40 YEARS OF THE ORIGIN OF KOLMOGOROV RANDOMNESS THEORY

A.L. Semenov, An.A. Muchnik

Institute of New Technologies

Kolmogorov's work on what is called today 'Kolmogorov complexity' was originated by his work [1]. We follow it up; in particular solve the problem on exact bound of complexity of tests of randomness.

As Kolmogorov wrote ([1]), "The set theoretic axioms of the calculus of probability ... had solved the majority of formal difficulties ... so successfully that the problem of finding the basis of real applications ... became rather secondary to many investigators."

We consider the simplest situation of a sequence of trials with the outcomes $\{0, 1\}$ and want to verify that digits appear independently with probability $1/2$. As a criterion for this von Mises proposed the closeness of frequency of zeros to $1/2$ in the sequence itself and in all subsequences selected by "admissible" rules. The notion of admissible rule was clarified by Church. Both von Mises and Church spoke about infinite sequences. Kolmogorov in [1] gave his notion of admissible rule (which is invariant with respect to computable permutations of digits of the sequence) and proposed the following (frequency) definition of randomness of a finite sequence: the frequencies of zeros and ones in all long enough subsequences selected by simple enough rules are close to $1/2$. Certainly, we should specify an exact meaning for 'long enough', 'simple enough', 'close' by concrete estimations (which may depend on the length of the original sequence). The problem from [1] that the authors have solved was to find the exact estimations of basic parameters for which random sequences exist.

Kolmogorov's approach to randomness exposed in [1] was called 'combinatorial' one in [2]. In the paper [2] he introduced also an 'algorithmic' approach and specified "simple enough rules" as programs of small entropy (Kolmogorov complexity). For each law of probability theory the exceptional set of sequences that do not satisfy it has a small enough cardinality and can be enumerated by a simple program. Thus, the Kolmogorov entropy of each sequence from this set is small compared with its length. For the law of large numbers the fraction of the exceptional set among sequences of length L is less than $2^{-\delta L}$ (where δ is a positive constant). We show, in a way, that for sequences which are random according to the Kolmogorov frequency definition it is satisfied every

Institute of New Technologies, 10 Nizhnyaya Radishevskaya, Moscow, 109004, Russia.
Phone: +7(095)9156296.
Fax: +7(095)9156963.
E-mail: alsemenov@mtu-net.ru, muchnik@lpcs.math.msu.ru

law of probability theory such that the fraction of the exceptional set is less than $2^{-L \ln\ln L/\ln L}$. In other words, for any sequence $\mathbf{t}$ of length L

> the frequencies of zeros and ones in all long enough subsequences selected from $\mathbf{t}$ by simple enough rules are close to $1/2$
>
> $\Downarrow$
>
> the entropy of $\mathbf{t}$ conditional to L is greater than $L(1 - \ln\ln L/\ln L)$.

The reverse implication is easy to prove, as was noted by Kolmogorov in [3].

We survey also another branch of intensive research originated by Kolmogorov — study of randomness of infinite sequences (cf. [4]).

References

[1] A. N. Kolmogorov. On Tables of Random Numbers. *Sankhyã: The Indian Journal of Statistics*, Series A, 1963, v. 25, part 4. (Reprinted in *Theoretical Computer Science*, 1998, vol. 207, pp. 387–395).

[2] A. N. Kolmogorov. Three Approaches to the Quantitative Definition of Information. *Problems of Information Transmission*, 1965, vol. 1, no 1, pp. 3–11.

[3] A. N. Kolmogorov. On Logical Foundations of Probability Theory. *Probability Theory and Mathematical Statistics*, Proceedings of Fourth USSR–Japan Symposium held in Tbilisi, USSR, August 23–29, 1982. K. Ito, J. V. Prokhorov, Eds., Lecture Notes in Mathematics, vol. 1021. 1983, Berlin: Springer-Verlag, pp. 1–5.

[4] An. A. Muchnik, A. L. Semenov, V. A. Uspensky. Mathematical Metaphysics of Randomness. *Theoretical Computer Science*, 1998, vol. 207, pp. 263–317.