Fibonacci Congruences and Applications

René Blacher
Laboratory LJK, Université Joseph Fourier, Grenoble, France
E-mail: rene.blacher@aliceadsl.fr
Received May 24, 2011; revised June 14, 2011; accepted June 20, 2011

Abstract

When we study a congruence \( T(x) \equiv ax \pmod{m} \) as pseudo random number generator, there are several means of ensuring the independence of two successive numbers. In this report, we show that the dependence depends on the continued fraction expansion of \( m/a \). We deduce that the congruences such that \( m \) and \( a \) are two successive elements of Fibonacci sequences are those having the weakest dependence. We will use this result to obtain truly random number sequences \( x_n \). For that purpose, we will use non-deterministic sequences \( y_n \). They are transformed using Fibonacci congruences and we will get by this way sequences \( x_n \). These sequences \( x_n \) admit the IID model for correct model.

Keywords: Fibonacci Sequence, Linear Congruence, Random Numbers, Dependence, Correct Models

1. Introduction

In this paper, we present a new method using Fibonacci sequences to obtain real IID sequences \( x_n \) of random numbers\(^1\). To have random number two methods exists: 1) use of pseudo-random generators (for example the linear congruence), 2) use of random noise (for example Rap music).

But, up to no completely reliable solution had been proposed ([1]-[3]). To set straight this situation, Marsaglia has created a Cd-Rom of random numbers by using sequences of numbers provided by Rap music. But, he has not proved that the sequence obtained is really random.

However, by using Fibonacci congruence, there exists simple means of obtaining random sequences whose the quality is sure (cf [4]): one uses the same method as Marsaglia, but one transforms the obtained sequence by Fibonacci congruences. Then, one obtains sequence of real \( x_n \) such that the IID model is a correct model of \( x_n \).

1.1. Fibonacci Congruence

Linear congruences \( T(x) \equiv ax \pmod{m} \) are often used as pseudo-random generators. In this case, we try to choose \( a \) and \( m \) so that successive pseudorandom numbers behave as independent. Of course, we can only ensure that it is the case of \( p \) successive numbers \( p \) where \( 2^p \leq m \). To choice \( a \) and \( m \), one can use the spectral test or the results of Dieter (cf [5]) which allow to choose the best “\( a \)”.

Unfortunately, the conditions which ensure the independence of three successive numbers are not those which ensure the best independence of two successive numbers, for example.

Indeed, in this paper, we will study the conditions which ensure the independence of only two successive numbers and we will see with astonishment that this is the Fibonacci congruence which provides the best empirical independence.

We shall study the set
\[
E_z = \left\{ \ell \left( \frac{\ell}{(\ell)} \right) \mid \ell \in \{0,1,\ldots,m-1\} \right\}
\]
when \( \tau \equiv z \pmod{m} \) and \( 0 \leq \tau < m \) if \( z \in \mathbb{Z} \). We will understand that this dependence depends on the continued fraction \( \frac{m}{a} \), i.e. it depends on sequences \( r_n \) and \( h_n \) defined in the following way.

Notations 1.1 Let \( r_0 = m \) and \( r_1 = a \). One denotes by \( r_n \) the sequence defined by \( r_n = h_{n-1}r_{n-1} + r_{n+1} \) the Euclidean division of \( r_n \) by \( r_{n+1} \) when \( r_{n+1} \neq 0 \). Moreover, one denotes by \( d \) the smallest integer such as \( r_{d+1} = 0 \). One sets \( r_{d+2} = 0 \).

One sets \( k_0 = 0 \), \( k_1 = 1 \) and \( k_{n+2} = h_{n+1}k_{n+1} + k_n \) if \( n+1 \leq d \).

Then, dependence depends on the \( h_i \): more they are small, more the dependence is weak.

Theorem 1 Let \( (x_0, y_0) \in E_z \). Let \( R^d = \left\{ (x_0, x_0 + k) \bigotimes (y_0, y_0 + r_{d-2}) \right\} \) and let \( R_0 = R^0 \).
be the rectangle $R^0$ modulo $m$. Then

If $n$ is even,

$$E_2 \cap R_0 = \left\{(x_0 + k_{n-1} \ell, y_0 + r_{n-1} \ell) | \ell = 0, 1, 2, \ldots, h_{n-1}\right\}.$$ 

Moreover the points

$$\left(x_0 + k_{n-2} + k_{n-1} \ell, y_0 + r_{n-2} - r_{n-1} \ell\right)$$

are lined up modulo $m$.

If $n$ is odd, $E_2 \cap R_0$

$$= \left\{(x_0 + k_{n-2} + k_{n-1} \ell, y_0 + r_{n-2} - r_{n-1} \ell) \right| \ell = 0, 1, 2, \ldots, h_{n-1}\right\}.$$ 

Moreover, the points

$$\left(x_0 + k_{n-2} + k_{n-1} \ell, y_0 + r_{n-2} - r_{n-1} \ell\right)$$

are lined up modulo $m$.

Of course, in general, it is only on the border that $R_0$, the rectangle modulo $m$, satisfies $R_0 \neq R^0$. If not, $R_0$ is a normal rectangle.

For example if $x_0 = y_0 = 0$, this theorem means that the rectangle $[0, k_0/2] \cap [r_{n-2}/2, r_{n-1}/2]$ does not contain points of $E_2$ if $n$ is even:

$$E_2 \cap [0, k_0/2] \cap [r_{n-2}/2, r_{n-1}/2] = \emptyset.$$ 

If $h_{n-1}$ is large, that will mean that an important rectangle of $\mathbb{R}^2$ is empty of points of $E_2$ that will mark a breakdown of independence.

As $h_1 \geq 1$, the congruence which defines the best independence of $E_2$ will satisfy $h_1 = 1$ and $h_2 = 2$. In this case we call it congruence of Fibonacci. Indeed, there exists $n_0$ such that $a = \beta_{n_0}$ and $m = \beta_{n_0+1}$, where $\beta_n$ is the sequence of Fibonacci: $\beta_0 \beta_1 = 1$, $\beta_{n+2} = \beta_{n+1} + \beta_n$. As a matter of fact the sequence $r_n$ is the sequence of Fibonacci except for the last terms (i.e. except for $f_{n+1} = f_1 = 1$). It is also the case for sequence $k_n$.

Remark 1.1 In fact, when we use sequence $h_n$, we use Euclidean Algorithm. Now, Dieter has also used this algorithm to compute the dependence of $(T^n(x_0), T^{2^n}(x_0))$ when $m = 2^2$. But he has not understood the part of the $h_n$’s in this dependence.

1.2. Application: Building of Random Sequence

Unfortunately, congruences of Fibonacci cannot be used in order to directly generate good pseudo random sequences because $T^2 = \pm I^2$ where $I^2$ is the identity (cf page 141 of [6]). Indeed in this case, the pseudo random sequence $x_n = \overline{T^n(x_0)}$ checks $x_{n+2} = \pm x_n$.

However, one can use congruence of Fibonacci in order to build IID sequences by transforming some random noise $y_n$.

Definition 1.2 Let $q \in \mathbb{N}^*$. Let $T$ be the congruence of Fibonacci modulo $m$. We define the function of Fibonacci $T_q$ by $T_q = P_q \overline{T}$ where

1) $\overline{T}(x) = \overline{T(mx)/m}$,

2) $P_q(z) = 0, b, b, \ldots \ b$ when $z = 0, b, b, \ldots$ is the binary writing of $z$.

We choose $y_n \in \{0/m, 1/m, \ldots, (m-1)/m\}$, $n = 1, 2, \ldots, N$. Then $y_n$ admits for correct model a sequence of random variables $Y_n$ defined on a probability space $(\Omega, \mathcal{A}, P)$. Then, we will impose to $y_n$ that the conditional probabilities of $Y_n$ admit densities with Lipschitz coefficient bounded by $K_0$ not too large.

In fact, since $Y_n$ has discrete value, we can always assume that $Y_n$ has a continuous density.

Notations 1.3 We denote by $\mu_n$ be the uniform measure defined on $\{0/m, 1/m, \ldots, (m-1)/m\}$ by $\mu_n(k/m) = 1/m$ for all $k \in \{0, 1, \ldots, m-1\}$.

For all permutation $\phi$ of $\{1, 2, \ldots, N\}$, for all $n \in \{1, 2, \ldots, N\}$, we denote by $f_{n, \phi}\left(y_1', y_2', \ldots\right)$ the conditional density with respect to $\mu_n$ of $Y_{\phi(n)} = y$ given $Y_{\phi(1)} = y_1', Y_{\phi(2)} = y_2', \ldots$.

Since $Y_n$ is discrete, we can also assume that $f_{n, \phi}(y_1', y_2', \ldots)$ has a finite Lipschitz coefficient.

Notations 1.4 We denote by $K_0$ a constant such that, for all permutation $\phi$ of $\{1, 2, \ldots, N\}$, for all $n \in \{1, 2, \ldots, N\}$,

$$f_{n, \phi}(y_1', y_2', \ldots) \leq K_0 |y - y'|.$$ 

In order to simplify the proofs we suppose $K_0 > 1$.

Now, we shall prove easily that the conditional probabilities of $T_q(Y_{\phi})$

$$P\left[T_q(Y_{\phi}) = x_n | Y_{\phi(n)} = y_1', Y_{\phi(2)} = y_2', \ldots, Y_{\phi(N)} = y_N'\right]$$

$$= 1/m \left[1 + O(1)K_0 2^n/m\right].$$

Then we shall choose $m$ and $q$ such that

$$|\epsilon| \leq K_0 2^n/m$$

is small enough. We shall deduce that, for all Borel set $B_0 \subset \{0/2^n, 1/2^n, \ldots, (2^n - 1)/2^n\}^N$,

$$P\left[\left\{x_1, \ldots, x_n\right\} \in B_0\right] = L(B_0) \left[1 + O(1)N\epsilon\right]$$

where $L$ is the measure corresponding to the Borel measure in the case of discrete space: $L \left[k_1/2^n, \ldots, k_N/2^n\right] = 1/2^{Nq}$. Then

$$x_n = T_q(y_n)$$

cannot be differentiated from an IID sequence. Indeed, it is well known that, for a sample $x_n$, there is many models correct: in particular, if $x_n$ is extracted of an IID sequence, models such that

$$P\left[\left\{x_1, \ldots, x_n\right\} \in B_0\right] = L(B_0) \left[1 + \epsilon\right]$$

are correct if $\epsilon$ is small enough with respect to N. Reciprocally, if the sequence of random variables $X_n$ checks

$$P\left[\left\{x_1, \ldots, x_n\right\} \in B_0\right] = L(B_0) \left[1 + \epsilon_Bo\right],$$

the model IID is also a correct model for the sequence $X_n$.

Thus one will be able to admit that the IID model is a correct model for the sequences $x_n$. As a matter of fact, one will be able to admit that there exists another correct model $Y_{n^0}$ of $Y_n$ such that $T_q(Y_{n^0})$ is exactly the IID sequence.

Now there exists noises $y_n$ such that $K_0$ is not too large. For example these sequences can be built by using texts. In this case we can prove the result: in order that $x_n$ is IID, it suffices that $y_n$ admits a correct model
such that $K_n$ is not too large. However, it is a condition which can be imposed easily by transforming some noises. The advantage compared with the CD-ROM of Marsaglia is that this result is proved. Of course, we tested such sequences.

So finally we can indeed build sequences $x_n$ admitting for correct model the IID model by using Fibonacci congruences. This means that, a priori, these sequences $x_n$ behave as random sequences. It is always possible that they do not satisfy certain tests. But it will be a very weak probability as we know it is the case for samples of sequences of IID random variables.

We point out that a first version of these results are in [4]. Moreover, all these results and the proofs are detailed in [7].

Note that to use the congruence of Fibonacci method is completely different from the method using Fibonacci sequence with $X_{n+1} = X_n + X_{n-1}$ modulo m, which is moreover a bad generator; cf page 27 of [1].

2. Dependence Induced by Linear Congruences

In this section, we study the set $E_2 = \{\ell, T(\ell) | \ell \in \{0, 1, \cdots, m-1\}\}$ when $T$ is a congruence $T(x) \equiv ax \mod m$.

2.1. Notations

We recall that we define sequences $r_n$ and $h_n$ by the following way: we set $r_0 = m$, $r_1 = a$ and $r_n = h_{n+1}r_{n+1} + r_{n+2}$, the Euclidean division of $r_n$ by $r_{n+1}$, when $r_{n+1} \neq 0$. One denotes by $d$ the smallest integer such as $r_{d+1} = 0$. One sets $r_{d+2} = 0$. Moreover, $k_0 = 0$, $k_1 = 1$ and $h_{n+1} = h_{n+1}k_{n+1} + k_n$ if $n+1 \leq d$.

Then $m/a = h_1 + 1/(h_2 + 1/(h_3 + \cdots))$.

Therefore, $h_n \geq 1$ for all $n = 1, 2, \cdots, d$ and $r_{d+1} = h_1r_1 + r_{d+2} = h_1r_1 + 0 = h_1r_1$. The full sequence $r_n$ is thus the sequence $r_0 = m$, $r_1 = a$, $\cdots$, $r_{d+1} = 0$, $r_{d+2} = 0$. Then, if $T$ is a Fibonacci congruence, $r_n$ is the Fibonacci sequence $f_n$, except for the last terms.

Remark that if $h_1 = 1$ for $n = 1, 2, \cdots, d - 1$, $K_n$ is also the Fibonacci sequence for $n = 1, 2, \cdots, d$. Indeed by definition, $k_0 = 0$, $k_1 = 1$ and $h_{n+1} = h_{n+1}k_{n+1} + k_n$ if $n+1 \leq d$.

2.2. Theorems

Now, in order to prove the theorem 1, it is enough to prove the following theorem.

Theorem 2 Let $n \in \{2, 3, \cdots, d\}$. Then, if $n$ is even,

\[
E_2 \cap \left\{(0, k_n) \mid 0, r_{n-2} \right\} = \left\{(k_{n+1}, r_{n-1}) \mid \ell = 0, 1, 2, \cdots, h_{n-1}\right\}.
\]

Moreover the points $(k_{n+1}, r_{n-1})$ are lined up.

If $n$ is odd,

\[
E_2 \cap \left\{(0, k_n) \mid 0, r_{n-2} \right\} = \left\{(k_{n+1} + k_n \ell, r_{n-1} - r_{n-2} \ell) \mid \ell = 0, 1, 2, \cdots, h_{n-1}\right\}.
\]

Moreover, the points $(k_{n+1} + k_n \ell, r_{n-1} - r_{n-2} \ell)$ are lined up.

Then, if there exists $h_1$ large, there is a breakdown of independence. For example if $n = 2$, it is a well-known result. Indeed, $m = r_0 = r_1 = 1$ and $k_2 = h_1 = [m/a]$ where $[x]$ means the integer part of $x$. Thus, the rectangle $\text{Rect}_a = [0, m/(2a)] \times [m/2, m]$ will not contain any point of $E_2$. However, this rectangle has its surface equal to $m^2/(4a)$. Thus if “$a$” is not sufficiently large, i.e if $h_1$ is too large, there is a breakdown of independence.

We confirm by graphs the previous conclusion. We suppose $m = 21$. If $a = 13$, we have a Fibonacci congruence; cf Figure 1. If one chooses $a = 10$, $\sup(h_1) = 20$: cf Figure 2. If one chooses $a = 5$, $\sup(h_1) = 5$: cf Figure 3.

Then, in order to avoid any dependence, it is necessary that $\sup(h_1)$ is small.

2.3. Distribution of $T([c, c'])$ When $T$ is a Fibonacci Congruence

We assume that $T$ is a Fibonacci congruence. Let $I = [c, c' \cap \{0, 1, \cdots, m-1\}]$ where $c, c' \in \{0, 1, \cdots, m-1\}$.

We are interested by $\overline{T}(I)$ or $\overline{T}(I')$ because $T^2 = \pm Id$. Since $\overline{T}(I)$ behaves as independent of $I$, normally, we should find that $\overline{T}(I)$ and, therefore $\overline{T}^{-1}(I')$, is well distributed in $\{0, 1, \cdots, m-1\}$. As a matter of fact it is indeed the case.

Indeed, let $k' = n = 1, 2, \cdots, c' - c$, be a permutation of $\{c, c+1, \cdots, c' - 1\}$ such that $\overline{T}^{-1}(k') < \overline{T}^{-1}(k^2) < \overline{T}^{-1}(k^3) < \cdots < \overline{T}^{-1}(k^{c' - c})$. Then, for all numerical simulations which we executed, one has always obtained

\[
\overline{T}^{-1}(k')/m-r|N(I) \leq \varphi(m)/N(I)
\]

where $\varphi(m) \ll \log(m)$. In fact, it seems that $\varphi(m)$ is of the order of $\log(\log(m))$. Moreover, $\max_{k = 0, 1, \cdots, N(I) - 1} |N(I) \overline{T}^{-1}(k')/m-r|$ seems maximum when $I$ is large enough: $c' - c > m/2$.

For example, in Figures 4, 5 and 6, we have the graphs $N(I) \overline{T}^{-1}(k')/m-r$, $r = 0, 1, \cdots, N(I) - 1$ for
various Fibonacci congruences when \( c' - c = 100 \).

3. Proof of Theorem 2

In this section, the congruences are congruences modulo \( m \). Now the first lemma is obvious.

**Lemma 3.1** For \( n = 3, 4, \ldots, d + 1 \), \( k_{n+1} > k_n > k_{n-1} \).

Moreover \( k_{n+2} = h_{n+1}k_n + k_{n+1} \) is the Euclidean division.
of $k_{n+2}$ by $k_{n+1}$.

Now, we prove the following results.

**Lemma 3.2** Let $n = 0, 1, 2, \cdots$, $d$. If $n$ is even, $k_{n+1}a = m - r_n$. If $n$ is odd, $k_{n+1}a = r_n$.

**Proof.** We prove this lemma by recurrence. For $n = 0$, $k_0a = 0 = 0 = m - m = m - r_0$. For $n = 1$, $k_1a = a = a = r_1$.

We suppose that it is true for $n$.

One supposes $n$ even. Then, $k_{n+1}a = ah_kk_{n+1} + ak_{n+1} = -h_nr_n + r_{n+1} = r_{n+1}$.

One supposes $n$ odd. Then, $k_{n+1}a = ah_kk_{n+1} + ak_{n+1} = h_nr_n - r_{n+1} = -r_{n+1} = m - r_{n+1}$.

Therefore, $k_{n+1}a = m - r_{n+1}$.

**Lemma 3.3** Let $n = 2, 3, \cdots, d + 1$. Let $t \in [1, 2, \cdots, k_{n+1} - 1]$. If $n \geq 2$ is even, $r_{n+1} \leq \overline{at} < m - r_n$.

If $n \geq 3$ is odd, $m - r_{n+1} \geq \overline{at} > r_n$.

Moreover, if $n \geq 2$ is even, $k_{n+1}a = m - r_n$. If $n \geq 3$ is odd, $k_{n+1}a = r_n$.

**Proof.** The second assertion is Lemma 3.2. Now, we prove the first assertion by recurrence.

One supposes $n = 2$. Then, $m = r_0 = h_r1 + r_2 = h_0a + r_2$.

Moreover, $k_3 = h_1$. If $1 \leq t < h_1 = k_2$, $r_1 = a$ at $< \overline{at} < m - r_1$.

If $h_1 = k_2 = 1$, $k_3 = h_1k_2 + k_1 = h_2 + 1$. Then, $1 \leq t < h_2$. Then, $\overline{at} = \overline{ta} = \overline{tr}_2$.

Moreover, $m - r_2 \geq m - r_2 \geq m - h_rk_2 = r_0 - h_rk_2 = r_0 - \overline{tr}_2$.

Therefore, because $at = m - r_2$, $\overline{at} = m - r_2$.

Therefore, $m - r_2 \geq \overline{at} > r_2$.

One supposes the first assertion is true for $n$ where $2 \leq n \leq d$.

Let $0 < t' < k_{n+1}$. Let $t' = fk_n + e$ be the Euclidean division of $t$ by $k_n$: $e \leq k_n$.

Then, $f \leq h_m$. If not, $t' \geq (h_m + 1)k_n + e \geq h_mk_n + k_{n+1} = k_{n+1}$.

One supposes $n$ even.

In this case, $r_{n+1} \leq \overline{at} < m - r_n$ for $t \in [1, 2, \cdots, k_{n+1} - 1]$.

Moreover, $\overline{at'} = f\overline{ak}_n + e = f(m - r_n) + ea = \overline{fr}_a + ea$.

First, one supposes $e = 0$. Then, $f \geq 1$.

Moreover, because $n \geq 2$, $m - r_2 \geq m - fr_n \geq m - h_nr_n = m - (r_{n+1} - r_{n+1})$.

Therefore, because $\overline{at} = \overline{fr}_a$, $\overline{at'} = m - fr_n$.

Now, one supposes $f < h_n$ and $e > 0$.

By recurrence, $m - r_n \geq ae \geq ae - fr_n \geq r_{n+1} - fr_n \geq r_{n+1} - (h_{n+1} - 1)r_n$.

Therefore, because $at' = \overline{fr}_a + ae$, $\overline{at'} = \overline{ae} - fr_n$.

Therefore, $m - r_n \geq \overline{at'} > r_{n+1}$.

One supposes $f = h_n$, $e \neq k_{n+1}$ and $e > 0$.

If $e \neq k_{n+1}$, $ae \neq \overline{ak}_{n+1}a$. Indeed, if not, $a(e - \overline{ak}_{n+1}a) = 0$. For example, if $e - \overline{ak}_{n+1}a > 0$, $k_{n+1} > e - \overline{ak}_{n+1}a$. Then, because our recurrence, $a(e - \overline{ak}_{n+1}a) > r_{n+1} > 0$: it is impossible.

Now, if $n = 2$, $k_{n+1}a = \overline{ak}_a = a = r_{n+1}$.

Moreover, if $n > 2$, $n \geq 4$. Then, by recurrence $k_{n+1}a = r_{n+1}$.

Then, if $e = k_{n+1}$, $ae = \overline{ak}_{n+1}a = r_{n+1}$. Then, $\overline{ae} > r_{n+1}$.

Moreover, $m - r_{n+1} \geq \overline{at} > r_{n+1}$.

One supposes $f = h_n$ and $e = k_{n+1}$. Then, $t' = h_nk_n + k_{n+1} = k_{n+1}$. It is opposite to the assumption.

Then, in all the cases, for $t' \in [1, 2, \cdots, k_{n+1} - 1]$, $m - r_{n+1} \geq \overline{at} > r_{n+1}$. Therefore, the lemma is true for $n + 1$ if $n$ is even. Then, it is also true for $n + 1 = 3$.

One supposes $n$ odd with $n \geq 3$. One proves the recurrence by the same way as if $n$ is even (cf [7]). Then the lemma is true for $n + 1$.

**Lemma 3.4** The following inequalities holds: $k_{d+1} \leq m$.

**Proof.** If $t' \in [1, 2, \cdots, k_{d+1} - 1]$, by lemma 3.3, $r_d \leq \overline{at} < m - r_{d+1}$ or $m - r_{d+1} \geq \overline{at} > r_{d+1}$, i.e. $r_d \leq \overline{at} < m$ or $m - r_{d+1} \geq \overline{at} > 0$ where $r_d > 0$. Then, $0 < \overline{at} < m$ or $m > \overline{at} > 0$.

Then, if $k_{d+1} > m$, there exists $t_0 \in [1, 2, \cdots, k_{d+1} - 1]$ such that $t_0 = m$, i.e. $\overline{at_0} = am = 0$. It is impossible.

**Lemma 3.5** Let $t, t' \in [1, 2, \cdots, k_{d+1} - 1]$ such that $at = \overline{at'}$. Then, $t = t'$.

**Proof.** Suppose $t > t'$. Then, $a(t - t') \equiv 0$ and $a(t - t') = 0$. Then, by lemma 3.3, $r_d \leq a(t - t') < m - r_{d+1}$ or $m - r_{d+1} \geq a(t - t') > r_{d+1} = 0$ where $r_d > 0$. Then, $0 < a(t - t')$. It is a contradiction.

**Lemma 3.6** Let $n = 1, 2, \cdots, d$. Let $H_n = h_kk_1 + h_kk_2 + h_kk_3 + \cdots + h_kk_n$. Then, $H_{n+1} = h_{n+1} + k_{n+1}$

The proof is basic.

**Lemma 3.7** Let $n = 1, 2, 3, \ldots, d - 1$. Let $L_n = \{t | t = 0, 1, 2, \cdots, H_n\}$. Then, for all $n \geq 1$, $L_{n+1} = \{t \cdot g | g \in L_n, g \leq h_{n+1}\}$.

Copyright © 2011 SciRes. OJS
Proof. Let \( l \in L_n \), \( l \leq H_n \). Let \( g \leq h_{n+1} \). Therefore, if \( t = l + g k_{n+1}, t \leq H_n + h_{n+1} k_{n+1} = H_{n+1} \). Therefore, \( \{ t = l + g k_{n+1} \mid l \notin L_n, g \leq h_{n+1} \} \subseteq L_{n+1} \).

Reciprocally, let \( t \in L_n \), and let \( t = f k_{n+1} + e \), \( e < k_{n+1} \) be the Euclidean division of \( t \) by \( k_{n+1} \).

We know that \( H_n = k_{n+1} + k_n - 1 \geq k_{n+1} \). Therefore, \( e \leq H_n \). Therefore, \( e \in L_n \).

Therefore, if \( f \leq h_{n+1} \), \( t = f k_{n+1} + e \in \{ t = l + g k_{n+1} \mid l \in L_n, g \leq h_{n+1} \} \).

Moreover, if \( f > h_{n+1} + 1 \), \( t = f k_{n+1} + e \in \{ t = l + g k_{n+1} \mid l \in L_n, g \leq h_{n+1} \} \).

Therefore, \( t \in L_{n+1} \).

Then, suppose \( f = h_{n+1} + 1 \). Then, \( t = f k_{n+1} + e \in \{ t = l + g k_{n+1} \mid l \in L_n, g \leq h_{n+1} \} \).

Therefore, \( e \in L_n \).

Lemma 3.8 Let \( F = \{ \bar{a} k + \bar{b} \mid \bar{a}, \bar{b} \in Z \} \). We set \( E_1 = \{ \alpha^* s \mid s \in Z \} \) where \( \alpha^* = 0 \) and \( \alpha^* > \alpha^*_s \) for all \( s \in Z \).

Then, for all \( s \in Z \), \( \alpha^*_s - \alpha^* = r_s \) or \( \alpha^*_s - \alpha^* = r_s \) or \( \alpha^*_s - \alpha^* = r_s \).

Proof We prove this lemma by recurrence.

Suppose \( n = 1 \). Then, \( r_1 = a, H_1 = h_k = k_2 = h_1 \).

Therefore, \( F_1 = \{ \bar{a} k + \bar{b} \mid \bar{a}, \bar{b} \in Z \} \).

Then, \( E_1 = \{ \alpha^* s \mid s \in Z \} \).

Therefore, the lemma is true for \( n = 1 \).

Suppose the lemma is true for \( n \).

Then, \( E_{n+1} = \{ \bar{a} k + \bar{b} \mid \bar{a}, \bar{b} \in Z \} \), where \( H_{n+1} = h_k + h_k + h_k + \ldots + h_k = H_n + h_k k_{n+1} \).

Because \( t \in H_{n+1} \), \( t = l + g k_{n+1} \) where \( g \leq h_{n+1} \). By lemma 3.7, \( \bar{a} k = a(t + g k_{n+1}) = \bar{a} t + (-1)^{n+2} \).

Therefore, \( \{ \bar{a} t + (-1)^{n+2} \} \subseteq E_2 \).

Suppose that \( n \) is even.

Then, \( \alpha^* + (-1)^n \).

Therefore, \( \alpha^* + (-1)^n \).

Use the recurrence. Suppose \( \alpha^*_s - \alpha^* = r_s \).

Then, \( \alpha^*_s + (-1)^n \).

Therefore, \( \alpha^*_s + (-1)^n \).

Suppose that \( n \) is odd. One proves this result by the same way as when \( n \) is even (cf [7]).

Proof 3.9 Now one proves theorem 2.

Suppose that \( n \) is even.

Then, \( k_{n+1} = r_{n+1}, 2k_{n+1} = 2r_{n+1}, \ldots \).

Therefore, \( \bar{a} k = a(t + g k_{n+1}) = \bar{a} t + (-1)^{n+2} \).

Therefore, \( \{ \bar{a} t + (-1)^{n+2} \} \subseteq E_2 \).

Moreover, \( r_{n+2} = r_{n+1} \).

On the other hand, by lemma 3.8, all the points of \( E_2 = \{ t, \bar{a} \} \), \( t \leq H_n \), have ordinates distant of \( r_s \) or \( r_s \).

Therefore, if \( \alpha^*_s \), then there is other points of \( E_3 \cap [0, H_n] \cap [0, r_{n+2}] \) that the points \( \{ (k_{n+1}, r_{n+1}) \} \subseteq E_2 \).

Moreover, \( r_{n+2} = r_{n+1} \).

There exists \( \epsilon_0 \in [1, 2, \ldots, h_{n+1}] \).
(x_1, y_1) \in E_\ell \cap \left[ \left[ 0, H_{n-\ell} \right] \times \left[ 0, r_{n-\ell} \right] \right] \quad \text{such that} \quad r_{n-\ell} y = y_1 = r_n.

Because \( H_{n-\ell} = k_n + k_{n-\ell} - 1 < k_{n+1} \leq k_{d+1} \), by lemma 3.5, there exists an only \( t \in \{1, \ldots, H_{n-\ell} \} \), such that \( at = y_1 \), \( t = x_1 \). Because \( y_1 \neq 0 \), there exists an only \( t \in \{1, \ldots, H_{n-\ell} \} \), such that \( at = y_1 \).

Now, \( r_{n-\ell} a y = y_1 = at \ell k_{n-\ell} - at = r_n - ak_{n-\ell} \). Then, \( at \ell k_{n-\ell} - ak_{n} = at \). Then, \( a(1 \ell k_{n-\ell} + k_{n}) = at \).

Because \( r_{d-1} = h_{d-1} + h_{d} \) with \( r_{d-1} > r_{d} \), \( h_{d} \geq 2 \).

Moreover, \( d \geq n \geq 2 \). Then, \( d-1 > 0 \). Then, \( k_{d-1} > 0 \).

Then, by lemma 3.4,
\[
2k_n - k_{n-\ell} \leq 2k_n + k_{d-1} - h_d k_d + k_{d-1} - k_{d+1} = m.
\]
Then, \( 0 < \ell}_t k_{n-\ell} + k_{n} < k_{d-1} \).

Then, by lemma 3.4,
\[
0 < k_{n-\ell} + k_{n} \leq \ell}_t k_{n-\ell} + k_{n} + h_d k_d + k_{d-1} - k_{d+1} = m.
\]
Then, \( 0 < \ell}_t k_{n-\ell} + k_{n} < k_{d-1} \).

Now \( 0 \leq t \leq H_{n-1} = k_n + k_{n-\ell} - 1 < k_{d-1} \leq k_{d+1} \).

Moreover, \( 0 < \ell}_t k_{n-\ell} + k_{n} < k_{d-1} \).

Then, because \( a(1 \ell k_{n-\ell} + k_{n}) \neq at \), by lemma 3.5,
\[
t = \ell}_t k_{n-\ell} + k_{n}.
\]
Then, \( t = \ell}_t k_{n-\ell} + k_{n} \geq k_{d-1} + k_{n} > H_{n-\ell} \). It is a contradiction.

Therefore, there is not other points of \( E_\ell \cap \left[ \left[ 0, H_{n-\ell} \right] \times \left[ 0, r_{n-\ell} \right] \right] \) that \( \{k_{n-\ell}, \ell, r_{n-\ell}, t\} \mid t = 0, 1, 2, \ldots, h_{n-1} \).

Therefore, there is not other points of \( E_\ell \cap \left[ \left[ 0, k_n \right] \times \left[ 0, r_{n-\ell} \right] \right] \) that the points \( \{k_{n-\ell}, \ell, r_{n-\ell}, t\} \mid t = 0, 1, 2, \ldots, h_{n-1} \).

Therefore,
\[
E_\ell \cap \left[ \left[ 0, k_n \right] \times \left[ 0, r_{n-\ell} \right] \right] = \{k_{n-\ell}, \ell, r_{n-\ell}, t\} \mid t = 0, 1, 2, \ldots, h_{n-1} \}.
\]

According to what precedes,
\[
\{k_{n-\ell}, \ell, ak_{n-\ell} - t\} \mid t = 0, 1, 2, \ldots, h_{n-1} \}
\]

is located on the straight line \( y = (r_{n-\ell} \ell k_{n-\ell}) x \) if \( n \) is even.

Suppose that \( n \) is odd. One proves this result by the same way as when \( n \) is even (cf [7]).

4. Models Equivalent with a Margin of \( \varepsilon \)

4.1. Correct Models

In general terms, one can always suppose that \( Y_n \) is the realization of a sequence of random variables \( Y_n \) defined on a probability space \((\Omega, A, P): y_n = y_n(\omega)\) where \( \omega \in \Omega \) and where \( Y_n \) is a correct model of \( y_n \).

As a matter of fact, there exist infinity of correct models of \( y_n \). It is thus necessary to be placed in the set of all the possible random variables.

Notations 4.1 One considers the sequences of random variables \( Y_n, n = 1, \ldots, N \), defined on the probabilities spaces \((\Omega, A, P): \Theta \in \Theta\):
\[
\{Y^0, Y^1, \ldots, Y^N\}: \Omega \rightarrow \{0/m, 1/m, \ldots, (m-1)/m\}^N. One assumes that \( Y^0 = Y_n \) for all \( \Theta \in \Theta \).
\]

For example, one can assume that \( \Omega = \{0/m, 1/m, \ldots, (m-1)/m\}^N \) and \( (Y_n, \ldots, Y_N) = (Id, \ldots, Id) \).

It thus raises the question to define what is a correct model. Indeed, if a model \( Y^0 \) is not correct, it is however possible that \( y_n = Y^0(\omega) \). Now, in the case where the model \( Y^0 \) is IID, to define a correct model is a generalization of the problem of the definition of an IID sequence. Then, it is a very complex problem (cf [1]).

However, generally, one feels well that correct models exist. In fact, it is a traditional assumption in science. In weather for example, the researchers seek a correct model, which implies its existence (if not, why to try to make forecasts?).

One could thus admit that like a conjecture or a postulate without defining exactly what is a correct model. Cependant, a more detailed study is in [7].

4.2. Models Equivalent

4.2.1. The Problem

Let \( Y^0_n \) and \( Y^1_n \) be two sequences of random variables such that, for all Borel set \( B_0 \),
\[
P\left(\{Y^0_n, \ldots, Y^N_n\} \in B_0\right) = P\left(\{Y^0_n, \ldots, Y^N_n\} \in B_0\right) \left[1 + Ob(1)\varepsilon\right],
\]
where \( Ob(1) \) means the classical \( O(1) \) with the additional condition \( |Ob(1)| \leq 1 \). One supposes that \( Y^0 \) is a correct model of the sequence \( y_n, n = 1, 2, \ldots, N \). One wants to prove that \( Y^0_n \) is also a correct model of \( Y_n \) if \( \varepsilon \) is small enough.

4.2.2. Example

Let us suppose that we have a really IID sequence of random variables \( X^0_n \) with uniform distribution on \([0,1/2]\) and \([1/2,1]\) and with a probability such as \( P\left(X^0_n \in [1/2,1]\right) = 0.500 \left[1 + \varepsilon\right] \) where \( \varepsilon = 0.001 \).

Then, this sequence has not the uniform distribution on \([0,1]\). However, if we have a sample with size 10, we will absolutely not understand that \( X^0_n \) has not the uniform distribution on \([0,1]\). It is wellknown that one need samples with size larger than \( N = 1000 \) minimum in order to test this difference.

For example, one cannot test significantly \( H_0: \text{"} X^0_n \text{"} \) has the uniform distribution” against \( H_1(\varepsilon): \)
"P\{X^\theta_n \in Bo\} = L(Bo)\left[1 + Ob(1)\epsilon\right]" if $\sqrt{N} \epsilon \leq 1/10$.

Indeed, if $\sqrt{N} \epsilon = 1/10$ and $b = 2$, the probability of obtaining
\[ \sum_{n=1}^{N} \left[1 + \frac{(X^\theta_n)^2}{4}\right] \geq 2 \] is about 0.0466 under $H_1(\epsilon)$ and about 0.0455 under $H_0$: i.e. the probability of rejecting the assumption IID, $H_0$, under $H_1(\epsilon)$ is not much bigger than that of rejecting $H_0$ if $X^\theta_n$ is really IID (cf also section 4.3 of [8]).

Then it is no possible to differentiate the IID model and models such that
\[ P\{X^\theta_1, \cdots, X^\theta_N \in Bo\} = L(Bo)\left[1 + Ob(1)\epsilon\right]. \]

### 4.2.3. Border of Correct Models

Now there is a problem: for example, use a realization $x_\theta_n$ of the IID model, and let $X^\delta_n$ be a model checking
\[ P\{X^\delta_1, \cdots, X^\delta_N \in Bo\} = L(Bo)\left[1 + Ob(1)\epsilon^\delta\right] \]
where $\epsilon^\delta$ is small enough but not very small. Let $X^\delta_n$ be a model such that
\[ P\{X^\delta_1, \cdots, X^\delta_N \in Bo\} = P\{X^\delta_1, \cdots, X^\theta_N \in Bo\} = L(Bo)\left[1 + Ob(1)\epsilon\right]. \]

Then, $X^\delta_n$ can be not a correct model: it is enough that $\epsilon^\delta$ is in extreme cases of the possible values of the $\epsilon$'s such that
\[ P\{X^\delta_1, \cdots, X^\delta_N \in Bo\} = L(Bo)\left[1 + Ob(1)\epsilon\right], \]
\[ sup_{\delta} (Ob(1)) = 1, \] imply that $X^\delta_n$ is a correct model.

Then, there are models more correct than others. These are models $Y^\delta_n$ such that, if $P\{Y^\delta_1, \cdots, Y^\delta_N \in Bo\}$, $Y^\delta_n$ is also a correct model where $\delta$ is small enough, but not too small. For example, $\epsilon = 1/10$, 1/100 or at worst $\epsilon = 1/N$ if need be (cf section 5-7 of [7]).

It seems clear that such models exist. For example it is assumed that this is the case when $x_\theta_n$ is sample of an IID sequence $X^\theta_n$ and that it is a good realization of $X^\theta_n$.

On the other hand, we know that it should exist estimates of models (these estimates are easier to calculate in some cases as texts). Then, we can choose as model $Y^\delta_n$, the model provided by these estimates: close models will also correct models.

All these points are detailed in [7].

### 4.3. Exact IID Model

Then, generally, if $Y^\theta_n$ is a correct model such that $T^\theta_n(Y^\theta_n)$ cannot be differentiated with the IID model, one will be able to choose another correct model $Y^\delta_n$ close to $Y^\theta_n$ and such that $T^\delta_n(Y^\delta_n)$ is exactly the IID model. Indeed one proves easily the following proposition (cf proposition 5-1 of [8]).

**Proposition 4.1** One assumes that $m$ is large enough. Let $Y^\delta_n$ be a correct model of the sequence $Y^\delta_n$. One assumes that there exists $\epsilon^\delta > 0$ such that if $Y^\delta_n$ is a model satisfying, for all Borel set $Bo$,
\[ P\{X^\delta_1, \cdots, X^\delta_N \in Bo\} = P\{X^\delta_1, \cdots, X^\delta_N \in Bo\} = L(Bo)\left[1 + Ob(1)\epsilon^\delta\right], \]
then $Y^\delta_n$ is a correct model of $Y^\delta_n$.

One assumes also that, for all $(k_1, \cdots, k_N)$,
\[ P\left\{T^\delta_n(Y^\delta_n) = k_{1} / 2^\delta \cap \cdots \cap T^\delta_n(Y^\delta_n) = k_{N} / 2^\delta\right\} = \frac{1}{2^{\delta N}} \]
where $sup_{\delta} (\epsilon^\delta) = \epsilon^\delta(q)$. One assumes that $\epsilon^\delta(q)$ is increasing, that $\epsilon^\delta(1) = \epsilon^\theta(1)$ and that there exists $q_0 \in N^*$ such that $\epsilon^\delta(q_0)$ is small enough.

Then, there exists $q_0 \in N^*$ and a correct model $Y^\delta_0$ of the sequence $\left\{y^\delta_n\right\}_{n=1, \cdots, N}$ such that, for all $(k_1, \cdots, k_N)$,
\[ P\left\{T^\delta_0(Y^\delta_0) = k_{1} / 2^\delta \cap \cdots \cap T^\delta_0(Y^\delta_0) = k_{N} / 2^\delta\right\} = \frac{1}{2^{\delta 0 N}} \]

### 5. Approximation Theorem

#### 5.1. Theorem

In this section, we assume that $T$ is a Fibonacci congruence and we use Fibonacci function $T_\gamma$ in order to build IID sequences.

**Theorem 3** We keep the notations 1.3 and 1.4 and notations of section 2.3. Let $\gamma(m) = \left[2 + \phi(m)\right]$. We assume $\gamma(m)N\delta_0.2^m \approx 0$ and $m / K_0 \gg 1$. Then, for all Borel set $Bo$,
\[ P\{\{X_\gamma, \cdots, X_N \in Bo\} = L(Bo)\left[1 + \frac{\gamma(m)Ob(1)}{\gamma(m)N\delta_0.2^m}\right]. \]

where $\gamma(m)Ob(1)$ is increased by a number close to 1.

If $K_0$ is not too large, there is no difficulty to choose $m$ and $q$ in such a way that $\epsilon \leq \gamma(m)2^{-m}K_0/m$ is small enough. Therefore,
\[ P\{\{X_\gamma, \cdots, X_N \in Bo\} = L(Bo)\left[1 + Ob(1)\epsilon\right]. \]

#### 5.2. Proof

Because, by Section 2.3, the points of $\overline{T}^{-1}(ml)$ are well distributed in $\{0, \cdots, m-1\}$, it is easy to prove that the sum of points of $\overline{T}^{-1}(ml)$ will be close
\[ card(\{ml \cap \{0, \cdots, m-1\}\}) / m \] (e.g. cf Figure 7). Then, we have the following lemma (cf also proposition 6-1 of [7]).

**Lemma 5.1** Let $h_n$ be the probability density function of $Y \in \{0/m, 1/m, \cdots, (m-1)/m\}$, with respect to $\mu_n$:
Figure 7. Points of $h_k^* \left( T^t (mI_k^*) \right)$ when $h_k^* (t) = \sin(4\pi t) + 1$.

$$\int_{0}^{1} h_n^* (u) \mu_n (du) = 1.$$ Let $h_n^* = (1/c_0) h_n^*$ such that

$$\int_{0}^{1} h_n^* (u) du = 1.$$

Let $K_n^* \in R$ such that $|h_n^*(r) - h_n^*(r')| \leq K_n^* |r - r'|$ and $|h_n^*(r) - h_n^*(r')| \leq K_n^* |r - r'|$ when $r, r' \in [0, 1]$.

One supposes that for all

$$n \geq 1.$$

Then, the following equality holds:

$$\eta_{\gamma_n^*_1 \cdots \gamma_n^*_N} = \sum_{\gamma_n^*_1 \in \gamma_1} \cdots \sum_{\gamma_n^*_N \in \gamma_N} P \left\{ \bigcap_{n=1}^{N} \gamma_n^*_1 \cdots \gamma_n^*_N = \gamma_n^*_1 \cdots \gamma_n^*_N \right\}.$$

Then, we deduce that

$$P \left\{ X_{\gamma(n)} \in I_k \right\} \left\{ X_{\gamma(n-1)} = x_1^*, X_{\gamma(n-2)} = x_2^*, \cdots \right\} = L \left( I_k \right) \left[ 1 + \gamma(m) Ob' \left( 1 \right) K_n \right] \frac{1}{m^{2q}}.$$

Then, one proves by basic methods (cf proposition 6.2 of [7]) that, for all

$$I_{k_1} \otimes \cdots \otimes I_{k_N},$$

$$P \left\{ \left( X_{1}, \cdots, X_{N} \right) \in I_{k_1} \otimes \cdots \otimes I_{k_N} \right\} = \prod_{n=1}^{N} \left[ L \left( I_{k_n} \right) \left[ 1 + Ob \left( 1 \right) \varepsilon \right] \right],$$

where $\varepsilon \leq \gamma(m) Ob' \left( 1 \right) K_n \frac{1}{m^{2q}}$. Because

$$\gamma(m) N K_n 2^q / m \approx 0,$$

we deduce that

$$P \left\{ \left( X_{n}^1, \cdots, X_{n}^N \right) \in I_{k_1} \otimes \cdots \otimes I_{k_N} \right\} = \frac{1}{2^{Nq}} \left[ 1 + \gamma(m) Ob' \left( 1 \right) N K_n \right] \frac{1}{m^{2q}}.$$

Now, we deduce that, for all Borel set

$$B_0 \subset \left\{ 0 / 2^q, \cdots, \left( 2^q - 1 \right) / 2^q \right\},$$

$$P \left\{ \left( X_{1}, \cdots, X_{N} \right) \in B_0 \right\} = L \left( B_0 \right) \left[ 1 + \frac{\gamma(m) Ob' \left( 1 \right) N K_n}{m^{2q}} \right].$$

6. Choice of Random Noises

6.1. Use of Texts

Now, we suppose that we use sequences $y_n^*$ and

$$y_n^* \in \left\{ 0 / m, 1 / m, \cdots, \left( m - 1 / m \right) \right\}, n = 1, 2, \cdots, N,$$

obtained from independent texts. In order to reduce $K_n$ we add modulo $m$ a text and a text written backward:

$$y_n = \left[ y_n^* + y_{n-1}^* + ranD_{a,n} \right] / m$$

where $ranD_{a,n}$ is pseudo-random sequences which have good empirical independence assumptions for $p$ successive pseudo random numbers when $p \geq 3$. In an obvious way, the texts are realizations of sequences of random variables : for example, one can take as model, the set of the possible texts provided with the uniform probability.

As a matter of fact, we add $ranD_{a,n}$ to have
sequences  \( y_n \) which have a good randomness (cf [9], or chapter 3 of [6]).

In particular, a priori, “\( P\{Y_n = y\} \) is not too different from \( 1/m \)” is a reasonable assumption. Moreover, \( (Y_n, Y_{n+1}, Y_{n+2}) \) has an empirical distribution close to independence and texts behave as Q-dependent sequences (cf [6]). Then, for every permutation \( \phi \), a three-dimensional model \( \{Y_{\phi(n)}, Y_{\phi(n+1)}, Y_{\phi(n+2)}\} \) with a continuous density and a Lipschitz coefficient not too big will be a good model. By the same way,

\[
P\{Y_{\phi(n)} = y, Y_{\phi(n+1)} = y', Y_{\phi(n+2)} = y'', \cdots\} \text{ is not too different from } P\{Y_n = y\}
\]

which is not too different from \( 1/m \) (cf [7]). In this case, one can prove that generally \( K_0 \) is small (cf [7]).

On the other hand, to increase \( K_0 \) a good way is to use the Central Limit theorem. In fact one can combine the two methods : cf [7].

### 6.2. Example

Now it may be necessary to do some transformations to get the \( m y_n \in \{0, 1, \cdots, m-1\} \) in the case where the letters and symbols are provided by sequences a(j), \( j = 1, 2, \cdots, N_0, \) a(j) \( \in \{0, 1, \cdots, 255\}, \) \( j = 1, 2, \cdots, N_0. \)

One sets \( N_0 = \left[ N_1 / r_1 \right]. \) We choose two consecutive elements a and m of the Fibonacci sequence : m can be chosen with respect to \( N_0. \) Then, we choose \( r_1 \) such that  \( a < 32^1 \leq m. \)

1) We set \( c(j) = a(j) \mod \kappa = 32. \)

2) We set \( d(n) = \sum_{j=0}^{N_0} c(j) (r_1 (n-1) + r) \kappa^{-1} \) for \( j = 1, 2, \cdots, N_0. \)

3) We set \( y_n = \left[ d(n) m / \kappa \right] / m \) for \( j = 1, 2, \cdots, N_0. \)

By using this technique, we have created real IID sequences \( x_n. \) We have used a sequence \( c(j) \) with \( N_1 = 20,000,000. \) This sequence was obtained from dictionary, encyclopedia, and Bible. We choose \( r_1 = 20, \)

\( a < 4 \times 10^{10} \leq m, \) \( q = 70. \) Then \( N_0 = 10^8. \) Then, we have estimated \( K_0 = 0.01. \) In order to avoid any error we have choose \( K_0 = 10^8 \) in the building of \( x_n. \)

We have tested the sequence \( x_n. \) We have used the classical Diehard tests (cf [1] [2]) and the higher order correlation coefficients (cf [10]). Results are in accordance with what we waited: the hypothesis “randomness” is accepted by all these tests (cf [7]).

One can can download this sequence in [11].

### 7. Conclusion: Building of Random Sequence

By theorem 3 one can find models correct \( Y_n^0 \) such that

\[
P\{X_1^0, \cdots, X_n^0 \in Bo\} = L(Bo) [1 + Ob(1) e] \text{ where } e
\]

is small if \( K_0 \) is not too large. Now it is possible to build such sequences concretely, for example by using texts studied in section 6. In this case, coefficient \( K_0 \) depend on the choice of \( m, \) i.e. of \( r_1. \) But, \( K_0 \) increases very little when \( r_1 \) increases. Even, in some cases, it seems that it decreases. Then, at most \( 2^{r_1} / m \) decreases much more quickly than \( K_0 \) increases.

So by taking \( m \) large enough and by choosing well q, we found \( e \) small enough in a way that there exists correct models which checks the conditions of proposition 4.1. Then, there exists \( m \) sufficiently large and \( q \) sufficiently small and a correct model \( Y_n^0 \in \{0/m, 1/m, \cdots, (m-1)/m\} \) such that \( T_q \{Y_n^0\} \) is the IID model.

Then, this result show that one can build sequences \( x_n \) such that the model IID is a correct model of \( x_n. \)

That means that \( x_n \) behaves like any IID sample: a priori, \( x_n \) can check not the properties which one expects from a IID sample like certain tests, but that occurs only with a probability equal to that of any IID sample.

By this method, we therefore have a mean to value the technique used by Marsaglia to create its CD-ROM. We arrive in fact to prove mathematically that the sequence obtained can be regarded a priori as random, what Marsaglia did not.

**Remark 7.1** One might wonder if the sequence built adding text and pseudo-random sequences is not an IID sequence. It is a similar hypothesis which Marsaglia does when he built its CD-Rom. This also corresponds to results of [9]. But in fact, nothing is proved.

It is maybe possible to prove it but that seems complicated. Finally, it is much easier to apply the functions \( T_q^r \) : in this case, it requires only that \( K_0 \) is not too big. It’s an hypothesis much simpler to be verified and it does not require many efforts in some cases. That is why we choose to build IID sequences using this technique.

### 8. References


