Dokl. Akad. Nauk. SSSR
Tom 227 (1976), No. 1

Soviet Math. Dokl.
Vol. 17 (1976), No. 2

UNIFORM TESTS OF RANDOMNESS

UDC 519.211+517.11

L. A. LEVIN*

1. In the theory of complexity we find the definition of a series of concepts: complexity, randomness, ~~and~~ information content ~~of~~, a priori probability (see, for example, [1]–[9]). In this paper we propose a unique approach to concepts of this kind starting from a general system of constructions. With the help of such constructions we can apparently define many other useful quantities.

The work is based on the fact that instead of constructing separate tests of randomness for every computable measure (as is done in [2]), we develop a general test $d(\omega/P)$—the deficiency of randomness of a sequence ω with respect to an arbitrary measure P. This test is applicable not only to computable but to arbitrary probability distributions; in particular, what is significant for us, the test applies to semicomputable (what we call here enumerable) distributions. It turns out that with respect to ~~a~~ some universal enumerable distribution M all sequences are random, and therefore it deserves the name a priori probability. We note that the very existence of a measure with respect to which all sequences are random is inevitable if we wish to define the concept of a "sequence ω, random relative to a measure P" so that the set of all pairs (ω, P) is closed and for every P the set of ω random with respect to P has positive measure. If we now take a distribution on pairs of random variables (α, β) which are independent and have individually the same universal distribution M, then it is natural to regard the deficiency of randomness $d((\alpha, \beta)/M \times M)$ of the pair of sequences (α, β) with respect to the distribution $M \times M$ as the "deficiency of independence" of these sequences, or the information content $I(\alpha : \beta)$. Considering other natural semicomputable distributions, we may define many other interesting quantities, for example, $I(\alpha : \beta/\gamma)$, the information in α about β knowing γ, and so on.

2. **Terminology.** Our presentation is given for the space of infinite binary sequences Ω; however, it is adaptable for automatic transfer to any other "good" compact space with a countable base. Since connected topological spaces, unlike Ω, do not have a basis of open-closed sets, it will be more convenient for us to consider a measure not as an additive set function, but as a linear functional on continuous functions (as is done in contemporary analysis).

A continuous function on Ω, given in the form of a table and with set of values consisting of a finite number of nonnegative rational numbers, will be called elementary. The set of elementary functions will be denoted by S and the set of continuous real functions by K.

AMS (MOS) subject classifications (1970). Primary 68A20, 94A15.

**Editor's note.* The present translation incorporates corrections made by the author.

A monotone linear functional P from K to R will be called a measure, and a monotone normed linear operator A from K to K will be called a stochastic operator. An operator (or measure) is computable if the following two sets are enumerable: the set of pairs of elementary functions f, g such that $f < A(g)$ and the set for which $f > A(g)$. It is obvious that every deterministic operator (in the usual sense) from Ω to Ω, which is continuous, computable, and defined everywhere, corresponds to a stochastic operator, and that the class of computable measures is closed under composition with computable stochastic operators. To consider operators $\Omega \to \Omega$ not defined everywhere, we have to introduce the concept of "semimeasure". A semimeasure is a concave functional P ($P(\alpha f + \beta g) \geq \alpha P(f) + \beta P(g)$ for $\alpha, \beta \geq 0$) from K to R that is monotone. A semimeasure is called enumerable if the set of elementary functions f such that $P(f) \geq 1$ is enumerable. An enumerable semimeasure is analogous to a semicomputable measure in the old terminology (see [5]). With every elementary function $f \neq 0$ there is ~~an~~ associated a semimeasure, which we will denote by P_f, defined by the expression $P_f(g) = \min_\omega g(\omega)/f(\omega)$. By the symbols $\succcurlyeq$, $\preccurlyeq$ and $\asymp$ we shall denote inequalities and equivalence to within an additive constant.

3. Let us define the concept of a uniform test of randomness. This test will give the deficiency of randomness $\log_2 t(\omega/Q)$ of the sequence ω with respect to the probability distribution (semimeasure) Q. It will be more convenient for us to use the quantity $t(P/Q) = \int_\Omega t(\omega/Q)\, dP$.

Definition. Let $\hat{t}(f/g)$ be a semicomputable, homogeneous, nonnegative functional, i.e. such that $\hat{t}(c_1 \cdot f/c_2 \cdot g) = (c_2/c_1)\hat{t}(f/g)$ and the set of pairs (f, g) for which $\hat{t}(f/g) > 1$ is enumerable. Let $t(P/Q)$ be the smallest function on pairs of semimeasures P, Q, monotonically decreasing (nonstrictly) with respect to Q, increasing and concave relative to P ($t(P_1 + P_2/Q) \geq t(P_1/Q) + t(P_2/Q)$) and such that

$$t\left(\frac{P}{P(f)}\Big/\frac{Q}{Q(g)}\right) \geq \hat{t}\left(\frac{f}{g}\right).$$

And suppose the inequality $t(P/P) \leq 1$ holds for all P. Then the function t is called a uniform test of randomness.

The first two statements of the following theorem can be proved by analogy with Kolmogorov's theorem (see [1]) on the existence of an optimal algorithm for the complexity of words.

Theorem 1. a) *Among all uniform tests there exists a largest to within a multiplicative constant. Its binary logarithm (optimal with additive precision) will be denoted by* $d(P/Q)$, *and for* $P_\omega(f) = f(\omega)$ *we shall write* $d(\omega/Q)$.

b) *Among all enumerable semimeasures there exists a largest to within a multiplicative constant, denoted by* M.

The quantity $[-\log_2 M(f/\max_\omega f(\omega))]$ will be denoted by $KM(f)$.

c) *The function* $d(\omega/M)$ (*and* $d(P/M)$ *for normalized* P: $P(1) = 1$) *is uniformly bounded, i.e. all sequences are random with respect to* M.

Statement c) presents some technical difficulties, and the thrust of its proof consists of the application of the following lemma of Sperner.

Lemma (Sperner). *For an arbitrary simplicial decomposition of an n-dimensional simplex and an arbitrary mapping of the set of vertices of the decomposition into the set of vertices of the same simplex such that every vertex of the decomposition lying in a face of some dimension is mapped into one of the vertcies of the same face, there exists a simplex of the decomposition on whose vertices this mapping is one-to-one.*

From this lemma follows the existence of a measure with respect to which every sequence is random;(1) the rest is easily proved.

Theorem 2 (invariance of randomness). *For an arbitrary computable stochastic operator A and semimeasures P, Q we have the inequality*

$$d(P\cdot A/Q\cdot A)\prec d(P/Q).$$

Let us now consider the semimeasure $M\times M$ on the set of pairs $(\alpha, \beta)\in\Omega\times\Omega$, under which α and β are independent and identically distributed relative to a universal semimeasure M. Then it is natural to regard the deficiency of randomness $d((\alpha, \beta)/M\times M)$ with respect to this distribution as the deficiency of independence of α and β, or the information content in α about β.

The last theorem establishes a connection between the quantities examined in this paper and earlier expressions for complexity, information and deficiency of randomness.

Theorem 3. a) *The quantity $d(\alpha, \beta/M\times M)$ is related to the quantity $I(\alpha:\beta)$ defined in* [9] *by the inequality*

$$d((\alpha, \beta)/M\times M)\succ I(\alpha:\beta).$$

b) *With respect to an arbitrary computable measure Q those and only those sequences ω will be random (i.e. $d(\omega/Q)<\infty$) which are random in the Martin-Löf sense with respect to the same measure.*

c) *Let f_i be an arbitrary enumerable sequence of elementary functions with disjoint supports. Then $KM(f_i)\asymp KP(i)$, where KP is the prefix complexity used in the papers* [7], [9], [6].

Theorems 2 and 3a) show that the quantity $d(\alpha, \beta/M\times M)$, taken as the definition of information, satisfies Theorems 2 and 4 in [9].

In conclusion, the author wishes to thank Academician A. N. Kolmogorov for discussing the results and for valuable remarks. The author also takes this opportunity to express thanks to A. A. Tužilin for encouraging this work.

Received 7/JUNE/75

BIBLIOGRAPHY

1. A. N. Kolmogorov, Problemy Peredači Informacii 1 (1965), no. 1, 3; English transl., Selected Transl. Math. Statist. and Probability, vol. 7, Amer. Math. Soc., Providence, R. I., 1968, p. 293. MR 32 #2273.

2. Per Martin-Lof, Information and Control 9 (1969), 602. MR 36 #6228.

3. C. P. Schnorr, Lecture Notes in Math., vol. 218, Springer-Verlag, Berlin and New York, 1971.

(1) This makes use only of the fact that the set $((\omega, P): d(\omega, P)\leq 0)$ is closed and the inequality $P\{\omega: d(\omega, P)\leq 0\}>0$, which follows from the conditions $t(P/P)<1$ and $P(1)=1$.

4. R. J. Solomonoff, Information and Control 7 (1964), 1. MR 30 #2963.

5. A. K. Zvonkin and L. A. Levin, Uspehi Mat. Nauk 25 (1970), no. 6 (156), 85 = Russian Math. Surveys 25 (1970), no. 6, 83. MR 46 #7004.

6. P. Gač [Gacs], Dokl. Akad. Nauk SSSR 218 (1974), 1265 = Soviet Math. Dokl. 15 (1974), 1477.

7. L. A. Levin, *Some theorems on the algorithmic approach to probability theory and information theory*, Candidate's Dissertation, Novosibirsk, 1971. (Russain)

8. ———, Dokl. Akad. Nauk SSSR 212 (1973), 548 = Soviet Math. Dokl. 14 (1973), 1413.

9. ———, Problemy Peredači Informacii 10 (1974), no. 3, 30 = Problems of Information Transmission 10 (1974), 206.

Translated by T. I. BARTHA