PSEUDO-RANDOM NUMBER GENERATORS

by

LEE KIM-HUNG

A Thesis

Submitted to

the Graduate School of

The Chinese University of Hong Kong

(Division of Mathematics)

In Partial Fulfillment

of the Requirements for the Degree of

Master of Philosophy (M. Phil.)

HONG KONG

May 1978

THE CHINESE UNIVERSITY OF HONG KONG

Graduate School

The undersigned certify that we have read a thesis, entitled "Pseudo-Random Number Generators" submitted to the Graduate School by Mr. Lee Kim-Hung (李劍鏗) in partial fulfillment of the requirement for the degree of Master of Philosophy in Mathematics. We recommend that it be accepted.

Dr. N.N. Chan, Supervisor

Dr. W.L. Chan

Dr. S.Y. Lee

John Aitchison

Professor J. Aitchison
External Examiner

PREFACE

The study of the generation of random variates is mainly concerned with the uniform distribution sampling and the nonuniform distribution sampling. The former focuses on the properties of pseudo-random number generators while the latter on the techniques of generating random numbers of the required nonuniform distribution by using the pseudo-random numbers over the interval $[0, 1)$ (generated in the former). Though the two parts seem to have developed in different directions, they both aim at providing efficient methods of generating random numbers of the desired distribution that require only a small amount of computer memory but possess good statistical properties and pass most of the statistical tests. It would be even better if the methods can be easily programmed.

In this thesis, only pseudo-random number generators are dealt with. A brief description of the generators commonly in use is given in chapter 2. In chapter 3, the Fibonacci generator is considered. As the Fibonacci generator is not satisfactory, a new pseudo-random number generator is proposed in chapter 4. This generator may be written

$$y_i \equiv \alpha\, y_{i-1} + y_{i-2} \qquad (\mathrm{mod}\ \ 2^n) \ ,$$

where α is an odd integer and the initial values $y_0 = 0$ and y_1 is odd. This generator is found to be efficient and proved to possess some desirable properties. Statistical tests are applied 84 times out of which only one fails at 5 percent significance level. The generator even passes the 'sum of N' test and the 'runs up and down' test which are thought to be quite sensitive. The generator can therefore generate satisfactory pseudo-random number sequences.

I am greatly indebted to my supervisor, Dr. N.N. Chan, for his valuable advice and encouragement during my graduate study that led to the presentation of this thesis. I should also like to thank Mr. Billy Lam for his typing of the entire manuscript.

PSEUDO-RANDOM NUMBER GENERATORS

Chapter 1: Introduction

Chapter 2: Linear recurrence generators

Section 1: Linear recurrence generators

Section 2: Some well-known special cases of Linear recurrence generators

Chapter 3: Fibonacci pseudo-random number generator

Section 1: Preliminary results

Section 2: Numbers contained in the Fibonacci sequence modulo 2^n

Section 3: The serial correlation $\rho_x(s)$, when $s \equiv 1$ or $5 \pmod 6$

Section 4: The serial correlation $\rho_x(s)$, when $s \equiv 3 \pmod 6$

Chapter 4: A new generator

Section 1: Fibonacci generator and a new generator

Section 2: Statistical tests

CHAPTER 1. INTRODUCTION

In recent years, Monte Carlo and simulation methods have become a useful tool in problem solving, especially when theoretical results are hard or impossible to obtain. Hence an efficient procedure to generate a sequence of random numbers is necessary. Tables of random numbers were constructed and special physical devices were invented to produce random numbers. The most popular method in use with the aid of a computer is to set up a subroutine to generate a sequence of random numbers by a deterministic process. This kind of method is called the arithmetic method.

The first arithmetic method in pseudo-random number generation was introduced by Von Neumann in about 1946 which was known as "mid-square" method. Suppose we want to generate a sequence of t-digit integers. Given an initial integer x_o, x_i is the middle t-digit of the x_{i-1}^2 which is expressed as a 2t-digit integer, where $i = 1, 2, 3, \ldots$. For example, $t = 4$ and $x_o = 1341$. Then $x_o^2 = 01798281$ and hence $x_1 = 7982$. The sequence will be 1341, 7982, 7123, 7371, 3316, 9958, ... However, the "mid-square" method has been found to be poor.

One famous arithmetic method is to use the linear recurrence generator and will be discussed in Chapter 2. This kind of generator generates a sequence of integers $\{y_i\}$ by a linear recurrence relation

$$y_i \equiv \sum_{k=1}^{r} a_k \, y_{i-k} + b \qquad (\text{mod } M) \, .$$

When $r = 1$, we have the Lehmer congruential generator which is very commonly used. Another special case is the so called linear recurrence mod 2 method for which $M = 2$. These two special cases together with the additive random number generator are considered in section 2 of chapter 2.

In Chapter 3, we deal with an old generator - Fibonacci generator. The Fibonacci generator has the form

$$y_i \equiv y_{i-1} + y_{i-2} \qquad (\text{mod } M) .$$

Due to the strong regularities appearing in the Fibonacci pseudo-random number sequences, no much attention has been paid to this generator. Jansson (1966) gave a good study of the Fibonacci pseudo-random numbers and his work is very useful in this thesis. The numbers contained in the Fibonacci pseudo-random number sequence will be discussed in Section 2 while the serial correlation properties in Sections 3 and 4. In these sections, it is shown that under certain conditions, the exact mean, variance, and serial correlation of lag s, when s is odd, can be calculated. Moreover the computed values are all found to be reasonably close to what we expect of a "truly random" sequence.

In Chapter 4, a new generator is suggested. The new generator is strongly related to the Fibonacci generator. Hence properties of the new generator can be studied from the Fibonacci generator. The new generator may be written

$$y_i \equiv \alpha y_{i-1} + y_{i-2} \qquad (\text{mod } 2^n) ,$$

where α is an odd integer, $y_0 = 0$ and y_1 is odd. This generator passes nearly all the statistical tests given in Section 2 of Chapter 4 and is thus considered a good generator. The Lehmer congruential generator which takes the form

$$y_i \equiv \alpha y_{i-1} + b \qquad (\mathrm{mod}\ 2^n) ,$$

is similar to the new generator. One would expect that some nice properties would result if the constant b in the Lehmer congruential generator is replaced by y_{i-2} . Yet, the linear recurrence generator of order 2 (i.e. $r = 2$) is seldom discussed. The new generator proposed here is of this type and appears to be efficient for most practical purposes.

CHAPTER 2. LINEAR RECURRENCE GENERATORS

Section 1: Linear recurrence generators

A pseudo-random number generator simply means an algorithm that generates numbers $x_o, x_1, x_2, \ldots$ in the interval $[0, 1)$ such that the sequence $\{x_i\}$ behaves as if a sequence of random sample from the uniform distribution over $[0, 1)$. Of course, it is impossible to generate a "truely random" number sequence in such a deterministic procedure and hence the prefix "pseudo" is used.

Before considering pseudo-random number generators, it is convenient to introduce the following definitions.

Definition 2.1: For a sequence $\{x_i\}$, if there exist positive integers t and r such that

$$x_k = x_{k+r} \qquad \text{for all} \quad k \geq t ,$$

the sequence is said to be eventually periodic. The least such value of r is called the period of the sequence $\{x_i\}$, denoted by $p(\{x_i\})$.

Definition 2.2: A sequence $\{x_i\}$ is said to be periodic if it is eventually periodic with the corresponding t value in definition 2.1 being zero.

Definition 2.3: An integer-valued sequence $\{x_i\}$ is said to be a b-ary sequence if

$$0 \leq x_i \leq b - 1 \qquad \text{for all} \quad i = 0, 1, 2, \ldots .$$

A b-ary sequence is said to be pseudo-random if it behaves as if it is drawn from the discrete uniform distribution on $(0, 1, 2, \ldots, b-1)$.

Let $y_0, y_1, \ldots, y_{r-1}$ be non-negative integers less than a given positive integer M. A sequence $\{y_i\}$ can be defined by using the following linear recurrence relation

$$y_i \equiv a_1 y_{i-1} + a_2 y_{i-2} + \ldots + a_r y_{i-r} + b \pmod{M}, \quad i = r, r+1, \ldots \tag{2.1}$$

where $a_1, a_2, \ldots, a_{r-1}$ and b are non-negative integers, a_r and r are positive integers and $a_1, a_2, \ldots, a_r, b < M$.

Now we have an M-ary sequence $\{y_i\}$ and the required pseudo-random number sequence $\{x_i\}$ is usually defined by $x_j = \frac{y_j}{M}$ for all $j = 0, 1, 2, \ldots$. Generators of the form (2.1) are called linear recurrence generators.

Of course linear recurrence generators are not the only mechanism for generating pseudo-random numbers. They are, however, the most commonly used generators. It is obvious that the pseudo-random number sequence $\{x_i\}$ of the linear recurrence generator (2.1) satisfies the equation

$$x_i = \left\{a_1 x_{i-1} + a_2 x_{i-2} + \ldots + a_r x_{i-r} + \frac{b}{M}\right\}_F, \quad i = r, r+1, \ldots \tag{2.2}$$

Here $\{z\}_F$ stands for the fractional part of z.

The following theorem is given to indicate that linear recurrence generators may provide a reasonable source of random numbers.

<u>Theorem 2.1</u>: If $X_o, X_1, \ldots, X_{r-1}$ are independent random variables with uniform distribution over $[0, 1)$, then for any non-negative integer k the random variables $X_k, X_{k+1}, \ldots, X_{k+r-1}$, that are defined recursively by (2.2), are independent each having the uniform distribution over $[0, 1)$.

<u>Proof</u>: It is sufficient to show that $X_1, X_2, \ldots, X_r$ are independent, each having the uniform distribution over $[0, 1)$.

To prove this, it is convenient to bring forward the following equality: For any non-zero integer a and real constant c,

$$\int_o^1 e^{t\{ax + c\}_F}\, dx = \frac{1}{a}\int_c^{a+c} e^{t\{x\}_F}\, dx = \int_o^1 e^{tx}\, dx \quad . \tag{2.3}$$

Now

$$E(\exp(\sum_{i=1}^{r} t_i x_i))$$

$$= \int_o^1 \cdots \int_o^1 \exp(\sum_{i=1}^{r-1} t_i x_i + t_r\{\sum_{j=1}^{r} a_j x_{r-j} + \tfrac{b}{M}\}_F)\, dx_o \ldots dx_{r-1}$$

$$= \int_o^1 \cdots \int_o^1 \exp(\sum_{i=1}^{r-1} t_i x_i) \int_o^1 \exp(t_r\{a_r x_o + \sum_{j=1}^{r-1} a_j x_{r-j} + \tfrac{b}{M}\}_F) dx_o \ldots dx_{r-1}$$

$$= \int_o^1 \cdots \int_o^1 \exp(\sum_{i=1}^{r-1} t_i x_i) \int_o^1 \exp(t_r x_o) dx_o\, dx_1 \ldots dx_{r-1} \qquad \text{from (2.3)}$$

$$= \prod_{i=1}^{r} M(t_i)$$

where $M(t_i) = \int_o^1 \exp(t_i x) dx$.

Hence the theorem follows by the use of the properties of moment generating functions.

Q.E.D.

Theorem 2.1 cannot generatee the randomness of the pseudo-random number sequences generated by the linear recurrence generators. This is mainly because the initial values $y_0, y_1, \ldots, y_{r-1}$ in (2.1) are not in general randomly selected.

Clearly every M-ary sequence $\{y_i\}$ that satisfies (2.1) is eventually periodic with period less than or equal to M^r. Theorem 2.2 gives a sufficient condition to the periodicity of the sequence $\{y_i\}$. The proof of the theorem is simple and is therefore left out.

<u>Theorem 2.2:</u> Every sequence $\{y_i\}$ (also $\{x_i\}$) generated by (2.1) is periodic if $(a_r, M) = 1$, i.e. a_r and M are relatively prime.

An elementary requirement for (2.1) to provide a good source of pseudo-random numbers is that the pseudo-random number sequence thus generated must have long period. In determining the period of a sequence, the following theorems (Jansson, 1966; Knuth, 1968) are useful.

<u>Theorem 2.3:</u> Let $\{y_i\}$ be a sequence of non-negative integers generated by (2.1), with $M = m_1 m_2$ where $(m_1, m_2) = 1$. Then

$$p(\{y_i\}) = \text{l.c.m}\,(p(\{y_i, \bmod m_1\}), p(\{y_i, \bmod m_2\})).$$

(The symbol l.c.m(a, b) stands for the least common multiple of a and b.)

Theorem 2.4: Let $\{y_i\}$ be a sequence of non-negative integers satisfying the equation

$$y_i = a_1 y_{i-1} + a_2 y_{i-2} + \ldots + a_r y_{i-r} + b ,$$

where $a_1, a_2, \ldots, a_r$ and b are non-negative integers. Suppose

that M is a prime integer and n is a positive integer such that $M^n > 2$. Then we have, for every positive integer t,

$$p(\{y_i, \bmod M^{n+t}\}) = M^t p(\{y_i, \bmod M^n\}) \quad ,$$

provided that $p(\{y_i, \bmod M^{n+1}\}) \neq p(\{y_i, \bmod M^n\})$.

Section 2: Some well-known special cases of linear recurrence generators.

A very commonly used generator nowadays is the Lehmer congruential generator which was suggested by D.H. Lehmer in 1951. This generator is a special case of linear recurrence generator (2.1) with $r = 1$, that is

$$y_i \equiv a\, y_{i-1} + b \pmod M \quad i = 1, 2, \ldots . \tag{2.4}$$

(2.4) is said to be a mixed congruential generator if $b \neq 0$ and is said to be a multiplicative generator if $b = 0$. The numbers y_i/M are then used to form a pseudo-random number sequence.

On a binary computer, M is often chosen to be 2^n where n is the word-length of the particular computer so that the computation in (2.4) can be carried out more efficiently.

For suitable choices of a, b, M and y_o, the sequences generated by (2.4) pass most of the standard statistical tests (Gorenstein, 1967; Jansson, 1966).

The period length of the sequence has also been extensively studied (Fuller, 1976; Hull and Dobell, 1962). In particular, when $M = 2^n$ and $b \neq 0$, the maximum period length 2^n can be achieved if $a \equiv 1 \pmod 4$ and b is odd. However, when $M = 2^n$ and $b = 0$, the maximum period length will only be 2^{n-2} which is attainable when $a \equiv \pm 3 \pmod 8$ and y_o is odd.

Besides the long period length, a good serial correlation property is also necessary. Exact serial correlations have been calculated (Dieter and Ahrens, 1971; Jansson, 1966; Knuth, 1968) and found to be extremely small for most of these generators used. Moreover Dieter (1971) found that the exact joint distribution of each pair (x_i, x_{i+s}), where s is a given positive integer, was close to the desired joint distribution for most of the congruential generators that are commonly in use.

Another well-known method of generating random numbers is the linear recurrence modulo 2 method which generates a 2-ary sequence $\{y_i\}$ by the recurrence relation:

$$y_i \equiv a_1 y_{i-1} + a_2 y_{i-2} + \dots + a_r y_{i-r} \pmod 2, \quad i = r, r+1, \dots .$$

Here a_i are zero or one for all $i = 1, 2, \ldots, r$.

The sequence $\{y_i\}$ has maximum period $2^r - 1$ if and only if its characteristic polynomial $c(x) = 1 + a_1 x + a_2 x^2 + \ldots + a_r x^r$ is primitive over GF(2) , the Galois field with only two elements 0 and 1 (Zierler, 1959).

Tausworthe (1965) suggested the pseudo-random numbers x_i to be

$$x_i = \sum_{t=1}^{L} 2^{-t} y_{vi+k-t} ,$$

where k , v and L are integers such that $0 \leq k \leq 2^r - 1$, $L \leq r$, $v \geq L$ and $(v, 2^r - 1) = 1$.

Tausworthe (1965) also proved some outstanding properties of this generator when the maximum period was attained. In practice, the characteristic polynomial c(x) is chosen to be $x^p + x^q + 1$ and hence the generator usually has the form

$$y_i \equiv y_{i-q} + y_{i-p} \pmod 2 .$$

The additive random number generator is again famous. It generates the sequence $\{y_i\}$ by the equation,

$$y_i \equiv y_{i-1} + y_{i-r} \pmod M .$$

The numbers $x_i = y_i/M$ are the required pseudo-random numbers. This generator was tested to be quite satisfactory by Green, Smith and Klem (1959). However, not much theoretical results of this generator are known.

A special case of the additive random number generators is the Fibonacci pseudo-random number generator which takes the form $y_i \equiv y_{i-1} + y_{i-2} \pmod{M}$. Properties of the Fibonacci generator will be discussed in chapter 3.

CHAPTER 3. FIBONACCI PSEUDO-RANDOM NUMBER GENERATOR

Section 1: Preliminary results

The Fibonacci pseudo-random number generator is a special kind of linear recurrence generator (2 . 1) of chapter 2 with $r = 2$ and $a_1 = a_2 = 1$, that is,

$$y_i \equiv y_{i-1} + y_{i-2} \pmod{M}, \; i = 2, 3, \ldots . \tag{3.1}$$

The pseudo-random number sequence $X = \{x_i\}$ is then defined to be $\{y_i/M\}$. A sequence $\{y_i\}$ that satisfies (3.1) is then called a Fibonacci sequence mod M.

From theorem 2.2, the sequence $\{y_i\}$ is periodic whatever the value of the modulus M is. For binary computers, it is convenient to have $M = 2^n$, where n is the number of binary places available in the computer. In this case, the maximum period length of the sequence $\{y_i\}$ (also of $\{x_i\}$) is $3 \times 2^{n-1}$, denoted by H_n, which is attainable when y_o and y_1, the initial values, are not both even (Jansson, 1966). Therefore the Fibonacci generator of the following form is especially important:

$$y_{n,i} \equiv y_{n,i-1} + y_{n,i-2} \pmod{2^n}, \; i = 2, 3, \ldots , \tag{3.2}$$

with the initial values $y_{n,o}$ and $y_{n,1}$ not both even.

It is convenient to define the following equivalence relation over a set of periodic sequences.

<u>Definition 3.1</u>: Given a set A of periodic sequences, two sequences in A are said to be equivalent if one is a shift of the other. The symbol $\{s_i\} \overset{A}{\sim} \{t_i\}$ is used to mean that $\{s_i\}$ and $\{t_i\}$ in A are equivalent.

Now let A_n be the set of all possible sequences $\{y_{n,i}\}$ that are generated by (3.2). It was proved by Jansson (1966, p.63) that there exist exactly 2^{n-1} equivalence classes in A_n. Clearly if two sequences in A_n are equivalent, they have the same period, mean and serial correlation. If from each equivalence class we select one sequence, there are 2^{n-1} different sequences, say, $\{w_{n,o,i}\}, \{w_{n,1,i}\}, \ldots, \{w_{n,2^{n-1}-1,i}\}$.

Define $\bar{w}_{n,r} = \frac{1}{H_n} \sum_{i=o}^{H_n-1} w_{n,r,i}$ and $E(\bar{w}_n) = \frac{1}{2^{n-1}} \sum_{r=o}^{2^{n-1}-1} \bar{w}_{n,r}$. The term $E(\bar{w}_n)/2^n$, denoted by $E(x_n)$, is actually the expectation of the Fibonacci pseudo-random numbers, $x_{n,i}$ $(x_{n,i} = y_{n,i}/2^n)$, generated by (3.2). The value of $E(x_n)$ can be found by simple calculation as follow.

$$\begin{aligned} \sum_{r=o}^{2^{n-1}-1} \bar{w}_{n,r} &= \frac{1}{H_n} \sum_{r=o}^{2^{n-1}-1} \sum_{i=o}^{H_n-1} w_{n,r,i} \\ &= \frac{1}{3 \times 2^{n-1}} [2^{n-1} \sum_{k=o}^{2^{n-1}-1} 2k + 2^n \sum_{k=o}^{2^{n-1}-1} (2k+1)] \\ &= 2^{2n-2} - 2^{n-1}/3 \ . \end{aligned}$$

It follows that

$$E(x_n) = E(\bar{w}_n)/2^n = \frac{1}{2} - \frac{1}{3 \times 2^n} \approx \frac{1}{2} \quad . \tag{3.3}$$

Similarly, let $\overline{w^2_{n,r}} = \frac{1}{H_n}\sum_{i=o}^{H_n-1} w^2_{n,r,i}$, $E(\overline{w}_n^{\,2}) = \frac{1}{2^{n-1}}\sum_{r=o}^{2^{n-1}-1} \overline{w}^2_{n,r}$

and $$E(x_n^2) = E(\overline{w}_n^{\,2})/2^{2n} .$$

Then

$$\sum_{r=o}^{2^{n-1}-1} \overline{w^2_{n,r}} = \frac{1}{H_n}\sum_{r=o}^{2^{n-1}-1}\sum_{i=o}^{H_n-1} w^2_{n,r,i}$$

$$= \frac{1}{3 \times 2^{n-1}}\left[2^{n-1}\sum_{k=o}^{2^{n-1}-1}(2k)^2 + 2^n\sum_{k=o}^{2^{n-1}-1}(2k+1)^2\right]$$

$$= 2^{2n-1}(2^n - 1)/3 .$$

Hence

$$E(x_n^{\,2}) = \frac{1}{2^{2n}}E(\overline{w}_n^{\,2}) = \frac{1}{3} - \frac{1}{3 \times 2^n} \approx \frac{1}{3} . \qquad (3.4)$$

It is found that the values $E(x_n)$ and $E(x_n^{\,2})$ are reasonably close to what we expect of a "truely random" sequence. The properties of each individual sequence will be discussed in the following sections.

Section 2: Numbers contained in the Fibonacci sequence mod 2^n

In order to find out the numbers contained in an individual sequence in A_n , we assume, without loss of generality, that $w_{n,r,o} = 2r$ and $w_{n,r,1} = 1$ (Jansson, 1966). Moreover for $r \geq 2^{n-1}$, we define $\{w_{n,r,i}\} = \{w_{n,r(\text{mod } 2^{n-1}),i}\}$.

Lemma 3.1, 3.2, 3.3, 3.5 and theorem 3.4 that can be found in Jansson (1966), are very useful for the later work.

Lemma 3.1: $w_{n,r,i}$ is even if and only if $i \equiv 0 \pmod 3$.

Lemma 3.2: $w_{n,r,i} \equiv w_{n,o,i} + 2rw_{n,o,i-1} \pmod{2^n}$.

Lemma 3.3: $w_{n,o,i+j} \equiv w_{n,o,i-1}\, w_{n,o,j} + w_{n,o,i}\, w_{n,o,j+1} \pmod{2^n}$.

Theorem 3.4:
$$w_{n,r,\frac{H_n}{2}+v} = \begin{cases} w_{n,r,v} & \text{when } v \equiv 0 \pmod 3 \\ 2^{n-1} + w_{n,r,v} \pmod{2^n} & \text{when } v \not\equiv 0 \pmod 3, \end{cases}$$

when $n \geq 3$.

Lemma 3.5: For $n \geq 4$,

$$w_{n,r,\frac{H_n}{4}+6v} \equiv w_{n,r,6v} + (r+1)2^{n-1} \pmod{2^n},$$

and
$$w_{n,r,\frac{H_n}{4}+6v+3} \equiv w_{n,r,6v+3} + r\,2^{n-1} \pmod{2^n}.$$

Define a integer-valued function ψ_n on A_n such that, for all $\{y_{n,i}\} \in A_n$,

$$\psi_n(\{y_{n,i}\}) = r \quad \text{if} \quad \{y_{n,i}\} \overset{A_n}{\sim} \{w_{n,r,i}\}.$$

Theorem 3.6 is another useful theorem of Jansson (1966). The expression of the theorem is different from the original in order to suit our requirements. The notation $\text{freq}_{n,Y}(x)$ means the frequency of x in a periodic 2^n-ary sequence Y over the entire period and in general $\text{freq}_n(x)$ is used when the sequence Y is understood.

Theorem 3.6: For any $Y = \{y_{n,i}\} \in A_n$, with $n \geq 2$, we have

$$\mathrm{freq}_{n,Y}(2k+1) = \begin{cases} 3 & \text{if } k \text{ is even} \\ 1 & \text{if } k \text{ is odd} \end{cases}, \quad k = 0, 1, 2, \ldots, 2^{n-1}-1,$$

if $\psi_2(\{y_{n,i}, \bmod 2^2\}) = 0$. Also we have

$$\mathrm{freq}_{n,Y}(2k+1) = \begin{cases} 1 & \text{if } k \text{ is even} \\ 3 & \text{if } k \text{ is odd} \end{cases}, \quad k = 0, 1, 2, \ldots, 2^{n-1}-1,$$

if $\psi_2(\{y_{n,i}, \bmod 2^2\}) = 1$.

Applying lemma 3.5, we have

Lemma 3.7: For $n \geq 4$, we have

$$2\left(w_{n,r,\frac{H_n}{4}+3k} - w_{n,r,3k}\right) \equiv w_{n+1,r,\frac{H_{n+1}}{4}+3k} - w_{n+1,r,3k} \pmod{2^{n+1}}. \quad (3.5)$$

Proof: Let $k = 2v + t$, where $t = 0$ or 1.

Suppose $t = 0$. Applying lemma 3.5, we have

$$w_{n,r,6v+\frac{H_n}{4}} - w_{n,r,6v} \equiv (r+1)2^{n-1} \pmod{2^n}.$$

It implies that

$$2\left(w_{n,r,6v+\frac{H_n}{4}} - w_{n,r,6v}\right) \equiv (r+1)2^n \pmod{2^{n+1}}.$$

From lemma 3.5, we have

$$w_{n+1,r,6v+\frac{H_{n+1}}{4}} - w_{n+1,r,6v} \equiv (r+1)2^n \pmod{2^{n+1}}.$$

Therefore we have

$$2\left(w_{n,r,6v+\frac{H_n}{4}} - w_{n,r,6v}\right) \equiv w_{n+1,r,6v+\frac{H_{n+1}}{4}} - w_{n+1,r,6v} \pmod{2^{n+1}} .$$

Hence the lemma is true when $k = 2v$. Similarly, the lemma can be proved when $k = 2v + 1$ by applying lemma 3.5.

Q.E.D.

Remark: It is obvious from lemma 3.7 that when $n \geq 4$, we have

$$w_{n,r,3k+\frac{H_n}{4}} = w_{n,r,3k} \text{ if and only if } w_{n+1,r,3k+\frac{H_{n+1}}{4}} = w_{n+1,r,3k} . \quad (3.6)$$

Lemma 3.8: If $n \geq 4$, then

$$w_{n,o,\frac{H_n}{8}} = 2^{n-2} ,$$

$$w_{n,o,\frac{H_n}{8}-1} = 1 + 7 \times 2^{n-3} ,$$

and $$w_{n,o,\frac{H_n}{8}+1} = 1 + 2^{n-3} .$$

Proof: For $n = 7$, $w_{7,o,\frac{H_7}{8}} = 32$, $w_{7,o,\frac{H_7}{8}-1} = 113$ and $w_{7,o,\frac{H_7}{8}+1} = 17$.

Hence the lemma is true when $n = 7$.

Suppose the lemma holds when $n = \alpha$ where $\alpha \geq 7$. We have

$$w_{\alpha+1,o,\frac{H_{\alpha+1}}{8}} = w_{\alpha+1,o,2\frac{H_\alpha}{8}}$$

$$\equiv w_{\alpha+1,o,\frac{H_\alpha}{8}} \left(w_{\alpha+1,o,\frac{H_\alpha}{8}-1} + w_{\alpha+1,o,\frac{H_\alpha}{8}+1}\right) \pmod{2^{\alpha+1}} \text{ from lemma 3.3.}$$

$$\equiv \left(w_{\alpha,o,\frac{H_\alpha}{8}} + \beta_1 2^\alpha\right)\left(w_{\alpha,o,\frac{H_\alpha}{8}-1} + w_{\alpha,o,\frac{H_\alpha}{8}+1} + \beta_2 2^\alpha\right) \pmod{2^{\alpha+1}}$$

for some integers β_1 and β_2,

$$\equiv (2^{\alpha-2} + \beta_1 2^\alpha)(1 + 7 \times 2^{\alpha-3} + 1 + 2^{\alpha-3} + \beta_2 2^\alpha) \pmod{2^{\alpha+1}}$$

$$\equiv 2^{\alpha-1} \pmod{2^{\alpha+1}}$$

$$= 2^{\alpha-1} \quad .$$

And $w_{\alpha+1,o,\frac{H_{\alpha+1}}{8}-1} = w_{\alpha+1,o,\frac{H_\alpha}{8}+\frac{H_\alpha}{8}-1}$

$$\equiv w^2_{\alpha+1,o,\frac{H_\alpha}{8}-1} + w^2_{\alpha+1,o,\frac{H_\alpha}{8}} \pmod{2^{\alpha+1}}, \text{from lemma 3.3.}$$

$$\equiv (1 + 7 \times 2^{\alpha-3} + \beta_1 2^\alpha)^2 + (2^{\alpha-2} + \beta_2 2^\alpha)^2 \pmod{2^{\alpha+1}}$$

for some integers β_1 and β_2,

$$= 1 + 7 \times 2^{\alpha-2} \quad .$$

Similarly, we have

$$w_{\alpha+1,o,\frac{H_{\alpha+1}}{8}+1} = w_{\alpha+1,o,\frac{H_\alpha}{8}+1+\frac{H_\alpha}{8}}$$

$$\equiv w^2_{\alpha+1,o,\frac{H_\alpha}{8}} + w^2_{\alpha+1,o,\frac{H_\alpha}{8}+1} \pmod{2^{\alpha+1}}, \text{from lemma 3.3.}$$

$$\equiv (2^{\alpha-2} + \beta_1 2^\alpha)^2 + (1 + 2^{\alpha-3} + \beta_2 2^\alpha)^2 \pmod{2^{\alpha+1}}$$

for some integers β_1 and β_2,

$$= 1 + 2^{\alpha-2} \quad .$$

Hence the lemma is proved by induction.

Q.E.D.

From lemma 3.2 and 3.3, we have

$$w_{n,r,3v+\frac{H_n}{8}} \equiv w_{n,o,3v+\frac{H_n}{8}} + 2r\, w_{n,o,3v+\frac{H_n}{8}-1} \pmod{2^n}\text{, from lemma 3.2.}$$

$$\equiv w_{n,o,3v-1}\, w_{n,o,\frac{H_n}{8}} + w_{n,o,3v}\, w_{n,o,\frac{H_n}{8}+1}$$

$$+ 2r(w_{n,o,\frac{H_n}{8}-1}\, w_{n,o,3v-1} + w_{n,o,\frac{H_n}{8}}\, w_{n,o,3v}) \pmod{2^n}$$

, from lemma 3.3.

$$\equiv w_{n,o,3v-1}(w_{n,o,\frac{H_n}{8}} + 2r\, w_{n,o,\frac{H_n}{8}-1})$$

$$+ w_{n,o,3v}(w_{n,o,\frac{H_n}{8}+1} + 2r\, w_{n,o,\frac{H_n}{8}}) \pmod{2^n}\ . \qquad (3.7)$$

When $n \geq 7$, it follows from lemma 3.8 that

$$w_{n,r,3v+\frac{H_n}{8}} \equiv w_{n,o,3v-1}[2^{n-2} + 2r(1 + 7 \times 2^{n-3})]$$

$$+ w_{n,o,3v}[1 + 2^{n-3} + 2r(2^{n-2})] \pmod{2^n}$$

$$\equiv w_{n,o,3v} + 2r\, w_{n,o,3v-1} + w_{n,o,3v}(2^{n-3} + 2^{n-1}r)$$

$$+ w_{n,o,3v-1}[2^{n-2} + 2r(7 \times 2^{n-3})] \pmod{2^n}$$

$$\equiv w_{n,r,3v} + 2^{n-3} w_{n,o,3v}(1 + 4r)$$

$$+ 2^{n-2}\, w_{n,o,3v-1}(1 + 7r) \pmod{2^n}$$

$$\equiv w_{n,r,3v} + 2^{n-3} w_{n,o,3v} + 2^{n-2} w_{n,o,3v-1}(1 + 3r) \pmod{2^n}. \qquad (3.8)$$

Using the equation (3.8), we have the following lemma.

<u>Lemma 3.9</u>: When $n \geq 6$, we have

$$w_{n,r,3v+\frac{H_n}{8}} = w_{n,r,3v} \text{ if and only if } w_{n+1,r,3v+\frac{H_{n+1}}{8}} = w_{n+1,r,3v} .$$

<u>Proof:</u> When $n = 6$, we have $w_{6,o,\frac{H_6}{8}} = 16$, $w_{6,o,\frac{H_6}{8}-1} = 25$ and $w_{6,o,\frac{H_6}{8}+1} = 41$.

$$\therefore \quad w_{6,r,3v+\frac{H_6}{8}}$$

$$\equiv w_{6,o,3v-1}\left(w_{6,o,\frac{H_6}{8}} + 2r\, w_{6,o,\frac{H_6}{8}-1}\right) + w_{6,o,3v}\left(w_{6,o,\frac{H_6}{8}+1} + 2r\, w_{6,o,\frac{H_6}{8}}\right)$$

$$(\text{mod } 2^6)\text{ , from (3.7).}$$

$$\equiv w_{6,r,3v} + 8w_{6,o,3v}(5 + 4r) + 16w_{6,o,3v-1}(1 + 3r) \qquad (\text{mod } 2^6)$$

$$\equiv w_{6,r,3v} + 8w_{6,o,3v} + 16w_{6,o,3v-1}(1 + 3r) \qquad (\text{mod } 2^6) .$$

Hence it follows that (3.8) is true when $n = 6$. Therefore when $n \geq 6$, we have

$$w_{n,r,3v+\frac{H_n}{8}} = w_{n,r,3v}$$

$$\Leftrightarrow \quad 2^{n-3}w_{n,o,3v} + 2^{n-2}w_{n,o,3v-1}(1 + 3r) \equiv 0 \qquad (\text{mod } 2^n)$$

$$\Leftrightarrow \quad 2^{n-2}w_{n,o,3v} + 2^{n-1}w_{n,o,3v-1}(1 + 3r) \equiv 0 \qquad (\text{mod } 2^{n+1})$$

$$\Leftrightarrow \quad 2^{n-2}w_{n+1,o,3v} + 2^{n-1}w_{n+1,o,3v-1}(1 + 3r) \equiv 0 \qquad (\text{mod } 2^{n+1})$$

$$\Leftrightarrow \quad w_{n+1,r,3v+\frac{H_{n+1}}{8}} = w_{n+1,r,3v} \qquad \text{, from (3.8)}$$

Q.E.D.

The frequency of an odd number in a full period can be easily found by the use of theorem 3.6. In order to find out the frequency of a given even number, the following terms are introduced. Define

$$V_{n,r,1} = \{v : 0 \leq v \leq 2^{n-1} - 1 \text{ and } w_{n,r,3v} \neq w_{n,r,3v+\frac{H_n}{4}}\} ,$$

$$V_{n,r,2} = \{v : 0 \leq v \leq 2^{n-1} - 1 ;\ w_{n,r,3v} = w_{n,r,3v+\frac{H_n}{4}} \text{ and } w_{n,r,3v} \neq w_{n,r,3v+\frac{H_n}{8}}\} ,$$

and $V_{n,r,3} = \{v : 0 \leq v \leq 2^{n-1} - 1 \; ; \; w_{n,r,3v} = w_{n,r,3v+\frac{H_n}{4}}$

$\qquad\qquad$ and $w_{n,r,3v} = w_{n,r,3v+\frac{H_n}{8}} \}$.

The sets $V_{n,r,j}$ and $V_{n+1,r,j}$ where $j = 1, 2,$ or 3 are related in the following sense. This is an immediate consequence of theorem 3.4, lemma 3.9 and (3.6).

<u>Lemma 3.10</u>: For $n \geq 6$,

$$V_{n+1,r,j} = \{v : v \in V_{n,r,j} \quad \text{or} \quad v - 2^{n-1} \in V_{n,r,j}\} ,$$

where $j = 1, 2$ or 3.

Lemma 3.10 enables us to find out $V_{n,r,j}$, where $n \geq 7$, from $V_{6,r,j}$. By numerical inspection, it is found that either $V_{6,r,2}$ or $V_{6,r,3}$ must be empty. Moreover, when $0 \leq v < 2^5$, $v \in V_{6,r,1}$ if and only if $v \pm 1 \notin V_{6,r,1}$. Given that $w_{6,r,3v} = 0$ where $0 \leq v < 2^5$, we have $v \in V_{6,r,1}$. These facts evidence the following results:

$$\begin{aligned}
&1. \quad V_{n,r,2} = \phi \text{ if and only if } V_{n,r,3} \neq \phi \text{ when } n \geq 6 . \\
&2. \quad \text{When } 0 \leq v < 2^{n-1} ,\ v \in V_{n,r,1} \text{ if and only if } v \pm 1 \notin V_{n,r,1} . \qquad (3.9) \\
&3. \quad \text{When } 0 \leq v < 2^{n-1} , \text{ we have } v \in V_{n,r,1} \text{ if } w_{n,r,3v} = 0 .
\end{aligned}$$

The above relations are simple but useful in the following sections.

The notation $freq_{n,r,j}(x)$ is used to denote the value of $\sum_{v \in V_{n,r,j}} \chi_{\{x\}} (w_{n,r,3v})$ where $j = 1, 2$ or 3. ($\chi_{\{x\}}$ is the indicator function of $\{x\}$.). It is obvious that $freq_{n,w}(2k) = \sum_{j=1}^{3} freq_{n,r,j}(2k)$, where $w = \{w_{n,r,i}\}$. Using these notations, we have

Lemma 3.11: For $n \geq 6$,

$$freq_{n+1,r,1}(x) = freq_{n+1,r,1}(x + 2^n) = freq_{n,r,1}(x) ,$$

where $0 \leq x \leq 2^n - 2$.

Proof: Clearly we have when $0 \leq x \leq 2^n - 2$,

$$freq_{n+1,r,1}(x) + freq_{n+1,r,1}(x + 2^n) = 2\ freq_{n,r,1}(x) . \tag{3.10}$$

Suppose $v \in V_{n,r,1}$. Let $v^* \equiv v + 2^{n-3} \pmod{2^{n-1}}$. It is obvious that $v^* \in V_{n,r,1}$. Since

$$w_{n+1,r,3v} \not\equiv w_{n+1,r,3v^*} \pmod{2^{n+1}} ,$$

we have

$$freq_{n+1,r,1}(x) = freq_{n+1,r,1}(x + 2^n) ,$$

where $0 \leq x \leq 2^n - 2$. From (3.10), it follows that

$$freq_{n+1,r,1}(x) = freq_{n+1,r,1}(x + 2^n) = freq_{n,r,1}(x) ,$$

where $0 \leq x \leq 2^n - 2$.

Q.E.D.

Lemma 3.12: For $n \geq 6$,

$$\mathrm{freq}_{n+1,r,2}(x) = \mathrm{freq}_{n+1,r,2}(x + 2^n) = \mathrm{freq}_{n,r,2}(x) ,$$

where $0 \leq x \leq 2^n - 2$.

Proof: Similar to the proof of lemma 3.11, we have for $0 \leq x \leq 2^n - 2$,

$$\mathrm{freq}_{n+1,r,2}(x) + \mathrm{freq}_{n+1,r,2}(x + 2^n) = 2\ \mathrm{freq}_{n,r,2}(x) . \qquad (3.11)$$

Suppose $v \in V_{n,r,2}$ and $v^* \equiv v + 2^{n-3} \pmod{2^{n-1}}$. It is not difficult to show that $v^* \in V_{n,r,2}$. For every pair v and v^* in $V_{n,r,2}$, we have

$$w_{n+1,r,3v} = w_{n+1,r,3v+\frac{H_{n+1}}{4}} \nleftrightarrow w_{n+1,r,3v^*} = w_{n+1,r,3v^*+\frac{H_{n+1}}{4}} ,$$

and

$$w_{n+1,r,3v} \equiv w_{n+1,r,3v^*} \pmod{2^n} .$$

Hence

$$\mathrm{freq}_{n+1,r,2}(x) = \mathrm{freq}_{n+1,r,2}(x + 2^n) ,$$

where $0 \leq x \leq 2^n - 2$. From (3.11), it follows that

$$\mathrm{freq}_{n+1,r,2}(x) = \mathrm{freq}_{n+1,r,2}(x + 2^n) = \mathrm{freq}_{n,r,2}(x) ,$$

where $0 \leq x \leq 2^n - 2$.

Q.E.D.

By induction on lemma 3.11 and lemma 3.12, we obtain the following lemma.

Lemma 3.13: For $n \geq 6$,

$$\mathrm{freq}_{n,r,1,2}(x) = \mathrm{freq}_{6,r,1,2}(x) ,$$

where $y \equiv x \pmod{2^6}$.

($freq_{n,r,1,2}(x)$ stands for the expression $\sum_{v \in V_{n,r,1} \cup V_{n,r,2}} \chi\{x\}(w_{n,r,3v})$.)

It is desirable that a "truely random" 2^n-ary sequence should have the property that for any pair of integers M and N such that $0 \leq M$, $N < 2^n$, M and N should have equal frequency of occurring in the sequence. Therefore the value

$$\max_{0 \leq x < 2^n} freq_n(x) - \min_{0 \leq x < 2^n} freq_n(x)$$

can be used to "measure" the randomness of a 2^n-ary sequence $\{w_{n,r,i}\}$. For any Fibonacci sequence mod 2^n, $\{w_{n,r,i}\}$, it can be shown that when $n \geq 6$,

$$\min_{0 \leq x < 2^n} freq_n(x) = 0 .$$

From theorem 3.6, we have

$$\max_{\substack{0 \leq x < 2^n \\ x \text{ is odd}}} freq_n(x) = 3 .$$

From lemma 3.13, we have

$$\max_{0 \leq x < 2^n} freq_{n,r,1,2}(x) = \max_{0 \leq x < 2^6} freq_{6,r,1,2}(x) \leq 8 .$$

However the value $\max_{0 \leq x < 2^n} freq_{n,r,3}(x)$ is likely to increase as n increases, when $V_{n,r,3}$ is non-empty. Table 3.1 gives the values of $\max_{0 \leq x < 2^6} freq_{n,r,3}(x)$ for some values of n and r and table 3.2 shows $freq_{n,r,3}(x)$ for some values of n and x. Both tables 3.1 and 3.2 evidence that the presence of $V_{n,r,3}$ will make the value of

$$\max_{0 \leq x < 2^n} freq_n(x) - \min_{0 \leq x < 2^n} freq_n(x)$$

increase . Hence the choice of r such that $V_{n,r,3} = \phi$ is preferred.

Table 3.1

n	6	7	8	9	10	11	12
r	1	1	1	1	1	1	1
$\max_{0 \leq x < 2^n} \mathrm{freq}_{n,r,3}(x)$	8	16	16	32	32	64	64
Values of x that have maximum frequency	2,18	18	2,18,66,146	322	2,258,322,834	1282	2,1062,1282,3330
n	6	7	8	9	10	11	12
r	5	5	5	5	5	5	5
$\max_{0 \leq x < 2^n} \mathrm{freq}_{n,r,3}(x)$	8	16	16	32	32	64	64
Values of x that have maximum frequency	10,58	10	10,58,122,138	122	58,122,314,634	314	58,314,1082,2362
n		7	8	9	10	11	12
r		33	33	33	33	33	33
$\max_{0 \leq x < 2^n} \mathrm{freq}_{n,r,3}(x)$		16	16	32	32	64	64
Values of x that have maximum frequency		82	66,82,130, 210	386	66,322,386,898	322	66,322,2370,3138
n			8	9	10	11	12
r			29	29	29	29	29
$\max_{0 \leq x < 2^n} \mathrm{freq}_{n,r,3}(x)$			16	32	32	64	64
Values of x that have maximum frequency			42,58,186,234	298	298,746,810,1002	1002	746,1002,1770,3050

Table 3.2

r = 1

n	6	7	8	9	10	11	12	13	14	20
$freq_{n,r,3}(2)$	8	8	16	16	32	32	64	64	128	1024

n	10	11	12	13	14	15	16
$freq_{n,r,3}(746)$	32	32	64	64	128	256	256

From lemma 3.10 and the direct calculation of $V_{6,r,3}$, we find that $V_{n,r,3} = \phi$ if and only if $r \equiv 0$ or $3 \pmod 4$, when $n \geqslant 6$. Therefore it seems suitable to choose r such that $r \equiv 0$ or $3 \pmod 4$. This suggestion coincides with the idea of Jansson (1966). Now under the condition $r \equiv 0$ or $3 \pmod 4$, we have

$$freq_6(x) = freq_6(x + 2^5) = freq_5(x) ,$$

where $0 \leqslant x < 2^5$. Hence we have the following result.

<u>Theorem 3.14</u>: For $n \geqslant 5$, $\{y_{n,i}\}$ is a Fibonacci sequence mod 2^n such that at least one of the initial values is odd. If

$$\psi_5(\{y_{n,i} \bmod 2^5\}) = 0, 3, 4, 7, 8, 11, 12 \text{ or } 15$$

then

$$freq_n(x) = freq_5(t)$$

where $t \equiv x \pmod{2^5}$, $0 \leqslant x < 2^n$ and $freq_5(t)$ means the frequency of t in $\{y_{n,i} \bmod 2^5\}$ over the entire period.

Note that $freq_5(2k + 1)$ in theorem 3.14 can be calculated from theorem 3.6 and

$$\text{freq}_5\,(2k) = \begin{cases} 2 & \text{if } 2k = 0,\ 8,\ 16,\ 24 \\ 8 & \text{if } 2k = t_r\text{, where } r = \psi_5(\{y_{n,i} \bmod 2^5\}) \\ 0 & \text{otherwise} \end{cases} .$$

The values of t_r are listed in the following table.

Table 3.3: Values of t_r

r	0	3	4	7	8	11	12	15
t_r	2	6	10	14	18	22	26	30

Jansson (1966) constructed a table of subperiods from which theorem 3.14 can be deduced. However the proof of the table was not given and the restriction on n was not clearly stated.

Under the conditions of theorem 3.14, the sum of $y_{n,i}$ and $y^2_{n,i}$ over the whole period can be calculated exactly. If $k \leqslant n$, $\{y_{k,i}\}$ is defined by the equation $y_{k,i} \equiv y_{n,i} \pmod{2^k}$. Clearly $\{y_{k,i}\} \in A_k$.

<u>Corollary 3.15</u>: Under the conditions of theorem 3.14, we have

$$\sum_{i=0}^{H_n-1} y_{n,i} = 2^{n-k} \sum_{i=0}^{H_k-1} y_{k,i} + 3 \times 2^{n-2}(2^n - 2^k) \qquad (3.12)$$

$$\sum_{i=0}^{H_n-1} y^2_{n,i} = 2^{n-k} \sum_{i=0}^{H_k-1} y^2_{k,i} + 2^n(2^{n-k} - 1) \sum_{i=0}^{H_k-1} y_{k,i} + 2^n(2^n - 2^k)(2^{n-1} - 2^{k-2}) \qquad (3.13)$$

where $n \geqslant k \geqslant 5$.

<u>Proof</u>: The proof is obvious because from theorem 3.14, we have

$$\sum_{i=o}^{H_n-1} y_{n,i} = 2\sum_{i=o}^{H_{n-1}-1} y_{n-1,i} + 2^{n-1}H_{n-1}$$

and
$$\sum_{i=o}^{H_n-1} y_{n,i}^2 = \sum_{i=o}^{H_{n-1}-1} y_{n-1,i}^2 + \sum_{i=o}^{H_{n-1}-1} (y_{n-1,i} + 2^{n-1})^2 .$$

Q.E.D.

The values of $\sum_{i=o}^{H_5-1} y_{5,i}$ and $\sum_{i=o}^{H_5-1} y_{5,i}^2$ for some values of r are given in table 3.4.

Table 3.4: Values of $\sum_{i=o}^{H_5-1} y_{5,i}$ and $\sum_{i=o}^{H_5-1} y_{5,i}^2$ for some values of r

r	0	3	4	7	8	11	12	15
$\sum_{i=o}^{H_{5-1}} y_{5,i}$	608	672	672	736	736	800	800	864
$\sum_{i=o}^{H_5-1} y_{5,i}^2$	12224	13504	12992	14784	14784	17088	17600	20416

<u>Example</u>: Consider the Fibonacci generator $y_{10,i} \equiv y_{10,i-1} + y_{10,i-2} \pmod{2^{10}}$. Given $y_{10,0} = 38$ and $y_{10,1} = 85$, it can be found that

$$\psi_5(\{y_{5,i}\}) = 3 .$$

Using corollary 3.15 with $k = 5$, we have

$$\sum_{i=o}^{H_{10}-1} y_{10,i} = 2^{10-5} \times 672 + 3 \times 2^8(2^{10} - 2^5) \text{, from table 3.4}$$

$$= 783360$$

$$\sum_{i=o}^{H_{10}-1} y_{10,i}^2 = 2^{10-5} \times 13504 + 2^{10}(2^{10-5} - 1) \times 672 \quad \text{, from table 3.4}$$

$$+ 2^{10}(2^{10} - 2^5)(2^{10-1} - 2^{5-2})$$

$$= 533731328 \text{ .}$$

Hence the mean and variance of the pseudo-random numbers $x_{10,i}$ $(x_{10,i} = y_{10,i}/2^{10})$ are

$$E(x_{10,i}) = \frac{1}{H_{10}} \sum_{i=o}^{H_{10}-1} y_{10,i}/2^{10}$$

$$= 783360 / (3 \times 2^{19})$$

$$= 0.498046875$$

and

$$\text{var}(x_{10,i}) = \frac{1}{H_{10}} [\sum_{i=o}^{H_{10}-1} y_{10,i}^2 / 2^{20} - \frac{1}{H_{10}} (\sum_{i=o}^{H_{10}-1} y_{10,i} / 2^{10})^2]$$

$$= \frac{1}{3 \times 2^9} (\frac{533731328}{2^{20}} - \frac{783360^2}{3 \times 2^{29}})$$

$$= 0.083333333 \text{ .}$$

Following directly from corollary 3.15 and table 3.4, we obtain lower and upper bounds for $E(x_{n,i})$ and $E(x_{n,i}^2)$:

<u>Corollary 3.16</u>: Under the conditions of theorem 3.14, we have

$$-\frac{5}{3}\, 2^{1-n} \leq E(x_{n,i}) - 0.5 \leq 2^{1-n} \quad \text{and}$$

$$5 \times 2^{2-2n} - \frac{5}{3}\, 2^{1-n} \leq E(x_{n,i}^2) - \frac{1}{3} \leq 5 \times 2^{2-2n} + 2^{1-n} \text{ .}$$

Now consider another Fibonacci generator

$$y_{10,i} \equiv y_{10,i-1} + y_{10,i-2} \qquad (\text{mod } 2^{10})$$

with $y_{10,0} = 25$ and $y_{10,1} = 28$. It is found that $\{y_{10,i}\}$ does not satisfy the conditions of theorem 3.14 ($\psi_5(\{y_{5,i}\}) \not\equiv 0$ or 3 (mod 4)). The corresponding values are

$$\sum_{i=o}^{H_{10}-1} y_{10,i} = 760832 \quad \text{and} \quad \sum_{i=o}^{H_{10}-1} y_{10,i}^2 = 508585984 \ .$$

Thus

$$E(x_{10,i}) = 0.483723958 < 0.5 - \frac{5}{3}\,2^{-9} = 0.496744792 \ .$$

$$E(x_{10,i}^2) = 0.315771739 < \frac{1}{3} + 5 \times 2^{-18} - \frac{5}{3}\,2^{-9} = 0.330097198 \ .$$

Both $E(x_{10,i})$ and $E(x_{10,i}^2)$ are less than the corresponding lower bounds stated in corollary 3.16.

Section 3: The serial correlation $\rho_x(s)$, when $s \equiv 1$ or 5 (mod 6).

Sections 3 and 4 are concerned with certain serial correlation properties of the Fibonacci pseudo-random numbers. First of all, we give the definition of serial correlation of a periodic pseudo-random number sequence.

Definition 3.2: Let $x = \{x_i\}$ be a periodic pseudo-random number sequence with period H . The serial correlation of lag s , say $\rho_x(s)$, is defined as

$$\rho_x(s) = \{ \frac{1}{H}\sum_{i=o}^{H-1} x_i x_{i+s} - \frac{1}{H^2} (\sum_{i=o}^{H-1} x_i)^2\}/\{ \frac{1}{H}\sum_{i=0}^{H-1} x_i^2 - \frac{1}{H^2} (\sum_{i=o}^{H-1} x_i)^2\} \ .$$

Let $\{y_{n,i}\}$ be in A_n such that the conditions of theorem 3.14 are satisfied. The sequence $\{y_{k,i}\}$ where $k \leq n$ is defined by equation

$y_{k,i} \equiv y_{n,i} \pmod{2^k}$. In studying the serial correlation of $x = \{x_{n,i}\}$ ($\{x_{n,i}\} = \{y_{n,i}/2^n\}$), the main difficulty is that of finding out the value of $\sum_{i=0}^{H_n - 1} y_{n,i} y_{n,i+s}$. In this section, we consider $\rho_x(s)$ only for $s \equiv 1$ or $5 \pmod 6$ and $n \geq 7$. Since $s \not\equiv 0 \pmod 3$, $y_{n-1,i}$ and $y_{n-1,i+s}$ cannot be both even; we are left with the three equally likely cases:

case I : Both $y_{n-1,i}$ and $y_{n-1,i+s}$ are odd.

case II: $y_{n-1,i}$ is odd and $y_{n-1,i+s}$ is even.

case III: $y_{n-1,i}$ is even and $y_{n-1,i+s}$ is odd.

Now we consider the three cases individually.

<u>Case I</u>: Assume $y_{n-1,i}$ and $y_{n-1,i+s}$ are odd, where $0 \leq i < H_{n-1}$. Then $y_{n,i}$ and $y_{n,i+s}$ must belong to one of the following subcases:

case Ia) $\quad y_{n,i} - y_{n-1,i} = y_{n,i+s} - y_{n-1,i+s}$ (3.14)

case Ib) $\quad y_{n,i} - y_{n-1,i} \not\equiv y_{n,i+s} - y_{n-1,i+s}$ (3.15)

In case Ia),

$$
\begin{aligned}
& y_{n,i}\, y_{n,i+s} + y_{n,i+\frac{H_n}{2}}\, y_{n,i+\frac{H_n}{2}+s} \\
= \; & y_{n-1,i}\, y_{n-1,i+s} + (y_{n-1,i} + 2^{n-1})(y_{n-1,i+s} + 2^{n-1}) \\
= \; & 2y_{n-1,i}\, y_{n-1,i+s} + (y_{n-1,i} + y_{n-1,i+s})2^{n-1} + 2^{2n-2} \,. \qquad (3.16)
\end{aligned}
$$

In case Ib),

$$
y_{n,i}\, y_{n,i+s} + y_{n,i+\frac{H_n}{2}}\, y_{n,i+\frac{H_n}{2}+s}
$$

$$= y_{n-1,i}(y_{n-1,i+s} + 2^{n-1}) + y_{n-1,i+s}(y_{n-1,i} + 2^{n-1})$$

$$= 2\, y_{n-1,i}\, y_{n-1,i+s} + (y_{n-1,i} + y_{n-1,i+s})2^{n-1} \quad . \qquad (3.17)$$

The only difference between (3.16) and (3.17) is the term 2^{2n-2}. The problem is then to find out how many i's, $0 \leq i < H_{n-1}$ are such that $y_{n-1,i}$ and $y_{n-1,i+s}$ are odd and that (3.14) is satisfied. To do this, the following lemmas are necessary.

<u>Lemma 3.17</u>: Let $\{y_{n,i}\}$ be a Fibonacci sequence mod 2^n with initial values $y_{n,o} = 0$ and $y_{n,1}$ being odd. Then for any non-negative integer t,

$$y_{n,\frac{H_n}{2}-t} \equiv (-1)^{t-1}\, y_{n,t} + \alpha_t\, 2^{n-1} \pmod{2^n}$$

where

$$\alpha_t = \begin{cases} 0 & \text{if } t \equiv 0 \pmod 3 \\ 1 & \text{if } t \not\equiv 0 \pmod 3 \end{cases} \quad .$$

<u>Proof</u>: From theorem 3.4,

$$-y_{n,\frac{H_n}{2}} \equiv 0 \equiv y_{n,o} \pmod{2^n} \quad .$$

$$y_{n,\frac{H_n}{2}-1} \equiv -y_{n,\frac{H_n}{2}} + y_{n,\frac{H_n}{2}+1} \equiv y_{n,\frac{H_n}{2}+1} \equiv y_{n,1} + 2^{n-1} \pmod{2^n}.$$

It follows that

$$-y_{n,\frac{H_n}{2}-2} \equiv y_{n,\frac{H_n}{2}-1} - y_{n,\frac{H_n}{2}} \equiv y_{n,o} + y_{n,1} + 2^{n-1} \equiv y_{n,2} + 2^{n-1} \pmod{2^n}$$

$$y_{n,\frac{H_n}{2}-3} \equiv y_{n,\frac{H_n}{2}-1} - y_{n,\frac{H_n}{2}-2} \equiv y_{n,1} + y_{n,2} + 2^n \equiv y_{n,3} \pmod{2^n}$$

$$\vdots \qquad\qquad \vdots$$

Clearly we have

$$(-1)^{t-1}\, y_{n,\frac{H_n}{2}-t} \equiv y_{n,t} + \alpha_t\, 2^{n-1} \pmod{2^n} ,$$

where
$$\alpha_t = \begin{cases} 0 & \text{if } t \equiv 0 \pmod 3 \\ 1 & \text{if } t \not\equiv 0 \pmod 3 \end{cases} .$$

Q.E.D.

The next lemma follows easily from lemma 3.17.

Lemma 3.18: Let $\{y_{n,i}\}$ be a Fibonacci sequence mod 2^n with initial values $y_{n,o} = 0$ and $y_{n,1}$ being odd. For any non-negative integer t such that $t \not\equiv 0 \pmod 3$, we have

$$y_{n,\frac{H_n}{2}-t} - y_{n-1,\frac{H_n}{2}-t} = \begin{cases} 2^{n-1} - y_{n,t} + y_{n-1,t} & \text{if } t \text{ is odd} \\ y_{n,t} - y_{n-1,t} & \text{if } t \text{ is even} \end{cases} .$$

By numerical inspection, it is not difficult to see that for all $n \geq 5$, $\psi_5(\{y_{5,i}\}) = 0, 3, 4, 7, 8, 11, 12$ or 15 if and only if there exists an integer t such that $y_{n,t} = 0$. Without loss of generality, we may therefore assume that $y_{n,o} = 0$ and $y_{n,1}$ is odd. From lemma 3.18, we have for $t \not\equiv 0 \pmod 3$,

$$y_{n,t} - y_{n-1,t} = y_{n,t+s} - y_{n-1,t+s}$$

if and only if

$$y_{n,\frac{H_n}{2}-t} - y_{n-1,\frac{H_n}{2}-t} \not\equiv y_{n,\frac{H_n}{2}-t-s} - y_{n-1,\frac{H_n}{2}-t-s} .$$

It shows that case Ia) and case Ib) have equal frequency of occurring. We thus have

$$\sum_{\substack{i=o \\ y_{n,i} \text{ and } y_{n,i+s} \\ \text{are both odd}}}^{H_n-1} y_{n,i}\, y_{n,i+s} = 2\sum_{\substack{i=o \\ y_{n-1,i} \text{ and} \\ y_{n-1,i+s} \text{ are} \\ \text{both odd}}}^{H_{n-1}-1} y_{n-1,i}\, y_{n-1,i+s} + 2^{n-1} \sum_{\substack{i=o \\ i\not\equiv o \pmod 3}}^{H_{n-1}-1} y_{n-1,i}$$

$$+ \frac{2^{2n-2}}{6} H_{n-1} \qquad (3.18)$$

Case II: Suppose $y_{n-1,i}$ is odd and $y_{n-1,i+s}$ is even. We have again two subcases:

case IIa) $\quad y_{n,i+s} = y_{n-1,i+s}$

case IIb) $\quad y_{n,i+s} = y_{n-1,i+s} + 2^{n-1}$.

In case IIa),

$$y_{n,i}\, y_{n,i+s} + y_{n,i+\frac{H_n}{2}}\, y_{n,i+s+\frac{H_n}{2}}$$

$$= y_{n-1,i}\, y_{n-1,i+s} + y_{n-1,i+s}(y_{n-1,i} + 2^{n-1})$$

$$= 2y_{n-1,i}\, y_{n-1,i+s} + 2^{n-1}\, y_{n-1,i+s} \qquad (3.19)$$

In case IIb),

$$y_{n,i}\, y_{n,i+s} + y_{n,i+\frac{H_n}{2}}\, y_{n,i+s+\frac{H_n}{2}}$$

$$= y_{n-1,i}(y_{n-1,i+s} + 2^{n-1}) + (y_{n-1,i} + 2^{n-1})(y_{n-1,i+s} + 2^{n-1})$$

$$= 2y_{n-1,i}\, y_{n-1,i+s} + (2y_{n-1,i} + y_{n-1,i+s})2^{n-1} + 2^{2n-2}. \qquad (3.20)$$

On the other hand, from theorem 3.14 we have

$$\text{freq}_n\,(x) = \text{freq}_n\,(x + 2^{n-1})$$

where $0 \leqslant x < 2^{n-1}$. It implies that the frequencies of case IIa) and case IIb) to occur are equal.

$$\therefore \sum_{\substack{i=0 \\ y_{n,i} \text{ is odd} \\ y_{n,i+s} \text{ is even}}}^{H_n-1} y_{n,i}\, y_{n,i+s} = 2 \sum_{\substack{i=0 \\ y_{n-1,i} \text{ is odd} \\ y_{n-1,i+s} \text{ is even}}}^{H_{n-1}-1} y_{n-1,i}\, y_{n-1,i+s} + 2^{n-1} \sum_{\substack{i=0 \\ i \equiv 0 \pmod 3}}^{H_{n-1}-1} y_{n-1,i}$$

$$+ 2^n \sum_{i \in F_{n-1,s,1}} y_{n-1,i} + \frac{2^{2n-2}}{6} H_{n-1} , \qquad (3.21)$$

where $F_{n-1,s,1} = \{i : 0 \leqslant i < H_{n-1},\ y_{n-1,i}$ is odd, $y_{n-1,i+s}$ is even and $y_{n,i+s} \geqslant 2^{n-1}\}$.

Case III: Let $y_{n-1,i}$ be even and $y_{n-1,i+s}$ be odd. Similar to case II, we have

$$\sum_{\substack{i=0 \\ y_{n,i} \text{ is even} \\ y_{n,i+s} \text{ is odd}}}^{H_n-1} y_{n,i}\, y_{n,i+s} = 2 \sum_{\substack{i=0 \\ y_{n-1,i} \text{ is even} \\ y_{n-1,i+s} \text{ is odd}}}^{H_{n-1}-1} y_{n-1,i}\, y_{n-1,i+s} + 2^{n-1} \sum_{\substack{i=0 \\ i \equiv 0 \pmod 3}}^{H_{n-1}-1} y_{n-1,i}$$

$$+ 2^n \sum_{i \in F_{n-1,s,2}} y_{n-1,i} + \frac{2^{2n-2}}{6} H_{n-1} , \qquad (3.22)$$

where $F_{n-1,s,2} = \{i : 0 \leqslant i < H_{n-1},\ y_{n-1,i}$ is even, $y_{n-1,i+s}$ is odd and $y_{n,i} \geqslant 2^{n-1}\}$.

Combining (3.18), (3.21) and (3.22), we obtain the following equation:

$$\sum_{i=o}^{H_n-1} y_{n,i}\, y_{n,i+s} = 2\sum_{i=o}^{H_{n-1}-1} y_{n-1,i}\, y_{n-1,i+s} + 2^{n-1}\sum_{i=o}^{H_{n-1}-1} y_{n-1,i} + 2^{n-1}\sum_{\substack{i=o\\ i\equiv 0 \pmod 3}}^{H_{n-1}-1} y_{n-1,i}$$

$$+\ 2^n \sum_{i\in F_{n-1,s,1}\,\cup\, F_{n-1,s,2}} y_{n-1,i} + 3\times 2^{3n-5}\ . \qquad (3.23)$$

We must find out the value of $\sum_{i\in F_{n-1,s,1}\,\cup\, F_{n-1,s,2}} y_{n-1,i}$ before making use of (3.23) as a recurrence relation between $\sum_{i=o}^{H_n-1} y_{n,i}\, y_{n,i+s}$ and $\sum_{i=o}^{H_{n-1}-1} y_{n-1,i}\, y_{n-1,i+s}$.

Define

$$G_{n-1,s,1} = \{i : 0 \leqslant i \leqslant H_{n-1}\ ,\ y_{n,i} \geqslant 2^{n-1} \text{ and } i \equiv 0 \pmod 3\}\ ,$$

$$G_{n-1,s,2} = \{i : 0 \leqslant i < H_{n-1}\ ,\ y_{n,i} < 2^{n-1} \text{ and } i \equiv 0 \pmod 3\}\ ,$$

$$Q_{n-1,s,1} = \sum_{i\in G_{n-1,s,1}} (y_{n-1,i-s} + y_{n-1,i+s})$$

and

$$Q_{n-1,s,2} = \sum_{i\in G_{n-1,s,2}} (y_{n-1,i-s} + y_{n-1,i+s})\ .$$

It is obvious that

$$\sum_{i\in F_{n-1,s,1}\,\cup\, F_{n-1,s,2}} y_{n-1,i} = Q_{n-1,s,1} \qquad (3.24)$$

and

$$Q_{n-1,s,1} + Q_{n-1,s,2} = \sum_{\substack{i=o\\ i\not\equiv 0 \pmod 3}}^{H_{n-1}-1} y_{n-1,i}\ . \qquad (3.25)$$

We shall evaluate the difference of $Q_{n-1,s,1}$ and $Q_{n-1,s,2}$ first and then make use of (3.25) to find out the value of $Q_{n-1,s,1}$. To do this, the following equality, which can be derived by similar method as that in the proof of lemma 3.17, is useful.

$$y_{n-1,\frac{H_n}{2}-t} \equiv (-1)^{t-1} y_{n-1,t} \pmod{2^{n-1}} . \tag{3.26}$$

Now divide all the possible i's such that $i \equiv 0 \pmod 3$ and $0 \leq i < H_{n-1}$, into the following three cases.

Case 1: Suppose i is even and $i \neq 0, \frac{H_n}{4}$. From lemma 3.17,

$$y_{n,\frac{H_n}{2}-i} = 2^n - y_{n,i} .$$

Hence one and only one of $y_{n,i}$ and $y_{n,\frac{H_n}{2}-i}$ is less than 2^{n-1}, i.e. either i or $\frac{H_n}{2} - i$ belongs to $G_{n-1,s,1}$. Applying (3.26), we have

$$y_{n-1,\frac{H_n}{2}-i-s} + y_{n-1,\frac{H_n}{2}-i+s} = y_{n-1,i+s} + y_{n-1,i-s} .$$

Therefore, no matter which one is in $G_{n-1,s,1}$, the difference of $Q_{n-1,s,1}$ and $Q_{n-1,s,2}$ is not affected.

Case 2: Suppose i is odd. Clearly i can be expressed as i^*, $H_{n-1} - i^*$, $H_{n-1} - i^* - \frac{H_{n-1}}{4}$ or $i^* + \frac{H_{n-1}}{4}$ where $0 \leq i^* < \frac{H_{n-1}}{4}$. From lemma 3.17 again, we have

$$y_{n,\frac{H_n}{2}-i^*} = y_{n,i^*}$$

and

$$y_{n,\frac{H_n}{2}-i^*-\frac{H_n}{8}} = y_{n,i^*+\frac{H_n}{8}} .$$

Since $i^*/3$ must be odd and $y_{n,o} = 0$, it can easily be proved that

$$y_{n,i^*} \neq y_{n,i^*+H_n/8}$$

and

$$y_{n,i^*} \equiv y_{n,i^*+H_n/8} \pmod{2^{n-1}} \qquad \text{from (3.9).}$$

So, either $H_n/2 - i^*$ and i^* or $H_n/2 - i^* - H_n/8$ and $i^* + H_n/8$ belong to $G_{n-1,s,1}$. From (3.26), we get

$$y_{n-1,\frac{H_n}{2}-i^*+s} + y_{n-1,\frac{H_n}{2}-i^*-s} + y_{n-1,i^*-s} + y_{n-1,i^*+s}$$

$$= y_{n-1,\frac{H_n}{2}-i^*-\frac{H_n}{8}+s} + y_{n-1,\frac{H_n}{2}-i^*-\frac{H_n}{8}-s} + y_{n-1,i^*+\frac{H_n}{8}+s} + y_{n-1,i^*+\frac{H_n}{8}-s} .$$

Hence the difference of $Q_{n-1,s,1}$ and $Q_{n-1,s,2}$ is not affected in this case.

Case 3: Assume $i = 0$ or $i = H_n/4$. Clearly $y_{n-1,o} = y_{n,o} = 0$, $y_{n-1,H_n/4} = y_{n-1,o} = 0$ and $y_{n,H_n/4} = 2^{n-1}$. It implies that $0 \in G_{n-1,s,2}$ and $H_n/4 \in G_{n-2,s,1}$. From (3.26), we have

$$y_{n-1,s} = y_{n-1,H_{n-1}-s}$$

and

$$y_{n-1,H_n/4+s} = y_{n-1,H_n/4-s} .$$

$$\therefore \quad |y_{n-1,s} + y_{n-1,H_{n-1}-s} - y_{n-1,\frac{H_n}{4}+s} - y_{n-1,\frac{H_n}{4}-s}| = 2^{n-1} .$$

Let $y_{n,s} = \sum_{i=o}^{n-1} \beta_{s,i} 2^i$ where $\beta_{s,i} = 0$ or 1 . Obviously,

$$y_{n-1,s} + y_{n-1,H_{n-1}-s} - y_{n-1,H_n/4+s} - y_{n-1,H_n/4-s} = 2^{n-1}$$

$$\Leftrightarrow \quad y_{n-1,s} > y_{n-1,H_n/4+s}$$

$$\Leftrightarrow \quad \beta_{s,n-2} = 1$$

From the above three cases and (3.25), we have

$$Q_{n-1,s,1} = R_{n-1,s} + (1-\beta_{s,n-2})2^{n-1} \tag{3.27}$$

where $R_{n-1,s} = \Bigl(\sum_{\substack{i=o \\ i\not\equiv 0 \pmod 3}}^{H_{n-1}-1} y_{n-1,i} - 2^{n-1} \Bigr) / 2$.

Define $E_{n,s} = \sum_{i=o}^{H_n-1} y_{n,i}\, y_{n,i+s}$, $T_n = \sum_{i=o}^{H_n-1} y_{n,i}$ and $T_n^* = \sum_{\substack{i=o \\ i\equiv 0 \pmod 3}}^{H_n-1} y_{n,i}$.

Now (3.23) can be expressed as

$$E_{n,s} = 2E_{n-1,s} + 2^{n-1}T_{n-1} + 2^{n-1}T_{n-1}^* + 2^n Q_{n-1,s,1} + 3 \times 2^{3n-5} .$$

From (3.27), we get

$$\begin{aligned} E_{n,s} &= 2E_{n-1,s} + 2^{n-1}T_{n-1} + 2^{n-1}T_{n-1}^* + 2^n R_{n-1,s} + (1-\beta_{s,n-2})2^{2n-1} + 3 \times 2^{3n-5} \\ &= 2E_{n-1,s} + 2^{n-1}T_{n-1} + 2^{n-1}T_{n-1}^* + 2^{n-1}(T_{n-1} - T_{n-1}^* - 2^{n-1}) + \\ &\quad (1-\beta_{s,n-2})2^{2n-1} + 3 \times 2^{3n-5} \\ &= 2E_{n-1,s} + 2^n T_{n-1} - \beta_{s,n-2}\, 2^{2n-1} + 3 \times 2^{3n-5} + 2^{2n-2} . \end{aligned}$$

Inductively, we have when $n \geq 7$,

$$E_{n,s} = 2^{n-6} E_{6,s} + 2^n \sum_{k=6}^{n-1} T_k - \sum_{k=6}^{n-1} T_k - \sum_{k=o}^{n-7} \beta_{s,n-2-k} \, 2^{2n-1-k}$$

$$+ 3\sum_{k=o}^{n-7} 2^{3n-5-2k} + \sum_{k=o}^{n-7} 2^{2n-2-k} \qquad (3.28)$$

By corollary 3.15, T_n can be calculated by

$$T_n = 2^{n-6} T_6 + 3 \times 2^{n-2} (2^n - 2^6) \quad \text{when} \quad n \geq 6 .$$

Substituting it to (3.28), we obtain

$$E_{n,s} = 2^{n-6}E_{6,s} + 2^n\sum_{k=6}^{n-1} [2^{k-6}T_6 + 3 \times 2^{k-2}(2^k - 2^6)] - \sum_{k=o}^{n-7} \beta_{s,n-2-k} \, 2^{2n-1-k}$$

$$+ 3\sum_{k=o}^{n-7} 2^{3n-5-2k} + \sum_{k=o}^{n-7} 2^{2n-2-k}$$

$$= 2^{n-6}E_{6,s} + 2^nT_6(2^{n-6} - 1) + 3 \times 2^n(2^{2n-2} - 2^{10})/3 - 3 \times 2^{n+6}(2^{n-2} - 2^4)$$

$$- \sum_{k=o}^{n-7} \beta_{s,n-2-k} \, 2^{2n-1-k} + (2^{3n-3} - 2^{n+9}) + 2^{2n-1} - 2^{n+5}$$

$$= 2^{n-6}E_{6,s} + 2^n(2^{n-6} - 1)T_6 - (\sum_{k=5}^{n-2} \beta_{s,k} \, 2^k)2^{n+1} + 47 \times 2^{n+5}$$

$$- 95 \times 2^{2n-1} + 3 \times 2^{3n-3} \quad .$$

Since $\sum_{k=5}^{n-2} \beta_{s,k} \, 2^k = y_{n-1,s} - y_{5,s}$, we have the following theorem.

<u>Theorem 3.19</u>: Let $\{y_{n,i}\}$ be a Fibonacci sequence mod 2^n with initial values

$y_{n,o} = 0$ and $y_{n,1}$ being odd. Then for $n \geq 7$ and $s \equiv 1$ or $5 \pmod 6$, we have

$$E_{n,s} = 2^{n-6} E_{6,s} + 2^{n}(2^{n-6} - 1)T_6 - 2^{n+1}(y_{n-1,s} - y_{5,s})$$
$$+ 47 \times 2^{n+5} - 95 \times 2^{2n-1} + 3 \times 2^{3n-3} .$$

Under the conditions of theorem 3.19, we can calculate the exact serial correlation $\rho_x(s)$ when $s \equiv 1$ or $5 \pmod 6$. An example is given below.

Example: Consider the Fibonacci generator $y_{11,i} \equiv y_{11,i-1} + y_{11,i-2} \pmod{2^{11}}$. $y_{11,o} = 0$ and $y_{11,1} = 1443$. Now $y_{6,1} = 35$. The values of $E_{6,1}$ and T_6 can be obtained from table 3.5 in section four. We have

$$E_{6,1} = 87680 \quad \text{and} \quad T_6 = 2880 .$$

$y_{10,1} - y_{5,1} = 416$. From theorem 3.19 with $s = 1$, we get

$$E_{11,1} = 2^5 E_{6,1} + 2^{11}(2^5 - 1)T_6 - 2^{12} \times 416 + 47 \times 2^{16} - 95 \times 2^{21} + 3 \times 2^{30}$$
$$= 2^5 \times 87680 + 2^{11}(2^5 - 1) \times 2880 - 2^{12} \times 416 + 47 \times 2^{16} - 95 \times 2^{21}$$
$$+ 3 \times 2^{30}$$
$$= 3209023488 .$$

Since $\psi_5(\{y_{5,i}\}) = 3$, we can compute the values of $\sum_{i=o}^{H_{11}-1} y_{11,i}^2$ and $\sum_{i=o}^{H_{11}-1} y_{11,i}$ by corollary 3.15 as follows

$$\sum_{i=o}^{H_{11}-1} y_{11,i}^2 = 2^{11-5} \sum_{i=o}^{H_5-1} y_{5,i}^2 + 2^{11}(2^6 - 1)\sum_{i=o}^{H_5-1} y_{5,i} + 2^{11}(2^{11} - 2^5)(2^{10} - 2^3)$$

$$= 2^6 \times 13504 + 2^{11} \times 63 \times 672 + 2^{11}(2^{11} - 2^5)(2^{10} - 2^3)$$

$$= 4282396672$$

$$\sum_{i=0}^{H_{11}-1} y_{11,i} = 2^{11-5}\sum_{i=0}^{H_5-1} y_{5,i} + 3 \times 2^9(2^{11} - 2^5)$$

$$= 2^6 \times 672 + 3 \times 2^9 \times 2016$$

$$= 3139584 .$$

Hence for the pseudo-random number sequence $x = \{x_{11,i}\}$, $(x_{11,i} = y_{11,i} / 2^{11})$,

$$\rho_x(1) = \left(\frac{1}{H_{11}} \frac{E_{11,1}}{2^{22}} - \frac{1}{H_{11}^2} \frac{3139584^2}{2^{22}} \right) / \left(\frac{1}{H_{11}} \frac{4282396672}{2^{22}} - \frac{1}{H_{11}^2} \frac{3139584^2}{2^{22}} \right)$$

$$= (0.249053001 - 0.249024391) / (0.332357725 - 0.249024391)$$

$$= 0.00034332 .$$

Section 4: The serial correlation $\rho_x(s)$, when $s \equiv 3 \pmod 6$

This section is a continuation of the previous section. Suppose we have a sequence $\{y_{n,i}\}$ in A_n such that the initial values $y_{n,o} = 0$ and $y_{n,1}$ is odd. The pseudo-random number sequence $x = \{x_{n,i}\}$ is defined as before. We want to determine the serial correlation $\rho_x(s)$ when $s \equiv 3 \pmod 6$ and $n \geq 7$. Now we have only two cases:

I') $y_{n-1,i}$ and $y_{n-1,i+s}$ are odd.

II') $y_{n-1,i}$ and $y_{n-1,i+s}$ are even.

These two cases are discussed as follows.

Case I': Assume $y_{n-1,i}$ and $y_{n-1,i+s}$ are odd, where $0 \leq i < H_{n-1}$.
Following the steps as that in Case I of section 3, we have

$$\sum_{\substack{i=0 \\ i \not\equiv 0 \pmod 3}}^{H_n-1} y_{n,i}\, y_{n,i+s} = 2 \sum_{\substack{i=0 \\ i \not\equiv 0 \pmod 3}}^{H_{n-1}-1} y_{n-1,i}\, y_{n-1,i+s} + 2^n \sum_{\substack{i=0 \\ i \not\equiv 0 \pmod 3}}^{H_{n-1}-1} y_{n-1,i} + \frac{2^{2n-1}}{6} H_{n-1} \qquad (3.29)$$

Case II': Assume $y_{n-1,i}$ and $y_{n-1,i+s}$ are even, where $0 \leq i < H_{n-1}$.
$(y_{n,i}\ ,\ y_{n,i+s})$ must belong to one of the four subcases:

Case IIa') $(y_{n,i}, y_{n,i+s}) = (y_{n-1,i}\ ,\ y_{n-1,i+s})$

Case IIb') $(y_{n,i}, y_{n,i+s}) = (y_{n-1,i} + 2^{n-1}, y_{n-1,i+s} + 2^{n-1})$

Case IIc') $(y_{n,i}, y_{n,i+s}) = (y_{n-1,i}, y_{n-1,i+s} + 2^{n-1})$

Case IId') $(y_{n,i}, y_{n,i+s}) = (y_{n-1,i} + 2^{n-1}, y_{n-1,i+s})$.

From lemma 3.17,

$$y_{n,\frac{H_n}{2}-i} \equiv (-1)^{t-1} y_{n,i} \qquad \pmod{2^n} .$$

Suppose $y_{n,i} \not\equiv 0$ or 2^{n-1} . Then

$$y_{n,\frac{H_n}{2}-i} = \begin{cases} y_{n,i} & \text{if } i \text{ is odd} \\ 2^n - y_{n,i} & \text{if } i \text{ is even} \end{cases} .$$

Therefore

$$y_{n-1,\frac{H_n}{2}-i} = \begin{cases} y_{n-1,i} & \text{if } i \text{ is odd} \\ 2^{n-1} - y_{n-1,i} & \text{if } i \text{ is even} \end{cases} .$$

It follows that

$$y_{n,\frac{H_n}{2}-i} - y_{n-1,\frac{H_n}{2}-i} = \begin{cases} y_{n,i} - y_{n-1,i} & \text{if } i \text{ is odd} \\ 2^{n-1} - y_{n,i} + y_{n-1,i} & \text{if } i \text{ is even} \end{cases} \quad . \tag{3.30}$$

When $0 \leq i < H_{n-1}$, it is found that $y_{n,i} = 0$ if and only if $i = 0$ and that $y_{n,i} = 2^{n-1}$ if and only if $i = H_n/4$. From (3.9) and lemma 3.17, we get

$$y_{n,s} = y_{n,\frac{H_n}{2}-s} = y_{n,\frac{H_n}{4}-s} = y_{n,\frac{H_n}{4}+s} \quad . \tag{3.31}$$

By (3.30) and (3.31), we have, similar to the case I in section three,

$$\text{freq(IIa')} + \text{freq(IIb')} = \text{freq(IIc')} + \text{freq(IId')} \quad ,$$

where freq(IIe') means the frequency of the occurrence of case IIe') where e = a, b, c or d .

By theorem 3.14, we know that

$$\text{freq(IIa')} + \text{freq(IIc')} = \text{freq(IIb')} + \text{freq(IId')}$$

and

$$\text{freq(IIa')} + \text{freq(IId')} = \text{freq(IIb')} + \text{freq(IIc')} \quad .$$

Thus we have

$$\text{freq(IIa')} = \text{freq(IIb')} = \text{freq(IIc')} = \text{freq(IId')} \quad .$$

In case IIa'),

$$y_{n,i}\, y_{n,i+s} + y_{n,i+\frac{H_n}{2}}\, y_{n,\frac{H_n}{2}+i+s}$$

$$= \quad 2\, y_{n-1,i}\, y_{n-1,i+s} \quad .$$

In case IIb'),

$$y_{n,i}\, y_{n,i+s} + y_{n,i+\frac{H_n}{2}}\, y_{n,\frac{H_n}{2}+i+s}$$

$$= 2[y_{n-1,i}\, y_{n-1,i+s} + (y_{n-1,i} + y_{n-1,i+s}) + 2^{n-1} + 2^{2n-2}] \ .$$

In case IIc'),

$$y_{n,i}\, y_{n,i+s} + y_{n,i+\frac{H_n}{2}}\, y_{n,\frac{H_n}{2}+i+s}$$

$$= 2(y_{n-1,i}\, y_{n-1,i+s} + 2^{n-1}\, y_{n-1,i}) \ ,$$

and in case IId')

$$y_{n,i}\, y_{n,i+s} + y_{n,i+\frac{H_n}{2}}\, y_{n,\frac{H_n}{2}+i+s}$$

$$= 2(y_{n-1,i}\, y_{n-1,i+s} + 2^{n-1}\, y_{n-1,i+s}) \ .$$

Hence

$$\sum_{\substack{i=o \\ i\equiv 0 \pmod 3}}^{H_n-1} y_{n,i}\, y_{n,i+s} = 2 \sum_{\substack{i=0 \\ i\equiv 0 \pmod 3}}^{H_{n-1}-1} y_{n-1,i}\, y_{n-1,i+s} + 2^n \sum_{\substack{i=o \\ i\equiv 0 \pmod 3 \\ y_{n,i} \geq 2^{n-1}}}^{H_{n-1}-1} (y_{n-1,i+s} + y_{n-1,i-s})$$

$$+ 2^{2n-1} H_{n-1} / 12 \qquad (3.32)$$

Recall the definitions of $G_{n-1,s,1}$, $G_{n-1,s,2}$, $Q_{n-1,s,1}$ and $Q_{n-1,s,2}$.

$$G_{n-1,s,1} = \{i \ : \ 0 \leq i < H_{n-1},\ y_{n,i} \geq 2^{n-1} \ \text{ and } \ i \equiv 0 \pmod 3\} \ .$$

$$G_{n-1,s,2} = \{i \ : \ 0 \leq i < H_{n-1},\ y_{n,i} < 2^{n-1} \ \text{ and } \ i \equiv 0 \pmod 3\} \ .$$

$$Q_{n-1,s,1} = \sum_{i\in G_{n-1,s,1}} (y_{n-1,i-s} + y_{n-1,i+s}) \ .$$

$$Q_{n-1,s,2} = \sum_{i \in G_{n-1,s,2}} (y_{n-1,i-s} + y_{n-1,i+s}) .$$

Clearly

$$\sum_{\substack{i=o \\ i \equiv 0 (\mathrm{mod}\ 3) \\ y_{n,i} \geq 2^{n-1}}}^{H_{n-1}-1} (y_{n-1,i+s} + y_{n-1,i-s}) = Q_{n-1,s,1} \qquad (3.33)$$

and

$$Q_{n-1,s,1} + Q_{n-1,s,2} = 2 \sum_{\substack{i=o \\ i \equiv 0 (\mathrm{mod}\ 3)}}^{H_{n-1}-1} y_{n-1,i} . \qquad (3.34)$$

We now find the difference of $Q_{n-1,s,1}$ and $Q_{n-1,s,2}$. Similar to section 3, we can prove that the difference of $Q_{n-1,s,1}$ and $Q_{n-1,s,2}$ is not affected by the value of i when $i \not\equiv s$ or $i \not\equiv H_n/8 - s \pmod{H_n/8}$. We know that

$$y_{n-1,H_n/2} + y_{n-1,H_n/2-2s} + y_{n-1,o} + y_{n-1,2s} = 2^{n-1} ,$$

$$y_{n-1,H_n/2-H_n/8} + y_{n-1,H_n/2-H_n/8-2s} + y_{n-1,H_n/8+2s} + y_{n-1,H_n/8} = 2^n ,$$

$$y_{n-1,H_n/2-H_n/8+2s} + y_{n-1,H_n/2-H_n/8} + y_{n-1,H_n/8-2s} + y_{n-1,H_n/8} = 2^n ,$$

and

$$y_{n-1,H_n/2-H_n/4+2s} + y_{n-1,H_n/2-H_n/4} + y_{n-1,H_n/4} + y_{n-1,H_n/4-2s} = 2^{n-1} .$$

From (3.31), we have

$$y_{n,s} = y_{n,H_n/2-s} = y_{n,H_n/4-s} = y_{n,H_n/4+s} .$$

Similarly, we get

$$y_{n,H_n/8+s} = y_{n,H_n/2-H_n/8-s} = y_{n,H_n/8-s} = y_{n,H_n/2-H_n/8+s} .$$

Moreover from (3.9),

$$y_{n,s} \neq y_{n,H_n/8+s} .$$

Thus s, $H_n/2-s$, $H_n/4-s$ and $H_n/4+s$ belong to the same $G_{n-1,s,j}$, where $j = 1$ or 2 , and $H_n/8+s$, $H_n/2-H_n/8-s$, $H_n/8-s$ and $H_n/2-H_n/8+s$ belong to the other.

Let $y_{n,s} = \sum_{i=o}^{n-1} \beta_{s,i} 2^i$ where $\beta_{s,i} = 0$ or 1 . From the above information, we have, similar to section 3,

$$Q_{n-1,s,1} = T^*_{n-1} + (1 - 2\beta_{s,n-1})2^{n-1} , \qquad (3.35)$$

where $T^*_{n-1} = \sum_{\substack{i=o \\ i\equiv 0 \pmod 3}}^{H_{n-1}-1} y_{n-1,i}$.

Using the symbols introduced in section 3, we add (3.29) to (3.32) giving the following equation :

$$\begin{aligned}
E_{n,s} &= 2E_{n-1,s} + 2^n(T_{n-1} - T^*_{n-1}) + \frac{2^{2n-1}}{6} H_{n-1} + 2^n Q_{n-1,s,1} + \frac{2^{2n-1}}{12} H_{n-1} \\
&= 2E_{n-1,s} + 2^n(T_{n-1} - T^*_{n-1}) + \frac{2^{2n-2}}{3} H_{n-1} + 2^n T^*_{n-1} + (1 - 2\beta_{s,n-1})2^{2n-1} \\
&\quad + \frac{2^{2n-2}}{6} H_{n-1} \qquad \text{from (3.35)} \\
&= 2E_{n-1,s} + 2^n T_{n-1} - 2^{2n}\beta_{s,n-1} + 3 \times 2^{3n-5} + 2^{2n-1} .
\end{aligned}$$

It follows that

$$E_{n,s} = 2^{n-6}E_{6,s} + 2^n\sum_{k=6}^{n-1} T_k - \sum_{k=o}^{n-7} \beta_{s,n-1-k}2^{2n-k} + 3\sum_{k=o}^{n-7} 2^{3n-5-2k} + \sum_{k=o}^{n-7} 2^{2n-1-k}$$

$$= 2^{n-6}E_{6,s} + 2^n\sum_{k=6}^{n-1} [2^{k-6}T_6 + 3 \times 2^{k-2}(2^k - 2^6)] - \sum_{k=o}^{n-7} \beta_{s,n-1-k}\, 2^{2n-k}$$

$$+ 3\sum_{k=o}^{n-7} 2^{3n-5-2k} + \sum_{k=o}^{n-7} 2^{2n-1-k} \quad \text{, from corollary 3.15,}$$

$$= 2^{n-6}E_{6,s} + 2^n(2^{n-6} - 1)T_6 - \sum_{k=o}^{n-7} \beta_{s,n-1-k}2^{2n-k} + 23 \times 2^{n+6}$$

$$- 47 \times 2^{2n} + 3 \times 2^{3n-3}$$

$$= 2^{n-6}E_{6,s} + 2^n(2^{n-6} - 1)T_6 - 2^{n+1}(y_{n,s} - y_{6,s}) + 23 \times 2^{n+6}$$

$$- 47 \times 2^{2n} + 3 \times 2^{3n-3} \quad .$$

Theorem 3.20: Let $\{y_{n,i}\}$ be a Fibonacci sequence mod 2^n with initial values $y_{n,o} = 0$ and $y_{n,1}$ being odd. For $n \geq 7$ and $s \equiv 3 \pmod 6$, we have

$$E_{n,s} = 2^{n-6}E_{6,s} + 2^n(2^{n-6} - 1)T_6 - 2^{n+1}(y_{n,s} - y_{6,s}) + 23 \times 2^{n+6}$$

$$- 47 \times 2^{2n} + 3 \times 2^{3n-3} \quad .$$

Theorems 3.19 and 3.20 express the value of $E_{n,s}$ in terms of n, s, $y_{n,s}$, T_6 and $E_{6,s}$. The values of T_6 and $E_{6,s}$ for some values of s are listed in table 3.5.

Table 3.5

r	$y_{6,0}$	$y_{6,1}$	T_6	$E_{6,1}$	$E_{6,3}$	$E_{6,5}$	$E_{6,7}$	$E_{6,9}$
0	0 0	1 33	2752	79744	81664	79232	78208	77568
3	0 0	19 51	2880	85632	85248	84096	85120	89344
4	0 0	21 53	2880	85376	84736	86912	85888	88832
7	0 0	23 55	3008	93312	92416	93824	94848	96512
8	0 0	25 57	3008	93056	91904	92544	95616	96000
11	0 0	11 43	3136	103040	103680	101504	102528	99584
12	0 0	13 45	3136	102784	103168	104320	103296	99072
15	0 0	15 47	3264	110720	110848	111232	112256	106752
16	0 0	17 49	2752	77696	77568	77184	76160	81664
19	0 0	3 35	2880	87680	89344	86144	87168	85248
20	0 0	5 37	2880	87424	88832	84864	87936	84736
23	0 0	7 39	3008	95360	96512	95872	92800	92416
24	0 0	9 41	3008	95104	96000	94592	93568	91904
27	0 0	27 59	3136	100992	99584	103552	100480	103680
28	0 0	29 61	3136	100736	99072	102272	101248	103168
31	0 0	31 63	3264	108672	106752	109184	110208	110848

($y_{6,0}$ and $y_{6,1}$ are the initial values and $r = \psi_6(\{y_{6,i}\})$.)

Example: Consider the Fibonacci generator $y_{11,i} \equiv y_{11,i-1} + y_{11,i-2} \pmod{2^{11}}$, $y_{11,0} = 0$ and $y_{11,1} = 1443$. As $y_{6,1} = 35$, we have from table 3.5, $T_6 = 2880$ and $E_{6,3} = 89344$. Apply theorem 3.20 with $s = 3$. Clearly $y_{11,3} = 838$ and $y_{11,3} - y_{6,3} = 832$. Therefore

$$E_{11,3} = 2^5 \times 89344 + 2^{11}(2^5 - 1) \times 2880 - 2^{12} \times 832 + 23 \times 2^{17}$$
$$- 47 \times 2^{22} + 3 \times 2^{30}$$
$$= 3209404416 .$$

Thus

$$\rho_x(3) = \left(\frac{1}{H_{11}} \frac{E_{11,3}}{2^{22}} - \frac{1}{H_{11}^2} \frac{3139584^2}{2^{22}}\right) / \left(\frac{1}{H_{11}} \frac{4282396672}{2^{22}} - \frac{1}{H_{11}^2} \frac{3139584^2}{2^{22}}\right)$$
$$= 0.00069809 .$$

(The values 3139584 and 4282396672 copy directly from the example in section three.)

Under the conditions of Theorem 3.19, we can of course express $E(x_{n,i}\ x_{n,i+s})$ as a function of $E(x_{6,i}\ x_{6,i+s})$ and $E(x_{6,i})$ by using Theorems 3.19 and 3.20. The next corollary shows this.

Corollary 3.21: Let $\{y_{n,i}\}$ be a Fibonacci sequence mod 2^n with initial values $y_{n,o} = 0$ and $y_{n,1}$ being odd. Take $\{y_{k,i}\} = \{y_{n,i} \pmod{2^k}\}$ for all $k < n$ and $\{x_{j,i}\} = \{y_{j,i}/2^j\}$ for all $0 \leq j \leq n$. Then when $n \geq 7$, we have

$$E(x_{n,i}\ x_{n,i+s}) = 2^{12-2n}E(x_{6,i}\ x_{6,i+s}) + 2^{12-2n}(2^{n-6} - 1)E(x_{6,i})$$
$$- 2^{2-2n}(y_{n-1,s} - y_{5,s})/3 + 47 \times 2^{6-2n}/3 - 95 \times 2^{-n}/3 + 0.25 \quad (3.36)$$

if $s \equiv 1$ or $5 \pmod 6$.

If $s \equiv 3 \pmod 6$,

$$E(x_{n,i}\ x_{n,i+s}) = 2^{12-2n}E(x_{6,i}\ x_{6,i+s}) + 2^{12-2n}(2^{n-6} - 1)E(x_{6,i})$$

$$- 2^{2-2n}(y_{n,s} - y_{6,s})/3 + 23 \times 2^{7-2n}/3 - 47 \times 2^{1-n}/3 + 0.25 \quad (3.37)$$

Since n is usually greater than 30, from corollary 3.21, $E(x_{n,i}\ x_{n,i+s})$ when s is odd is close to 0.25 as what we desire. It follows that the exact serial correlation $\rho_x(s)$ when s is odd is very small if the conditions of corollary 3.21 are satisfied.

CHAPTER 4. A NEW GENERATOR

Section 1: Fibonacci generator and a new generator

It appears, in view of the satisfactory properties of the mean, variance and serial correlation, $\rho_x(s)$, for odd integer s, that the Fibonacci pseudo-random number sequences are acceptable. However, there exists strong relation between $x_{n,i}$, $x_{n,i+1}$ and $x_{n,i+2}$. Indeed all the points $(x_{n,i}, x_{n,i+1}, x_{n,i+2})$, $i = 0, 1, 2, \ldots$ fall on two hyperplanes:

$$x_{n,i+2} = x_{n,i+1} + x_{n,i}$$

and

$$x_{n,i+2} = x_{n,i+1} + x_{n,i} - 1 \quad .$$

Thus the direct use of the Fibonacci pseudo-random numbers is dangerous. One reasonable application of the generator is given by Gebhardt (1967). He used the idea of composite generators. Of course nothing can prevent one from combining a Fibonacci generator and another generator, and one hopes to generate a "more random" sequence in this way. However theoretical analysis of this type of sequences is difficult. In what follows, we shall modify the Fibonacci generator in another way to yield a new generator.

Let $\{y_{n,i}\}$ be a Fibonacci sequence mod 2^n with initial values $y_{n,o}$ and $y_{n,1}$ that are not both even. To remove the regularities in $\{y_{n,i}\}$, one can use just a subsequence of $\{y_{n,i}\}$. A simple choice is the subsequence $\{y_{n,pi}\}_{i=0,1,2,\ldots}$, for some integer p. Obviously, this subsequence has a maximum period length $3 \times 2^{n-1}$ if and only if $(H_n, p) = 1$, i.e. $(6, p) = 1$. When $(6, p) = 1$, the subsequence $\{y_{n,pi}\}$ shares the same period, mean and variance with $\{y_{n,i}\}$. Let $x_p = \{x_{n,pi}\}$ and $x = \{x_{n,i}\}$. Clearly $\rho_{x_p}(s) = \rho_x(ps)$. Hence, in view of the properties of x, x_p should possess some properties of a good pseudo-random number sequence. Of course, it is time-consuming to generate x_p from x. Direct method is thus necessary.

Denote by $\{u_i\}$ the Fibonacci sequence that satisfies

$$u_i = u_{i-1} + u_{i-2} ,$$

with initial values $u_0 = 0$ and $u_1 = 1$. Suppose $\{y_{n,i}\}$ is a Fibonacci sequence mod 2^n. It is obvious that

$$y_{n,i} \equiv u_i\, y_{n,1} + u_{i-1}\, y_{n,0} \pmod{2^n} . \tag{4.1}$$

<u>Lemma 4.1</u>: With $\{u_i\}$ and $\{y_{n,i}\}$ as defined above, we have

$$y_{n,ip} \equiv (u_{p+1} + u_{p-1})y_{n,(i-1)p} + (-1)^{p+1}\, y_{n,(i-2)p} \pmod{2^n}. \tag{4.2}$$

<u>Proof</u>: From (4.1), it is easily seen that

$$y_{n,ip} \equiv u_{2p}\, y_{n,(i-2)p+1} + u_{2p-1}\, y_{n,(i-2)p} \pmod{2^n}$$

and

$$y_{n,(i-1)p} \equiv u_p\, y_{n,(i-2)p+1} + u_{p-1}\, y_{n,(i-2)p} \pmod{2^n} .$$

Moreover it is well-known that

$$u_{2p} = u_p(u_{p+1} + u_{p-1}) ,$$

$$u_{2p-1} = u_p^2 + u_{p-1}^2$$

and

$$u_p^2 - u_{p-1}\, u_{p+1} = (-1)^{p+1} \quad .$$

Thus,

$$\begin{aligned} y_{n,ip} - (u_{p+1} + u_{p-1})y_{n,(i-1)p} &\equiv u_{2p}y_{n,(i-2)p+1} + u_{2p-1}y_{n,(i-2)p} - u_p(u_{p+1} + u_{p-1})\times \\ & \quad y_{n,(i-2)p+1} - u_{p-1}(u_{p+1} + u_{p-1})y_{n,(i-2)p} \pmod{2^n} \\ &\equiv (u_p^2 - u_{p-1}\, u_{p+1})y_{n,(i-2)p} \pmod{2^n} \\ &\equiv (-1)^{p+1}\, y_{n,(i-2)p} \pmod{2^n}. \end{aligned}$$

$$\therefore \quad y_{n,ip} \equiv (u_{p+1} + u_{p-1})y_{n,(i-1)p} + (-1)^{p+1} y_{n,(i-2)p} \pmod{2^n} \; .$$

Q.E.D.

Equation (4.2) can be used to generate x_p directly. The following theorem is useful in introducing a new generator.

<u>Theorem 4.2</u>: Let $\{v_{n,i}\}$ be a sequence of integers produced by the recurrence relation

$$v_{n,i} \equiv \alpha v_{n,i-1} + v_{n,i-2} \pmod{2^n} .$$

Then α is an odd integer if and only if there exist a positive integer p, which is relatively prime to 6, and non-negative integers $y_{n,o}$ and $y_{n,1}$ such that

$$\{v_{n,i}\} = \{y_{n,pi}\} .$$

<u>Proof</u>: By the use of (4.2), to prove the necessity, it is sufficient to show

that for any odd integer α and positive integer n, there exists an odd integer p such that $(6, p) = 1$ and $\alpha \equiv u_{p+1} + u_{p-1} \pmod{2^n}$.

We prove this statement by induction.

When $n = 1$, then $p = 1$. When $n = 2$, we have $p = 1$ if $\alpha \equiv 1 \pmod 4$ and $p = 5$ if $\alpha \equiv 3 \pmod 4$.

Suppose the statement is true when $n = k \geq 2$. Then for any odd integer α, there exists a positive integer p such that $(6, p) = 1$ and

$$\alpha \equiv u_{p+1} + u_{p-1} \pmod{2^k}.$$

It implies that

$$\alpha \equiv u_{p+1} + u_{p-1} \pmod{2^{k+1}}$$

or

$$\alpha \equiv u_{p+1} + u_{p-1} + 2^k \pmod{2^{k+1}}. \tag{4.3}$$

As $(6, p) = 1$, we have

$$u_{(p+H_{k+1}/2)+1} + u_{(p+H_{k+1}/2)-1} \equiv u_{p+1} + u_{p-1} + 2^k \pmod{2^{k+1}}.$$

Thus from (4.3),

$$\alpha \equiv u_{a+1} + u_{a-1} \pmod{2^{k+1}},$$

where $a = p$ or $p + H_{k+1}/2$.

Hence the statement is proved by induction since $(6, p + H_{k+1}/2) = (6, p)$, when $k \geq 2$. The proof of sufficiency follows immediately from (4.2).

Q.E.D.

Theorem 4.2 suggests that we adopt the following new generator

$$v_{n,i} \equiv \alpha v_{n,i-1} + v_{n,i-2} \qquad (\mathrm{mod}\ 2^n)\ , \tag{4.4}$$

where α is an odd integer. The pseudo-random number sequence $Z = \{z_{n,i}\}$ is then defined by $z_{n,i} = v_{n,i}/2^n$. From theorem 4.2, we have $Z = X_p$ for some positive integer p. Therefore there is relation between Z and X $(X = \{x_{n,i}\})$. In order to apply the theorems in sections 2, 3 and 4 of Chapter 3 to the sequence Z, we assume $v_{n,o} = 0$ and $v_{n,1}$ is odd. From the properties of X, we have the following equalities:

$$E(z_{n,i}) = 0.5 + E(z_{k,i})/H_n - 2^{k-n-1}\ , \quad \text{when } n \geq k \geq 5\ . \tag{4.5}$$

$$E(z_{n,i}^2) = \frac{1}{3} + [E(z_{k,i}^2) + (2^{n-k} - 1)E(z_{k,i})]/(2^{n-k}H_n) - (3 - 2^{k-n})/(3 \times 2^{n-k+1})\ . \text{ when } n \geq k \geq 5\ . \tag{4.6}$$

$$E(z_{n,i}\, z_{n,i+s}) = 0.25 + 2^{12-2n}[E(z_{6,i}\, z_{6,i+s}) + (2^{n-6} - 1)E(z_{6,i})] - [2^{2-2n}(v_{n-1,s} - v_{5,s}) - 47 \times 2^{6-2n} + 95 \times 2^{-n}]/3$$
$$\text{when } s \equiv 1 \text{ or } 5 \ (\mathrm{mod}\ 6)\ . \tag{4.7}$$

$$E(z_{n,i}\, z_{n,i+s}) = 0.25 + 2^{12-2n}[E(z_{6,i}\, z_{6,i+s}) + (2^{n-6} - 1)E(z_{6,i})] - [2^{2-2n}(v_{n,s} - v_{6,s}) - 23 \times 2^{7-2n} + 47 \times 2^{1-n}]/3$$
$$\text{when } s \equiv 3 \ (\mathrm{mod}\ 6)\ . \tag{4.8}$$

Here $v_{k,i} \equiv v_{n,i} \pmod{2^k}$, when $k < n$.

The mean, variance and serial correlation of odd lag of Z can be computed by using equations (4.5) - (4.8). The values are close to what we expect of a "truely random" sequence.

Instead of choosing p such that $\{v_{n,i}\} = \{y_{n,pi}\}$, it seems more inviting to select a "good" α . The use of $\alpha = 2^{\beta} + 1$, where β is a positive integer, is attractive because multiplication of such an α is simply a shift and add when the sequence is generated in a binary computer.

Section 2: Statistical tests

Seven statistical tests are applied to the new generator (4.4), with $n = 32$ and $\alpha = 2^{\beta} + 1$, where $\beta = 7$, 17 and 22. Moreover we require that $v_{n,o} = 0$ and $v_{n,1}$ is odd. The tests include the 'frequency' test and 'serial' test which are elementary. The remaining five tests are 'sum of N' test when N = 2 and 3, 'Max of N' and 'Min of N' test when N = 2, 3, 4 and 5, 'runs up and down' test and the 'poker' test. Since the tests are quite standard, the descriptions of them are left out here and details can be found in Downham and Roberts (1967), Knuth (1968) and Lewis (1975). The 'poker' test is the one suggested by Knuth (1968). Each test is applied to the same pseudo-random number sequence and hence the test results are not independent. The results together with the degrees of freedom of χ^2 and the numbers from the sequence tested are listed in table 4.1. All the calculations are carried out on the Hewlett-Packard 9830A Calculator in the Department of Mathematics.

The test results are satisfactory. All the tests, except one, are passed at 5 percent significance level. Thus the new generator is acceptable.

Statistical tests have also been applied to the new generator for the case $\alpha = 11$. The results are, however, not satisfactory. Hence the value of α should not be too small or too large in comparision with 2^n . It is still an open problem as to which value of the odd integer α is most appropriate.

Table 4.1

Test		Degrees of freedom	Numbers from the sequence tested	$\beta = 7$		$\beta = 17$		$\beta = 22$	
				run 1	run 2	run 1	run 2	run 1	run 2
Frequency test		127	10000	0.6664	0.1251	0.1587	0.8264	0.5160	0.7764
Serial test of $(z_{n,i}, z_{n,i+1})$		255	2×5000	0.7995	0.5948	0.6217	0.0016*	0.1251	0.8980
Sum of N test	N = 2	127	2×5000	0.8508	0.5517	0.8770	0.0618	0.7157	0.5359
	N = 3	127	3×5000	0.6179	0.8438	0.9278	0.6103	0.8980	0.6255
Max. of N test	N = 2	99	2×2000	0.8023	0.1271	0.3745	0.1949	0.0901	0.8413
	N = 3	99	3×2000	0.6064	0.5359	0.5517	0.2514	0.2946	0.7910
	N = 4	99	4×2000	0.1635	0.5199	0.8554	0.1736	0.3050	0.7881
	N = 5	99	5×2000	0.9916	0.9726	0.8577	0.1112	0.7224	0.4013
Min. of N test	N = 2	99	2×2000	0.4483	0.4721	0.4090	0.3156	0.5438	0.3228
	N = 3	99	3×2000	0.8830	0.6985	0.5160	0.5359	0.8907	0.8212
	N = 4	99	4×2000	0.3085	0.7967	0.3483	0.8340	0.8106	0.2483
	N = 5	99	5×2000	0.7088	0.2946	0.2709	0.3121	0.7357	0.3015
Runs up and down test		5	10000	(0.10,0.20)	(0.30,0.50)	(0.05,0.10)	(0.50,0.70)	(0.50,0.70)	(0.80,0.90)
Poker test		3	5×2000	(0.10,0.20)	(0.995,1)	(0.05,0.10)	(0.20,0.30)	(0.10,0.20)	(0.30,0.50)

(The tabulated value is the probability that the appropriate Chi-square variate will exceed the computed value. (a, b) in the last two rows indicates the interval in which the probability falls. The only value that calls for rejection at significance level 0.05 is starred.)

REFERENCES:

1. Dieter U. (1971), Pseudo-Random Numbers: The Exact Distribution of Pairs, Math. Computation 25, 855-883.

2. Dieter U. and Ahrens J. (1971), An Exact Determination of Serial Correlations of Pseudo-Random Numbers, Numerische Mathematik 17(2), 101-123.

3. Downham D.Y. and Roberts F.D.K. (1967), Multiplicative Congruential Pseudo-Random Number Generators, Computer J. 10, 74-77.

4. Fuller A.T. (1976), The period of Pseudo-Random Numbers generated by Lehmer's Congruential Method, Computer J. 19, 2, 173-177.

5. Gebhardt F. (1967), Generating Pseudo-Random Numbers by shuffling a Fibonacci sequence, Math. Computation 21, 708-709.

6. Gorenstein S. (1967), Testing a Random Number Generator, Comm. ACM. 10, 2, 111-118.

7. Green B.F., Smith J.E. and Klem L. (1959), Empirical Tests of an Additive Random Number Generator, J.ACM. 6, 527-537.

8. Hull T.E. and Dobell A.R. (1962), Random Number Generators, SIAM Rev. 4, 230-254.

9. Jansson B. (1966), Random Number Generators, Stockholm: Almqvist and Wiksell.

10. Knuth D.E. (1968), The Art of Computer Programming, vol 2: Seminumerical Algorithms, Addison Wesley Publishing Company.

11. Lehmer D.H. (1951), Mathematical methods in large scale computing units, Annals Comp. Lab. Harvard Univ. 26, 141-146.

12. Lewis T.G. (1975), Distribution Sampling for Computer Simulation, Lexington Books.

13. Tausworthe R.C. (1965), Random Numbers generated by Linear Recurrence Modulo Two, Math. Computation 19, 201-209.

14. Zierler N. (1959), Linear Recurring Sequences, J. SIAM 7, 1, 31-48.

* * * * *