Dokl. Akad. Nauk SSSR
Tom 212 (1973), No. 3

Soviet Math. Dokl.
Vol. 14 (1973), No. 5

ON THE NOTION OF A RANDOM SEQUENCE

UDC 519.211

L. A. LEVIN

In [1] A. N. Kolmogorov offered a definition of a random object. The necessity for introducing such a notion is connected with a number of difficulties in justifying probability theory as a natural science theory. In the indicated paper the quantity $k(x)$, the algorithmic complexity of an object x, was introduced, and those objects were considered random for which $k(x)$ differed little from the logarithm of the probability of x. (Their difference is called randomness deficiency.)

However, this approach in its original form was suitable only for a finite number of equiprobable objects. Passing to the nonequiprobable case (which is always unavoidable when considering a random variable with an arbitrary integral value or a countable sequence of random variables) resulted in difficulties. To overcome these difficulties P. Martin-Lof gave up the introduction of an invariant (independent of a probability distribution) quantity of the type $k(x)$ and introduced a separate criterion (test) of randomness (cf. [2] for each computable distribution. However, the randomness deficiency defined by Martin-Lof was not expressed in a natural way by a probability distribution and some invariant quantity. Kolmogorov's original definition has an advantage in this respect which it would be a pity to lose. We shall show in particular how this definition can be improved so that it is suitable for the most general case.

Of the already well-known results on this subject mention should be made of Schnorr's result (cf. [4]), which gives a criterion of weak randomness in terms of the usual Kolmogorov complexity, and of P. Gač's results [6].

We shall consider sequences of natural numbers, finite (corteges) and infinite. We call a sequence in which only the numbers 0 and 1 appear, *binary*. We call two sequences x and y, one of which is the beginning of the other ($x \subset y$ or $y \subset x$), *coordinated*. We recall that a denumerable set A of pairs of corteges (x, y) such that, if $(x, y) \in A$ and $(x', y') \in A$ and x is coordinated with x', then y is coordinated with y', is called a *computable operator* (cf. [1]).

Let α be a finite or infinite sequence. Then all corteges y such that for some $x \subset \alpha$ the pairs $(x, y) \in A$ are the beginnings of a sequence β (finite or infinite), which is called the *image of the sequence* α ($\beta = A(\alpha)$).(1)

Definition. The minimal length of a binary cortege x such that $A(x) \supset y$ is called the *monotone complexity of the cortege* y with respect to the operator A ($km_A(y)$).

Theorem 1. *Among all computable operators an "optimal one" exists with respect*

AMS (MOS) subject classifications (1970). Primary 94A15.

(1) The definition of a computable operator was encountered in this form by Ju. T. Medvedev.

to which complexity is minimal to within an additive constant. We denote this complexity by $km(x)$.

Let P be an arbitrary computable probability distribution on the set of sequences of natural numbers. ($P(x)$ is the probability that a sequence begins with the cortege x.)

Theorem 2. a) *For any sequence*(2) α

$$km(\alpha_n) \preccurlyeq |\log_2 P(\alpha_n)|.$$

b) *For P-almost all* α

$$km(\alpha_n) \asymp |\log_2 P(\alpha_n)|,$$

and the probability that $|\log_2 P(\alpha_n)| - km(\alpha_n)$ *will be greater than* m *does not exceed* 2^{-m}.

c) *Those* α *for which* $km(\alpha_n) \asymp |\log_2 P(\alpha_n)|$, *and only they, satisfy all "efficient" laws of probability theory* (i.e. *they withstand any test in the Martin-Lof sense*).

Thus the Kolmogorov approach will be corrective in the general case if $k(x)$ is replaced by $km(x)$.

In [3] Levin introduced a universal semicomputable measure $R(x)$, which we also call the *a priori probability of the sequence* x. We denote the absolute value of its binary logarithm by $kM(x)$.

An underlying relationship exists between $km(x)$ and $kM(x)$. In particular it has not been known until now whether these quantities coincide. (Only their asymptotic coincidence is well known.)

It is, however, easy to prove that $km(x) \succeq kM(x)$. At any rate, it is possible to show that $kM(x)$ also satisfies all items of Theorem 2, it being the minimal semicomputable function satisfying item b) of that theorem. Expounding item c), we obtain the following assertion.

Theorem 3. *A sequence* α *is random with respect to the distribution* P *in the Martin-Lof sense if and only if the probability ratio* $P(\alpha_n)/R(\alpha_n)$ *is bounded below.*

This theorem gives an intuitive definition of randomness: a sequence is *random with respect to the distribution* P when its probability with respect to that distribution is not too small (in comparison with the a priori probability, i.e. that $P(\alpha_n)/R(\alpha_n)$ is bounded).

If a cortege x is not m-random with respect to the distribution P, it is easy to establish this fact effectively; however, it is not in general possible to establish the converse fact effectively. (The situation here is the same as with possibility of establishing the applicability of an algorithm.) It is interesting to consider weaker definitions of randomness, but with better algorithmic properties.

In conclusion we consider the notion of a sequence which is random relative to a class of distributions. Martin-Lof introduced the notion of a "Bernoulli sequence". Let us agree to denote by B_p the Bernoulli measure on binary sequences with the

(2) (α_n) is the cortege of the first n numbers of α: the sign $\preccurlyeq$ denotes less than or equal to, to within an additive constant; the sign $\asymp$ denotes equal to, with the same accuracy.

probability p of one appearing (different trials are independent). Martin-Lof constructed a computable test which is correct relative to all measures B_p. (Recall that Martin-Lof called the set of pairs (x, n), where x is a cortege and n is a number denoting the lower bound of the "randomness deficiency", a *test*. A sequence *withstands a test* if all numbers encountered in a pair with its initial fragments are bounded (above). A test is *computable* if its set of pairs is denumerable. A test is *correct* relative to a measure P if the set of sequences for which the test has randomness deficiency $\geq m$ has P-measure $\leq 2^{-m}$.) He showed that if a sequence withstands this test, it is a von Mises collective relative to some p. This result can be strengthened by showing that a sequence withstands a Martin-Lof Bernoulli test if and only if there is a p for which the sequence withstands any test which is correct relative to the measure B_p and computable relative to p. What is more, this stronger result can be proved in a very general case. We call a set of measures P which satisfy a condition of the form

$$t_1 < P(x_1) < t_1', \ldots, t_n < P(x_n) < t_n',$$

where $x_1, \cdots, x_n$ is a finite collection of corteges, a *cylindrical set*. We call the union of a denumerable totality of cylindrical sets *constructively open* and the complement of the constructively open sets, constructively closed. (These are all standard notions of constructive topology.)

Theorem 4. *Let M be a constructively closed class of measures.*

Then there is a computable test T which is correct relative to all measures in M and such that for every sequence withstanding it a measure $P \in M$ exists such that the sequence withstands any test which is correct relative to p and computable relative to it.

Note that classes of measures which are not closed cannot be considered, since for every computable test the class of measures relative to which it is correct will be constructively closed.

The last theorem is important when the type of a random process is given (e.g., Markov) but its parameters are not given and we are interested in randomness for some parameters.

The results of the present article were announced at the symposium on algebraic complexities (Erevan, May 1971) and the All-Union symposium-school on the foundations of mathematics (Obninsk, June 1971). The author is grateful to all the participants of these symposia who took part in the discussion.

The author express particular gratitude to Academician A. N. Kolmogorov, as well as to M. I. Kanovič and N. V. Petri for valuable discussion.

Institute of Information Transmission

Academy of Sciences of the USSR

Received 1/JULY/72

BIBLIOGRAPHY

1. A. N. Kolmogorov, *Three approaches to the definition of the concept of the "amount of information"*, Problemy Peredači Informacii 1 (1965), no. 1, 3–11; English transl., Selected Transl. in Math. Statist. and Probability, vol. 7, Amer. Math. Soc., Providence, R. I., 1968, pp. 293–302. MR 32 #2273.

2. P. Martin-Löf, *The definition of random sequences*, Information and Control 9 (1966), 602–619. MR 36 #6228.

3. A. K. Zvonkin and L. A. Levin, *The complexity of finite objects and the development of the concepts of information and randomness by means of the theory of algorithms*, Uspehi Mat. Nauk 25 (1970), no. 6 (156), 85–127 = Russian Math. Surveys 25 (1970), no. 6, 83–124.

4. C. P. Schnorr, *Zufälligkeit und Wahrscheinlichkeit, eine algorithmische Bergründung der Wahrscheinlichkeitstheorie*, Lecture Notes in Math., vol. 218, Springer-Verlag, Berlin and New York, 1971.

5. L. A. Levin, *Some theorems on an algorithmic approach to probability theory and information theory*, Moscow, 1971. (Russian)

6. P. Gač, [Gács], *On the complexity of random sequences*, Budapest, 1971 (preprint). (Russian)

Translated by F. M. GOLDWARE