PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 25 (39), 1979, pp. 11—15

ON ALGORITHMICAL TESTING TABLES OF RANDOM NUMBERS

D. Banjević and *Z. Ivković*

(Received September 20, 1977)

A. N. Kolmogorov [1] has introduced the notion of tables random with respect to the system of the admissible algorithms. In Section 1. we discuss certain questions involving the definition of the algorithm given in [1]. Further on, we give statistical interpretations to the table randomness tests, and we estimate the mumber of algorithms for these tests. In Section 2. we define randomness test for table generator and we prove some of its properties.

Let the table (of numbers) be a finite binary sequence $T=(t_1, t_2, \ldots, t_N)$. We select subsequences from this table using the system of algorithms. Roughly speaking the table is random if in these subsequences the frequency of occurrence of 1's is "stable". A precise definition of these algorithms is given in [1]. According to this definition the selection of an element does not depend of its value. Such definition of subsequence selection formalizes the ideas of von Mieses. We give this definition.

The system of functions $F=(F_0\equiv\text{const}, F_1, \ldots, F_{N-1})$ defines a permutation $(x_1, x_2, \ldots, x_N)$ of $(1, 2, \ldots, N)$ dependent on $T=(t_1, t_2, \ldots t_N)$ by

$$x_i=F_{i-1}(x_1, t_{x_1}; x_2, t_{x_2}; \ldots; x_{i-1}, t_{x_{i-1}}), \qquad i=1, 2, \ldots, N.$$

Let the system of functions $H=(H_0\equiv\text{const}, H_1, \ldots, H_{N-1}, H_N\equiv 1)$ and $G=(G_0\equiv\text{const}, G_1, \ldots, G_{N-1})$ have the properties $H_i, G_i\in\{0, 1\}$ and $H_i(x_1, t_{x_1}; \ldots; x_i, t_{x_i})\leqslant H_{i+1}(x_1, t_{x_1}; \ldots, x_i, t_{x_i}; x_{i+1}, t_{x_{i+1}})$. Let $s=s(T)=\min\{i: H_i(x_1, t_{x_1}; \ldots; x_i, t_{x_i})=1\}$. The functions F, H, G and the table T define the subset $A\subset\{1, 2, \ldots, N\}$ by $x_k\in A$ iff $k\leq s$ and $G_{k-1}(x_1, t_{x_1}, \ldots, x_{k-1}, t_{x_{k-1}})=1$ The algorithm generated by F, H, G selects the sequence $(t_{x_{i_1}}, t_{x_{i_2}}, \ldots, t_{x_{i_\nu}})$ out of the table $T=(t_1, t_2, \ldots, t_N)$, where $\{x_{i_1}, x_{i_2}, \ldots, x_{i_\nu}\}=A$.

Let $\nu=\nu(A)$ be the number of element in A. Table T is (n, ε, p) — random with respect to $R=(F, H, G)$ if $\nu\geqslant n$ and

$$\left|\frac{1}{\nu}\sum_{k\in A} t_k - p\right|<\varepsilon,$$

or if $v<n$. Let $\mathcal{R}=\{R_i\}$ be a system of algorithms. Table T is (n, ε, p) — random with respect to $\mathcal{R}$ if it is (n, ε, p) — random with respect to each $R_i \in \mathcal{R}$.

1. It is convenient to use the methods of the Probability Theory for the following statistical interpretations. We consider the table $(t_1, t_2, \ldots, t_N)$ as a realization of Bernoulli sequence (abrv. $\mathcal{B}(N, p)$ sequence) $(\xi_1, \xi_2, \ldots \xi_N)$.

In Mathematical Statistics tests are used where the error of the first type is some small probability α. We shall consider given algorithmical tests as a special case of statistical tests at a given level α. The null hypothesis is that sequence $(\xi_1, \xi_2, \ldots, \xi_N)$ is a $\mathcal{B}(N, p)$ sequence. It fact, in this case the probability α is proportional to that part of the tables which are nonrandom with respect to the given system of algorithms. Also, it is reasonable to introduce the level α if we consider the nonrandomness as a rare property [2].

Definition 1. *The system of algorithms $\mathcal{R}$ is α-admissible (denoted by $\mathcal{R}^\alpha$) if the probability of $\mathcal{B}(N, p)$ sequence being nonrandom with respect to $\mathcal{R}$ is not greater then α. The algorithm R is α-admissible (denoted by R^α) if the system $\{R\}$ is α-admissible.*

It is evident that two algorithms given by different set of functions F, G, H may produce the same set of non random tables. Therefore we give following.

Definition 2. *The system of algorithms $\mathcal{R}$ is minimal if for every $R \in \mathcal{R}$ exists at least one table nonrandom only with respect to that algorithm.*

Every system $\mathcal{R}$ may be reduced to the minimal system $\overline{\mathcal{R}}$, so that systems $\mathcal{R}$ and $\overline{\mathcal{R}}$ produce the same set of nonrandom tables. Therefore in what follows we may consider only minimal systems.

Let $R=(F, G, H)$ be an algorithm. The system of the functions F corresponds one sequence to another by permutations of indices. Let us show that if the original sequence is $\mathcal{B}(N, p)$ one, then the image is also a $\mathcal{B}(N, p)$ sequence. For fixed $x_1, t_{x_1}, \ldots, x_{i-1}, t_{x_{i-1}}$ we have

$$P(\xi_{x_i}=1 \mid x_1, t_{x_1}; \ldots, x_{i-1}, t_{x_{i-1}}) = P(\xi_{x_i}=1) = p,$$

and

$$P(\xi_{x_1}=t_{x_1}, \ldots, \xi_{x_N}=t_{x_N}) = P(\xi_{x_1}=t_{x_1})\, P(\xi_{x_2}=t_{x_2} \mid \xi_{x_1}=t_{x_1}) \ldots$$

$$P(\xi_{x_N}=t_{x_N} \mid \xi_{x_1}=t_{x_1}, \ldots, \xi_{x_{N-1}}=t_{x_{N-1}}) = p^{\Sigma t_{x_i}} (1-p)^{N-\Sigma t_{x_i}}$$

The system F preserving distribution is not the most general if we abandon reccurent evaluation of $x_1, x_2, \ldots$

Proposition 1. *Let Φ be a transformation in the set of binary sequences such that: $\Phi(x_1, \ldots, x_N)=(y_1, \ldots, y_N)$ implies $\sum_{i=1}^{N} y_i = \sum_{i=1}^{N} x_i$. Let $(\xi_1, \ldots, \xi_N)$ be a $\mathcal{B}(N, p)$ sequence. The sequence*

$$(\eta_1, \ldots, \eta_N) = \Phi(\xi_1, \ldots, \xi_N)$$

is $\mathcal{B}(N, p)$ sequence if and only if Φ is one to one transformation.

Proof: Let Φ be one to one transformation. Then

$$P(\eta_1=y_1, \ldots, \eta_N=y_N)=P(\xi_1=x_1, \ldots, \xi_N=x_N;\ \Phi(x_1, \ldots, x_N)=$$

$$=(y_1, \ldots, y_N))=p^{\Sigma x_i}(1-p)^{N-\Sigma x_i}=p^{\Sigma y_i}(1-p)^{N-\Sigma y_i}.$$

If the distribution is the same, then

$$p^{\Sigma y_i}(1-p)^{N-\Sigma y_i}=P(\eta_1=y_1, \ldots, \eta_N=y_N)=$$

$$=\sum_{x_1, \ldots, x_N} P(\xi_1=x_1, \ldots, \xi_N=x_N;\ \Phi(x_1, \ldots, x_N)=(y_1, \ldots, y_N))=$$

$$=\sum_{\substack{x_1, \ldots, x_N \\ \Phi=(y_1, \ldots, y_N)}} p^{\Sigma x_i}(1-p)^{N-\Sigma y_i}=p^{\Sigma y_i}(1-p)^{N-\Sigma y_i}\sum_{\substack{x_1, \ldots, x_N \\ \Phi=(y_1, \ldots, y_N)}} 1$$

meaning that the number of sequences $(x_1, \ldots, x_N)$ corresponding to $(y_1, \ldots, y_N)$ is exactly one.

Proposition 1 implies that the system of functions F defines a one to one transformation.

Now we consider some properties of system $\mathcal{R}$ which depend on the number ρ of algorithms in $\mathcal{R}$ and involve α-admissibility.

Let ρ^* be such a number that every system of ρ^* algorithms is α-admissible. We introduce the upper bound for ρ^*

$$r_\alpha=r(n, \varepsilon, p, \alpha)=\sup\ \rho^*\geqslant 0$$

Let $\bar{\rho}$ be such a number that no system of $\bar{\rho}$ algorithms is α-admissible. If we consider only minimal systems, let

$$\inf \bar{\rho}=\sigma(n, \varepsilon, p, \alpha)=\sigma_\alpha$$

It is clear that $0\leqslant r_\alpha\leqslant\sigma_\alpha\leqslant 2^N$.

If the system $\mathcal{R}$ is α-admissible then it is β-admissible for $\beta>\alpha$, which implies $r_\alpha\leqslant r_\beta$, $\sigma_\alpha\leqslant\sigma_\beta$, $\alpha<\beta$.

In the same way

$$r_\alpha(n)\leqslant r_\alpha(n+1), \quad \sigma_\alpha(n)\leqslant\sigma_\alpha(n+1);$$

$$r_\alpha(\varepsilon)\leqslant r_\alpha(\delta), \quad \sigma_\alpha(\varepsilon)\leqslant\sigma_\alpha(\delta), \quad \varepsilon<\delta.$$

We shall deal with some estimations of the numbers r_α, σ_α. Let $P(n, \varepsilon, p \mid R)$ be the probability that the $\mathcal{B}(N, p)$ sequence is nonrandom with respect to R. Let

$$P(n, \varepsilon, p)=\sup_R P(n, \varepsilon, p \mid R).$$

Then $P(n, \varepsilon, p \mid \mathcal{R})\leqslant\sum_{R\in\mathcal{R}} P(n, \varepsilon, p \mid R)\leqslant\rho P(n, \varepsilon, p)$. If we put $\rho P(n, \varepsilon, p)\leqslant\alpha$ we get $r_\alpha\geqslant\dfrac{\alpha}{P(n, \varepsilon, p)}$.

Kolmogorov [1] gives an estimation

$$P(n, \varepsilon, p) \leqslant P\left(\sup_{k \geqslant n} \left| \frac{S_k}{k} - p \right| \geqslant \varepsilon\right) \leqslant 2\, e^{-2n\varepsilon^2(1-\varepsilon)}$$

which implies

$$r_\alpha \geqslant \frac{\alpha}{2}\, e^{2n\varepsilon^2(1-\varepsilon)}.$$

Let $p \leqslant \frac{1}{2}$ and let the system $\mathcal{R}$ of $\rho \leqslant 2^N$ algorithms be minimal. Then at least ρ sequences are nonrandom with respect to $\mathcal{R}$ and

$$(*) \qquad P(n, \varepsilon, p \mid \mathcal{R}) \geqslant \binom{N}{0} p^N + \cdots + \binom{N}{k} p^{N-k}(1-p)^k +$$

$$+ \left[\rho - \binom{N}{0} - \cdots - \binom{N}{k}\right] p^{N-k-1}(1-p)^{k+1} = Q(p, \rho).$$

where k is such that $\binom{N}{0} + \cdots + \binom{N}{k} \leqslant \rho < \binom{N}{0} + \cdots + \binom{N}{k} + \binom{N}{k+1}$. Then $\sigma_\alpha \leqslant \inf\{\rho : Q(p, \rho) > \alpha\} = \tilde{\rho}$.

As $Q\left(\frac{1}{2}, \rho\right) = \rho\, 2^{-N}$, it follows $\sigma\left(n, \varepsilon, \frac{1}{2}, \alpha\right) \leqslant \alpha\, 2^N + 1$.

Using normal approximation we get from (*) that

$$\binom{N}{0} + \cdots + \binom{N}{k^*} \leqslant \tilde{\rho} < \binom{N}{0} + \cdots + \binom{N}{k^*+1}$$

for $k^* = \mathcal{F}^{-1}(\alpha)\sqrt{Np(1-p)} + Np$.

2. We shall call the random variables $(\xi_1, \xi_2, \ldots, \xi_N)$ the generator $\mathcal{G}$ of the tables $T = (t_1, t_2, \ldots, t_N)$. Let $\mathcal{H}$ be the hypothesis that $\mathcal{G}$ is $\mathcal{B}(N, p)$ sequence and let $\mathcal{R}^\alpha$ be a system of algorithms. Random variable S_M is the number of nonrandom tables with respect to $\mathcal{R}^\alpha$ in the set of M tables produced by $\mathcal{G}$.

Definition 3. *The generator $\mathcal{G}$ is rejected as nonrandom with respect to $(\mathcal{R}^\alpha, M, \delta)$, $(0 < \delta < 1)$ by M tables if*

$$\frac{S_M}{M} \geqslant \alpha + u_\alpha$$

where u_α is such number that $\sum_{k \geqslant (\alpha + u_\alpha) M} \binom{M}{k} \alpha^k (1-\alpha)^{n-k} \leqslant \delta$.

Supposing that $\mathcal{H}$ is true and that the probability that T is nonrandom with respect to $\mathcal{R}^\alpha$ is exactly α, we get $\delta \geqslant P_{\mathcal{H},\alpha}\left(\frac{S_M}{M} \geqslant \alpha + u_\alpha\right)$. Therefore δ is upper bound for probability of error of the first type for $\mathcal{H}$.

Proposition 2. *Let r, $r<\alpha$, be the probability that T is nonrandom with respect to $\mathcal{R}^\alpha$. Then*

$$P_{\mathcal{H},r}\left(\frac{S_M}{M} \geqslant \alpha + u_\alpha\right) \leqslant \delta.$$

Proof: The function $x^k(1-x)^{M-k}$ increases for $0 \leqslant x \leqslant \frac{k}{M}$, $0 \leqslant k \leqslant M$. Then we have $r^k(1-r)^{M-k} \leqslant \alpha^k(1-\alpha)^{M-k}$ for $M(\alpha+u_\alpha) \leqslant k \leqslant M$ because

$$\alpha \leqslant \frac{M(\alpha+u_\alpha)}{M} \leqslant \frac{k}{M}.$$

Hence

$$P_{\mathcal{H},r}\left(\frac{S_M}{M} \geqslant \alpha + u_\alpha\right) = \sum_{k \geqslant M(\alpha+u_\alpha)} \binom{M}{k} r^k (1-r)^{M-k} \leqslant$$

$$\leqslant \sum_{k \geqslant M(\alpha+u_\alpha)} \binom{M}{k} \alpha^k (1-\alpha)^{M-k} \leqslant \delta.$$

Definition 3. Gives the critical region W for $\mathcal{H}$ and by Proposition 3. $\sup_{r \leqslant \alpha} P_{\mathcal{H},r}(W) = P_{\mathcal{H},\alpha}(W) \leqslant \delta$.

It means that the probability of error of the first type does not depend on the exact probability that T is nonrandom with respect to $\mathcal{R}^\alpha$.

Proposed test for randomness of table generator is based on the simple fact that if the generator is random then the part of the tables which are nonrandom with respect to $\mathcal{R}^\alpha$ is approximately α.

REFERENCES:

[1] A. N. Kolmogorov, *On tables of random numbers*, Sankhya, ser. A 25 (1963), 369—376.

[2] D. Banjević i Z. Ivković, *Jedna definicija pravilnosti i slučajnosti zasnovana na idejama A. N. Kolmogorova*, Matematički vesnik 1 (1978), Beograd.