PSEUDO-RANDOM SEQUENCES

Gerard Bruere-Dawson

MAC Technical Memorandum 16

October 1970

Massachusetts Institute of Technology

PROJECT MAC

Cambridge Massachusetts 02139

PSEUDO-RANDOM SEQUENCES

Gerard Bruere-Dawson

MAC Technical Memorandum 16

October 1970

Massachusetts Institute of Technology

PROJECT MAC

Cambridge Massachusetts 02139

PSEUDO-RANDOM SEQUENCES

Technical Memorandum 16

(This report was reproduced from an M.S. Thesis, MIT, Department of Electrical Engineering, June 1970.)

Gerard Bruere-Dawson

October 1970

PROJECT MAC

Massachusetts Institute of Technology

Cambridge Massachusetts 02139

ACKNOWLEDGMENT

The author wishes to thank Professor Albert R. Meyer for his guidance in supervising this thesis and also for his suggestions for the general idea of this paper and many of the proofs. Miss Marsha E. Baker deserves the credit for having done a beautiful job of typing this thesis.

Work reported herein was supported in part by Project MAC, an M.I.T. research project sponsored by the Advanced Research Projects Agency, Department of Defense, under Office of Naval Research Contract Nonr-4102(01).

TABLE OF CONTENTS

INTRODUCTION

The purpose of this paper is to study some notions of randomness for infinite sequences of 0's and 1's.

We consider $S = s_1\ s_2\ \ldots\ s_n\ldots$, where s_i is either 0 or 1 with equal probability; this probability being independent of the value of the other elements of S. If such a sequence is obtained by choosing 0 or 1 at random, one can state properties which will be verified, with probability one, by some of the initial segments S_n of S. We denote by $S_n = s_1\ s_2\ \ldots\ s_n$ the initial segment of length n of $S = s_1\ s_2\ \ldots\ s_n\ldots$. For example: The limit of the relative frequency of 1 in S_n is $\frac{1}{2}$, when n increases indefinitely. Given such a property or law, we can say that a sequence is random if it has this property.

We shall restrict our attention on effectively testable properties, and see under what conditions one can generate effectively (i.e. with a program) sequences with some of these properties. Such sequences will be called pseudo-random. We consider now some of those properties in order to define random sequences.

a) The first point will be that a random sequence is unpredictable. That is to say, given an initial segment of the sequence there is no way to predict accurately what will follow. This notion has been introduced by Von Mises, who defined:

The probability of an event is the ultimate frequency of the occurrence of this event, after an infinite number of independent trials.

Upon this, he built up the definition of "kollektiv" or random sequence. We will state precisely this notion, as well as the formulations of Wald and Church, in the first chapter.

b) Second property: If a sequence is easy to describe; if it contains some kind of pattern for example, then, it is not likely to be random.

Kolmogorov formalized this idea and defined the descriptive complexity for finite sequences. This complexity is then used to define random infinite sequences.

c) The third property will use a completely different approach, formulated by Martin-Lof. Indeed, if we want to speak of random elements of a set S, we need to introduce a probability measure on S. Random elements are then characterized by properties verified by a subset of S of measure 1.

There we introduce a measure μ on the set of infinite binary sequences:

$$\Omega = \{0,1\}^{\omega}.$$

Which is the ω-product of the equiprobable measure on $\{0,1\}$. This measure is defined for the Borel sets of the topology T, with basis:

$[x_1\ x_2\ \ldots\ x_n]$: set of infinite sequences beginning with $x_1\ x_2\ \ldots\ x_n$, where x_i is either 0 or 1. Therefore to say that a property is verified almost everywhere on Ω (with respect to μ) is equivalent to say that there is an open set of arbitrarily small measure including the set of exceptions to this property. This will give us the definition of sequential test in the second chapter.

We shall study the interrelations of those concepts and consider extensions of those definitions.

CHAPTER I

VON MISES' DEFINITION

We first present the concepts of Von Mises about randomness, then the related works of Wald and Church. We give three definitions of random sequences or "Kollektivs".

Those definitions will lead us to those of gambling procedures and to some interesting areas of research, as the study of Pseudo-random sequences.

1.1 Definition of a Kollektiv

A Kollektiv is an infinite sequence

$$S = s_1 s_2 \cdots s_n \cdots$$

over a finite alphabet, such that:

1) Any element of the alphabet occurs in S with a certain limiting frequency.

2) If we select an infinite set of indexes (places) $I = \{i_1, i_2, \ldots i_n \ldots\}$, such that the decision as to whether or not $i_n \in I$ depends only on the value of $(i_n, s_1, s_2, \ldots, s_{i_n-1}, s_{i_n+1} \ldots)$; then each element occurs with the same limiting frequency in the subsequence:

$$S_I = s_{i_1} s_{i_2} \cdots s_{i_n} \cdots \quad .$$

We will in this paper consider sequences of 0's and 1's and the case where the limiting frequency of 0 (or 1) is $\frac{1}{2}$.

Definition Let $X = \{0,1\}^*$ = set of finite binary sequences

A selector f is a 0-1 valued function defined on X.

A place Selection P_f is the mapping which associates to each infinite sequence $S = s_1 s_2 \ldots$, the subsequence (which may be finite)

$$P_f(S) = s_{i_1} s_{i_2} \ldots s_{i_n} \ldots$$

where i_1 = the least i such that $f(s_1 s_2 \ldots s_{i-1}) = 1$

i_n = the least i, bigger than i_{n-1}, such that $f(s_1 s_2 \ldots s_{i-1}) = 1$

Notation. Given a place selection P_f and an infinite sequence S.

We write P for P_f

P(S) for the subsequence selected by P on S

$P(S_n)$ for the subsequence selected on the first n digits of S.

$\# P(S_n)$ for the number of elements selected

$\#_0 P(S_n)$ ($\#_1 P(S_n)$) for the number of 0's (1's) selected.

1.2 Definition of A.WALD [13]

Wald noticed that one ought to put certain restrictions on that definition, since:

Given an increasing sequence of integers $\{n_i\}$, the process which extracts from

$$S = s_1 s_2 \ldots s_n \ldots.$$

the subsequence $S' = s_{n_1} s_{n_2} \ldots s_{n_m} \ldots$

is a place selection.

But if we consider all possible sequences $\{n_i\}$, for any S with an infinite number of 0's or 1's there will be one $\{n_i\}$ such that

$$S_{n_i} = 1 \quad \text{identically (or } S_{n_i} = 0)$$

Therefore no sequence would be a "kollektiv".

To avoid this, WALD proposed:

Definition: Consider a countable set of places selection including that one which selects every place; a sequence will be a "kollektiv" if:

For all places selection selecting an infinite number of places the limiting frequence of the number of 0's (or 1's) is $\frac{1}{2}$.

1.3 Definition of Church [1]

We can remark that, in order for a system of place selection to be applicable, we ought to be able to reproduce each place selection indefinitely.

It is equivalent to say, by Church's thesis, that the selectors of those place selections are recursive function of X. Formally

Given a one-one recursive encoding t of X in $\{0,1,2,\ldots\}$ a place selection P_f is effective, iff the function $f(t(\cdot))$ is a recursive function.

Definition. A sequence S will be a "kollektiv" (in the sense of Church) iff for all effective places selections, the limiting frequency of the number of 0's (or 1's) is $\frac{1}{2}$.

Note that there is a countable number of places selections, and thus, this definition is consistent with that of WALD .

1.4 Definition of Gambling Algorithms

For defining random sequences we shall use an equivalent notion.

Notation: Given an infinite sequence S, S can be considered as the characteristic function of a subset

Σ of {1, 2....} i.e. $n \in \Sigma \Leftrightarrow s_n = 1$

We shall often write S for Σ, and not distinguish between them.

Definitions: A gambling procedure is a total function $g(x, S)$ of one integer and one set variable such that:

$$g(x, S) = \Psi(x, S - \{x\})$$

for some total recursive Ψ^* with range in {0,1,2}.

These may be called F (future)-algorithms, for emphasis.

A P(past)-algorithm is as above with

$$g(x, S) = \Psi (x, S \cap \{0,1,\ldots,x-1\}).$$

Definition:

$$\gamma(g, S, x) = |\{y \leq x \mid g(y, S) \neq 2 \}|$$

= number of guesses up to x by g about S.

$$k(g, S, x) = |\{y \leq x \mid g(y, S) = s_y\}|$$

= number of good guesses up to x

---

*Cf. H. Rogers Theory of recursive functions and effective computability. Chapter 15.

$$\alpha(g, S, x) = \frac{k(g, S, x)}{\gamma(g, S, x)}$$

We call $\alpha(g, S, x)$ the accuracy of g on S at x.

$$\alpha(g, S) = \lim_{x \to \infty} \alpha(g, S, x) \text{ if such a limit exists}$$

Definition: A procedure g is applicable to S iff $\lim \gamma(g, S, x) = +\infty$

A procedure g has a bias for S iff

$$\overline{\lim_{x = \infty}} \alpha(g, S, x) > \frac{1}{2} .$$

Having defined gambling procedures, we shall show the equivalence, within our subject, of place selections and P-algorithms.

Given a P algorithm P, we define:

P_0 the place selection which selects s_n whenever $P(n, S) = 0$, and does not select otherwise.

P_1 will do the same thing for $P(n, S) = 1$

Theorem

Given a sequence S if there exists a P-algorithm, P, applicable to S such that either

1) $\alpha(P, S, x)$ has no limit when $x \to +\infty$

or 2) $\lim \alpha (P, S, x) \neq \frac{1}{2}$

then there exists a place selection Q such that either

$$\overline{\lim_{n \to \infty}} \quad \frac{\#_0 Q(S_n)}{\# Q(S_n)} > \frac{1}{2}$$

or $$\overline{\lim_{n \to \infty}} \quad \frac{\#_1 Q(S_n)}{\# Q(S_n)} > \frac{1}{2}$$

Proof: The first two conditions are equivalent to either

a) $\overline{\lim}\ \alpha(P, S, x) > \frac{1}{2}$

or b) $\underline{\lim}\ \alpha(P, S, x) < \frac{1}{2}$

If the second case is true, we may use a P algorithm P'

$P'(S, x) = 1 \dot{-} P(S, x)$ if $P(S, X) \neq 2$

$P'(S, x) = P(S, x) = 2$ otherwise.

Then for P'

$\overline{\lim}\ \alpha(P', S, x) > \frac{1}{2}$.

So we can restrict our attention to case a). That is:

$$(\exists \varepsilon > 0)\ (\overset{\infty}{\exists} x)\ [\alpha(P, S, x) > \tfrac{1}{2} + \varepsilon\ ]$$

Considering now P_0 and P_1. We have

$$\gamma(P, S, n) = \# P_0(S_n) + \# P_1(S_n)$$

$$k(P, S, n) = \#_0\ P_0\ (S_n) + \#_1\ P_1\ (S_n)$$

$$\text{Let } \alpha_0(n) = \frac{\#_0\ P_0(S_n)}{\#\ P_0\ (S_n)} \qquad \alpha_1(n) = \frac{\#_1\ P_1\ (S_n)}{\#\ P_1\ (S_n)}$$

$$\alpha(P, S, n) = \frac{\alpha_0(n).\ \#\ P_0\ (S_n) + \alpha_1(N).\ \#\ P_1\ (S_n)}{\#\ P_0\ (S_n) + \#\ P_1\ (S_n)}$$

In order to prove this theorem, we have to consider two cases:

Case 1): P guesses a finite number N of, say, 0's. Then for large n such that:

$$\alpha(P, S, n) > \frac{1}{2} + \varepsilon$$

$$\alpha_1(S_n) > \left(\frac{1}{2} + \varepsilon\right)\left(1 + \frac{N}{\#\ P_1\ (S_n)}\right) - \frac{N}{\#\ P_1\ (S_n)}$$

As $N/\#\ P_1\ (S_n)$ can be made arbitrarily small:

$$(\exists\, \varepsilon > 0)\ [\alpha_1\ (Sn) > \frac{1}{2} + \varepsilon\ \ (\text{i. o})]$$

Case 2: P guesses an infinite number of 0's and 1's.

Then $\alpha(P, S, n) > \frac{1}{2} + \varepsilon \Rightarrow \alpha_1(n) > \frac{1}{2} + \varepsilon$

$$\text{or}\quad \alpha_0(n) > \frac{1}{2} + \varepsilon$$

Then since

$$(\exists^{\infty} n)\ [\alpha\ (P, S, n) > \frac{1}{2} + \varepsilon\ ]$$

one of α_1 or α_0 is infinitely often bigger than $\frac{1}{2} + \varepsilon$.

Q.E.D.

Let us now consider random sequences

Definition (Church)

A sequence S is random iff for any P-algorithm P

$$\lim_{x \to \infty} \alpha (P, S, x) = \frac{1}{2}$$

Notation: We shall write "random (VM)" for random in the sense of Von Mises (Version of Church).

1.4.1. Discussion

The first obvious remark is that a periodic or ultimately periodic sequence like

$$S = 001001001 \ldots\ldots$$

will not be a random sequence. Moreover, there is no way to predict accurately a random (VM) sequence.

We have the important property, using the measure μ defined in the introduction over $\Omega = \{0,1\}^{\infty}$.

Theorem (Church)

$$\mu \{S \mid S \text{ is random (VM)}\} = 1$$

That is, a sequence S is random almost surely. In order to prove this theorem we shall use another theorem (optional sampling Theorem)

Theorem (Doob) [14]

Given a place selection P such that:

P(S) is an infinite sequence, almost surely.

Let $P(S) = S' = s'_1, s'_2 \ldots s'_n \ldots$.

then $P : S \rightarrow P(S)$ is a measure preserving transformation. That is: if Λ is a Borel set on Ω, then

$P^{-1}(\Lambda)$ is also a Borel set and $\mu(\Lambda) = \mu[P^{-1}(\Lambda)]$

Proof:

Consider the set Σ of sequences S's such that:

(1) $(\exists\ P \text{ applicable to } S)\ \neg\ [\lim \alpha\ (P, S, x) = \frac{1}{2}\ ]$

We shall prove that Σ has measure 0. We know, by what is above, that (1) is equivalent to:

$$(\exists\ P \text{ applicable to } S) \qquad \overline{\lim}\ \alpha\ (P, S, x) > \frac{1}{2}\ ]$$

Then $\Sigma = \bigcup_P \bigcup_m \Gamma_{P,m}$ where $\Gamma_{P,m} = \{S \mid (\overset{\infty}{\exists}\ x)\ \alpha\ (P, S, x) > \frac{1}{2} + \frac{1}{m}\}$

Since there is a countable number of P's.

$$(\forall\ P)\ \ (\overset{\infty}{\forall}\ m)\ [\mu(\Gamma_{P,m}) = 0] \quad \Leftrightarrow \quad \mu(\Sigma) = 0$$

Assume for some P and m: $\Gamma_{P,m} > 0$. Then from P, we extract P_0 and P_1 (See Theorem above)

$\Sigma_0 = \{S \mid S \in \Sigma,$ the subsequence $P_0(S_x)$ has a frequency of 0's $> \frac{1}{2} + \frac{1}{m}\}$

$\Sigma_1 = \{S \mid S \in \Sigma,$ the subsequence $P_1(S_x)$ has a frequency of 1's $> \frac{1}{2} + \frac{1}{m}\}$

$\Sigma = \Sigma_0 \cup \Sigma_1$.

Assume $\mu(\Sigma_0) > 0$

Let $\Sigma_0' = \{S \mid$ the frequency of zero's $> \frac{1}{2} + \frac{1}{m}$ (i. o.)$\}$

$(\forall S \in \Sigma_0)\ P_0(S) \in \Sigma_0'$.

But applying the strong law of large numbers, we have

$\mu(\Sigma_0') = 0$

$\mu[P^{-1}(\Sigma_0')] = 0$

and $\Sigma_0 \subset P^{-1}(\Sigma_0') \Rightarrow \mu(\Sigma_0) = 0$.

Therefore $\mu(\Sigma) = 0$ Q.E.D.

Remark: In the proof of this theorem we use only the fact that there is a countable number of places selections.

The theorem would be true also for a larger definition of random sequences. e. g. using r.e. gambling procedures where g(x, S) divergent is interpreted as a no guess answer.

We know that the characteristic function of a recursive set is not random (VM), since this characteristic function is recursive.

This is also true for the characteristic function of a recursively enumerable set (or its complement).

Fact: The characteristic function of a r.e set is not random (VM).

Proof: If this set is infinite, we use a recursive function enumerating it without repetition, to construct a guessing algorithm.

Remark: By the same method; if the set, or its complement includes an infinite r.e set, then it is not random (VM).

This leads us to the question: how non-recursive a sequence S has to be in order to be random?

We shall use the Kleene hierarchy of sets.

The Kleene hierarchy classifies the "arithmetical" sets in classes Σ_n, Π_n, 0, 1, 2,... defined as follows:

Σ_n is the class of all sets A of the form:

$$A = \{(a_1,\ldots,a_m)\ (Q_1\ x_1)\ (Q_2\ x_2)\ldots(Q_n\ x_n)\ P(a_1,\ldots,a_m,\ x_1,\ldots,x_n)\}$$

where $P(a_1,\ldots,a_m,\ x_1,\ldots,x_n)$ is a recursive predicate, the Q_{2k+1} are existential quantifiers and the Q_{2k} are universal quantifiers.

Π_n is the class of all sets A as above except that the Q_{2k+1} are universal quantifiers and the Q_{2k} are existential quantifiers.

Summarizing some basic properties of this hierarchy of sets (see Rogers):

(1) $\Sigma_0 = \pi_0 = \Sigma_1 \cap \pi_1$ = the collection of all recursive sets;

(2) $A \in \Sigma_n \Leftrightarrow \bar{A} \in \pi_n$, all n;

(3) $\Sigma_n \subset \Sigma_{n+1}$, $\pi_n \subset \Sigma_{n+1}$, $\Sigma_n \subset \pi_{n+1}$ and $\pi_n \subset \pi_{n+1}$ all n;

(4) $\Sigma_n \not\subset \pi_n$ and $\pi_n \not\subset \Sigma_n$ for $n > 0$

(5) $\Sigma_n \cup \pi_n \subset \Sigma_{n+1} \cap \pi_{n+1}$ for $n > 0$ and containment is proper.

Then we have

Theorem (Loveland [6]): There exists recursively random sets properly in

$$\Delta_i = \Sigma_i \cap \pi_i \quad \text{for} \quad i = 2, 3...$$

1.4.2. Critique of this Definition

From the point of view of gambling it may be that a particular sequence is guessed accurately by a P algorithm, but there is no effective way to find this good gambling procedure.

The notion of "accurately guessing" is also artificial. may be that we have, for a sequence S, a procedure which will be accurate infinitely often, but this procedure may be also very inaccurate most of the time.

For a random sequence and a given P algorithm it may also be that the accuracy goes to $\frac{1}{2}$ from above. This does not correspond to the intuitive idea of a random sequence. More precisely, we will state a theorem proved by J. Ville [12] (in a slightly different form).

Theorem (Ville [12]): There exists a sequence S randon in the sense of Church, such that:

In any initial segment of S, the number of 0's is not greater than the number of 1's.

1.5 Areas of Research

1) We can use a wider class of gambling procedures Kruse [15] studied this extension in its set theoretic aspect. Given a set and a probability measure on this set, we can define arbitrarily random elements as long as we keep the condition that almost surely any element is random.

   In a more restricted point of view, we may consider gambling procedures in the arithmetical hierarchy.

2) We will in 1.5.1 present some remarks about the general F-procedures as defined above.

3) One cannot effectively construct random sequences in the sense of Von Mises. But if we impose a bound on the time necessary to guess elements of a sequence, we can define and (effectively) construct sequences which will look random to all "fast" gambling procedures. We investigate this in 1.5.2.

1.5.1 F-Algorithms

Recall that a F-algorithm is a function F(x, S) such that $F(x,S) = \Psi(x, S - \{x\})$ where Ψ is a general recursive function of one integer and one set variable, ranging in {0,1,2}.

Our motivation for considering F-algorithms can be explained as follows:

D. Loveland [5], made the remark that there are selection rules, practically applicable, which are not place selections. On this basis he built an extension of the Von Mises theory of random sequences. Our extension of P-algorithms to F-algorithms follows the same pattern.

A P-algorithm, applied to a sequence S, is analogous to a process of extrapolation. For example, if we consider $S_n: s_1\ s_2 \ldots s_n$ as the history of S up to time n, we want to predict what will occur next.

On the other hand, a F-algorithm is analogous to a process of interpolation. Then, if we consider a sequence S we want to predict the value of s_n. For this purpose, we can ask a finite number of questions about other elements of S.

In the next section, we will compare F and P-algorithms. Our results are inconclusive. We will state a few results and remarks.

The first point is that Doob's theorem (optional sampling theorem) no longer applies to extended place selections.

Definition: A F-place selection is a place selection with the difference that the selector f is a function of a set variable and an integer:

$$f(S, x) = \Psi(S - \{x\}, x)$$

where Ψ is general recursive.

We have

Fact: There exist F-place selections which modify the distribution.

We define a selector f:

$$f(S, 1) = \begin{cases} 0 & \text{if } s_2 = 1 \\ 1 & \text{otherwise} \end{cases}$$

$$f(S, n) = 1 \quad \text{for} \quad n = 2, 3, \ldots$$

We see that with probability 3/4, the first element selected will be 1.

However, it is certainly possible to define random sequences with respect to F-algorithms as in Section 1.4. This class of random sequences will certainly be included in the class of random (VM) sequences. In some special cases, we can decide whether the containment is proper.

Theorem: If we consider gambling procedures with outputs in $\{0,1\}$, that is guessing at each argument, then: there are sequences which are random with respect to P-algorithms but not for F-algorithms.

Proof: We know already

$$(\exists\, S \in \Omega)\ (\forall\, P \in \rho)\ [\alpha\ (P, S) = \tfrac{1}{2}] \tag{1}$$

Where ρ is the set of P-algorithms

Considering such a sequence $S = s_1\ s_2 \ldots s_n \ldots$, and defining

$S' = s'_1\ s'_2 \ldots s'_n \ldots$

$$s'_1 = s_1$$

$$s'_x = \begin{cases} \text{If } (\exists\ y < x)\ (y + 2^y = x) \text{ Then } s'_y \\ \text{else } s_x \end{cases}$$

A F-algorithm may thus ask the value of s_{x+2^x} and gives this value as output. If will be always right. Assuming there exists a P-algorithm with a bias on S' i.e.

$$\alpha(P, S', x) = \frac{k(P,S',x)}{\gamma(P,S',x)} > \frac{1}{2} + \frac{1}{p} \quad \text{(i.o), for some } p \subset N$$

Here, with our restriction, $\gamma(P, S', x) = x$.

$$\text{so } \alpha(P,S',x) = \frac{k(P,S',x)}{x} > \frac{1}{2} + \frac{1}{p}$$

Let R = range [f(n)], where $f(n) = n+2^n$.

Then $(\forall\ x \notin R)\ [s_n = s'_x]$

Ther are less than log x elements in R smaller than x,

Since $y + 2^y \leq x \Rightarrow 2^y < x \Rightarrow y < \log x$.

So if we apply the same algorithm to S, it will have

$$\alpha(P,S,x) = \frac{k(P,S,x)}{x} \geq \frac{k(P,S,x) - \log x}{x}$$

$$\geq \frac{1}{2} + \frac{1}{p} - \frac{\log x}{x}$$

$$\geq \frac{1}{2} + \frac{1}{2p} \quad \text{(i.o)}$$

which is in contradiction with equation (1)

Q.E.D.

To conclude this section, we give, without proof, a theorem of Loveland, stated in [5] in a different and more general form:

Theorem (Loveland):

Ther exists a random (VM)sequence S and a F-algorithm, F, such that $\alpha(F,S) = 1$.

1.5.2. Pseudo-Random Sequences

A recursive sequence of 0's and 1's is obviously not random, in the sense of Church. Nevertheless we would like to construct sequences which would be very difficult to predict.

To measure this difficulty, we will use the complexity theory as introduced by Blum:

Let P.R. be the set of partial recursive functions, R being the set of recursive functions.

Definition: For a Godel numbering $\{\varphi_i\}$ of P.R., a sequence $\Phi_0, \Phi_1, \ldots \Phi_n, \ldots$ of functions in P.R., is a measure of complexity iff:

1) dom Φ_i = dom φ_i

2) $\lambda\,(x, y)[\Phi_i(x) = y]$ is a recursive predicate.

Definition: Given a function $g \in R$. f in R. is g-computable iff

$(\exists\, \varphi_i = f)$ $[\Phi_i(x) \leq g(x)$ except in a finite number of points$]$.

We want now to introduce a measure of the complexity of a P-algorithm P(S,x), which can be considered as a function recursive in the set S.

$$P(S,x) = \varphi_i^S(x) \quad \text{for some } i$$

We define for a function $\varphi_i^S(x)$, a relativized measure Φ_i^S as a function recursively enumerable in S, with the properties:

1) $(\forall S)$ [domain (Φ_i^S) = domain (φ_i^S)]

2) λ (i,x,y) $[\Phi_i^S(x) = y]$ is a predicate recursive in S.

The complexity of P(S,x) is noted $\pi(S,x)$. $\pi(S,x)$ may represent the number of steps necessary for a universal Turing machine, with an oracle on S, to compute P(S,x).

Definition: Given g in R, a P-algorithm P is g-computable on S if $\pi(S,x) \leq g(x)$ for all but a finite number of x's.

Definition: Given g in R, an infinite sequence S is random at level g, if any P-algorithm g-computable on S guesses r with a limit accuracy $\frac{1}{2}$.

Our aim is to generate recursive sequences random at level g. Since a sequence S is recursive.

$$(\exists\, i)\ \varphi_i(x) = s_x$$

Obviously if S is random at level g then the function $f(x) = s_x$ is not g-computable. The reverse is not true and was proved by A. Meyer and J. McCrieght.

Theorem (Meyer): $(\forall\, g \in R)\ (\forall\, d \in R)\ (\exists$ 0.1 valued $C \subset R)$

$(\forall_i)$ $[\varphi_i = C \Rightarrow \Phi_i(x) > g(x)$ a.e. and

$(\forall\, x)\ (C(x) = 1 \Rightarrow (\forall\, y)\ (x < y \leq x + d(x) \Rightarrow C(y) = 0))]$

Informally this means that there exist recursive sequences, difficult to compute, with an arbitrarily small frequency of 1's.

In order to construct a pseudo-random sequence, we could use an extension of a procedure by Levin, Minsky, and Silver.

This procedure given a countable set of P-algorithms yields a sequence which is random with respect to this set, and recursive in an enumerating function of that sequence.

We present a different construction, which yields a recursive sequence random at level g and which allows us to control the variations of accuracy.

Theorem: For any $g \in R$, and any positive computable function $\varepsilon(x)$ with $\lim_{x=\infty} \varepsilon(x) = 0$ and $\lim_{x=\infty} x\varepsilon^2(x) = +\infty$, one can construct a sequence S such that $x \to \infty$:

1) S is random at level g.

2) If we let $\gamma(P,S,x) = |\{y \leq x \mid P(S, y) \neq 2 \ \& \ \pi(S, y) \leq g(y)\}|$

$k'(P,S,x) = |\{y \leq x \mid P(S, y) = s_y \ \& \ \pi(S, y) \leq g(y)\}|$

$\alpha'(P,S,x) = k'(P,S,x)/\gamma'(P,S,x)$

Then $[\frac{1}{2} - \varepsilon(y) < \alpha'(P,S,x) < \frac{1}{2} + \varepsilon(y)]$, with $y = \gamma'(P,S,x)]$ (a.e.)

Proof: We use a diagonal argument developed by McCreight.

By definition a P-algorithm P(S,x) can be written as $\varphi_i^S(x) = P(S,x)$ for some i.

To each $\varphi_i^S(x)$ we associate the measure $\Phi_i^S(x)$, as above. Consider the list $\{\varphi_i^S\}$. This is not an enumeration of the P-algorithms, but all P-algorithms are in this list.

Assign to each element in the list an initial weight $w_0(i) = 1/(i+i)^2$. This weight may be changed at some stages. We define S in stages. At stage x, S_{x-1} is defined and we compute s_x.

Stage x

Define $I = \{i \leq x \mid \Phi_i^{S_{x-1}}(x) \leq g(x)\}$ where $\Phi_i^{S_{x-1}}(x) \leq g(x)$ means that $\varphi_i^S(x)$ did not use the oracle for $y \geq x$ and that $\Phi_i^S(x) \leq g(x)$.

Let $A(x) = \{i \in I \mid \varphi_i^S(x) = 0\}$

$B(x) = \{i \in I \mid \varphi_i^S(x) = 1\}$

$W_a = \sum_{i \in A(x)} W(i) \qquad W_b = \sum_{i \in B(x)} W(i)$

Let $\theta(x) = \frac{\varepsilon(x)}{4}$.

Two cases

a) If $w_a > w_b$
1) multiply all weights in A(x) by $1-\theta(x)$ and all weights in B(x) by $1 + \theta(x)$
2) set $s_x = 1$

b) If $w_a \leq w_b$
1) multiply all weights in A(x) by $1 + \theta(x)$ and all weights in B(x) by $1 - \theta(x)$
2) set $s_x = 0$

END.

To show this algorithm gives us the desired result; we define for a P-algorithm P, and its complexity

Property Q(n):

$$(\exists\, x) \quad [\gamma'(P,S,x) = n \quad \text{and} \quad \alpha'(P,S,x) > \frac{1}{2} + \varepsilon(n)]$$

Consider a P-algorithm $P(S,x) = \varphi_i^S(x)$. Assume it has property Q(n). Then at stage x

$$w(i) = C_x \, w_0(i)$$

with $$C_x = \prod_{i=1}^{m} (1-\theta(x_i)) \prod_{i=1}^{p} (1+\theta(y_i))$$

where

$$m + p = n \quad \text{and} \quad \frac{p}{m+p} > \frac{1}{2} + \varepsilon(x)$$

and

$\{x_i\}$ are the points z: $P(S,z) \neq s_z$

$\{y_j\}$ are the points z: $P(S,z) = s_z$

Then $C_x \geq (1-\theta(x))^n (1+\theta(n))^{n+\varepsilon(n)n}$

But $(1-\theta(n))^n (1+\theta(n))^{n+n\,\varepsilon(n)} \longrightarrow +\infty$ when $n \to +\infty$

As $x \geq n$, If P(S,x) has property Q infinitely often, then C_x can be made arbitrarily large.

Initially $\sum_{i=1}^{\infty} w_0(i) < +\infty$, and at any stage this sum cannot increase. Therefore this sum will remain finite, for all i.

Thus any P-algorithm has property Q at most a finite number of times.

We have also proved:

$$\alpha'(P,S,x) < \frac{1}{2} + \varepsilon(y) \quad \text{(a.e.)} \quad y = \gamma'(P,S,x)$$

Assume

$$\alpha'(P,S,x) \leq \frac{1}{2} - \varepsilon(y) \quad \text{(i.o)} \qquad y = \gamma'(P,S,x)$$

Then from P, we can deduce another P-algorithm P', with the same complexity on S, such that

$$\alpha'(P',S,x) \geq \frac{1}{2} + \varepsilon(y) \quad \text{(i.o)} \quad y = \gamma'(P',S,x)$$

Which is a contradiction.

Moreover if P is g-computable on S, then $\alpha(P,S) = \frac{1}{2}$. Therefore S is random at level g.

Q.E.D.

CHAPTER II

SEQUENTIAL TESTS

2.1 Purposes and Definitions

As we saw in the preceding chapter, the definition of random sequences using a countable number of place selections (or equivalently gambling procedures) presents some inconsistencies with the intuitive notion of randomness. See, for example the remark of Ville.

So let us look back at probability theory. Consider a random sequence as illustrated by an indefinite repetition of independent events, with a finite number of possible outcomes (e.g. 0 or 1).

Extending the notion of probability for a finite number of possible events, we defined in the introduction a probability measure μ over the set of infinite sequences of 0's and 1's:

$$\Omega = (0,1)^{\infty}.$$

We characterize random elements in this set by the properties they have almost surely. So, with Martin Lof [8], we will say, informally:

Definition: A sequence $\omega \in \Omega$ is random if it satisfies all "almost surely" type theorem of probability theory.

For example, a sequence random in the sense of Wald, will obey the strong law of large numbers, (which is of first order) but not the law of the iterated logarithm (which is of second order).

In order to make precise this notion, we look at what we call "almost surely" type theorems.

An "almost surely" type theorem is a property verified by a subset of measure 1 of Ω. Examples: Strong law of large number: The limiting frequency of the number of 1's in a sequence $\omega \in \Omega$, is almost surely $\frac{1}{2}$.

Law of the iterated logarithm: Let $\sigma_n(\omega)$ be the sum of the n first digits of the sequence ω. Then

$$\overline{\lim_{n \to \infty}} \text{ (resp } \underline{\lim} \text{)} \frac{2\sigma_n(\omega)-n}{\sqrt{2n \log \log n}} = +1 \text{ (resp. } -1) \text{ almost surely}$$

For such a theorem, then, we can say that the set of all sequences violating the law has measure zero. By definition this means that to every $\varepsilon > 0$ there exists an open $\mathcal{U}$ covering this set such that

$$\mu(\mathcal{U}) < \varepsilon .$$

For $x \in \{0,1\}^*$, let [x] denotes the set of all infinite sequences beginning with x. Then, instead of $\mathcal{U}$, we may consider the set

$$U = \{x \mid [x] \subset \mathcal{U}\} \subset \{0,1\}^*$$

Note that, conversely

$$U = \bigcup_{x \in U} [x]$$

If and only if $\mathcal{U}$ is open. We say that $\mathcal{U}$ is generated by U. Further, U has the property that it contains all possible extensions of any of its elements (sequentiality); y being an extension of x (in symbol $y \succeq x$) if the string y begins with x. In other words, U may be regarded as the critical region of a sequential test on the level ε . The definition of a null set may hence be stated in statistical terms as follows: For every $\varepsilon > 0$, there exists a sequential test on that level which rejects all sequences of the set.

In order to be able to construct effectively these tests we will impose some more restrictions. That is for a given sequential test:

1) the U's are recursively enumerable.

2) given m, one can effectively enumerate U_m such that

$$\mu \left[\bigcup_{x \in U_m} [x] \right] < 2^{-m}$$

Definition 2.1.1. Let $X = \{0,1\}^*$

A subset U of $N \times X$ is a sequential test if

1) U is recursively enumerable.

2) Its intersections $U_m = \{x \in X \mid (m,x) \in U\}$ are sequential. That is,

$$(\forall\, x \in U_m)\ \ (\forall\, y \in X)\ [x\, y\ \in U_m]$$

3) We have $X = U_0 \supseteq U_1 \supseteq U_2 \supseteq \ldots$

4) And $\mathcal{U}_m$ the open generated by U_m; verifies

$$\mu\, [\mathcal{U}_m] < 2^{-m}.$$

From each sequential test U in $N \times X$, one obtains immediately a sequential test $(\mathcal{U}_0, \mathcal{U}_1, \ldots)$ in Ω. The relation between $\mathcal{U}$ and U is reversible. We shall consider then as synonyms.

All effective tests from probability theory of the space Ω (with μ) are sequential tests in this sense.

The main property of this definition is that we can define a test which will include all tests of the type defined above.

Definition 2.1.2 A sequential test U is called universal if there exists, to each sequential test V an integer $C \geq 0$ such that:

$$V_{m+C} \subseteq U_m \quad (m = 1,2,\ldots)$$

2.2. Properties

Theorem (Martin-Lof) 2.2.1

There exist universal sequential tests.

Sketch of the proof: We define a Godel numering of the set of all sequential tests: $U^{(0)}, U^{(2)}, \ldots, U^{(m)}, \ldots$ and we define U universal by its intersections:

$$U_m = \bigcup_{i=0}^{\infty} U_{m+i}^{(i)}$$

Definition 2.2.2. A sequence is random in this definition (we shall write random (ML)) if it doesn't belong to $\bigcap_{m=1}^{\infty} \mathcal{U}_m$, for $\mathcal{U}$ universal.

We will call this set the universal constructive null set. This set is the union of the null sets: $\cap \mathcal{V}_m$, for all sequential tests $\mathcal{V}$.

Since the universal constructive null set has measure zero, we have:

Fact: Almost all sequences are random (ML).

We shall first study the position of some random (ML) sequences in the arithmetical hierarchy, then relate this definition to the notion of Kollektiv.

Theorem 2.2.3: The characteric function of a recursively enumerable set (or its complement) is not random (ML).

Proof: Let A be this set and h a recursive function enumerating A without repetitions. We assume A infinite.

Let h_n = {n first elements of A enumerated by h}.

$\mathcal{U}_n = \{S | h_n \subset S\}$

We have

1) $\mu[\mathcal{U}_n] \leq 2^{-n}$, since n coordinates are fixed

2) the corresponding U_n is sequential and

3) $U_{n+1} \subseteq U_n$ for all n

4) Since h is recursive, U_n is also recursive.

Then if A or its complement is r.e., its characteristic function C_A will not be random (ML).

Corollary: C_A is random (ML) implies that A and its complement intersect every infinite r.e. set.

So there is no random (ML) sequences, in Σ_1 and π_1. We show that there is one in $\Delta_2 = \Sigma_2 \cap \pi_2$ (in fact $\Delta_2 - (\Sigma_1 \cup \pi_1)$)

Theorem 2.2.4. There exists Δ_2 sequences which are random (ML).

Proof: We construct a characteristic function recursive in a recursively enumerable set. The sequence representing this characteristic function will be random (ML).

Let U be a universal sequentail test, x and y binary strings.

We know that $\mu(\mathcal{U}_1) \leq \frac{1}{2}$

Define C as follows:

$$x \in C \Leftrightarrow (\exists\, n)\ (\forall\, y)\ [\text{length}\ (y) = n \Rightarrow xy \in U_1]$$

Note $x \in U_1 \Rightarrow x \in C$

Since U_1 is recursively enumerable

$$V_n = \{x \mid (\forall\, y)\ [\text{length}(y) = n \Rightarrow xy \in U_1]\ \text{ is also r.e.}$$

$$x \in C \Leftrightarrow (\exists\, n)\ \ [x \in V_n]$$

So C is recursively enumerable. Moreover $\mu(\mathcal{U}_1) \leq \frac{1}{2}$ implies that at least half of the sequences of length n are not in C.

Using an oracle for C, we now construct a sequence S, in stages.

stage 0 Assume $0 \notin C$, Let $S_1 = 0$

stage n+1 Assume $S_n \notin C$, then $S_n\ 1$ or $S_n\ 0$ doesn't belong to C_0.

If $S_n\ 1 \notin C$ then $S_{n+1} = S_n 1$ otherwise $S_{n+1} = S_n\ 0$. END

No initial segment of the sequence S so constructed will be in C, and therefore cannot be in U_1 so $S \notin \mathcal{U}_1$, S is random (ML) Q.E.D.

Using the same method, we could prove the following theorem, given without proof:

Theorem 2.2.5. There exists random (ML) sets properly in

$$\Delta_i = \Sigma_i \cap \pi_i \qquad \text{for} \quad i = 2, 3, \ldots$$

Let us now investigate the relation between this definition of randomness and that of Church.

Let VM = {S| there exists a P-algorithm with a bias for S}. VM is the set of sequences not random in the sense of Church.

Theorem 2.2.6. If a sequence is random (ML), then it is random (VM)

Proof: Given a P-algorithm P, we extract the two corresponding places selections: P_0, P_1, as in chapter I. We define the set of finite strings (for m, n integers):

$$A_n^{q,0} = \{S' \in X \mid \exists\, S \text{ initial segment of } S', \text{ such that:}$$

1) $\# P_0(S) = n.$

2) $\#_0 P_0(S) / \# P_0(S) > \frac{1}{2} + \frac{1}{q}\ \}$

Let $\mathcal{A}_n^{q,0}$ be the open set of Ω generated by $A_n^{q,0}$.

1) We have

$$\mathcal{A}_n^{q,0} = \bigcup_{m=n}^{\infty} \Gamma_m^{q,0}$$

where

$$\Gamma_m^{q,0} = \{S \mid \text{The first m places selected by } P_0 \text{ contains a number of 0's} > (\tfrac{1}{2} + \tfrac{1}{q}).\}$$

From Doob's theorem, if S_n is the initial segment of length m of S:

$$P_r\{\Gamma_m^{q,0}\} = P_r\{S \mid S_m \text{ contains more than m } (\tfrac{1}{2} + \tfrac{1}{q}) \text{ 0's}\}$$

Let $\lambda = \frac{1}{2} + \frac{1}{q}$, $\lambda > \frac{1}{2}$

We have

$$P_r\{\Gamma_m^{q,0}\} \leq 2^{-m} \cdot \sum_{p \geq \lambda m}^{m} \binom{m}{p}$$

If we consider the entropy function for $\frac{1}{2} < \lambda \leq 1$:

$$H(\lambda) = \lambda \log \frac{1}{\lambda} + (1-\lambda) \log \frac{1}{1-\lambda}$$

We have

$$P_r\{\Gamma_m^{q,0}\} \leq 2^{-m}\, 2^{mH(\lambda)}$$

$$\leq 2^{m(H(\lambda)-1)}$$

Since $\lambda > \frac{1}{2} \Rightarrow 1-H(\lambda) = \alpha > 0.$

$$\Rightarrow P_r\{\Gamma_m^{q,0}\} \leq 2^{-\alpha m}$$

So

$$P_r\{\bigcup_{m \geq n} \Gamma_m^{q,0}\} \leq \sum_{m=n}^{\infty} 2^{-\alpha m} = \frac{2^{-\alpha n}}{1-2^{-\alpha}}$$

Therefore $P_r\{\mathcal{A}_n^{p,0}\} \leq \frac{2^{-\alpha n}}{1-2^{-\alpha}} \leq 2^{-\alpha n+1}$

We have also

2) $A_{n+1}^{q,0} \supseteq A_n^{q,0} \quad (\forall\, n)$

3) $x \in A_n^{q,0} \Rightarrow (\forall\, y)\ [xy \in A_n^{q,0}]$.

4) $A_n^{q,0}$ is r.e.

Let

$U_n^{q,0} = A^{q,0}_{[\frac{1+n}{\alpha}]}$. where $[x]$ is the smallest integer greater than x.

Then $U_n^{q,0}$ is a sequential test in the sense of Martin-Lof.

We could, in the same manner, construct $U_n^{q,1}$ corresponding to P_1 and some q.

Now if a sequence S is not random (VM),

$$(\exists\, P,\ P\text{-algorithm})\ (\forall\, q)\quad [\alpha[P,S,x] > \frac{1}{2} + \frac{1}{q}\quad (i.o)]$$

which implies

$$(\forall\, q')\ (\forall\, n)\ [S \in \mathcal{U}_n^{q',i}] \quad \text{where i is either 0 or 1 ,}$$

and hence S is not random (ML). Q.E.D.

2.3. As a conclusion we can say that, some random (VM) sequences are not random (ML). This was affirmed by Martin-Lof in a private communication, here is a straight-forward proof:

The law of the iterated logarithm, as given above, may be stated as a sequential test. Thus, all sequences which do not obey this law will be in the null set of that test.

Therefore, a sequence which does not obey the law of the iterated logarithm will not be random (ML).

But by Ville [12] theorem, one can construct a random (VM) sequence, where the ratio of the number of 1's to the number of 0's, is always not less than 1. This sequence will not follow the law of the iterated logarithm and therefore will not be random (ML).

CHAPTER III

DESCRIPTIVE COMPLEXITY

After this survey of gambling algorithms and measure theoretic arguments, we shall take another point of view, related to the difficulty of description of a random sequence.

We can note that, if binary strings of length n are classified according to the number of 0's in them, the strings in the largest class will have [n/2] zero's. Thus, if we draw a string at random, it will have with a great probability, approximately the same number of 0's and 1's. By the same kind of combinatorial argument, a string of length n, chosen at random, has a small probability to contain some kind of periodic pattern.

From those simple remarks, we can deduce another definition of randomness:

One characteristic of a binary string, made entirely with 1's (or 0's) or a repeating pattern, is their easy description. In fact, it is sufficient to have the length of the string and the pattern in order to reconstruct it.

Kolmogorov, in [10], formalized this idea. He gave a new definition of the relative entropy $H(x|y)$, x being a binary string. This entropy will measure the difficulty of description of the string x, given the information y (e.g. its length). This will enable us to define random elements as those with the largest entropy.

But, we have to make clear that a description of some element x, will make sense only if we make precise the means to reconstruct x from it.

We consider, in this chapter, a description of a binary string, as a "program" for a specific Turing machine (with binary strings as outputs).

Note that we restrict our attention to effective reconstruction; but we might as well consider more powerful means (using Turing machines with an oracle, for example).

Given a Turing Machine A, with two inputs, we define:

$$H_A(x|y) = \min_{A(p,y)=x} \ell(p)$$

p is the program for x, $\ell(p)$ its length.

Definition: The Kolmogorov Complexity (or descriptive complexity) of a string x with respect to algorithm A is:

$$K_A(x) = \min_{A(p)=x} \ell(p)$$

If there exists a string p such that $A(p) = x$, otherwise $K_A(x) = \infty$.

The Kolmogorov conditional complexity of x given y, with respect to A, is:

$$K_A(x|y) = \min_{A(p,y)=x} \ell(p)$$

If such a p exists, otherwise $K_A(x|y) = \infty$.

There are several basic properties noted by Kolmogorov [9] which apply to all two measures.

Fact 1 There exists a universal algorithm B such that for an arbitrary algorithm A and for x.

$$K_B(x \mid \ell(x)) \leq K_A(x \mid \ell(x)) + c$$

where c depends only on A and B.

Fact 2 If B_1 and B_2 are two universal algorithms then there exists a constant c, such that for all x:

$$|K_{B_1}(x \mid \ell(x)) - K_{B_2}(x \mid \ell(x))| \leq c$$

So two universal algorithms are equivalent up to a constant.
We shall hereafter refer to $K_U(x \mid \ell(x))$ for an universal algorithm U as $K(x \mid \ell(x))$.

Fact 3. There exists a constant c such that

$$K(x \mid \ell(x)) \leq n + c \qquad \text{for all } x$$

Fact 4 Less than 2^r strings of length n satisfy

$$K(x \mid n) < r.$$

3.1 Definition of Random Sequences

Consequently, we are led to the definition: A finite string x will be random if $K(x \mid \ell(x))$ is maximum for $\ell(x)$ fixed.

We want to generalize this definition to infinite sequences of 0's and 1's.

First idea: a sequence will be random if all its initial segments are random. And since the complexity is defined up to an additive constant, we would have:

$$S, \text{ is random} \Leftrightarrow (\exists c)\ (\overset{\infty}{\forall} n)\ [K(S_n|n) > n-c]$$

But such sequences, as shown by Martin Lof, do not exist. Indeed, from probability theory, we know that a random sequence has almost surely continuous sequences of 0's or 1's. It is clear that the description of such segments of infinite sequences can be substantially simplified.

More precisely

Theorem (Martin-Lof) [17]: Let f be a real-valued function:

If $\sum_{n=1}^{\infty} 2^{-f(n)} = +\infty$ then

for all $S \in \Omega$ $(\overset{\infty}{\exists} n)$ $[K(S_n|n) < n - f(n)]$.

Therefore if we want to have a consistent definition with the fact that almost all sequences are random, we can have:

Definition I (Chaitin [8]):

The set C_∞ of patternless or random infinite binary sequences is:

$$C_\infty = \{S|\ (\overset{\infty}{\forall} n)\ \ K(S_n|\ n) > n-f(n)\}$$

where $f(n) = 3 \log n$ or any function such that

$$\sum_{n=1}^{\infty} 2^{-f(n)} < +\infty$$

we will verify below that $\mu(C_\infty) = 1$.

Definition II (Martin-Lof):

The set R of random infinite binary sequences is

$$R = \{S \mid (\exists c)\ (\overset{\infty}{\forall} n)\ [K(S_n \mid n) > n-c]$$

we will also show that $\mu(R) = 1$, and that $R \subset C_\infty$.

3.2. Properties

We use the second definition. We will write "random in the sense of definition II" as "random (K)".

Theorem 3.2.1

$$\mu\{S \mid S \text{ is random (K)}\} = 1.$$

Proof:

Let K be the complement of R in Ω:

$$S \in K \Leftrightarrow (\forall c)\ (\exists n_0)\ (\forall n \geq n_0)\ [K(S_n|n) \leq n-c]$$

$$K = \bigcap_c \bigcup_{n_0} \bigcap_{n \geq n_0} \Gamma_{n,c} \qquad \Gamma_{n,c} = \{S \mid K(S_n|n) \leq n-c\}$$

We know

$$\mu[\Gamma_{n,c}] \leq 2^{-c} \Rightarrow \mu[\bigcap_{n \geq n_0} \Gamma_{n,c}] \leq 2^{-c}$$

$$B_{n_0,c} = \bigcap_{n \geq n_0} \Gamma_{n,c} \qquad B_{n_0,c} \subseteq B_{n_0+1,c} \subset \cdots$$

$$\Rightarrow \mu[\cup B_{n_0,c}] \leq 2^{-c}$$

$$\Rightarrow \mu[K] = 0$$

We prove now that definition I gives also a set of measure 1.

Theorem 3.2.2. Let f(n) be a function such that

$\sum_{n=1}^{\infty} 2^{-f(n)} < +\infty$, Then for almost all S: $(\forall^{\infty} n)\ [K(S_n|n) > n-f(n)]$

Proof Let $\Upsilon = \{S | (\exists^{\infty} n)\ [K(S_n|n) \leq n-f(n)]\}$

$$\Upsilon = \bigcap_{n_0} \bigcup_{n \geq n_0} \Gamma_n \quad , \quad \Gamma_n = \{S | K(S_n|n) \leq n-f(n)\}$$

By Fact 4: $\mu(\Gamma_n) < 2^{-f(n)}$

and $\sum_{n=1}^{\infty} 2^{-f(n)} < +\infty$ implies by Borel-Cantelli Lemma, that

$$\mu(\Upsilon) = 0$$

To prove that a random (K) sequence is also random in the sense of definition I, we use:

Theorem 3.2.3. (Martin-Lof) Given a function f(n). If $\sum_{n=1}^{\infty} 2^{-f(n)} < +\infty$ and if given m, one can compute effectively N such that

$$\sum_{n=N}^{\infty} 2^{-f(n)} \leq 2^{-m}$$

Then, for all random (K) sequences

$$(\overset{\infty}{\forall}\ n)\quad [K(S_n|n) > n-f(n)]$$

The proof uses f(n) to construct a sequential test and uses Theorem 3.2.4 below.

Theorem 3.2.4.

S is random (K) $\Rightarrow$ S is random (ML).

Proof. Assume that for some universal sequential test:

$$S \in \overset{\infty}{\underset{m=1}{\cap}} \mathcal{U}_m$$

This means $(\forall\ m)\ (\exists\ n_0)\ (\forall\ n \geq n_0)\ [S_n \in \mathcal{U}_m]$ (1)

As 1) U is recursively enumerable

2) U_m contains less than 2^{n-m} strings of length n.

We can describe an algorithm A generating S_n: Assume $S_n \in U_m$. A is given a program for generating the element of U, the number m and a number z less than 2^{n-m}. Given such data, A will enumerate U_m and outputs the z^{th} element. The program of A will therefore be of size:

Constant + log m + log 2^{n-m} = n-m + log m + constant

1) $\Rightarrow$ $(\forall\ m)\ (\overset{\infty}{\forall}\ n)\ [K_A(S_n|n) \leq n-m + \log m + c]$

By Fact 2: $K(S_n|n) \leq K_A(S_n|n) + c'$

$(\forall\ m)\ (\overset{\infty}{\forall}\ n)\ [K(S_n|n) \leq n-m + \log m + c'']$

where c'' is a constant independent of S and n.

Thus $(\forall\, c)\ (\overset{\infty}{\forall}\, n)\ [K(S_n|n) < n-c]$

So S is not random (K)

3.3 Definition of K as a Null Set of a Test

$$X = \{0,1\}^*$$

$$T_m = \{x \in X \mid (\forall\, y \in X)\ [K(xy \mid \ell(xy)) \leq \ell(xy)-m]\}$$

Then

1) T_m is sequential: $x \in T_m \Rightarrow (\forall\, y \in X)\ [xy \in T_m]$

2) $T_1 \supseteq T_2 \supseteq \ldots\ldots \supseteq T_m \supseteq \ldots$

3) $\mathcal{T}_m$ = open in Ω, generated by T_m: $\mu(\mathcal{T}_m) \leq 2^{-m}$

Let $\mathcal{T} = \cap\, \mathcal{T}_m$, $\mathcal{T}$ is a null set.

Remark. The T_m above defines a sequential test in the sense of Martin-Lof except for recursive enumerability.

What is the degree of uneffectiveness of T.

Theorem 3.3.1. T is π_2^0.

Proof. Let $\Sigma_m = \{x|K(x|\ell(x)) < \ell(x)-m\}$

Σ_m is a recursively enumerable set.

$$T_m = \{x \mid (\forall\, y)\ [xy \in \Sigma_m]\}$$

or $x \in T_m \Leftrightarrow (\forall\, y)\ [xy \in \Sigma_m]$

Therefore T_m and T are of the degree of π_2^0.

Fact Using definition II we can see

S is random (K) $\Leftrightarrow S \in \bigcap \mathcal{T}_m$.

We have therefore defined K as the null set of a test in π_2^0. Using the same method that in Chapter II. We can see:

Theorem 3.3.2. There are characteristic functions of sets in Δ_3 which are random (K).

That is an open problem whether T is properly in π_2^0. Or equivalently, since we know by Theorem 3.2.4 that M L $\subset$ K: if this inclusion is proper.

By the precedings, we know that this notion of randomness is the largest of the three in the sense that, its null set of non-random sequences includes the other two.

3.4. Pseudo-Random Sequences

Given a Turing Machine A, we defined the complexity of a string x, as the minimal length of a program with which A will generate x.

We can, as in Chapter I, put a bound on the time necessary for A to generate x. We shall present in this section a few remarks and a theorem of McCreight [2], which may lead to interesting research.

Given a Turing machine A, with two inputs x,y, we define a measure of the computation of A, with inputs x,y, we call this measure $\alpha(x,y)$:

1) $\alpha(x,y)$ is finite $\Leftrightarrow$ the computation A(x,y) halts

2) $\alpha(x,y) = z$ is a recursive predicate.

We can take as example the number of steps of the computation A(x,y).

Definition 3.4.1. Given a recursive function g, the pseudo-complexity of a string $x = x_1 x_2 \ldots x_n$

$$K'_g(x|n) = \min_{A(p,n)=x} \ell(p)$$

where A is a universal algorithm and

$$(\forall\, i \leq n)\ [A(p, i) = x_1 x_2 \ldots x_i \text{ and } \alpha[p, i] \leq g(i)]$$

This definition is related to this of uniform complexity by Loveland [5]. We give a tentative

Definition. Given a recursive function g, a sequence S is random at level g, if

$$(\overset{\infty}{\forall}\, n)\ [K'_g(S_n|n) > n-f(n)], \text{ where } f(n) \text{ will be fixed further.}$$

Rabin gives a construction of a 0.1 valued recursive function φ_i such that $\Phi_i(x) > g(x)$ (a.e.).

But with this property, the sequence

$$S = \varphi_i(1)\ \varphi_i(2) \ldots \varphi_i(n) \ldots$$

is not necessarily random at level g.

Assume that S has the property:

$$(\overset{\infty}{\exists}\, n)\ [K'_g(S_n|n) \leq n-f(n)]$$

Then, for arbitrarily large n, the string $S_n = s_1 s_2 \ldots s_n$ can be described by a program p: $\ell(p) \leq n - 3 \log n$. We can construct a new program for S of the form $\alpha \gamma \beta \gamma p$, where γ is some binary sequence which serves to separate α, β, p. α is the binary encoding of the following instructions:

> "Given input x, see if x-f(x) ≤ length of the string to the right of the second γ. If so simulate A(p,x) and give the x^{th} digit of the output as result. Otherwise compute s_x according to the instructions given by β"

Let i be the Godel number of this program : $\log i = k + n - f(n)$ where k is a constant.

Let $h(n) = n - f(n)$. The program φ_i for the sequence S, will have the property:

$\Phi_i(x) \leq g(x)$ on at least $[h^{-1}(\log i - k)]$ inputs.

Let us now state a theorem by McCreight [2]

Theorem: $(\forall \varepsilon > 0)\ (\forall g \in R_1)\ (\exists k \in N)\ (\exists$ 0.1 valued $c \in R_1)\ (\forall i \in N)$

$[\varphi_i = c \Rightarrow \Phi_i(x) > g(x)$ for all but $k + (1 + \varepsilon) \log i$ values of x].

and moreover this c is effective given g, ε.

Then we let $f(n) = \varepsilon'.n$ and construct the function c of the theorem above with $\varepsilon < \varepsilon'$.

If the sequence c(1), c(2),...,c(n),... were random, then there exists arbitrarily large i such that

$\varphi_i = c$ and $\Phi_i \leq g$ on at least $\frac{\log i - k}{1 - \varepsilon'}$, which is ultimately larger than $(1+\varepsilon) \log i + c$. This sequence is therefore random if we take $f(n) = \varepsilon' . n$ We have:

Theorem. Given g, and $\varepsilon > 0$, one can effectively construct sequences such that

$$(\overset{\infty}{\forall} n)\ [K'_g(S_n|n) > (1-\varepsilon)n].$$

Remark. It remains an open question whether the bound in McCrieght theorem can be decreased to k + log i.

If that is so, then we would be able to construct sequences such that

$$(\exists\ c)\ (\overset{\infty}{\forall} n)\ [K'g(S_n|n) > n-c]$$

which would be a definition of pseudo-random sequences consistent with the Kolmogorov definition.

CONCLUSION

Each of these three definitions of randomness is in fact based upon some set of statistical tests. We considered in this paper only effective tests, i.e., usable with computer programs. We could expand this theory to a more complete form by considering tests arbitrarily high in the arithmetical hierarchy.

If we let 0 denote the recursive T-degree*, we can define a n-guessing algorithm as a total function $g(x, S)$ of one integer and one set variable.

$$g(x, S) = \Psi(x, S \cap \{1, 2, \ldots, x-1\})$$

where Ψ is recursive in the n^{th} jump of 0: $0^{(n)}$. A sequence S will be random (VMn) if no n-guessing algorithm has a bias for it. Note that Ville's result applies again: there are random (VMn) sequences which do not follow the law of the iterated logarithm.

The definition of Chapters 2 and 3 could also be generalized by considering sequential tests as subsets of $N \times X$ recursively enumerable in $0^{(n)}$, this will give us the definition of random (MLn) sequences; and we can generalize the Kolmogorov complexity by using Turing machines with an oracle for $0^{(n)}$, and hence define random (Kn) sequences.

Each of these extended definitions will yield a set of random sequences of measure 1. The inclusion results hold also for these definitions relativized to $0^{(n)}$. A random (Kn) sequence will be random (MLn) and, in turn, a random (MLn) sequence will be random (VMn).

---

*H. Rogers: Theory of recursive functions. Chapter 13.

One other aspect of this paper, which could lead to interesting developments, is the generation of pseudo-random sequences. Using a measure of the complexity of a test, we constructed sequences which look random to all simple randomness tests.

Those sequences could be useful for the generation of random numbers with any distribution, with application in various fields, like simulation or coding theory.

REFERENCES

[1] A. Church: On the Concept of Random Sequence. Bulletin American Math. Soc. 46 (1940) (pp. 130-135).

[2] E. McCreight: A note on Complex Recursive Characteristic Functions. Unpublished.

[3] E. McCreight and A. R. Meyer: Classes of Computable Functions Defined by Bound on Computation. ACM Symposium on Theory of Computation. (1969)

[4] Levin, Minsky and Silver: On the Problem of the Effective Definition of "Random Sequence". Memo 36 (revised) M.I.T. Computation Center.

[5] D. Loveland: A New Interpretation of the Von Mises' Concept of of Random Sequence". Zeit, Math. Logic und Grundl. Math. 12.1 (1967)

[6] D. Loveland: The Kleene Hierarchy Classification of Recursively Random Sequences. Trans. AMS. 125-3 (497-519).

[7] Martin-Lof: The Definition of Random Sequences. Information and Control. 9 (1966).

[8] Martin-Lof: Algorithm and Randomness. Europ. Meeting of Statist. London (1966).

[9] Kolmogorov: Three Approaches to the Quantitative Definition of of Information Transmission. (Trans. for Russian) Problemy Pederachi Informatsii (1965).

[10] Kolmogorov: Logical Basis for Information Theory and Probability Theory. IEEE Trans. on Info. Theory. Vol. IT 11 No. 5 (1968).

[11] Knuth: The Art of Computer Programming (Vol. 2) Seminumerical Algorithms (Addison-Wesley)

[12] Ville: Etude Critique de la notion de Collectif. Gauthier. Villars.

[13] Wald: Sur la notion de Collectif dans le calculdes Probabilites. Cptes. rendus Acad. des Sc. Vol. 202 (1936) pp. 180-183).

[14] Doob. Note on Probability. Annals of Maths. (2) Vol. 37 (1936).

[15] Kruse: Some Notions of Random Sequence and Their Set-Theoretic Foundations. Zeit. f Math. Logik u Grundl d. Math. (1967)

DOCUMENT CONTROL DATA - R&D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY *(Corporate author)* Massachusetts Institute of Technology Project MAC	2a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED 2b. GROUP None

3. REPORT TITLE

Pseudo-Random Sequences

4. DESCRIPTIVE NOTES *(Type of report and inclusive dates)*

Technical Memorandum

5. AUTHOR(S) *(Last name, first name, initial)*

Bruere-Dawson, Gerard

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
October 1970	54	15

8a. CONTRACT OR GRANT NO. Nonr-4102(01) b. PROJECT NO. c. d.	9a. ORIGINATOR'S REPORT NUMBER(S) TM-16 9b. OTHER REPORT NO(S) *(Any other numbers that may be assigned this report)*

10. AVAILABILITY/LIMITATION NOTICES

Distribution of this document is unlimited.

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
None	Advanced Research Projects Agency 3D-200 Pentagon Washington, D.C. 20301

13. ABSTRACT

Three definitions of random binary sequences are presented. The consistency of those definitions with the laws of probability theory, and the inclusion relationship of the three sets of random sequences, are investigated.

These sequences, considered as characteristic functions of sets, are then placed in the Kleene arithmetical hierarchy. Some restrictions on these definitions, using Blum's complexity theory, lead to the definition of pseudo-random sequences, which can be generated effectively.

14. KEY WORDS

Recursive Functions Church Random Sequences Sequential Tests
Probability Laws Descriptive Complexity Kleene Hierarchy

DD FORM 1 NOV 65 1473 (M.I.T.)