit would tend to be followed more often by any one digit than by any other -- i.e. -- the frequency of occurrence of each of the t^2 possible 2-digit configurations would be the same, and therefore equal to n/t^2. Kendall and Babington-Smith [24] proposed a test for this property which they called the Serial test. If the frequency of occurrence of the 2-digit configuration $a_i a_j$ is denoted g_{ij}, then the extent to which the observed set deviates from expectation may be measured by

$$X^2 = \sum_{i,j=1}^{t} (g_{ij} - n/t^2)^2/(n/t^2) \ .$$

Kendall and Babington-Smith asserted that this statistic had asymptotically the χ^2 distribution with $(t^2 - t)$ degrees of freedom, and this fact was much used (by the RAND Corporation among others) in tests of random digits.

A modification of this test for application to random numbers was used by Juncosa [107]. In this modification, the unit interval was partitioned into k (= 10) subintervals. For a

set $\{u_i\}$ of numbers, the number of occasions on which a number x_r falling in interval i was followed by a number x_{r+1} in interval j was tallied as the frequency f_{ij}. Again the extent of deviation from expected behaviour may be measured by a χ^2_k statistic,

$$X_2^2 = \sum_{i,j=1} (f_{ij} - n/k^2)^2/(n/k^2) .$$

Juncosa then tested the significance of this measured value by comparison with the values of χ^2 for $k^2 - 1$ (99) degrees of freedom.

Subsequently I. J. Good [52] [53] demonstrated that X_2^2 did not have asymptotically a χ^2 distribution, but that, if we set $f_i = \sum_{j=1}^{k} f_{ij} = \sum_{j=1}^{k} f_{ji}$ then

$$\sum_{i,j=1}^{k} (f_{ij} - n/k^2)^2/(n/k^2) - \sum_{i=1}^{k} (f_i - n/k)^2/(n/k) = X_2^2 - X_1^2$$

has asymptotically a χ^2 distribution with $k^2 - k$ degrees of freedom, and also

$$\sum_{i,j=1}^{k} (f_{ij} - n/k^2)^2/(n/k^2) - 2\sum_{i=1}^{k} (f_i - n/k)^2/(n/k) = X_2^2 - 2X_1^2$$

has asymptotically a χ^2 distribution with $(k - 1)^2$ degrees of freedom. The latter of these measures was used by the authors of the RAND table in a correction [121] to their earlier test; we shall use the former in the experimental work of Chapter 4, in testing for the independence of successive digits.

Independence -- Serial Correlation Test

Tests which are particularly useful in testing for randomness against the alternative of a trend or a cyclic fluctuation

are the serial correlation measures. The values of such expressions as

$$R_h = 1/N \sum_{i=1}^{N} X_i X_{i+h} ,$$

$$\delta_h^2 = 1/N \sum_{i=1}^{N} (X_{i+h} - X_i)^2$$

$$C = 1 - \delta_1^2/2\sigma^2$$

where $\sigma^2 = 1/N \sum_{i=1}^{N} (X_i - \bar{X})^2$

are used as measures of the serial correlation, and have been widely studied. For the case in which $h = 1$, it is found [37] [84] that for large N, R is approximately normal with expectation

$$E(R) = (S_1^2 - S_2)/(N-1)$$

and variance

$$\sigma^2(R) = \frac{(S_2^2 - S_4)}{n-1} + \frac{(S_1^4 - 4S_1^2 S_2 + 4S_1 S_3 + S_2^2 - 2S_4) - E^2(R)}{(n-1)(n-2)}$$

where $S_k = x_1^k + x_2^k + \ldots x_N^k$

and the sequence is assumed to be randomly drawn from a distribution with low order moments.

Williams [87] and von Neumann [80] [81] have studied the moments of δ_1^2, and Young [92] has proposed the related statistic C, which behaves like a conventional correlation coefficient. The analogous expressions for $h \neq 1$ measure a serial correlation with lag h, and provide a basis for further tests of randomness against the alternative of trend or regular fluctuation.

Independence -- Runs Tests

A study of the distribution of runs yields several measures which are used as tests of randomness. The article by A. M. Mood [68] has an extensive bibliography of the initial papers on the topic and of related studies to 1940. The analysis of runs up and down has perhaps been the most thoroughly studied; the work of Wolfowitz and Levene [63] [64] has given the expected values and the covariance matrix for statistics based on runs up and down, and they have studied the properties of tests based on these statistics. Their article [64] incidentally shows that the test procedure used by Kermack and McKendrick [61] is not correct.

Letting r_p denote the number of runs up or down of length p and r'_p denote the number of runs up or down of length greater than or equal to p, then the expected values of r_p and r'_p in a set of size n, are given by

$$E(r_p) = 2n(p^2+3p+1)/(p+3)! - 2(p^3+3p^2-p-4)/(p+3)!$$

$$E(r_p) = 2n(p+1)/(p+2)! - 2(p^2+p-1)/(p+2)!$$

These results make possible a test of goodness of fit of the observed to the expected number of runs up and down in the observed sequence.

Similar statistics may be based on the observed number of runs above and below the median [68], runs above and below the mean [68], and the total number of runs [75]. The sign tests [66] [69] and the U-test [130] are of a similar nature. A comprehensive discussion of this class of order statistics is found in Wilks [88].

The ω_n statistic of Kendall and Sherman [38] [23] and the low order moments of the sample (empirical) distribution provide further tests of randomness.

The d^2 test of Gruenberger and Mark [56] is designed for the case in which the sequence tested is to be used in Monte Carlo calculations -- in particular those in which two successive numbers are used as the coordinates of a "random" point in the unit square. The test is based on the probability that the squared distance between two successive points will exceed a value α^2. The theoretical probabilities are tabulated in [56], on the basis of the relation

$$\text{Prob}\left[d^2 \leq \alpha^2\right] = \alpha^2 - 8\alpha^3/3 + \alpha^4/2 \quad \text{for} \quad 0 \leq \alpha^2 \leq 1$$

$$\text{Prob}\left[d^2 \leq \alpha^2\right] = 1/3 + (\pi-2)\alpha^2 + 4(\alpha^2-1)^{1/2} + 8/3(\alpha^2-1)^{3/2} - \alpha^4/2 - 4\alpha^2 \operatorname{Sec}^{-1}\alpha \quad \text{for} \quad 1 \leq \alpha^2 \leq 2 .$$

Finally we note that a test of the randomness of a set of numbers may be based on the empirical distribution of some test statistic computed for each of several subsets of the set. The observed distribution of these computed values may then be tested for goodness of fit to the theoretical distribution of the test statistic. Such a procedure is used by Taussky and Todd [117] and by Dodd [48]; it will be used also in our analysis of experimental results in Chapter 4.

On the basis of discussions in [18] [23] [50] further tests of randomness could be constructed. The foregoing, however, describes or gives reference to all of the standard tests used in evaluating the arithmetic methods described in the following chapter.

Chapter Three. The Generation of Pseudo-Random Sequences

Having an elaborate background for the testing of pseudo-random sequences, we need now to obtain some numbers. As indicated in the introduction, we shall confine the discussion to the generation of sequences by an arithmetic relation. For the sake of clarity we shall refer to a specific recursion relation

$$x_{j+1} = R(x_j, x_{j-1}, \ldots, x_{j-t}; a_1, a_2, a_3, \ldots, a_t)$$

with given parameter values as a pseudo-random generator, while a class of such relations, of similar form but with unspecified values for the parameters, will be called a method. There are three basic methods -- the mid-square method, the multiplicative congruential method, and the additive congruential method. These each offer special cases which will be mentioned separately. The discussion will generally be phrased in terms of relations suitable for a binary computer.

The Mid-Square Method

(i) Generation. The mid-square method suggested by von Neumann squares a $2r$ bit number u_j, $0 \leq u_j < 1$, extracts the middle $2r$ bits from the result, and uses this number as u_{j+1}. There is no convenient analytic expression to describe this method, but for a $2r$ digit number u_j, one can write the relation

$$u_{j+1} = 2^r \left[u_j^2 \bmod 2^{-r} \right] \qquad (1)$$

with the understanding that only the $2r$ most significant (i.e. leftmost) bits of the result are used.

The calculation of each succeeding random number can there-

fore be carried out in a binary computer with one multiplication and one shift operation. The subsequent multiplication by 2^r is achieved by the scaling convention in which the binary point is understood to be at the left-hand end of a register -- i.e. before the most significant binary digit.

(ii) Period. It is apparently not possible to determine analytically the number of numbers which may be obtained by any particular choice of u_o. But, the number of distinct iterates is clearly finite (in fact $\leq 2^{2r}$) and the method will cycle if at any time a value is repeated. Of further concern is the possibility that the process will degenerate by accumulating zeros at either end, and thus terminate in zero.

Metropolis [111] and Forsythe [99] have studied the lengths and types of cycles produced by the method, and have concluded that in many cases this 'zero mechanism' is dominant in the termination of the sequence through cycling. If this is assumed, then a rough estimate of the length of the sequence may be made by observing that the probability of r zeros accumulating in either the leading or the trailing digits is 2^{-r}, and hence, assuming the sequence to be random, the probability of the sequence degenerating at any stage is 2×2^{-r}. Thus the expected length of sequence is approximately 2^{r-1}, or the square root of the largest value represented by 2r bits.

(iii) Properties. The method has been motivated on the basis of two observations.

a) If the variable x is uniformly distributed on (0, 1) then the variable $y = x^2$

has the density function

$p(y) = 1/2\ y^{-1/2}$ for $y \geq 0$.

b) If a random variable y_k is formed from a random variable y by the rule

$$y_k = 2^n [y \bmod 2^{-n}] \qquad (2)$$

then the limiting distribution as $n \to \infty$ is uniform on (0, 1).

A proof of (b) is found in Tocher [120], who also derives an estimate of the bias implied by (a). From this estimate or directly from consideration of (a) it is expected that the method will yield too many small numbers, and this expectation is confirmed in practice.

(iv) Tests. Tests on sequences produced by the mid-square method have been performed by Forsythe [98], who tested 4-digit mid-square sequences, by Votaw and Rafferty [125] and by Hammer [102], but in each case these tests were performed on the individual digits rather than the numbers. The results reported by Forsythe were negative, but Hammer, using 10-digit decimal numbers, and Votaw and Rafferty, using 8-digit decimal numbers, reported satisfactory results. Cashwell and Everett [7] report that their mid-square method using a 38 bit number yields a satisfactory sequence of length about 750,000.

(v) Assessment. The major disadvantage of the mid-square method is the danger of undetected short cycles in the sequence. Coupled with the facts that the method is not fast, and possesses a bias toward small values, this has generally led to the abandonment of the mid-square procedure in favour of other methods.

A mid-product method, and an off-center mid-product method (which Tocher shows to be less biased than a mid-square method) are tested also by Forsythe [99], but apparently are not satisfactory, and are not recommended.

The Multiplicative Congruential Methods

The least positive residues of the relation

$$X_{j+1} \equiv (kX_j + c) \bmod M \tag{3}$$

form a periodic sequence, and Lehmer [108] suggested that the relation

$$u_j = (1/M)X_j$$

may be suitable for generating a sequence of pseudo-random numbers. Several special cases of (3) are used sufficiently often to justify distinguishing them by name. The relation (for binary computers)

$$\begin{aligned} X_{j+1} &\equiv k'X_j \bmod 2^P \mp 1 \\ u_j &= 2^{-P}X_j \end{aligned} \tag{4}$$

is known as Lehmer's method, and is a special case of the relation

$$\begin{aligned} X_{j+1} &\equiv kX_j \bmod M \equiv k^{j+1}X_o \bmod M \\ u_j &= X_j/M \end{aligned} \tag{5}$$

which is called the power residue method. We shall use this term only in case $M = 2^P$.

To avoid the multiplication required by (4) or (5), Greenberger [101] proposed that the relation (5) employ

$k = 2^a + 3$ so that

$$X_{j+1} \equiv (2^a + 3)X_j \mod 2^P \tag{6}$$

$$u_j = 2^{-P}X_j$$

and the multiplication could be accomplished by a shift and add procedure.

For the same reason Rotenberg [116] proposed to use a method which is a special case of (3), setting

$$\begin{aligned} X_{j+1} &\equiv (2^a+1)X_j + C \mod 2^P \\ u_j &= 2^{-P}X_j \end{aligned} \tag{7}$$

We shall describe the properties of the power residue method in some detail, and quote corresponding results for the other cases.

(i) Generation. The sequence $\{u_i\}$ of numbers is defined by the relations

$$X_{j+1} \equiv kX_j \mod 2^P \equiv k^{j+1}X_o \mod 2^P \tag{8}$$

$$u_j = 2^{-P}X_j \tag{9}$$

and can therefore be generated by a single multiplication, provided P is less than or equal to the word length of the computer used.

(ii) Period. Clearly the sequence (8) is simply periodic, with the period given by the least solution of the congruence relation

$$X_{j+n} \equiv X_j \mod 2^P$$

But $X_j \equiv k^jX_o \mod 2^P$

$$X_{j+n} \equiv k^{j+n}X_o \mod 2^P .$$

If k odd, $(k, 2^P) = 1$, and we have $X_{j+n} \equiv k^nX_j \equiv X_j \mod 2^P$

$$(k^n-1)X_j \equiv 0 \mod 2^P$$

If also X_o odd, then X_j is odd for all j, and $(X_j, 2^P) = 1$

Hence

$$\begin{aligned} k^n - 1 &\equiv 0 \mod 2^P \\ k^n &\equiv 1 \mod 2^P \end{aligned} \tag{10}$$

Number theory methods show that the least solution of this relation is greatest when k is of the form

$$k \equiv \pm 3 \mod 8 \tag{11}$$

That is, a necessary and sufficient condition that the relation (8) generate a sequence with maximal period is that

$$\begin{aligned} k &\equiv \pm 3 \mod 8 \\ X_o &\equiv 1 \mod 2 \text{ -- i.e. -- } X_o \text{ odd.} \end{aligned} \tag{12}$$

For such choice of k and X_o, the period of the sequence is 2^{P-2} numbers.

Multipliers of the form 5^{2n-1} satisfy (11), for

$$\begin{aligned} 5^{2n-1} = (1+4)^{2n-1} &= 1^{2n-1} + (2n-1)1^{2n-2}4^1 + 4^2[\cdots \\ &= 1^{2n-1} + 8n-4 + 4^2[\cdots \\ &\equiv -3 \mod 8 \end{aligned}$$

Consequently the relations studied by Juncosa [107], by Davis and Rabinowitz [11], and at the National Bureau of Standards [117], have maximal period.

(iii) Properties. If k and X_o are both odd, then X_j is odd for all j. Since there are 2^{P-2} numbers in the maximal sequence (8), and 2^{P-1} distinct odd numbers in S, exactly one half of all the odd numbers occur in the sequence. Further, it may be shown, as Juncosa does for the case $k = 5^{13}$, that if

$$k \equiv -3 \mod 8$$

and the number r occurs in the sequence (8), then $r + 2$ cannot.

If $k \equiv +3 \bmod 8$, and r occurs in (8), then $r + 4$ cannot. Consequently the numbers of the sequence $\{u_i\}$ are uniformly distributed over the set S of distinguishable numbers.

If X_j is to be always odd, its least significant digit must be constantly 1. The next digit position, by the above argument, is likewise constant, but may be either zero or one. The periodicity of digit positions then increases to the left, only the most significant digit finally having period 2^{P-2}. For this reason, in any application requiring random digits, only the most significant digits of each number generated may be used.

(iv) Tests. Taussky and Todd, [117], Juncosa [107], Moshman [113], and others have tested extensively power residue methods using $k = 5^r$ where r is odd. Satisfactory results were obtained in tests of uniformity, low order moments, runs, and correlation as determined by the serial matrix test.

(v) Assessment. The multiplicative congruential method is faster than the mid-square method, and produces a sequence which over a full period is uniformly distributed. A predictable and maximal length of period may be obtained by suitable choice of multipliers, and such generators yield sequences which pass all the customary tests of randomness.

Lehmer's method uses the relation (4); the generator originally proposed by Lehmer (the first published account of a multiplicative congruential method) used $k = 23$

$$M = 10^8 + 1 .$$

For binary schemes, the reduction modulo $2^P + 1$ may be accomplished by observing that if we represent a number greater than 2^P in a computer with P-bit word length as

$$a + b \cdot 2^P = a - b + b(2^P + 1)$$

then $(a - b)$ is the least residue mod $2^P + 1$.
Hence we may generate the sequence (4) simply by forming $y_{i+1} = kX_i$, dropping the most significant bits of y_i beyond the pth, and subtracting the dropped portion from the remainder.

The scheme has the advantage that it removes the periodicity of the low order digits in (8), but this of course is at the cost of extra instructions, and consequently extra time.

A special case of (5) which has the advantage of greater speed is the method proposed as Greenberger's Method. In this case the multiplication operation is replaced by the faster shift and add procedure; the generator used took the values $k = 2^{18} + 3$, $p = 35$.

Alternative procedures utilize (3) rather than (5), and thereby need not be restricted to the odd numbers of the set S. Thus they may possess a period greater than the sequences produced by the power residue method. A modification proposed by Thompson [119] uses the relation

$$X_{j+1} \equiv (4k+1)X_j + k \mod 2^P$$

$$\text{or} \quad X_{j+1} \equiv (4k+1)X_j + 3k \mod 2^P$$

$$u_j = 2^{-P}X_j$$

where k must be odd, and for this relation the sequence has the full period 2^P. The same is true for the method proposed by Rotenberg [116] using a shift and add technique as indicated by relation (7), provided c is odd.

With these results, there is little to be gained in further development of multiplicative congruential methods. The alternative is to attempt further improvements in the speed of generation, by studying methods using addition rather than multiplication.

Additive Congruential Methods.

(i) Generation. The general relation, given t initial values $\{X_i\}$ $0 \leq i \leq t$

$$X_{j+1} \equiv \sum_{j-t+1}^{j} a_i X_i \mod 2^P \qquad (14)$$

has been suggested as a pseudo-random generator, apparently by van Wijngaarden [122], and mentioned briefly by Tocher [120]. The special case

$$\begin{aligned} X_{j+1} &\equiv X_j + X_{j-1} \mod 2^P & X_o &= 0 \\ u_j &= 2^{-P} X_j & X_1 &= 1 \end{aligned} \qquad (15)$$

is known as the reduced Fibonacci series, and has been studied in some detail. It may be generated with a single addition instruction, and is therefore the fastest relation yet studied. The slightly more general case

$$\begin{aligned} X_{j+1} &\equiv X_j + X_{j-n} \mod 2^P \\ u_j &= 2^{-P} X_j \end{aligned}$$

also requires a single addition with, however, the necessity of some indexing technique.

(ii) Period. A full analysis of the period of the reduced Fibonacci series (15) and of the series with arbitrary initial values has been given by Wall [120]. In his paper it is shown

that the period of the sequence is $3 \cdot 2^{P-1}$ and independent of the starting values.

(iii) Properties. The reduced Fibonacci series method is closely related to the power residue method. If the relation (15) is solved as a difference equation, then, approximately,

$$X_j \equiv \frac{\left[\frac{1}{2}(\sqrt{5}+1)\right]^j - \left[\frac{1}{2}(\sqrt{5}-1)\right]^j}{\sqrt{5}} \mod 2^P .$$

Since $\frac{\sqrt{5}-1}{2} < 1$, as $j \to \infty$

$$X_j \sim \left[\tfrac{1}{2}(\sqrt{5}+1)\right]^j \cdot \frac{1}{\sqrt{5}}$$

that is, $\{u_j\}$ approximates a power residue method with

$$k = \tfrac{1}{2}(\sqrt{5}+1)$$

$$X_0 = 1/\sqrt{5} .$$

(iv) Tests. The sequences generated by (15) have been tested by Taussky and Todd.[117] It is found that, though the tests of uniformity and of moments yield satisfactory results, the runs tests indicate serious deviations from the expected behaviour of a random sequence. Satisfactory results may apparently be obtained by discarding alternate numbers, but with this modification the method offers no advantage over the power residue methods.

The more general relation (16) has been studied by Green et al [100] and found to be satisfactory only if either alternate numbers were discarded, or n was taken greater than or equal to 16. Either measure involves some programming inconvenience, and detracts significantly from the advantages of an additive method.

Multiple Method

A proposal of theoretical interest is based on a theorem of Kronecker and Sierpinski [17; page 383] which states

Theorem: If t is irrational, then the points $\{nt\}$ mod 1 are uniformly distributed on $[0, 1]$.

The generating process thus consists of forming the sequence $u_n = nt \bmod 1$ or, in terms of the finite computer representation of t, may be formulated in terms of integers, so that $u_n = na \bmod 2^P$ where a is odd, and less than 2^P. The method is not, however, used in practice, and we shall not go into a discussion of it.

Chapter 4. Empirical Results

Pseudo-random sequences find application in problems with widely varying characteristics. Two applications programmed for the ALWAC III-E computer at the University of British Columbia display in common a feature which is characteristic of a wide class of problems, and is of importance in determining a pseudo-random generator suitable for them: they both employ fairly large quantities of random numbers in small, essentially isolated blocks. Between blocks, parameters of the calculation are varied over a preassigned range and the output of the program is studied as a function of these parameter values. Clearly it is essential that the individual blocks of numbers display no significant deviation from the mean behaviour expected of a random sequence -- otherwise the observed results may be found to depend in a significant way on the blocks of pseudo-random numbers, and will not accurately reflect the influence of varying parameter values.

It seemed not at all obvious that the standard methods discussed in Chapter 3 would be suitable under these circumstances. The problem of determining a generating procedure suited to such applications was therefore undertaken as an empirical study using the facilities of the University of British Columbia Computing Centre, with the hope that empirical results might also suggest an analytic solution to the problem.

The question of local randomness has been mentioned briefly in several papers,[24] [112] [119] but has apparently not been studied to any extent. In this literature, a sequence has

conventionally been called 'locally random' to emphasize the fact that not only were the conditions of randomness satisfied, but that also the block of numbers in itself passed a class of tests of randomness. We have used the term pseudo-random to denote the fact that a block of numbers under consideration passes a class of tests of randomness; for the problem at hand we wished to study the possibility that successive sub-blocks of length N in a pseudo-random sequence be found to yield in themselves statistically non-significant results on all of a class C of tests of randomness. If this condition holds, we say the sequence is locally pseudo-random for domains of order N.

Then the conjecture studied first was that the standard generators described in Chapter 3 need not be locally pseudo-random for domains of order N, where N is small relative to the modulus of the generator. In particular, we studied the case where N was 2^8, 2^9, or 2^{10} -- i.e. 256, 512, or 1024, and the modulus was 2^{32}. On statistical grounds such a conjecture is plausible. The fact that the standard generators have been found to satisfy tests of randomness over long cycles suggests immediately that if the sequence were partitioned into blocks, about 5% of these blocks would show deviations from expected behaviour significant at the 5% level. If not, doubt would be cast on the randomness of the sequence. Since this would be true of each of several independent tests, it seemed possible that a substantial number of sub-blocks generated by standard methods would in themselves be unsatisfactory for use as random numbers.

In investigating this question empirically, two tests were considered to constitute a minimal class C of tests of randomness: a chi-square test for the uniformity of distribution in 8 equal intervals of $[0, 1]$, and a chi-square test on the uniformity of an 8 x 8 serial matrix f_{ij} described in Chapter 2. A 5% level of significance was employed.

Thus, in testing blocks of 256 numbers, the distribution over the unit interval was considered to deviate significantly from uniformity if, employing the notation of Chapter 2,

$$X_1^2 = \sum_{i=1}^{8} (f_i - 32)^2/32 \geq 14.1$$

where 14.1 is the 95% value of the tabulated chi-square distributions for 7 degrees of freedom.

Using the fact that

$$X_2^2 - X_1^2 = \sum_{i,j=1}^{8} (f_{ij} - 4)^2/4 - \sum_{i=1}^{8} (f_i - 32)^2/2$$

is asymptotically distributed as chi-square with 56 degrees of freedom, and using the normal approximation to the chi-square distribution, the distribution of pairs within the matrix was said to deviate significantly from uniformity if

$$\sqrt{2\chi^2} - \sqrt{2r-1} \geq 1.64$$

i.e. if $\chi^2 \geq 74.18$

where 1.64 is the 95% value of the unit normal curve, and r, the number of degrees of freedom, is 56. For blocks of 512 and 1024 numbers, a similar measure was used, with the same critical values.

Table I summarizes the results of tests for 100 blocks of 256 numbers each, generated by each of the standard methods discussed in Chapter 3, and for blocks of 512 and 1024 numbers

To Follow Page 31

TABLE I

Number of "Unsatisfactory" Blocks in 100 Blocks

Generated by Standard Methods with Maximum Modulus

Method	Generator	Block Size	Number of Blocks Rejected			Total Rejected
			X_1^2 Test	X_2^2 Test	Both	
Rotenberg's Method	$X_{i+1} \equiv (2^7+1)X_i+1 \mod 2^{32}$	256	6	5	3	8
Lehmer's Method	$X_{i+1}=23X_i \mod 2^{32}+1$	256	3	15	3	15
Fibonacci Series	$X_{i+1}=X_i+X_{i-1} \mod 2^{32}$	256	4	11	4	11
Power Residue	$X_{i+1}=62,973X_i \mod 2^{32}$	256	5	7	0	12
Power Residue	$X_{i+1}=62,973X_i \mod 2^{32}$	512	6	4	1	9
Power Residue	$X_{i+1}=62,973X_i \mod 2^{32}$	1024	4	6	0	10

each generated by the power residue method. From the Table it will be seen that approximately the expected number (10%) of sub-blocks in each case fails to pass these rather weak requirements, and that serious disadvantages therefore accompany the use of these generators in applications of the type we describe.

It was therefore proposed to test the conjecture that a power residue method with modulus and multiplier chosen to yield a maximal period equal to the number of elements necessary in the sub-blocks would be suitable. Again there is a theoretical consideration to support the proposal, namely the theorem quoted in Chapter 3 which states that over a full period the elements of a sequence generated by a power residue method are uniformly distributed on the set S of distinguishable numbers.

This conjecture also was tested and verified empirically. In Chapter 3 it was mentioned that the maximal period for the power residue method with modulus 2^P is 2^{P-2}, and that this period is attained if the multiplier k satisfies

$$k \equiv \pm 3 \bmod 8 \ .$$

Therefore moduli 2^{10}, 2^{11}, 2^{12} were employed to generate sequences with maximal period 2^8, 2^9, 2^{10}, respectively. All possible multipliers of the form

$$k \equiv \pm 3 \bmod 8$$

were employed to generate blocks of length equal, in each case, to the period of the generator.

These blocks were <u>a priori</u> uniformly distributed; it was found, with certain striking exceptions, that they also displayed

no significant deviation from uniformity over the serial matrix. The blocks displaying significant deviations from expected behaviour were consistently associated with multipliers falling in particular residue classes. This information is summarized in Table II, and on the basis of this Table it is possible to specify a method which guarantees that each sub-block of length N (N = 256, 512, 1024) in a long sequence of pseudo-random numbers will pass the two specified tests. That is, by restricting the multipliers k so as not to lie in any one of the residue classes 3, 5, 43, 51, 85, 125, 131, 171, 205, 213, 251, or 253 (mod 256), one can construct a sequence of length greater than 50,000 numbers which is locally pseudo-random for domains of order 256; by restricting k so as not to lie in any one of the residue classes 3, 5, 51, 85, 171, 205, 251, or 253 (mod 256) one can construct a sequence of length greater than 220,000 numbers which is locally pseudo-random for domains of order 512; by restricting k so as not to lie in any one of the residue classes 3, 5, 11, 13, 51, 59, 85, 93, 163, 171, 197, 205, 245, 251, or 253 (mod 256), one can construct a sequence of length greater than 800,000 which is locally pseudo-random for domains of order 1024.

For our problem this is an important result. It gives empirical corroboration of the idea that arithmetic methods may be selected which eliminate significant local fluctuations in a pseudo-random sequence designed for uses in which local randomness is essential. Further, the fact that multipliers associated with "unsatisfactory" blocks were observed to be confined to a relatively small number of residue classes

To Follow Page 33

TABLE II

Residue Classes Containing Multipliers
Yielding "Unsatisfactory" Blocks in Power Residue Generators
With Maximal Period Equal to
the Length of Block

Block Size	$(2^8)256$	$(2^9)512$	$(2^{10})1024$
Modulus	2^{10}	2^{11}	2^{12}
Number of Multipliers k, $k \equiv \pm 3 \bmod 8$ $k <$ modulus	256	512	1024
Residue Classes (mod 256) Containing "Unsatisfactory" Multipliers	3 5 51 85 171 205 251 253 . . . 43 125 131 213	3 5 51 85 171 205 251 253 . . .	3 5 51 85 171 205 251 253 . . . 11 13 59 93 163 197 245

supports the belief that a number theoretic criterion may be found to characterize those multipliers which yield blocks with statistically non-significant properties under a given class of tests. Since the empirical classification of multipliers was to some extent consistent through the three moduli tested, it seems likely that any number-theoretic criterion would hold for a wider range of block sizes.

These results demonstrate that a generator of the power residue type with small modulus can be suitable when small blocks of random numbers are required and the two tests we described are sufficiently searching. Such a generator may be programmed precisely as in the case with maximum modulus; the only change is a rescaling of the initial value X_o as stored in the computer. On the other hand, the selection of suitable multipliers will not always be a convenient procedure to program in computer applications. It would be desirable to have a generating scheme which required only a single multiplier. For this reason an extension of the study was attempted, and achieved limited success. In Tables III and IV are displayed the results of tests performed on sets of 100 blocks of 256 numbers each, obtained using generators with modulus ranging from 2^{11} to 2^{17}. Since the length of the component blocks no longer is equal to the full period of the generators, it is no longer to be expected that the numbers in a block will be uniformly distributed. Table III sets out for each modulus the empirical distribution of the observed deviations from uniformity measured by the X_1^2 statistic. Since this statistic is expected under the null hypothesis to have asymptotically

To Follow Page 34

TABLE III

Distribution for Selected Moduli of 100 Values of X_1^2

Tabulated χ^2 Percentile	5%	10%	20%	30%	50%	70%	80%	90%	95%	
Tabulated χ^2 Value	2.17	2.83	3.82	4.67	6.35	8.38	9.80	12.0	14.1	Larger
Period of Generator	No. of Observed Values Falling in Indicated Intervals									
1x256	100									
2x256	22	14	20	12	16	8	4	4		
4x256	16	16	20	20	12	12	4			
8x256	11	1	11	4	21	24	14	0	14	
16x256	4	4	4	14	36	14	10	8	6	
32x256	7	4	10	13	23	12	12	12	7	
64x256	3	7	12	7	30	22	9	7	2	1
128x256	4	3	10	8	27	22	7	9	9	1
2^{22}x256	8	3	6	13	20	26	5	13	1	5

To Follow Page 34

TABLE IV

Distribution for Selected Moduli of 100 Values of X_2^2

Tabulated χ^2 Percentile	5%	10%	20%	30%	40%	50%	60%	70%	80%	90%	95%	
Tabulated χ^2 Value	39.6	42.9	47.1	50.2	53.0	55.5	58.2	61.2	64.8	69.9	74.2	Larger
Period of Generator	Number of Observed Values Falling in Indicated Intervals											
1x256	100											
2x256	76	4	12	2	4		2					
4x256	76	4	16	4								
8x256	11	11	18	14	24	5	6	3	1	5	2	
16x256	4	10	20	5	11	7	9	8	8	14	4	
32x256	7	16	10	12	22	12	4	6	5	4	2	
64x256	6	6	5	12	14	8	12	13	8	10	6	1
128x256	8	5	7	13	20	11	5	8	7	8	6	2
2^{22}x256	3	3	10	11	9	10	16	8	13	7	3	7

the chi-square distribution with 7 degrees of freedom, the Table shows the number from 100 observed values of X_1^2 which fall in each interval defined by tabulated χ^2 values. Likewise, Table IV shows for each modulus the empirical distribution of observed values of the statistic X_2^2 ; the intervals are defined by the normal approximation to the chi-square distribution with 56 degrees of freedom.

These Tables show that it is possible, using a single multiplier, to generate sequences of length up to 8192 numbers which are locally pseudo-random for domains of order 256. A method has so far not been found which will yield longer locally pseudo-random sequences using only a single multiplier. Nevertheless, as Table IV shows, a substantial improvement over the standard generators has been achieved. Using moduli of 2^{16}, 2^{17}, sequences of length up to 32,000 have been generated in which no more than 2% in total of the sub-blocks of length 256 display significant results on either of the two tests used.

We note also that as in all the above cases, the length of the sequence may be doubled merely by taking a new initial value X_o from among the $+2^{P-2}$ odd P-bit numbers not in the sequence of 2^{P-2} numbers produced by the generator with modulus 2^P and a given initial value. By the theorem quoted in Chapter 3, if r is in the set of numbers produced by a generator with initial value X_o, and $k \equiv -3 \bmod 8$, then $r + 2$ will not be in the set, and hence $X_o + 2$ is a suitable initial value to generate another sequence (disjoint from the first) of 2^{P-2} numbers; if $k \equiv 3 \bmod 8$, then $r + 4$ is a suitable new initial value.

These results indicate that even for applications requiring fairly large numbers of pseudo-random numbers, it is possible to find a generating scheme involving only one multiplier which yields a sequence in which fewer than 2 or 3% of the sub-blocks of length 256 need to be rejected as deviating significantly from properties of randomness.

For many applications, therefore, our procedure is a decided improvement over standard generators. When it is convenient to allow, in a computer program, for the selection of multipliers, the use of generators with small modulus can guarantee local pseudo-randomness. Even when the use of more than one multiplier is not convenient, a substantial improvement in the "quality" of small blocks of numbers may still be effected by the use of a generator with the least modulus in excess of the total number of numbers required.

Chapter 5. Summary and Conclusions

Randomness is an elusive concept, and the pursuit of randomness a rather uncertain task. Behind this thesis is the idea that a major advantage in the generation of pseudo-random numbers by arithmetic methods is the experimenter's control over his medium. As Juncosa points out [107]; it is possible, with deterministic methods, to avoid the significant deviations from mean behaviour which inevitably occur in a truly random situation, and which may give rise to seriously misleading results. We may avoid, if we wish, the possibility of significant local non-randomness. If, therefore, we take our chances on a pseudo-random sequence of long period in situations in which local randomness is critical, we are not utilizing the advantages offered by arithmetic procedures.

This thesis has not settled the question of generating locally pseudo-random sequences. Nor is it pretended that the empirical study here described is any substitute for an analytical treatment of the problem if such be possible. On the other hand, the study has demonstrated that in some quite plausible circumstances the standard generators are not suitable. It has demonstrated that better procedures can be devised, and that there is hope at least for an empirical classification of locally pseudo-random generators. There is no doubt in the writer's mind that the problem is worth further study.

BIBLIOGRAPHY

Chapter 1. Applications and Preliminary Theory

1. Bauer, W. F. The Monte Carlo Method. J. Soc. Indust. Appl. Math., vol. 6, Dec. 1958.

2. Box, G. E. P. and Muller, M. E. A Note on the Generation of Normal Deviates. Ann. Math. Statist., vol. 28, 1958, p. 610.

3. Brown, G. W. History of RAND's Random Digits -- A Summary. Monte Carlo Method, National Bureau of Standards, Applied Mathematics Series #12, p. 31.

4. Butcher, J. C. Random Sampling from the Normal Distribution. The Computer Journal, vol. 3, #4, 1961, p. 251.

5. Butler, J. W. Machine Sampling from Given Probability Distributions. Symposium on Monte Carlo Method, H. A. Meyer (Ed.), New York, Wiley, 1956.

6. Cameron, J. M. Monte Carlo Experiments on SEAC. National Bureau of Standards SEL Working Paper SEL-52-5.

7. Cashwell, E. D. and Everett, C. J. A Practical Manual on the Monte Carlo Method for Random Walk Problems. International Tracts in Computer Science and Technology. Permagon Press, Los Angeles, 1959.

8. Church, A. E. R. On the Means and Squared Standard Deviations of Small Samples from Any Population. Biometrika, 18, 1926, p. 321.

9. Clark, C. E. The Utility of Statistics of Random Numbers. Operations Research, vol. 8, 1960.

10. Curtiss, J. H. Sampling Methods Applied to Differential and Difference Equations. Seminar on Scientific Computation, I.B.M., New York, 1949.

11. Davis, P. and Rabinowitz, P. Some Monte Carlo Experiments in Computing Multiple Integrals. Math. Tables Aids Comput., vol. 10, p. 1.

12. Fisher, R. A. and Yates, F. Statistical Tables for Biological, Agricultural, and Medical Research. Edinburgh, Oliver and Boyd, 1953.

13. Fisher, R. A. Statistical Methods for Research Workers. Edinburgh, 4th ed. Oliver & Boyd, 1932, p. 83.

14. Franklin, J. N. On the Equidistribution of Pseudo-Random Numbers. Quart. Appl. Math., vol. xvi, #2, July, 1958.

15. Gage, R. Contents of Tippett's Random Sampling Numbers. J. Amer. Statist. Assoc., vol. 38, 1943.

16. Hammersley, J. M. Note on Electronic Computers and the Analysis of Stochastic Processes. Math. Tables Aids Comput., vol. 4, 1950, p. 56.

17. Hardy, G. H. and Wright, E. M. An Introduction to the Theory of Numbers. Oxford, Clarendon Press, 1956.

18. Hoel, P. G. Introduction to Mathematical Statistics. New York, J. Wiley & Sons, Inc., 1947.

19. Holz, B. W. and Clark, C. E. A Table of Exponentially Distributed Pseudo-Random Numbers. Operations Research Office - SP - 108, Washington, D. C., 1958.

20. Jones, H. L. How Many of a Group of Random Numbers will be Usable in Selecting a Particular Sample. J. Amer. Statist. Assoc., vol. 54, #285, 1959, pp. 102-122.

21. Kahn, H. Applications of Monte Carlo. Rand Report, #RM 1237, AEC, 1954.

22. Kendall, M. G. A Theory of Randomness. Biometrika 32, 1941.

23. Kendall, M. G. The Advanced Theory of Statistics. Vol. II. London, Griffin & Co., 1948.

24. Kendall, M. G. and Babington-Smith, B. Randomness and Random Sampling Numbers. J. Roy. Statist. Soc., vol. C1, 1938.

25. Kendall, M. G. and Babington-Smith, B. Second Paper on Random Sampling Numbers. J. Roy. Statist. Soc., vol. VI, (Supp.), 1939, p. 51.

26. Kendall, M. G. and Babington-Smith, B. Random Sampling Numbers. Department of Statistics, University College, London.

27. Metropolis and Ulam. The Monte Carlo Method. J. Amer. Statist. Assoc., vol. 44, 1949, p. 335.

28. Meyer, H. A. (Ed.) Symposium on Monte Carlo Methods. New York, Wiley, 1956.

29. Muller, M. E. Inverse Method for Generation of Random Normal Deviates on Large-Scale Computers. Math. Tables Aids Comput., 12, 1958.

30. Musk, F. I. A Monte Carlo Simulation of a Production Planning Problem. Computer J., vol. 2, #2, p. 90.

31. Monte Carlo Method. Applied Mathematics Series #12. Washington, D. C., U. S. Dept. of Commerce, National Bureau of Standards, 1951.

32. Neate, R. and Dacey, W. J. A Simulation of Melting Shop Operations. Computer J., vol. 2, #2, p. 59.

33. RAND Corportion, The. A Million Random Digits with 100,000 Normal Deviates. Free Press Publishers, Glencoe, Illinois, 1955.

34. Strachey, C. Two Contributions to the Techniques of Queuing Problems. Computer J., vol. 3, #2, p. 114.

35. "Student". The Probable Error of the Mean. Biometrika 6, 1908, p. 1-25.

36. Tippett, L. H. C. Random Sampling Numbers. Tracts for Computers #XV, Cambridge University Press, 1950.

Chapter 2. Statistical Tests for Randomness

37. Anderson, R. L. The Distribution of the Serial Correlation Coefficient. Ann. Math. Statist., vol. 13, 1942, p. 1.

38. Bartholomew, D. J. Note on Sherman's Statistic as a Test of Randomness. Biometrika 41, p. 556.

39. Bartlett, M. S. The Frequency Goodness of Fit Test for Probability Chains. Proc. Cambridge Philos. Soc., vol. 47, 1951, pp. 86-95.

40. Berkson, J. Some Difficulties of Interpretation Encountered in the Application of the Chi-Square Test. Amer. Statist. Assoc., vol. 33, 1938.

41. Cameron, J. M. Results of Some Tests of Randomness on Pseudo-Random Numbers. Ann. Math. Statist., vol. 23, 1952, (Abstract).

42. Camp, B. H. Multinomial Solid and the Chi Test. Trans. Amer. Math. Soc., vol. 31, 1929, p. 133.

43. Cochran, W. G. The χ^2 Test of Goodness of Fit. Ann. Math. Statist., vol. 23, 1952, p. 315.

44. Coveyou, R. R. Serial Correlation in the Generation of Pseudo-Random Numbers. J. Assoc. Comput. Mach., vol. 7, 1960, pp. 72.

45. David, F. N. Combinatorial Tests of Whether a Sample Has Come from a Given Population, Biometrika 37, 1956.

46. Dixon, W. J. Further Contributions to Problems of Serial Correlation. Ann. Math. Statist., vol. 15, 1944, p. 119.

47. Dodd, E. L. The Length of Cycles Which Result from the Graduation of Chance Elements. Ann. Math. Statist., vol. 10, 1939, p. 254.

48. Dodd, E. L. Certain Tests for Randomness Applied to Data Grouped into Small Sets. Econometrica 10, 1942, p. 249.

49. Fisher, R. A. On the Random Sequence. Quarterly Journal of the Royal Meteorological Society, vol. 52, 1926, p. 250.

50. Fraser, D. A. S. Nonparametric Methods in Statistics. New York, John Wiley & Sons, Inc., 1957.

51. Fry, T. C. The χ^2 Test of Significance. J. Amer. Statist. Assoc., vol. 33, 1938, p. 513.

52. Good, I. J. The Serial Test for Sampling Numbers and Other Tests for Randomness. Cambridge Philos. Soc. Proc., vol. 49, 1953, pp. 276-284.

53. Good, I. J. On the Serial Test for Random Sequences. Ann. Math. Statist., vol. 28, 1957, p. 262.

54. Greenwood, R. E. Coupon Collectors Test for Random Digits. Math. Tables Aids Comput., vols. 9-10, 1955-1956, p. 1.

55. Gruenberger, F. Tests of Random Digits. Math. Tables Aids Comput., vol. 4, p. 244.

56. Gruenberger, F. and Mark, A. M. The d^2 Test of Random Digits. Math. Tables Aids Comput., vol. 5, 1951, p. 109.

57. Gumbel, E. J. On the Reliability of the Classical χ^2 Test. Ann. Math. Statist., vol. 14, 1943.

58. Hoel, P. G. On the Chi-Square Distribution for Small Samples. Ann. Math. Statist., vol. 9, 1938, p. 158.

59. Hunter, D. G. N. Note on a Test for Repeating Cycles in a Pseudo-Random Number Generator. Computer J., vol. 3, 1960.

60. Iyer, P. V. K., & Rao, A. S. P. Theory of Probability Distribution of Runs in Sequences of Observations. Indian Soc. Agricultural Statist. J., vol. 5, 1953, pp. 29-77.

61. Kermack, W. O. and McKendrick, A. G. Tests for Randomness in a Series of Numerical Observations. Proc. Roy. Soc., 1936-1937, vol. 57, Part 3, pp. 228-240.

62. Koopmans, T. C. Serial Correlation and Quadratic Forms in Normal Variables. Ann. Math. Statist., vol. 13, 1942, p. 14.

63. Levene, H. & Wolfowitz, J. On the Power Function of Tests of Randomness Based on Runs Up and Down. Ann. Math. Statist., vol. 23, 1952, p. 34.

64. Levene, H. & Wolfowitz, J. The Covariance Matrix of Runs Up and Down. Ann. Math. Statist., vol. 15, 1944, p. 58.

65. McEwen, G. F. The Reality of Regularities Indicated in a Sequence of Observations. Proc. Berkeley Symposium on Math. Statist. and Probability, Ed. J. Neyman, University of California Press, 1949.

66. Mann, H. B. On a Test for Randomness Based on Signs of Differences. Ann. Math. Statist., vol. 16, 1945, p. 193.

67. Metropolis, N. C., Reitwiesner, G., and von Neumann, J. Statistical Treatment of First 2,000 Decimal Digits of e and of π Calculated on the Eniac. Math. Tables Aids Comput., vol. 4, p. 109.

68. Mood, A. M. The Distribution Theory of Runs. Ann. Math. Statist., vol. 11, 1940, p. 367.

69. Moore, G. H. and Wallis, W. A. Time Series Significance Tests Based on Signs of Differences. J. Amer. Statist. Assoc., vol. 38, 1943, pp. 153-165.

70, Moore, P. G. A Sequential Test for Randomness. Biometrika 40, 1953.

71. Nair, K. N. On Tippett's Random Sampling Numbers. Sankhya 4, 1938, p. 65.

72. Pearson, K. On the Criterion that a Given System of Deviations from the Probable in the Case of a Correlated System of Variables is Such that it can Reasonably be Supposed to Have Arisen from Random Sampling. Philosophical Magazine, vol. 50, 1900, p. 157.

73. Rubin, H. On the Distribution of the Serial Correlation Coefficient. Ann. Math. Statist., vol. 16, 1945, p. 211.

74. Slutzky, E. The Summation of Random Causes as a Source of Cyclic Processes. Econometrica, vol. 5, 1937, pp. 105-146.

75. Swed, F. S. and Eisenhart, C. Tables for Testing Randomness of Grouping in a Sequence of Alternatives. Ann. Math. Statist., vol. 14, 1943, p. 66.

76. Tate, M. W. and Clelland, R. C. Non-Parametric and Shortcut Statistics. Interstate Printers and Publishers, 1957.

77. Thompson, W. E. Ernie -- A Mathematical and Statistical Analysis. J. Roy. Statist. Soc. Ser. A, vol. 122, p. 301.

78. Tintner, G. Tests of Significance in Time Series. Ann. Math. Statist., vol. 10, 1939, p. 141.

79. Tompkins, C. B. The RAND Corporation's One Million Digits. Math. Tables Aids Comput., vol. 10, 1956, p. 39.

80. von Neumann, J. The Distribution of the Ratio of Mean Square Successive Difference to the Variance. Ann. Math. Statist., vol. 12, 1941, p. 367.

81. von Neumann, J., Kent, R. H., Bellman, H. R., and Hart, B.I. The Mean Square Successive Difference. Ann. Math. Statist., vol. 12, 1941, p. 153.

82. von Schelling, H. Coupon Collecting for Unequal Probabilities. Amer. Math. Monthly, vol. 61, 1954, pp. 306-311.

83. Wald, A. A. and Mann, H. B. On the Choice of the Number of Intervals in the Application of the Chi-Square Test. Ann. Math. Statist., vol. 13, 1942, p. 306.

84. Wald, A. and Wolfowitz, J. An Exact Test for Randomness in the Non-Parametric Case Based on Serial Correlation. Ann. Math. Statist., vol. 14, 1943, p. 378.

85. Wald, A. and Wolfowitz, J. On a Test Whether Two Samples are From the Same Population. Ann. Math. Statist., vol. 11, 1940, p. 147.

86. Williams, C. A. On the Choice of the Number and Width of Classes for Chi-Square Test of Goodness of Fit. J. Amer. Statist. Assoc., vol. 45, 1950.

87. Williams, J. D. Moments of the Ratio of the Mean Square Successive Difference to the Mean Square Difference in Samples from a Normal Universe. Ann. Math. Statist., vol. 12, 1941, p. 239.

88. Wilks, S. S. Order Statistics. Amer. Math. Soc. Bull., vol. 54, 1948, p. 6.

89. Wolfowitz, J. Note on Runs of Consecutive Elements. Ann. Math. Statist., vol. 15, 1944, p. 97.

90. Wolfowitz, J. Asymptotic Distribution of Runs Up and Down. Ann. Math. Statist., vol. 15, 1944, p. 163.

91. Wolfowitz, J. On the Theory of Runs with Some Applications to Quality Control. Ann. Math. Statist., vol. 14, 1943, p. 280.

92. Young, L. C. On Randomness in Ordered Sequences. Ann. Math. Statist., vol. 12, 1941, p. 293.

93. Yule, G. U. A Test of Tippett's Random Sampling Numbers, J. Roy. Statist. Soc., vol. 101, 1938, p. 167.

Chapter 3. Arithmetic Methods for the Generation of Pseudo-Random Sequences

94. Arthur, A. O. Random Digit Generation. Computing News, Sept., 1956.

95. Bofinger, E. and Bofinger, V. I. A Periodic Property of Pseudo-Random Sequences. J. Assoc. Comput. Mach., 1958, pp. 261-265.

95.b. Certaine, J. E. On Sequences of Pseudo-Random Numbers of Maximal Length. J. Assoc. Comput. Mach., vol. 5, 1958.

96. Duparc, H. J. A., Lekkerkerker, G. G., and Peremans, W. Reduced Sequences of Integers and Pseudo-Random Numbers. Mathematics Centrum, Amsterdam, Report ZW 1953 - 002, ZW 1952 - 013.

97. Edmonds, A. R. The Generation of Pseudo-Random Numbers on Electronic Digital Computers. Computer J., vol. 2, 1960, p. 181.

98. Forsythe, G. E. Generation and Testing of Random Digits at the National Bureau of Standards. Monte Carlo Method. National Bureau of Standards. A.M.S. 12, 1951, p. 34.

99. Forsythe, G. E. Generation and Testing of 1,217,370 Random Binary Digits on SWAC. Bull. Amer. Math. Soc., vol. 57, 1951, p. 304.

100. Green, B. F. Jr., Smith, J. E. K., and Klem, L. Empirical Tests of an Additive Random Number Generator. J. Assoc. Comput. Mach., vol. 6, #4, 1959, p. 527.

101. Greenberger, M., Orrcut, G. H., and Rivlin, A. M. Decision Unit Models and Simulation of the United States Economy.

102. Hammer, P. C. The Mid-Square Method of Generating Digits, Monte Carlo Method. National Bureau of Standards. A.M.S. #12.

103. Horton, H. B. A Method for Obtaining Random Numbers. Ann. Math. Statist., vol. 19, 1948, pp. 81-85.

104. Horton, H. B. and Smith, R. T. A Direct Method for Producing Random Digits in Any Number System. Ann. Math. Statist., vol. 20, 1949, pp. 82-90.

105. International Business Machines. Reference Manual -- Random Number Generating and Testing, IBM 1958.

106. Johnson, D. L. Generating and Testing Pseudo-Random Numbers on IBM 701. Math. Tables Aids Comput., vol. 10, 1956, pp. 8-13.

107. Juncosa, M. L. Random Number Generation of the BRL High Speed Computing Machines. Ballistics Research Laboratories. Report #855. Aberdeen Proving Ground, Maryland, 1953.

108. Lehmer, D. H. Mathematical Methods in Large-Scale Computing Units. Annals of the Computation Laboratory of Harvard University. Proceedings of a Second Symposium on Large-Scale Digital Calculating Machinery, 1951.

109. Lehmer, D. H. Review of Juncosa 'Random Number Generation of the BRL High Speed Computing Machines'. Math. Reviews, vol. 15, 1954, p. 559.

110. Mauchly, J. W. Pseudo-Random Numbers. (Address) American Statistics Association, 1949.

111. Metropolis, C. Phase Shifts -- Middle Squares -- Wave Equation. Symposium on Monte Carlo Methods. H. A. Meyer (Ed.) New York, Wiley, 1956.

112. Meyer, H. A., Gephart, L. S. and Rasmussen, N. L. On the Generation and Testing of Random Digits. WADC Tech. Rep. 54-55, Wright Patterson Air Force Base - Ohio - 1954.

113. Moshman, J. The Generation of Pseudo-Random Numbers on a Decimal Calculator. J. Assoc. Comput. Mach., vol. 1, 1954.

114. Page, E. S. Pseudo-Random Elements for Computers. Appl. Statist., vol. 8, 1959.

115. Reitwiesner, G. An Eniac Determination of π and e to More Than 2,000 Decimal Places. Math. Tables Aids Comput., vol. 4, p. 11.

116. Rotenberg, A. A New Pseudo-Random Number Generator. J. Assoc. Comput. Mach., vol. 7, 1960.

117. Taussky, O. and Todd, J. Generation and Testing of Pseudo-Random Numbers. Symposium on Monte Carlo Methods. Ed. H. A. Meyer. New York, Wiley, 1956, pp. 15-28.

118. Teichroew, D. Distribution Sampling with High Speed Computers. Dissertation. University of North Carolina, 1953.

119. Thompson, W. E. A Modified Congruence Method of Generating Pseudo-Random Numbers. Computer J., vol. 1, p. 83.

120. Tocher, K. D. The Application of Automatic Computers to Sampling Experiments. J. Roy. Statist. Soc., vol. 16, 1954, p. 39.

121. Tompkins, C. B. (reviewer) Random Number Generating Icosahedral Dice, Mathematics of Computation, vol. 15, #73, January, 1961, p. 94.

122. van Wijngaarden, J. Report on Proceedings of Symposium on Digital Computation. N. P. L., Spring, 1953.

123. Vickery, C. W. On Drawing a Random Sample From a Set of Punched Cards. J. Roy. Statist. Soc., vol. 6, 1939, p. 63.

124. von Neumann, J. Various Techniques Used in Connection with Random Digits. Monte Carlo Method. National Bureau of Standards, AMS #12, p. 36.

125. Votaw, D. F. Jr., and Rofferty, J. A. High Speed Sampling. Math. Tables Aids Comput., vol. 5, 1951, pp. 1-8.

126. Wall, D. D. Fibonacci Series Modulo m. Amer. Math. Monthly, vol. 67, #6, p. 525.

127. Walsh, J. E. Concerning Compound Randomization in the Binary System. Ann. Math. Statist., vol. 20, 1949, pp. 580-589.

128. Walsh, J. E. On a Method of Obtaining Random Binary Digits by Flipping Coins. Project RAND. Santa Monica, California, July 1948.

129. Walsh, J. E. An Experimental Method for Obtaining Random Digits and Permutations. Sankhyā 17, 1956/57.

Addendum:

130. Mann, H. B. and Whitney, D. R. On a Test of Whether One of Two Random Variables is Stochastically Larger Than the Other. Ann. Math. Statist., vol. 18, 1947, p. 50.