Journal of Scientific Computing, Vol. 6, No. 1, 1991

Random Sequences in Fréchet Spaces

John H. Halton[1]

Received December 21, 1989

This article deals with the generation of arbitrarily distributed sequences $\boldsymbol{\Phi}$ of random variables in a Fréchet space, using sequences of *canonical random variables* (c.r.v.)—i.e., independently uniformly distributed random variables taking real values in the unit interval $[0, 1)$—or *canonical random digits* (c.r.d.)—i.e., independently uniformly distributed random variables taking integer values in some finite interval $[0, B-1]$. Two main results are established. First, that the members of a sequence of real random variables in $[0, 1)$ are c.r.v. if and only if all the digits of all the *base-B digital representations* of the members of the sequence are c.r.d. Secondly, that, given any sequence $\boldsymbol{\Phi}$ of random variables in a Fréchet space, there is a sequence $\boldsymbol{\Psi}$ of functions $\psi_n(\xi_1, \xi_2,..., \xi_n)$, for $n = 1, 2, 3,...$ (where $\xi_1, \xi_2,..., \xi_n,...$ are c.r.v.) which is distributed identically to $\boldsymbol{\Phi}$.

KEY WORDS: Random sequences; Fréchet spaces; pseudorandom numbers.

1. INTRODUCTION

The performance of a stochastic simulation or Monte Carlo experiment depends on the availability of appropriately prescribed random sequences. A practical device (such as a book of tables, a deck of punched cards, a roulette wheel, a noisy electronic circuit, or a programmed algorithm) that yields such a sequence is called a *random generator*. It is clearly of great advantage to be able to limit random generators to as small a class as possible. In fact, nearly all available devices are approximations to the *canonical random generators* Λ and Λ_B defined below; and it is the purpose of this article to demonstrate that either of these suffices for all practical purposes.

[1] Computer Science Department, The University of North Carolina, Chapel Hill, North Carolina 27599.

2. PRELIMINARIES

The discussion will be clearer if we adopt certain conventions of notation. *Real numbers* (and unrestricted *integers*) will be denoted by lower case Italic letters:

$$a, b, c_r, \ldots, x, y, z_n \tag{2.1}$$

(The letters from i through r will usually denote integers.) *Infinite sequences* of real numbers will be denoted by corresponding boldface letters:

$$\begin{gathered} \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}_r, \ldots, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}_n \\ \boldsymbol{f} = [f_r]_r = [f_r]_{r=1}^{\infty} = [f_1, f_2, \ldots, f_r, \ldots] \\ \boldsymbol{f}_n = [f_{nr}]_r = [f_{nr}]_{r=1}^{\infty} = [f_{n1}, f_{n2}, \ldots, f_{nr}, \ldots] \end{gathered} \tag{2.2}$$

sequences of sequences will be denoted by corresponding boldface capital letters:

$$\begin{gathered} \boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}_r, \ldots, \boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}_n \\ \boldsymbol{F} = [\boldsymbol{f}_n]_n = [\boldsymbol{f}_1, \boldsymbol{f}_2, \ldots, \boldsymbol{f}_n, \ldots] \end{gathered} \tag{2.3}$$

and finite (*truncated*) sequences will be denoted by the same symbols, superscripted:

$$\begin{aligned} \boldsymbol{f}^m &= [f_r]_{r=1}^m = [f_1, f_2, \ldots, f_m] \\ \boldsymbol{f}_n^m &= [f_{nr}]_{r=1}^m = [f_{n1}, f_{n2}, \ldots, f_{nm}] \\ \boldsymbol{F}^m &= [\boldsymbol{f}_n]_{n=1}^m = [\boldsymbol{f}_1, \boldsymbol{f}_2, \ldots, \boldsymbol{f}_m] \end{aligned} \tag{2.4}$$

Probability spaces will be denoted by triples of the customary form, typified by

$$(M, \boldsymbol{M}, \mu) \tag{2.5}$$

where M is a set (the *sample space*), $\boldsymbol{M}$ is a σ-algebra of subsets of M (the set of *events*), and μ is a totally finite measure on $(M, \boldsymbol{M})$ with $\mu(M) = 1$ (the *probability*). Points in sample spaces will be denoted by lower-case Greek letters.

Functions in general will be denoted by both Italic and Greek letters. Real-valued measurable functions on probability spaces (*random variables*) will be denoted by lower-case Greek letters:

$$\alpha, \beta, \gamma_r, \ldots, \xi, \eta, \zeta_n \tag{2.6}$$

Infinite sequences of such random variables will be denoted by boldface and capital Greek letters, by analogy with (2.2)–(2.4):

$$\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}_r, \ldots, \boldsymbol{\xi}, \boldsymbol{\eta}, \boldsymbol{\zeta}_n$$
$$\boldsymbol{\phi} = [\phi_r]_r = [\phi_r]_{r=1}^{\infty} = [\phi_1, \phi_2, \ldots, \phi_r, \ldots] \tag{2.7}$$
$$\boldsymbol{\phi}_n = [\phi_{nr}]_r = [\phi_{nr}]_{r=1}^{\infty} = [\phi_{n1}, \phi_{n2}, \ldots, \phi_{nr}, \ldots]$$

sequences of sequences by capital letters:

$$\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{\Gamma}_r, \ldots, \boldsymbol{\Xi}, \boldsymbol{H}, \boldsymbol{Z}_n$$
$$\boldsymbol{\Phi} = [\boldsymbol{\phi}_n]_n = [\boldsymbol{\phi}_1, \boldsymbol{\phi}_2, \ldots, \boldsymbol{\phi}_n, \ldots] \tag{2.8}$$

and truncated sequences by superscripts:

$$\boldsymbol{\phi}^m = [\phi_r]_{r=1}^m = [\phi_1, \phi_2, \ldots, \phi_m]$$
$$\boldsymbol{\phi}_n^m = [\phi_{nr}]_{r=1}^m = [\phi_{n1}, \phi_{n2}, \ldots, \phi_{nm}] \tag{2.9}$$
$$\boldsymbol{\Phi}^m = [\boldsymbol{\phi}_n]_{n=1}^m = [\boldsymbol{\phi}_1, \boldsymbol{\phi}_2, \ldots, \boldsymbol{\phi}_m]$$

Digits (i.e., integers restricted to a finite interval, $0 \leqslant \mathsf{q} \leqslant B-1$), will be denoted by lower-case, sans-serif Roman letters:

$$\mathsf{a}, \mathsf{b}, \mathsf{c}_r, \ldots, \mathsf{x}, \mathsf{y}, \mathsf{z}_n \tag{2.10}$$

Again, by analogy with (2.2)–(2.4) and (2.7)–(2.9), *sequences* of digits will be denoted by corresponding boldface and capital letters:

$$\mathbf{a}, \mathbf{b}, \mathbf{c}_r, \ldots, \mathbf{x}, \mathbf{y}, \mathbf{z}_n$$
$$\mathbf{q} = [\mathsf{q}_r]_r = [\mathsf{q}_r]_{r=1}^{\infty} = [\mathsf{q}_1, \mathsf{q}_2, \ldots, \mathsf{q}_r, \ldots] \tag{2.11}$$
$$\mathbf{q}_n = [\mathsf{q}_{nr}]_r = [\mathsf{q}_{nr}]_{r=1}^{\infty} = [\mathsf{q}_{n1}, \mathsf{q}_{n2}, \ldots, \mathsf{q}_{nr}, \ldots]$$

$$\mathsf{A}, \mathsf{B}, \mathsf{C}_r, \ldots, \mathsf{X}, \mathsf{Y}, \mathsf{Y}_n$$
$$\mathsf{Q} = [\mathbf{q}_n]_n = [\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_n, \ldots] \tag{2.12}$$

$$\mathbf{q}^m = [\mathsf{q}_r]_{r=1}^m = [\mathsf{q}_1, \mathsf{q}_2, \ldots, \mathsf{q}_m]$$
$$\mathbf{q}_n^m = [\mathsf{q}_{nr}]_{r=1}^m = [\mathsf{q}_{n1}, \mathsf{q}_{n2}, \ldots, \mathsf{q}_{nm}] \tag{2.13}$$
$$\mathsf{Q}^m = [\mathbf{q}_n]_{n=1}^m = [\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_m]$$

Finally, we use lower-case script letters to denote *random digits*:

$$\mathscr{a}, \mathscr{b}, \mathscr{c}_r, \ldots, \mathscr{x}, \mathscr{y}, \mathscr{z}_n \tag{2.14}$$

Again, by analogy with (2.2)–(2.4), (2.7)–(2.9), and (2.11)–(2.13), *sequences* of random digits will be denoted by corresponding boldface and capital letters:

$$\boldsymbol{\mathscr{a}}, \boldsymbol{\mathscr{b}}, \boldsymbol{\mathscr{c}}_r, \ldots, \boldsymbol{\mathscr{x}}, \boldsymbol{\mathscr{y}}, \boldsymbol{\mathscr{z}}_n$$

$$\boldsymbol{\mathscr{q}} = [\mathscr{q}_r]_r = [\mathscr{q}_r]_{r=1}^{\infty} = [\mathscr{q}_1, \mathscr{q}_2, \ldots, \mathscr{q}_r, \ldots] \tag{2.15}$$

$$\boldsymbol{\mathscr{q}}_n = [\mathscr{q}_{nr}]_r = [\mathscr{q}_{nr}]_{r=1}^{\infty} = [\mathscr{q}_{n1}, \mathscr{q}_{n2}, \ldots, \mathscr{q}_{nr}, \ldots]$$

$$\mathscr{A}, \mathscr{B}, \mathscr{C}_r, \ldots, \mathscr{X}, \mathscr{Y}, \mathscr{Z}_n$$

$$\mathscr{Q} = [\boldsymbol{\mathscr{q}}_n]_n = [\boldsymbol{\mathscr{q}}_1, \boldsymbol{\mathscr{q}}_2, \ldots, \boldsymbol{\mathscr{q}}_n, \ldots] \tag{2.16}$$

$$\boldsymbol{\mathscr{q}}^m = [\mathscr{q}_r]_{r=1}^m = [\mathscr{q}_1, \mathscr{q}_2, \ldots, \mathscr{q}_m]$$

$$\boldsymbol{\mathscr{q}}_n^m = [\mathscr{q}_{nr}]_{r=1}^m = [\mathscr{q}_{n1}, \mathscr{q}_{n2}, \ldots, \mathscr{q}_{nm}] \tag{2.17}$$

$$\mathscr{Q}^m = [\boldsymbol{\mathscr{q}}_n]_{n=1}^m = [\boldsymbol{\mathscr{q}}_1, \boldsymbol{\mathscr{q}}_2, \ldots, \boldsymbol{\mathscr{q}}_m]$$

Let H be a topological space, and suppose that a homeomorphism (i.e., a one-to-one correspondence mapping open sets onto open sets) τ maps H onto an open subset H^0 of the *Fréchet metric space* F of real infinite sequences $\boldsymbol{f} = [f_r] = [f_r]_{r=1}^{\infty}$ (see, e.g., Pervin, 1964, pp. 112–114, or Sierpiński, 1956, pp. 133–142). (It is well known that, in particular, if H is any *separable metric space*, such a τ can always be found for some $H^0 \subseteq F$.) For simplicity, and with no danger of confusion, we shall identify the sets H^0 and H, so that every element of H will be associated with a distinct real infinite sequence $\boldsymbol{f} = [f_r]_r \in H^0$, and we shall then simply write

$$\boldsymbol{f} \in H \subseteq F \tag{2.18}$$

Clearly, with this identification, H is *metrizable*, by the *Fréchet metric*

$$d_F(\boldsymbol{x}, \boldsymbol{y}) = \sum_{r=1}^{\infty} \frac{1}{2^r} \frac{\Delta_r}{1 + \Delta_r} \tag{2.19}$$

where

$$\Delta_r = \Delta_r(\boldsymbol{x}, \boldsymbol{y}) = |x_r - y_r| \tag{2.20}$$

As is easily verified from (2.19) and (2.20), convergence in terms of this metric is equivalent to convergence in each component of the member sequences of F. Let $\boldsymbol{H}$ denote the σ-algebra generated by the open subsets of H.

Let $(M, \boldsymbol{M}, \mu)$ be a probability space and let $\boldsymbol{\phi}=[\phi_r]_r$ be a function mapping M into the set H of real sequences. That is to say, since $\boldsymbol{\phi}$ maps M into H; for any $\eta \in M$, $\boldsymbol{\phi}(\eta)$ must be a real infinite sequence—$[\phi_r(\eta)]_r$, say—and this defines unambiguously the functions ϕ_r: $M \to \mathbb{R}$, where $\mathbb{R}$ denotes the real line. Now, $\boldsymbol{\phi}$ is a *random variable* (r.v.) in H, if and only if,

$$(\forall P \in \boldsymbol{H})\, \boldsymbol{\phi}^{-1} P \in \boldsymbol{M} \tag{2.21}$$

that is, if and only if

$$\boldsymbol{\phi}^{-1} \boldsymbol{H} \subseteq \boldsymbol{M} \tag{2.22}$$

The probability space $(H, \boldsymbol{H}, \mu\boldsymbol{\phi}^{-1})$, induced by $\boldsymbol{\phi}$ on H, is the *distribution* of $\boldsymbol{\phi}$ in H. And further, as is easily verified, $\boldsymbol{\phi}$ is a r.v. if and only if each of its components ϕ_r $(r=1, 2, 3,...)$ is a r.v. in the real line $\mathbb{R}$.

Given a probability space $(M, \boldsymbol{M}, \mu)$; an *event* A (i.e., a set $A \in \boldsymbol{M}$) may be described as the set $\{\eta: \mathfrak{A}(\eta)\}$ of all points $\eta \in M$ for which the statement $\mathfrak{A}(\eta)$ is true. Then the (unconditional) probability of the event A will be denoted by

$$p_\mu[\mathfrak{A}] = \mu(A) \tag{2.23}$$

and the *conditional probability* of the event $A = \{\eta: \mathfrak{A}(\eta)\}$, given the occurrence of the event $C = \{\eta: \mathfrak{C}(\eta)\}$, will similarly be denoted by $p_\mu[\mathfrak{A} \mid \mathfrak{C}]$. As is well known, when $\mu(C) > 0$, we have

$$p_\mu[\mathfrak{A} \mid \mathfrak{C}] = \frac{\mu(A \cap C)}{\mu(C)} \tag{2.24}$$

Let $\boldsymbol{\Phi} = [\boldsymbol{\phi}_n]_n$ be an arbitrary sequence of r.v., each mapping $(M, \boldsymbol{M}, \mu)$ into H. The distribution $(K, \boldsymbol{K}, \kappa)$ of this *random sequence*, in the infinite Cartesian product set,

$$K = H^\infty = \mathop{\times}_{n=1}^{\infty} H \tag{2.25}$$

has the corresponding product-σ-algebra,

$$\boldsymbol{K} = \boldsymbol{H}^\infty = \mathop{\times}_{n=1}^{\infty} \boldsymbol{H} \tag{2.26}$$

and the probability

$$\kappa = \mu \boldsymbol{\Phi}^{-1} \tag{2.27}$$

where $\boldsymbol{\Phi}^{-1}$ denotes the inverse image under the mapping $\boldsymbol{\Phi}$: $M \to K$.

Given the random sequence $\boldsymbol{\Phi} = [\boldsymbol{\phi}_n]_n$, we can (for all positive integers n, r, and elements $A = [\boldsymbol{a}_n]_n$ of K) define the family of *conditional cumulative distribution functions* (c.c.d.f.) of the component ϕ_{nr} of $\boldsymbol{\phi}_n$,

$$F_{nr}(A) = F_{nr}(A^{n-1}, \boldsymbol{a}_n^{r-1} \mid a_{nr})$$
$$= p_\mu[\phi_{nr} < a_{nr} \mid \boldsymbol{\phi}_n^{r-1} = \boldsymbol{a}_n^{r-1}, \boldsymbol{\Phi}^{n-1} = A^{n-1}] \tag{2.28}$$

That is to say, we define $F_{nr}(A) = F_{nr}(A^{n-1}, \boldsymbol{a}_n^{r-1} \mid a_{nr})$ to be the probability—under $(M, \boldsymbol{M}, \mu)$—that, for some sample point $\eta \in M$, $\phi_{nr}(\eta)$, the rth component of the nth sequence $\boldsymbol{\phi}_n(\eta)$, takes a sample value less than a_{nr}; given that $\phi_{n1}(\eta) = a_{n1}$, $\phi_{n2}(\eta) = a_{n2}, \ldots, \phi_{n(r-1)}(\eta) = a_{n(r-1)}$, and that $\boldsymbol{\phi}_1(\eta) = \boldsymbol{a}_1$, $\boldsymbol{\phi}_2(\eta) = \boldsymbol{a}_2, \ldots, \boldsymbol{\phi}_{n-1}(\eta) = \boldsymbol{a}_{n-1}$.

The *random generator* corresponding to the random sequence $\boldsymbol{\Phi}$ will be denoted by

$$\Omega = \mathscr{F}(M, \boldsymbol{M}, \mu; \boldsymbol{\Phi}) = \mathscr{G}(K, \boldsymbol{K}, \kappa = \mu\boldsymbol{\Phi}^{-1}) \tag{2.29}$$

It selects a point η of M in accordance with the probability μ and generates successive elements $\boldsymbol{\phi}_n(\eta)$ of H.

Let $(R, \boldsymbol{R}, \rho)$ be a probability space and $\xi = [\xi_n]_{n=1}^{\infty}$ a sequence of r.v. mapping R into the unit interval $U = \{x \in \mathbb{R}: 0 \leqslant x < 1\}$, where $\mathbb{R}$ is the real line. If $L = U^{\infty}$ and $\boldsymbol{L}$ is the σ-algebra of Borel subsets of L, then the random generator

$$\Lambda = \mathscr{F}(R, \boldsymbol{R}, \rho; \xi) = \mathscr{G}(L, \boldsymbol{L}, \rho\xi^{-1}) \tag{2.30}$$

is called a *canonical real random generator* if and only if

$$\rho\xi^{-1} = \lambda \tag{2.31}$$

where λ is the infinite-dimensional Lebesgue measure on L, which ensures the statistical independence of the ξ_n. More loosely, we shall then say that the ξ_n are *canonical* (*real*) *random variables* (c.r.v.).

Similarly, for any integer $B \geqslant 2$, if $(S, \boldsymbol{S}, \sigma)$ is a probability space, $\boldsymbol{x} = [x_r]_{r=1}^{\infty}$ is a random sequence in the set $U_B = \{0, 1, 2, \ldots, B-1\}$, $L_B = U_B^{\infty}$, and $\boldsymbol{L}$ is the infinite-product-σ-algebra of $\boldsymbol{U}_B = 2^{U_B}$, the power set of U_B; then the random generator

$$\Lambda_B = \mathscr{F}(S, \boldsymbol{S}, \sigma; \boldsymbol{x}) = \mathscr{G}(L_B, \boldsymbol{L}_B, \sigma\boldsymbol{x}^{-1}) \tag{2.32}$$

is called a *canonical random digit generator* (*modulo-B*) if and only if

$$\sigma\boldsymbol{x}^{-1} = \lambda_B \tag{2.33}$$

where λ_B is the infinite-dimensional uniform product measure on L_B, which ensures the statistical independence of the $\mathscr{x}_r$. More loosely, we shall then say that the $\mathscr{x}_r$ are *canonical random digits* (c.r.d.) adding "(mod B)" whenever it is necessary for clarity.

Let us write the *digital representation*, to *base* B, of a real number x in $[0, 1)$, as

$$x = \mathscr{A}_B(\mathbf{x}) = (0 \cdot \mathbf{x})_B = (0 \cdot \mathsf{x}_1 \mathsf{x}_2 \mathsf{x}_3 \cdots \mathsf{x}_r \cdots)_B = \sum_{r=1}^{\infty} \mathsf{x}_r B^{-r} \quad (2.34)$$

with all integer $\mathsf{x}_r \in U_B$ (i.e., $0 \leqslant \mathsf{x}_r \leqslant B-1$). This is unique, except when x is an integer multiple of some B^{-r} (i.e., the digital fraction *terminates*), when there are two forms, one (the "finite" form) with $\mathsf{x}_r = \mathsf{q}$, say, and all $\mathsf{x}_s = 0$, for $s > r$, and the other (the "infinite" form) with $\mathsf{x}_r = \mathsf{q} - 1$ and all $\mathsf{x}_s = B - 1$, for $s > r$. (If $\mathsf{q} = 0$, we interpret "$\mathsf{q} - 1$" in the usual way as a "borrowing" subtraction, affecting digits x_s with $s < r$.) As we shall see later, this exceptional ambiguity will be found to make no difference to our considerations.

We shall require two theorems, in order to show that *either type of canonical random generator suffices for the generation of any random sequence* $\boldsymbol{\Phi}$, as defined above.

3. THE FIRST THEOREM

First, we need a preliminary lemma.

Lemma 1. The distribution of the random sequence $\boldsymbol{\Phi} = [\boldsymbol{\phi}_n]_n$ is determined by the family of c.c.d.f. $F_{nr}(A)$ defined in (2.28).

Proof. By Loève, 1960, p. 364 (or Loève, 1978, p. 30), since $\boldsymbol{\Phi}$ constitutes a countable family of r.v. in $(H, \boldsymbol{H})$, its distribution $(K, \boldsymbol{K}, \kappa)$ is determined by the family of conditional probabilities

$$p_\mu[\boldsymbol{\phi}_n \in P \mid \boldsymbol{\Phi}^{n-1} = A^{n-1}] \quad (3.1)$$

for all $P \in \boldsymbol{H}$ and all $A^{n-1} \in H^{n-1}$. By the same general result, since $\boldsymbol{\phi}_n = [\phi_{nr}]$ is a countable family of r.v. in the real line $\mathbb{R}$, its distribution (3.1) in $(H, \boldsymbol{H})$ (for fixed $\boldsymbol{\Phi}^{n-1} = A^{n-1}$) is determined by the family of conditional probabilities

$$p_\mu[\phi_{nr} \in B \mid \boldsymbol{\phi}_n^{r-1} = \boldsymbol{a}_n^{r-1}, \boldsymbol{\Phi}^{n-1} = A^{n-1}] \quad (3.2)$$

for all Borel sets $B \subseteq \mathbb{R}$; and, finally, by Loève, 1960, p. 170 (or Loève, 1977, p. 172), this last distribution is determined by the family of c.c.d.f. $F_{nr}(A)$ defined in (2.28). □

Theorem A. If $\xi = [\xi_n]_{n=1}^{\infty}$ is a random sequence of points in $[0, 1)$ with digital representation $\xi_n = (0 \cdot \boldsymbol{x}_n)_B$ [see (2.34)], then the r.v. ξ_n are c.r.v., if and only if all the random digits x_{nr} are c.r.d. (mod B).

Proof. First, let ξ_n ($n = 1, 2, 3, \ldots$) be c.r.v., with digital representation $(0 \cdot \boldsymbol{x}_n)_B$, as defined in (2.34), and joint distribution $(L, \boldsymbol{L}, \lambda)$. The distribution of the x_{nr} is determined by a family of conditional probabilities like the F_{nr} in (2.28). Since the ξ_n are all independently uniformly distributed in $[0, 1)$, by our hypothesis; for all a_r and c_{nr} in U_B, we have

$$\begin{aligned} p_\lambda[x_{nr} < \mathsf{a}_r \mid \boldsymbol{x}_n^{r-1} = \mathbf{a}^{r-1}, (\forall n' < n)\, \boldsymbol{x}_{n'} = \mathbf{c}_{n'}] \\ = p_\lambda[x_{nr} < \mathsf{a}_r \mid \boldsymbol{x}_n^{r-1} = \mathbf{a}^{r-1}] \\ = \frac{p_\lambda[(0 \cdot \mathsf{a}_1 \mathsf{a}_2 \cdots \mathsf{a}_{r-1} 0)_B \leqslant \xi_n < [0 \cdot \mathsf{a}_1 \mathsf{a}_2 \cdots \mathsf{a}_{r-1} \mathsf{a}_r]_B]}{p_\lambda[(0 \cdot \mathsf{a}_1 \mathsf{a}_2 \cdots \mathsf{a}_{r-1} 0)_B \leqslant \xi_n < [0 \cdot \mathsf{a}_1 \mathsf{a}_2 \cdots (\mathsf{a}_{r-1} + 1) 0]_B]} \\ = \frac{\mathsf{a}_r B^{-r}}{B^{-r+1}} = \frac{\mathsf{a}_r}{B} \end{aligned} \tag{3.3}$$

(If $\mathsf{a}_{r-1} + 1 = B$, so that a carry is required above, the probability in the denominator is unaffected.) This result is clearly in accordance with the distribution $(L_B, \boldsymbol{L}_B, \lambda_B)$, which requires that all the x_{nr} be independently uniformly distributed in U_B. Thus, all the x_{nr} are c.r.d. (mod B).

Conversely, let all the x_{nr} be c.r.d. (mod B), with joint distribution $(L_B, \boldsymbol{L}_B, \lambda_B)$. By our hypothesis, all the x_{nr} are independently uniformly distributed in U_B. We note that, if (2.34) holds and

$$a = \mathscr{A}_B(\mathbf{a}) = (0 \cdot \mathbf{a})_B = (0 \cdot \mathsf{a}_1 \mathsf{a}_2 \mathsf{a}_3 \cdots)_B \tag{3.4}$$

then the condition $x < a$ is equivalent to one and only one of the disjoint conditions, $\mathbf{x}^{r-1} = \mathbf{a}^{r-1}$ and $\mathsf{x}_r < \mathsf{a}_r$ ($r = 1, 2, 3, \ldots$). Thus, if

$$c_n = \mathscr{A}_B(\mathbf{c}_n) = (0 \cdot \mathbf{c}_n)_B = (0 \cdot \mathsf{c}_{n1} \mathsf{c}_{n2} \mathsf{c}_{n3} \cdots)_B \tag{3.5}$$

then, for all a and c_n in $[0, 1)$, we have

$$\begin{aligned} p_{\lambda_B}[\xi_n < a \mid \xi^{n-1} = c^{n-1}] \\ = \sum_{r=1}^{\infty} p_{\lambda_B}[x_{nr} < \mathsf{a}_r \wedge \boldsymbol{x}_n^{r-1} = \mathbf{a}^{r-1} \mid (\forall n' < n)\, \boldsymbol{x}_{n'} = \mathbf{c}_{n'}] \\ = \sum_{r=1}^{\infty} p_{\lambda_B}[x_{nr} < \mathsf{a}_r \wedge \boldsymbol{x}_n^{r-1} = \mathbf{a}^{r-1}] \\ = \sum_{r=1}^{\infty} p_{\lambda_B}[x_{nr} < \mathsf{a}_r] \times \prod_{s=1}^{r-1} p_{\lambda_B}[x_{ns} = \mathsf{a}_s] \\ = \sum_{r=1}^{\infty} \frac{\mathsf{a}_r}{B} \times \frac{1}{B^{r-1}} = a \end{aligned} \tag{3.6}$$

by (2.34), in accordance with the distribution $(L, \boldsymbol{L}, \lambda)$, which requires that all the ξ_n be independently uniformly distributed in [0, 1). Thus, all the ξ_n are c.r.v. ∎

4. THE SECOND THEOREM

Again, we begin with some preliminary results.

Lemma 2. If $\boldsymbol{\kappa} = [\kappa_r]_r$ is a random sequence on the real line $\mathbb{R}$, then we can always construct a sequence of functions

$$g(\xi) = [g_r(\xi^r)]_{r=1}^{\infty} \tag{4.1}$$

such that, if the ξ_r are c.r.v., then the random sequence $\boldsymbol{\varpi} = [\varpi_r]_{r=1}^{\infty}$, where

$$\varpi_r = g_r(\xi^r) = g_r(\xi_1, \xi_2, ..., \xi_r) \tag{4.2}$$

has the same distribution as $\boldsymbol{\kappa}$. (See Lévy, 1954, pp. 29–30, 71–72, and 121–123.)

Proof. The distribution of $[\kappa_r]_r$ is determined, as we have seen [compare (2.28)], by the family of conditional probabilities, for all integers r and all real sequences $\boldsymbol{u}$,

$$F_r(\boldsymbol{u}) = F_r(\boldsymbol{u}^{r-1} \mid u_r) = p_\mu[\kappa_r < u_r \mid \boldsymbol{\kappa}^{r-1} = \boldsymbol{u}^{r-1}] \tag{4.3}$$

Successively define the sequence of r.v.,

$$\varpi_r = g_r(\xi^r) = \inf\{h: \xi_r \leqslant F_r(g(\xi)^{r-1} \mid h)\} \tag{4.4}$$

where we write

$$g(\xi) = [g_1(\xi^1), g_2(\xi^2), g_3(\xi^3), ...] \tag{4.5}$$

and $\xi = [\xi_r]_r$ is a sequence of c.r.v. The distribution of $[\varpi_r]_r$ is determined by conditional probabilities

$$G_r(\boldsymbol{u}) = G_r(\boldsymbol{u}^{r-1} \mid u_r) = p_\lambda[\varpi_r < u_r \mid \boldsymbol{\varpi}^{r-1} = \boldsymbol{u}^{r-1}] \tag{4.6}$$

analogous to the $F_r(\boldsymbol{u})$ above. Since $F_r(\boldsymbol{u}^{r-1} \mid h)$ is monotone-non-decreasing with h, we see that

$$\begin{aligned} &\inf\{h: x \leqslant F_r(\boldsymbol{u}^{r-1} \mid h)\} < u_r \\ &\quad \Rightarrow (\exists h)[x \leqslant F_r(\boldsymbol{u}^{r-1} \mid h) \wedge h < u_r] \\ &\quad \Rightarrow x \leqslant F_r(\boldsymbol{u}^{r-1} \mid u_r) \end{aligned} \tag{4.7}$$

that is,

$$\begin{aligned}\{x\colon \inf\{h\colon x \leqslant F_r(\boldsymbol{u}^{r-1} \mid h)\} < u_r\} \\ \subseteq \{x\colon (\exists h)[x \leqslant F_r(\boldsymbol{u}^{r-1} \mid h) \wedge h < u_r]\} \\ \subseteq \{x\colon x \leqslant F_r(\boldsymbol{u}^{r-1} \mid u_r)\}\end{aligned} \tag{4.8}$$

On the other hand, since $F_r(\boldsymbol{u}^{r-1} \mid h)$ is continuous to the left in h, and since $\inf\{h\colon \mathfrak{S}(h)\}$ cannot exceed any particular h for which $\mathfrak{S}(h)$ is true, we have

$$\begin{aligned}x < F_r(\boldsymbol{u}^{r-1} \mid u_r) \\ \Rightarrow (\exists h)[x \leqslant F_r(\boldsymbol{u}^{r-1} \mid h) \wedge h < u_r] \\ \Rightarrow \inf\{h\colon x \leqslant F_r(\boldsymbol{u}^{r-1} \mid h)\} < u_r\end{aligned} \tag{4.9}$$

that is,

$$\begin{aligned}\{x\colon x < F_r(\boldsymbol{u}^{r-1} \mid u_r)\} \\ \subseteq \{x\colon (\exists h)[x \leqslant F_r(\boldsymbol{u}^{r-1} \mid h) \wedge h < u_r]\} \\ \subseteq \{x\colon \inf\{h\colon x \leqslant F_r(\boldsymbol{u}^{r-1} \mid h)\} < u_r\}\end{aligned} \tag{4.10}$$

But the sets $\{x\colon x \leqslant F_r(\boldsymbol{u}^{r-1} \mid u_r)\}$ and $\{x\colon x < F_r(\boldsymbol{u}^{r-1} \mid u_r)\}$ obviously differ by the single point $F_r(\boldsymbol{u}^{r-1} \mid u_r)$, whose probability, in a uniform distribution over $[0, 1)$, is zero; so that the probabilities induced by λ on these two sets are equal; whence, by (4.8) and (4.10), we have

$$p_\lambda[\inf\{h\colon \xi \leqslant F_r(\boldsymbol{u}^{r-1} \mid h)\} < u_r] = p_\lambda[\xi \leqslant F_r(\boldsymbol{u}^{r-1} \mid u_r)] \tag{4.11}$$

Therefore,

$$\begin{aligned}G_r(\boldsymbol{u}^{r-1} \mid u_r) &= p_\lambda[\varpi_r < u_r \mid \boldsymbol{\varpi}^{r-1} = \boldsymbol{u}^{r-1}] \\ &= p_\lambda[\inf\{h\colon \xi_r \leqslant F_r(\boldsymbol{g}(\xi)^{r-1} \mid h)\} < u_r \mid \boldsymbol{g}(\xi)^{r-1} = \boldsymbol{u}^{r-1}] \\ &= p_\lambda[\inf\{h\colon \xi_r \leqslant F_r(\boldsymbol{u}^{r-1} \mid h)\} < u_r] \\ &= p_\lambda[\xi_r \leqslant F_r(\boldsymbol{u}^{r-1} \mid u_r)] = F_r(\boldsymbol{u}^{r-1} \mid u_r)\end{aligned} \tag{4.12}$$

This demonstrates the identity of the distributions F_r and G_r, proving the lemma and providing a suitable sequence of functions f_r in (4.4). □

Now, let

$$z = [z_r]_r \tag{4.13}$$

be a sequence of real numbers, with $0 \leqslant z_r < 1$ for all $r = 1, 2, 3,...$, and write the corresponding base-B digital representations [compare (2.34), (3.4), and (3.5)] as

$$z_r = \mathscr{A}_B(\mathbf{z}_r) = (0 \cdot \mathbf{z}_r)_B = (0 \cdot \mathbf{z}_{r1}\mathbf{z}_{r2}\mathbf{z}_{r3} \cdots)_B \tag{4.14}$$

Let

$$\mathbf{Z} = [\mathbf{z}_r]_r \tag{4.15}$$

By the well-known diagonal interlacing technique of G. Cantor (which he invented to prove the countability of the rationals and, in general, of a countable collection of countable sets), we can combine all the digits of $\mathbf{Z}$ into a single sequence,

$$\begin{aligned} \mathbf{x} &= [\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4, \mathbf{x}_5, \mathbf{x}_6, \mathbf{x}_7, \mathbf{x}_8, \mathbf{x}_9, \mathbf{x}_{10}, \mathbf{x}_{11}, \mathbf{x}_{12},...] \\ &= [\mathbf{z}_{11}, \mathbf{z}_{12}, \mathbf{z}_{21}, \mathbf{z}_{13}, \mathbf{z}_{22}, \mathbf{z}_{31}, \mathbf{z}_{14}, \mathbf{z}_{23}, \mathbf{z}_{32}, \mathbf{z}_{41}, \mathbf{z}_{15}, \mathbf{z}_{24},...] \\ &= \mathscr{Q}_B(\mathbf{Z}) \end{aligned} \tag{4.16}$$

(see Halmos, 1974, pp. 153–154 and 159–160). This allows us to define a single new real number x with the representation (2.34).

Lemma 3. The mapping $\mathscr{Q}_B \colon L_B^\infty \to L_B$, defined in (4.16), is a bijection (an invertible, one-to-one mapping).

Proof. The set L_B is defined in connection with (2.32). The function $\mathscr{Q}_B$ maps the set L_B^∞ of all infinite sequences of infinite sequences of digits, in which $\mathbf{Z}$ lies, onto the set L_B of all infinite sequences of digits, in which $\mathbf{x}$ lies. If we write $\mathbf{x}_s = \mathbf{z}_{rk}$, then it is easily verified that

$$s = \mathscr{S}(r, k) = r + \sum_{t=1}^{r+k-2} t = r + \tfrac{1}{2}(r+k-1)(r+k-2) \tag{4.17}$$

Since, clearly, $r + k > r \geqslant 1$, we have

$$\tfrac{1}{2}(r+k-1)(r+k-2) < s \leqslant \tfrac{1}{2}(r+k)(r+k-1) \tag{4.18}$$

whence a little algebra shows that

$$r + k = \left\lceil (2s + \tfrac{1}{4})^{1/2} + \tfrac{1}{2} \right\rceil \tag{4.19}$$

where $\lceil x \rceil$ denotes the "roof" (or "ceiling") function—the integer supremum of x. From (4.16) and (4.17), we can easily derive that

$$r = \mathscr{R}(s) = s - \tfrac{1}{2}\left(\left\lceil (2s + \tfrac{1}{4})^{1/2} + \tfrac{1}{2} \right\rceil - 1\right)\left(\left\lceil (2s + \tfrac{1}{4})^{1/2} + \tfrac{1}{2} \right\rceil - 2\right) \tag{4.20}$$

$$k = \mathscr{K}(s) = \tfrac{1}{2}\left\lceil (2s + \tfrac{1}{4})^{1/2} + \tfrac{1}{2} \right\rceil\left(\left\lceil (2s + \tfrac{1}{4})^{1/2} + \tfrac{1}{2} \right\rceil - 1\right) - s + 1 \tag{4.21}$$

Thus, $\mathscr{S}\colon \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$ (where $\mathbb{Z}^+$ is the set of positive integers) is a *bijection* (an invertible, one-to-one mapping), whose inverse is $(\mathscr{R}, \mathscr{K})$. Since every digit can take any value in U_B, it follows immediately that $\mathscr{Q}_B$ itself is a bijection from L_B^∞ onto L_B. □

Lemma 4. The mapping $\mathscr{A}_B\colon L_B \to U$, defined in (2.34), is a surjection [i.e., $\mathscr{A}_B(L_B) = U$]. With respect to Lebesgue measure in $\mathbb{R}$, or to the uniform product measure in L_B, it is almost everywhere a bijection.

Proof. It is clear that $\mathscr{A}_B$ maps every digit-sequence into U. It is also evident that every real number x in U has a digital representation of the form shown in (2.34), through the algorithm

$$\begin{aligned} \mathsf{x}_1 &= \lfloor Bx \rfloor, & u_1 &= Bx - \mathsf{x}_1 \\ (\forall r \geqslant 1)\ \mathsf{x}_{r+1} &= \lfloor Bu_r \rfloor, & u_{r+1} &= Bu_r - \mathsf{x}_{r+1} \end{aligned} \tag{4.22}$$

where $\lfloor \mathbf{z} \rfloor$ denotes the "floor" function—the integer infinum of $\mathbf{z}$. In this representation, *terminating* fractions take the "finite" form, for some index r, with $\mathsf{x}_r = \mathsf{q}$, say, and all $\mathsf{x}_s = 0$, for $s > r$ [see the explanation after (2.34)]. Thus, $\mathscr{A}_B$ is a *surjection* from L_B onto U.

Define the set of digit-sequences,

$$\begin{aligned} T_B &= \{\mathbf{x} \in L_B\colon (\exists r)(\exists k_r)(\forall h \geqslant k_r)\ \mathsf{x}_{\mathscr{S}(r,h)} = 0\} \\ &\quad \cup \{\mathbf{x} \in L_B\colon (\exists r)(\exists k_r)(\forall h \geqslant k_r)\ \mathsf{x}_{\mathscr{S}(r,h)} = B - 1\} \\ &= \bigcup_{r=1}^{\infty} \bigcup_{k=1}^{\infty} T_B^{(r,k)} \end{aligned} \tag{4.23}$$

where $\mathscr{S}(r, h)$ is defined as in (4.17) and

$$\begin{aligned} T_B^{(r,k)} &= \{\mathbf{x} \in L_B\colon (\forall h \geqslant k)\ \mathsf{x}_{\mathscr{S}(r,h)} = 0\} \\ &\quad \cup \{\mathbf{x} \in L_B\colon (\forall h \geqslant k)\ \mathsf{x}_{\mathscr{S}(r,h)} = B - 1\} \end{aligned} \tag{4.24}$$

This means that, in T_B, at least one of the "unraveled" numbers obtained by reversing the interlacing—namely, $\mathbf{z}_r$ [see (4.14) and (4.15)]—*terminates* (taking either the "finite" or the "infinite" form).

Note, too, from (4.17), that, for any given r, s increases with k, and the least s that is greater than t requires

$$r + \tfrac{1}{2}(r + k - 1)(r + k - 2) > t \tag{4.25}$$

with minimal $k \geqslant 1$; this reduces to

$$(r + k - \tfrac{3}{2})^2 > 2t - 2r + \tfrac{1}{4}$$

i.e.,

$$\begin{cases} \text{if } r \leqslant t, \text{ then } k_r = \max\left\{1, \left\lfloor \frac{5}{2} - r + [2(t-r) + \frac{1}{4}]^{1/2} \right\rfloor \right\} \\ \text{if } r > t, \text{ then } k_r = 1 \end{cases} \tag{4.26}$$

Thus, the case of **x** itself terminating,

$$(\exists t)[(\forall s > t)\, \mathsf{x}_s = B - 1) \vee ((\forall s > t)\, \mathsf{x}_s = 0)] \tag{4.27}$$

requires termination of *every* $\mathbf{z}_r$ according to (4.26), and corresponds to the set

$$\bigcup_{t=1}^{\infty} \left\{ \left(\bigcap_{r=1}^{t} T_B^{(r,k_r)} \right) \cap \left(\bigcap_{r=t+1}^{\infty} T_B^{(r,1)} \right) \right\} \subseteq T_B \tag{4.28}$$

Now, since the sets $T_B^{(r,h)}$ are all finite, T_B is itself a countable set. Since the set $L_B = U_B^{\infty}$ is *uncountable infinite*, while its subset T_B is countable; in terms of the uniform product measure in L_B, the set T_B has measure zero. Similarly, the set

$$V_B = \mathscr{A}_B(T_B) \subseteq U \tag{4.29}$$

is countable, and therefore has Lebesgue measure zero.

The restriction of $\mathscr{A}_B\colon L_B \to U$ to

$$\mathscr{A}_B^{\dagger}\colon L_B \backslash T_B \to U \backslash V_B \tag{4.30}$$

is clearly a *bijection*; the excluded set T_B is of measure zero, so the bijective property applies *almost everywhere*. □

Let the countable set of r.v.

$$\boldsymbol{Z} = [\zeta_n]_n = [[\zeta_{nr}]_r]_n \tag{4.31}$$

be a set of c.r.v. By analogy with (4.14) and (4.16), write

$$\zeta_{nr} = \mathscr{A}_B(\varkappa_{nr}) = (0 \cdot \varkappa_{nr})_B = (0 \cdot \varkappa_{nr1}\varkappa_{nr2}\varkappa_{nr3}\cdots)_B \tag{4.32}$$

and (for $n = 1, 2, 3, \ldots$) define the sequence of r.v. in U,

$$\begin{aligned} \xi &= [\xi_n]_n = \mathscr{P}_B \circ \boldsymbol{Z} \\ &= [(0 \cdot \varkappa_{n11}\varkappa_{n12}\varkappa_{n21}\varkappa_{n13}\varkappa_{n22}\varkappa_{n31}\varkappa_{n14}\varkappa_{n23}\cdots)_B]_n \end{aligned} \tag{4.33}$$

By Theorem A, if the ζ_{nr} are c.r.v., then all the digits $\varkappa_{nrk}$ will be c.r.d., and therefore, again by Theorem A, the ξ_n must be c.r.v., too; and, vice versa, if the ξ_n are c.r.v., then all the digits $\varkappa_{nrk}$ will be c.r.d., and hence all the ζ_{nr} must be c.r.v., too.

In probabilistic terms, the measures used in Lemma 4 become probabilities [the Lebesgue measure of U is 1, whence $\lambda(L)=1$, and the uniform measure of U_B is 1, whence $\lambda_B(L_B)=1$], and anything that happens with probability zero may be neglected, if we append the rubric "(a.s.)," meaning "almost surely." Now, by Lemma 4, $\mathscr{A}_B$ is (a.s.) a bijection, and therefore (a.s.) invertible. Consider the product mapping $\mathscr{C}_B$: $L_B^\infty \to L$, defined by [compare (2.34)]

$$\mathscr{C}_B(\mathbf{Z})=[\mathscr{A}_B(\mathbf{z}_n)]_n \tag{4.34}$$

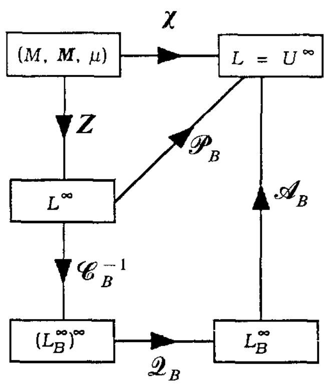
Then $\mathscr{C}_B$ will evidently be a bijection in the product set $(L_B\backslash T_B)^\infty$, whose complement has probability zero. Thus, $\mathscr{C}_B$ is (a.s.) invertible. Hence, we may write

$$\mathscr{P}_B=\mathscr{A}_B\circ\mathscr{Q}_B\circ\mathscr{C}_B^{-1} \quad \text{(a.s.)} \tag{4.35}$$

It follows that $\mathscr{P}_B$ is itself (a.s.) invertible, and

$$\mathscr{P}_B^{-1}=\mathscr{C}_B\circ\mathscr{Q}_B^{-1}\circ\mathscr{A}_B^{-1} \quad \text{(a.s.)} \tag{4.36}$$

The relationship between the various mappings discussed here is shown in the diagram below.



We can now extend the result of Lemma 2 from the real line to the Fréchet space H, in the theorem below.

Theorem B. If $\boldsymbol{\Phi}=[\phi_n]_n$ is a random sequence in H, then we can always construct a sequence of functions

$$\boldsymbol{\Psi}(\xi)=[\psi_n(\xi^n)]_{n=1}^\infty \tag{4.37}$$

where

$$\psi_n: U^n \to H \tag{4.38}$$

such that, if the ξ_n are c.r.v., then the random sequence $\boldsymbol{\Gamma} = [\gamma_n]_{n=1}^{\infty}$, where

$$\gamma_n = \psi_n(\xi^n) = \psi_n(\xi_1, \xi_2, ..., \xi_n) \tag{4.39}$$

has the same distribution $(K, \boldsymbol{K}, \kappa)$ as $\boldsymbol{\Phi}$.

Proof. First, take $n = 1$. We need to make $\psi_1(\xi_1)$ have the same distribution as $\boldsymbol{\phi}_1$. By Lemma 2 [see (4.4)], if $\boldsymbol{Z}$ is a countable set of c.r.v., defined as in (4.31), then $\boldsymbol{\zeta}_1 = [\zeta_{1r}]_r$ are c.r.v. and we can successively define the real-valued r.v. [see (2.28), (4.4), and (4.5)]

$$\gamma_{1r} = g_{1r}(\boldsymbol{\zeta}_1^r) = \inf\{h: \zeta_{1r} \leqslant F_{1r}(\boldsymbol{g}_1(\boldsymbol{\zeta}_1)^{r-1} \mid h)\} \tag{4.40}$$

and $\boldsymbol{\gamma}_1 = [\gamma_{1r}]_r$ will have the same distribution as $\boldsymbol{\phi}_1$. If we now define $\boldsymbol{\xi} = \mathscr{P}_B \circ \boldsymbol{Z}$, as in (4.33), so that $\boldsymbol{Z} = \mathscr{P}_B^{-1} \circ \boldsymbol{\xi}$ (a.s.) and $\boldsymbol{\xi} = [\xi_n]_n$ are c.r.v., we observe that $\mathscr{P}_B$ and $\mathscr{P}_B^{-1}$ are *pointwise* mappings (with respect to the index n) and we may, without fear of confusion, write

$$\xi_n = \mathscr{P}_B \circ \boldsymbol{\zeta}_n \qquad \text{and} \qquad \boldsymbol{\zeta}_n = \mathscr{P}_B^{-1} \circ \xi_n \tag{4.41}$$

Thus, we may put

$$\boldsymbol{\gamma}_1 = \psi_1(\xi_1) = \boldsymbol{g}_1(\mathscr{P}_B^{-1} \circ \xi_1) \tag{4.42}$$

and $\boldsymbol{\gamma}_1$ will have the same distribution as $\boldsymbol{\phi}_1$.

Now suppose that we have already defined $\boldsymbol{\gamma}_1 = \psi_1(\xi_1)$, $\boldsymbol{\gamma}_2 = \psi_2(\xi_1, \xi_2), ..., \boldsymbol{\gamma}_{n-1} = \psi_{n-1}(\xi_1, \xi_2, ..., \xi_{n-1})$, having the same joint distribution as $\boldsymbol{\phi}_1, \boldsymbol{\phi}_2, ..., \boldsymbol{\phi}_{n-1}$, and we write $\boldsymbol{G}(\boldsymbol{Z}) = [\boldsymbol{g}_n(\boldsymbol{\zeta}_n)]_n$ and define

$$\begin{aligned} \gamma_{nr} &= g_{nr}(\boldsymbol{Z}^{n-1}, \boldsymbol{\zeta}_n^r) \\ &= \inf\{h: \zeta_{nr} \leqslant F_{nr}(\boldsymbol{G}(\boldsymbol{Z})^{n-1}, \boldsymbol{g}_n(\boldsymbol{Z}^{n-1}, \boldsymbol{\zeta}_n)^{r-1} \mid h)\} \end{aligned} \tag{4.43}$$

Note that (4.43) reduces to (4.40) for $n = 1$. By Lemma 1, the distribution of all the $\boldsymbol{\gamma}_n$ is determined by the conditional probabilities [see (2.28)]

$$\begin{aligned} G_{nr}(\boldsymbol{A}) &= G_{nr}(\boldsymbol{A}^{n-1}, \boldsymbol{a}_n^{r-1} \mid a_{nr}) \\ &= p_\lambda[\gamma_{nr} < a_{nr} \mid \boldsymbol{\gamma}_n^{r-1} = \boldsymbol{a}_n^{r-1}, \boldsymbol{\Gamma}^{n-1} = \boldsymbol{A}^{n-1}] \end{aligned} \tag{4.44}$$

The argument yielding (4.7)–(4.11) in the proof of Lemma 2 is not affected if we replace $F_r(\boldsymbol{u}^{r-1} \mid h)$ by any other appropriate, monotonenondecreasing, continuous-to-the-left function of h; in particular, we may use the function $F_{nr}(A^{n-1}, \boldsymbol{a}_n^{r-1} \mid h)$. In place of (4.11), we then get

$$p_\lambda[\inf\{h: \zeta_{nr} \leqslant F_{nr}(A^{n-1}, \boldsymbol{a}_n^{r-1} \mid h)\} < a_{nr}] = p_\lambda[\zeta_{nr} \leqslant F_{nr}(A^{n-1}, \boldsymbol{a}_n^{r-1} \mid a_{nr})] \quad (4.45)$$

Arguing just as in deriving (4.12), we see that

$$\begin{aligned} G_{nr}(A) &= p_\lambda[\gamma_{nr} < a_{nr} \mid \gamma_n^{r-1} = \boldsymbol{a}_n^{r-1}, \boldsymbol{\Gamma}^{n-1} = A^{n-1}] \\ &= p_\lambda[\inf\{h: \zeta_{nr} \leqslant F_{nr}(A^{n-1}, \boldsymbol{a}_n^{r-1} \mid h)\} < a_{nr}] \\ &= p_\lambda[\zeta_{nr} \leqslant F_{nr}(A^{n-1}, \boldsymbol{a}_n^{r-1} \mid a_{nr})] \\ &= F_{nr}(A^{n-1}, \boldsymbol{a}_n^{r-1} \mid a_{nr}) = F_{nr}(A) \end{aligned} \quad (4.46)$$

Thus F and G are identical distributions; i.e., the distribution of γ_n, conditional on $\gamma_1, \gamma_2, \ldots, \gamma_{n-1}$, is the same as that of $\boldsymbol{\phi}_n$, conditional on $\boldsymbol{\phi}_1, \boldsymbol{\phi}_2, \ldots, \boldsymbol{\phi}_{n-1}$. Thus, the induction is completed, and we have shown that the distribution of $\boldsymbol{\Gamma}$, defined in (4.40) and (4.43), is the same as that of $\boldsymbol{\Phi}$.

Now, we note that, by (4.43), γ_n depends only on $\boldsymbol{Z}^n = [\zeta_1, \zeta_2, \ldots, \zeta_n]$; so that, by applying the transformation (4.41), we see that we can put

$$\gamma_n = \boldsymbol{\psi}_n(\xi_1, \xi_2, \ldots, \xi_n) = \boldsymbol{g}_n(\mathscr{P}_B^{-1} \circ \xi^n) \quad (4.47)$$

This completes the proof of Theorem B. □

5. CONCLUSION

Theorem A shows that, in an ideal situation, we may use Λ to generate $[x_n]_n$, or Λ_B to generate $[\xi_n]_n$. Theorem B shows that we can generate the behavior of any $[\boldsymbol{\phi}_n]_n$ by means of Λ (and thus also by means of Λ_B). However, some cautionary remarks are appropriate here.

First, the canonical real random generators Λ^*, say, which are used in practice, only *approximate* the theoretical ideal generator Λ. In fact, they are often deterministic numerical algorithms called *pseudorandom*, and, in many cases, the digits x_{nr}^* of the corresponding sequence $[\xi_n^*]_n$ are, for each n, less and less "random," as r increases. Thus it is advisable to use only the few most significant digits of the random numbers ξ_n^* to generate practically acceptable random digits.

Secondly, it will be noted that the computer algorithms Λ^* generate digital representations of finite length, so that they really are better viewed as canonical random digit generators Λ_C^* with C a large integer, such as 2^{36} or 2^{48}, the ostensive ξ_n^* really being x_n^*/C. Theorem A still applies; and so does Theorem B, to within the accuracy, $1/C$, of the computer arithmetic. Some care will be needed, however, to ensure that the functions ψ_m do not accumulate computer errors in such a way as to render them worthless.

REFERENCES

Halmos, P. R. (1974). *Measure Theory*, Van Nostrand, Princeton, New Jersey (1950), reprinted by Springer-Verlag, New York.

Kolmogorov, A. N. (1956). *Foundations of the Theory of Probability*, translated from the German by N. Morrison, Second Edition, Chelsea Publishing Co., New York.

Lévy, P. (1954). *Théorie de l'Addition des Variables Aléatoires*, Gauthier-Villars, Paris.

Loève, M. (1960). *Probability Theory*, Second Edition, Van Nostrand, Princeton, New Jersey.

Loève, M. (1977). *Probability Theory*, Fourth Edition, Springer-Verlag, New York, Vol. I.

Loève, M. (1978). *Probability Theory*, Fourth Edition, Springer-Verlag, New York, Vol. II.

Pervin, W. J. (1964). *Foundations of General Topology*, Academic Press, New York.

Sierpiński, W. (1956). *General Topology*, translated from the Polish by C. C. Krieger, Second Edition, University of Toronto Press, Toronto.

Printed in Belgium