Algorithmic tests and randomness with respect to a class of measures

Laurent Bienvenu*, Peter Gács†, Mathieu Hoyrup‡,
Cristobal Rojas§, Alexander Shen¶

March 9, 2011

Abstract

This paper offers some new results on randomness with respect to classes of measures, along with a didactical exposition of their context based on results that appeared elsewhere.

We start with the reformulation of the Martin-Löf definition of randomness (with respect to computable measures) in terms of randomness deficiency functions. A formula that expresses the randomness deficiency in terms of prefix complexity is given (in two forms). Some approaches that go in another direction (from deficiency to complexity) are considered.

The notion of Bernoulli randomness (independent coin tosses for an asymmetric coin with some probability p of head) is defined. It is shown that a sequence is Bernoulli if it is random with respect to *some* Bernoulli

*LIAFA, CNRS & Université Paris Diderot, Paris 7, Case 7014, 75205 Paris Cedex 13, France, e-mail: Laurent dot Bienvenu at liafa dot jussieu dot fr

†Department of Computer Science, Boston University, 111 Cummington st., Room 138, Boston, MA 02215, e-mail: gacs at bu dot edu

‡LORIA – B248, 615, rue du Jardin Botanique, BP 239, 54506 Vandœuvre-lès-Nancy, France, e-mail: Mathieu dot Hoyrup at loria dot fr

§Department of Mathematics, University of Toronto, Bahen Centre, 40 St. George St., Toronto, Ontario, Canada, M5S 2E4, e-mail: crojas at math dot utoronto dot ca

¶LIF, Universitè Aix – Marseille, CNRS, 39, rue Joliot-Curie, 13453 Marseille cedex 13, France, on leave from IITP RAS, Bolshoy Karetny, 19, Moscow. Supported by NAFIT ANR-08-EMER-008-01, RFBR 0901-00709-a grants. e-mail: sasha dot shen at gmail dot com.

measure B_p. A notion of "uniform test" for Bernoulli sequences is introduced which allows a quantitative strengthening of this result. Uniform tests are then generalized to arbitrary measures.

Bernoulli measures B_p have the important property that p can be recovered from each random sequence of B_p. The paper studies some important consequences of this orthogonality property (as well as most other questions mentioned above) also in the more general setting of constructive metric spaces.

1 Introduction

This paper, though intended to be rather self-contained, can be seen as a continuation of [10] (which itself built on earlier work of Levin) and [12].

Our enterprise is to develop the theory of randomness beyond the framework where the underlying probability distribution is the uniform distribution or a computable distribution. A randomness test $\mathbf{t}(\omega, P)$ of object ω with respect to measure P is defined to be a function of both the measure P and the point ω.

In some later parts of the paper, we will also go beyond the case where the underlying space is the set of finite or infinite sequences: rather, we take a constructive metric space with its algebra of Borel sets.

We will apply the above notion of test to define, following ideas of [15], for a class $\mathscr{C}$ of measures having some compactness property, a "class test" $\mathbf{t}_{\mathscr{C}}(\omega)$. This is a test to decide whether object ω is random with respect to any one measure P in the class $\mathscr{C}$. We will show that in case of the class of Bernoulli measures over binary sequences, this notion is equivalent to the class tests introduced by Martin-Löf in [19].

In case there is an effective sense in which the elements of the class are mutually orthogonal, we obtain an especially simple separation of the randomness test $\mathbf{t}(\omega, P)$ into two parts: the class test and an arbitrarily simple test for "typicality" with respect to the measure P. In some natural special cases, the typicality test corresponds to a convergence property of relative frequencies, allowing to apply the theory to any general effectively compact class of ergodic stationary processes.

There are some properties of randomness tests $\mathbf{t}(\omega, P)$ that depend on the measure P, which our tests do not necessarily possess, for example a kind of monotonicity in P. It is therefore notable that in case of the orthogonal classes,

randomness is equivalent to an "blind" notion of randomness, that only considers randomness tests that do not depend on the measure P.

Here is an outline of the paper. We start with the reformulation of the Martin-Löf definition of randomness (with respect to computable measures) in terms of tests. A randomness test provides a quantitative measure of non-randomness, called "randomness deficiency"; it is finite for random sequences and infinite for non-random ones. There are two versions of these tests ("average-bounded" and "probability-bounded" ones); a relation between them is established.

A formula that expresses the (average-bounded) randomness deficiency in terms of prefix complexity is given (in two forms). It implies the Levin-Schnorr criterion of randomness (with prefix complexity, as in the special case first announced in Chaitin's paper). Some approaches that go in another direction (from deficiency to complexity) are considered.

The notion of Bernoulli sequence (looking like the outcome of independent coin tosses for an asymmetric coin) is defined. It is shown that the set of Bernoulli sequences is the union (over all $p \in [0,1]$) of the sets of sequences that are random with respect to B_p, the Bernoulli measure with probability p; here we assume that p is given as an oracle). A notion of "uniform test" for Bernoulli sequences is introduced. Then the statement above is proved in the following quantitative form: the Bernoulli deficiency is the infimum of B_p deficiencies over all $p \in [0,1]$.

The notion of general uniform test (not restricted to the class of Bernoulli measures) is introduced. It is shown that it generalizes Martin-Löfs earlier definition of randomness (which was given only for computable measures).

Bernoulli measures B_p have the important property that p can be recovered from each random sequence of B_p. The paper studies some important consequences of this orthogonality property (as well as most other questions mentioned above) also in the more general setting of constructive metric spaces.

The following notation is useful, since inequalities hold frequently only within an additive or multiplicative constant.

Notation 1.1. We will write $f(x) \stackrel{*}{<} g(x)$ for inequality between positive functions within a multiplicative constant, that is for the relation $f(x) = O(g(x))$: precisely, if there is a constant c with $f(x) \leqslant cg(x)$ for all x. The relation $f \stackrel{*}{=} g$ means $f \stackrel{*}{<} g$ and $f \stackrel{*}{>} g$. Similarly, $f \stackrel{+}{<} g$ and $f \stackrel{+}{=} g$ means inequality within an additive constant.

Let Λ denote the empty string.

Logarithms are taken, as a default, to base 2. We use $|x|$ to denote the length of a string x. For finite string, x and finite or infinite string y let $x \sqsubseteq y$ denote that x is a prefix of y. If x is a finite or infinite sequence then its elements are written as $x(1), x(2), \ldots$, and its prefix of size n will be denoted by $x(1:n)$.

Let $\overline{\mathbb{R}}_+ = [0,\infty]$ be the set of nonnegative reals, with the special value ∞ added. The binary alphabet $\{0,1\}$ will also be denoted by $\mathbb{B}$. ⌟

2 Randomness on sequences, for computable measures

2.1 Lower semicomputable functions on sequences

In the first sections, we will study randomness over infinite binary sequences.

Definition 2.1 (Binary Cantor space, Baire space)**.** We will denote by Ω the set of infinite binary sequences, and call it also the *binary Cantor space*. For a finite string x let $x\Omega$ be the set of all infinite sequences that have finite prefix x. These sets will be called *basic open sets*, the set of all basic open set is called the *basis* of Ω (as a topological space). A subset of Ω is *open* if it is the union of a set of basis elements.

The set of infinite sequences of natural numbers will be called the *Baire space*. Basic open sets and open sets can be defined for it analogously. ⌟

A notion somewhat weaker than computability will play crucial role.

Definition 2.2. An open set $G \subseteq \Omega$ is called *effectively open*, or *lower semicomputable open*, or *c.e. open*, or *r.e. open* if it is the union of a computable sequence $x_i\Omega$ of basic elements. A set is *upper semicomputable closed*, or *effectively closed* if its complement is effectively open.

A set Γ is called *effectively* G_δ if there is a sequence of sets U_k, $k = 1,2,\ldots$ effectively open uniformly in k such that $\Gamma = \bigcap_k U_k$.

A function $t : \Omega \to [0,\infty]$ is *lower semicomputable* if

(a) For any rational r the set $\{\omega : r < t(\omega)\}$ is open in Ω, that is is a union of intervals $x\Omega$.

(b) Moreover, this set is effectively open uniformly in r, that is there exists an algorithm that gets r as input and generates strings $x_0, x_1, \ldots$ such that the union of interval $x_i\Omega$ is equal to $\{\omega : r < t(\omega)\}$.

⌟

This definition is a constructive version of the classical notion of lower semicontinuous function as in requirement (a). The same class of lower semicomputable functions has other (equivalent) definitions; here is one of them.

Definition 2.3. A function u defined on Ω and having rational values is called *basic* if the value $u(\omega)$ is determined by some finite prefix of ω. ⌟

If this prefix has length N, the function can be presented as a table with 2^N rows; each row contains N bits (the values of the first N bits of ω) and a rational number (the value of the function). Such a function is a finite object.

The proof of the following proposition is a simple exercise:

Proposition 2.4. *The (pointwise) limits of monotonic sequences of basic functions are exactly the lower semicomputable functions on* Ω.

Since the difference of two basic functions is a basic function, we can reformulate this criterion as follows: lower semicomputable functions are (pointwise) sums of computable series made of non-negative basic functions.

One more way to define a lower semicomputable function goes as follows.

Definition 2.5 (Generating)**.** Let T be a lower semicomputable function on the set $\{0,1\}^*$ of finite sequences of zeros and ones with non-negative (finite or infinite) values. This means that the set of pairs (x,r) such that $r < T(x)$ is enumerable. Then function t defined as

$$t(\omega) = \sup_{x \sqsubseteq \omega} T(x)$$

is a lower semicomputable function on Ω: we will say that function $T(\cdot)$ *generates* function $t(\cdot)$ if it is also monotone: $T(x) \leqslant T(y)$ if $x \sqsubseteq y$. ⌟

The monotonicity requirement can always be satisfied by taking $T'(x) = \max_{z \sqsubseteq x} T(z)$.

Proposition 2.6. *Any lower semicomputable function t on Ω is generated by an appropriate function T on $\{0,1\}^*$ this way.*

We may also assume that T is a computable function with rational values. Indeed, since only the supremum of T on all the prefixes is important, instead of

increasing $T(x)$ for some x we may increase $T(y)$ for all $y \sqsupseteq x$ of large length; this delay allows T to be computable.

For a given lower semicomputable function t on Ω there exists a maximal monotonic function T on finite strings that generates t (in the sense just described). This maximal T can be defined as follows:

$$T(x) = \inf_{\omega \sqsupseteq x} t(\omega). \tag{1}$$

Let us now exploit the finiteness of the binary alphabet $\{0,1\}$, which implies that the space Ω is a compact topological space.

Proposition 2.7. *The function T defined by* (1) *is lower semicomputable. In the definition, we can replace* inf *by* min.

Proof. Indeed, $r < \inf_{\omega \sqsupseteq x} t(\omega)$ if and only if there exists some rational $r' > r$ with $r' < t(\omega)$ for all $\omega \sqsupseteq x$. The last condition can be reformulated: the open set of all sequences ω such that $t(\omega) > r'$ is a superset of $x\Omega$. This open set is a union of an enumerable family of intervals; if these intervals cover $x\Omega$, compactness implies that this is revealed at some finite stage, so the condition is enumerable (and the existential quantifier over r' keeps it enumerable).

Since the function $t(\omega)$ is lower semicontinuous, it actually reaches its infimum on the compact set $x\Omega$, so inf can be replaced with min. □

2.2 Randomness tests

We assume that the reader is familiar with the basic concepts of measure theory and integration, at least in the space Ω of infinite binary sequences. A measure P on Ω is determined by the values

$$P(x) = P(x\Omega)$$

which we will denote by the same letter P, without danger of confusion. Moreover, any function $P : \{0,1\}^* \to [0,1]$ with the properties

$$P(\Lambda) = 1, \quad P(x) = P(x0) + P(x1) \tag{2}$$

uniquely defines a measure (this is a particular case of Caratheodory's theorem).

Definition 2.8 (Computable measure)**.** A real number is called *computable* if there is an algorithm that for all rational ε returns a rational approximation of x

with error not greater than ε. Computable numbers can also be determined as limits of sequences $x_1, x_2, \ldots$ for which $|x_n - x_{n+k}| \leqslant 2^{-n}$. An infinite sequence $s_1, s_2, \ldots$ of real numbers is a *strong Cauchy* sequence if for all $m < n$ we have $|s_m - s_n| \leqslant 2^{-m}$.

A function determined on words (or other constructive objects) is *computable* if its values are computable uniformly from the input, that is there is an algorithm that from each input and $\varepsilon > 0$ returns an ε-approximation of the function value on this input.

Measure P over Ω is said to be *computable* if the function $P : \{0,1\}^* \to [0,1]$ is computable. ⌟

Definition 2.9 (Randomness test, computable measure)**.** Let P be a computable probability distribution (measure) on Ω. A lower semicomputable function t on Ω with non-negative (possible infinite) values is an (*average-bounded*) *randomness test* with respect to P (or *P-test*) if the expected value of t with respect to P is at most 1, that is

$$\int t(\omega)\, dP \leqslant 1.$$

A sequence ω *passes* a test t if $t(\omega) < \infty$. A sequence is called *random* with respect to P it is passes all P-randomness tests (as defined above). ⌟

The intuition: when $t(\omega)$ is large, this means that test t finds a lot of "regularities" in ω. Constructing a test, we are allowed to declare whatever we want as a "regularity"; however, we should not find too many of them on average: if we declare too many sequences to be "regular", the average becomes too big.

This definition turns out to be equivalent to randomness as defined by Martin-Löf (see below). But let us start with the universality theorem:

Theorem 2.10. *For any computable measure P there exists a* universal *(maximal) P-test u: this means that for any other P-test t there exists a constant c such that*

$$t(\omega) \leqslant c \cdot u(\omega)$$

for every $\omega \in \Omega$.

In particular, $u(\omega)$ is finite if and only if $t(\omega)$ is finite for every P-test t, so the sequences that pass test u are exactly the random sequences.

Proof. Let us enumerate the algorithms that generate all lower semicomputable functions. Such an algorithm produces a monotone sequence of basic functions.

Before letting through the next basic function of this sequence, let us check that its P-expectation is less than 2. If the algorithm considered indeed defines a P-test, this expectation does not exceed 1, so by computing the values of P with sufficient precision we are able to guarantee that the expectation is less than 2. If this checking procedure does not terminate (or gives a negative result), we just do not let the basic function through.

In this way we enumerate all tests as well as some lower semicomputable functions that are not exactly tests but are at most twice bigger than tests. It remains to sum up all these functions with positive coefficients whose sum does not exceed $1/2$ (say, $1/2^{i+2}$). □

Recall the definition of randomness according to Martin-Löf.

Definition 2.11. Let P be a computable distribution over Ω. A sequence of open sets $U_1, U_2, \ldots$ is called a *Martin-Löf test* for P if the sets U_i are effectively open in a uniform way (that is $U_i = \bigcup_j x_{ij}\Omega$ where the double sequence x_{ij} of strings is computable), moreover $P(U_k) \leqslant 2^{-k}$ for all k.

A set N is called a *constructive (effective) null set* for the measure P if there is a Martin-Löf test $U_1, U_2, \ldots$ with the property $N = \bigcap_k U_k$. Note that effective null sets are constructive G_δ sets.

A sequence $\omega \in \Omega$ is said to *pass* the test $U_1, U_2, \ldots$ if it is not in N. It is *Martin-Löf-random* with respect to measure P if it is not contained in any constructive null set for P. ⌟

The following theorem is not new, see for example [18].

Theorem 2.12. *A sequence ω passes all average-bounded P-tests (=passes the universal P-test) if and only if it is Martin-Löf random with respect to P.*

Proof. If t is a test, then the set of all ω such that $t(\omega) > N$ is an effectively open set that can be found effectively given N. This set has P-measure at most $1/N$ (by Chebyshev's inequality), so the sets of sequences ω that do not pass t (that is $t(\omega)$ is infinite) is an effectively P-null set.

On the other hand, let us show that for every effectively null set Z there exists an average-bounded test that is infinite at all its elements. Indeed, for every effectively open set U the function 1_U that is equal to 1 inside U and to 0 outside U is lower semicomputable. Then we can get a test $\sum_i 1_{U_i}$. The average of this test does not exceed $\sum_i 2^{-i} = 1$, while the sum is infinite for all elements of $\bigcap_i U_i$. □

When talking about randomness for a computable measure, we will write *randomness* from now on, understanding Martin-Löf randomness, since no other kind will be considered.

Sometimes it is useful to switch to the logarithmic scale.

Definition 2.13. For every computable measure P, we will fix a universal P-test and denote it by $\mathbf{t}_P(\omega)$. Let $\mathbf{d}_P(\omega)$ be the logarithm of the universal test $\mathbf{t}_P(\omega)$:

$$\mathbf{t}_P(\omega) = 2^{\mathbf{d}_P(\omega)}.$$

With other kinds of test also, it will be our convention to use $\mathbf{t}$ (boldface) for the universal test, and $\mathbf{d}$ (boldface) for its logarithm. ⌟

In a sense, the function $\mathbf{d}_P$ measures the randomness deficiency in bits.

The logarithm, along with the requirement $\int \mathbf{t}_P(\omega)\, dP \leqslant 1$, implies that $\mathbf{d}_P(\omega)$ may have some negative values, and even values $-\infty$. By just choosing a different universal test we can always make $\mathbf{d}_P(\omega)$ bounded below by, say, -1, and also integer-valued. On the other hand, if we want to make it nonnegative, we will have to lose the property $\int 2^{\mathbf{d}_P(\omega)} dP \leqslant 1$, though we may still have $\int 2^{\mathbf{d}_P(\omega)} dP \leqslant 2$. It will still have the following property:

Proposition 2.14. *The function $\mathbf{d}_P(\cdot)$ is lower semicomputable and is the largest (up to an additive constant) among all lower semicomputable functions such that the P-expectation of $2^{\mathbf{d}_P(\cdot)}$ is finite.*

As we have shown, for any fixed computable measure P the value $\mathbf{d}_P(\omega)$ (and $\mathbf{t}_P(\omega)$) is finite if and only if the sequence ω is Martin-Löf random with respect to P.

Remarks 2.15. 1. Each Martin-Löf's test $(U_1, U_2, \dots)$ is more directly related to a lower semicomputable function $F(\omega) = \sup_{\omega \in U_i} i$. This function has the property $P[F(\omega) \geqslant k] \leqslant 2^{-k}$. Such functions will be called *probability-bounded* tests, and were used in [29]. We will return to such functions later.

2. We have defined $\mathbf{d}_P(\omega)$ separately for each computable measure P (up to a constant). We will later give a more general definition of randomness deficiency $\mathbf{d}(\omega, P)$ as a function of two variables P and ω that coincides with $\mathbf{d}_P(\omega)$ for every computable P up to a constant depending on P.

⌟

2.3 Average-bounded and probability-bounded deficiencies

Let us refer for example to [18, 25] for the definition of and basic properties of plain and prefix (Kolmogorov) complexity. We will define prefix complexity in Definition 2.18 below, though. We will not use complexities explicitly in the present section, just refer to some of their properties by analogy.

The definition of a test given above resembles the definition of prefix complexity; we can give another one which is closer to plain complexity. For that we use a weaker requirement: we require that the P-measure of the set of all sequences ω such that $t(\omega) > N$ does not exceed $1/N$. (This property is true if the integral does not exceed 1, due to Chebyshev's inequality.)

In logarithmic scale this requirement can be restated as follows: the P-measure of the set of all sequences whose deficiency is greater than n does not exceed 2^{-n}. If we restrict tests to integer values, we arrive at the classical Martin-Löf tests: see also Remark 2.15, part 1.

While constructing an universal test in this sense, it is convenient to use the logarithmic scale and consider only integer values of n. As before, we enumerate all tests and "almost-tests" d_i (where the measure is bounded by twice bigger bound) and then take the weighted maximum in the following way:

$$\mathbf{d}(\omega) = \max_i [d_i(\omega) - i] - c.$$

Then $\mathbf{d}$ is less than d_i only by $i + c$, and the set of all ω such that $\mathbf{d}(\omega) > k$ is the union of sets where $d_i(\omega) > k + i + c$. Their measures are bounded by $O(2^{-k-i-c})$ and for a suitable c the sum of measures is at most 2^{-k}, as required.

In this way we get two measures of non-randomness that can be called "average-bounded deficiency" $\mathbf{d}^{\mathrm{aver}}$ (the first one, related to the tests called "integral tests" in [18]) and "probability bound deficiency" $\mathbf{d}^{\mathrm{prob}}$ (the second one). It is easy to see that they define the same set of nonrandom sequences (=sequences that have infinite deficiency). Moreover, the finite values of these two functions are also rather close to each other:

Proposition 2.16.

$$\mathbf{d}^{\mathrm{aver}}(\omega) \stackrel{+}{<} \mathbf{d}^{\mathrm{prob}}(\omega) \stackrel{+}{<} \mathbf{d}^{\mathrm{aver}}(\omega) + 2\log \mathbf{d}^{\mathrm{aver}}(\omega).$$

Proof. Any average-bounded test is also a probability-bounded test, therefore $\mathbf{d}^{\mathrm{aver}}(\omega) \stackrel{+}{<} \mathbf{d}^{\mathrm{prob}}(\omega)$.

For the other direction, let d be a probability-bounded test (in the logarithmic scale). Let us show that $d - 2\log d$ is an average-bounded test. Indeed, the probability of the event "$d(\omega)$ is between $i-1$ and i" does not exceed $1/2^{i-1}$, the integral of $2^{d-2\log d}$ over this set is bounded by $2^{-i+1}2^{i-2\log i} = 2/i^2$ and therefore the integral over the entire space converges.

It remains to note that the inequality $a \stackrel{+}{<} b + 2\log b$ follows from $b \stackrel{+}{>} a - 2\log a$. Indeed, we have $b \geqslant a/2$ (for large enough a), hence $\log a \leqslant \log b + 1$, and then $a \stackrel{+}{<} b + 2\log a \stackrel{+}{<} b + 2\log b$. □

In the general case the question of the connection between boundedness in average and boundedness in probability is addressed in the paper [23]. It is shown there (and this is not difficult) that if $u : [1,\infty] \to [0,\infty]$ is a monotonic continuous function with $\int_1^\infty u(t)/t^2\,dt \leqslant 1$, then $u(t(\omega))$ is an average-bounded test for every probability-bounded test t, and that this condition cannot be improved. (Our estimate is obtained by choosing $u(t) = t/\log^2 t$.)

Remark 2.17. This statement resembles the relation between prefix and plain description complexity. However, now the difference is bounded by the logarithm of the *deficiency* (that is bounded independently of length for the sequences that are close to random), not of the *complexity* (as usual), which would be normally growing with the length. ⌟

Question 1. *It would be interesting to understand whether the two tests differ only by a shift of scale or in some more substantial way. For the confirmation of such a more substantial difference could serve two families of sequences ω_i and ω_i' for which*

$$\mathbf{d}^{\mathrm{aver}}(\omega_i') - \mathbf{d}^{\mathrm{aver}}(\omega_i) \to \infty$$

for $i \to \infty$, while

$$\mathbf{d}^{\mathrm{prob}}(\omega_i') - \mathbf{d}^{\mathrm{prob}}(\omega_i) \to -\infty.$$

The authors do not know whether such a family exists.

2.4 A formula for average-bounded deficiency

Let us recall some concepts connected with the prefix description complexity. For reference, consult for example [18, 25].

Definition 2.18. A set of strings is called *prefix-free* if no element of it is a prefix of another element. A computable partial function $T : \{0,1\}^* \to \{0,1\}^*$ is called a *self-delimiting interpreter* if its domain of definition is a prefix-free set. We define the complexity $Kp_T(x)$ of a string x with respect to T as the length of a shortest string p with $T(p) = x$. It is known that there is an *optimal* (self-deliminiting) interpreter: that is a (self-delimiting) interpreter U with the property that for every self-delimiting interpreter T there is a constant c such that for every string x we have $Kp_U(x) \leqslant Kp_T(x) + c$. We fix an optimal self-delimiting interpreter U and denote $Kp(x) = Kp_U(x)$.

We also denote $\mathbf{m}(x) = 2^{-Kp(x)}$, and call it sometimes *discrete a priori probability*. ⌟

The "a priori" name comes from some interpretations of a property that distinguishes the function $\mathbf{m}(x)$ among certain "weight distributions" called semimeasures.

Definition 2.19. A function $f : \{0,1\}^* \to [0,\infty)$ is called a *discrete semimeasure* if $\sum_x f(x) \leqslant 1$. ⌟

Lower semicomputable semimeasures arise as the output distribution of a randomized algorithm using a source of random numbers, and outputting some word (provided the algorithm halts; with some probability, it may not halt).

It is easy to check that $\mathbf{m}(x)$ is a lower semicomputable discrete semimeasure.

Recall the following fact.

Proposition 2.20 (Coding Theorem)**.** *Among lower semicomputable discrete semimeasures, the function $\mathbf{m}(x)$ is maximal within a multiplicative constant: that is for every lower semicomputable discrete semimeasure $f(x)$ there is a constant c with $c \cdot \mathbf{m}(x) \geqslant f(x)$ for all x.*

The universal average-bounded randomness test $\mathbf{t}_P 1$ (the largest lower semicomputable function with bounded expectation) can be expressed in terms of a priori probability (and therefore prefix complexity):

Proposition 2.21. *Let P be a computable measure and let $\mathbf{t}_P$ be the universal average-bounded randomness test with respect to P. Then*

$$\mathbf{t}_P(\omega) \stackrel{*}{=} \sum_{x \sqsubseteq \omega} \frac{\mathbf{m}(x)}{P(x)}.$$

(If $P(x) = 0$, then the ratio $\mathbf{m}(x)/P(x)$ is considered to be infinite.)

Proof. A lower semicomputable function on sequences is a limit of an increasing sequence of basic functions.

Withouth loss of generality we may assume that each increase is made on some cylinder $x\Omega$. In other terms, we increase the "weight" $w(x)$ of x and let our basic function on ω be the sum of the weights of all prefixes of ω. The weights increase gradually: at any moment, only finitely many weights differ from zero. In terms of weights, the average-boundedness condition translates into

$$\sum_x P(x)w(x) \leqslant 1,$$

so after multiplying the weights by $P(x)$, this condition corresponds exactly to the semimeasure requirement. Let us note that due to the computability of P, the lower semicomputability is conserved in both directions (multiplying or dividing by $P(x)$). More formally, the function

$$\sum_{x \sqsubseteq \omega} \frac{\mathbf{m}(x)}{P(x)}$$

is a lower semicomputable average-bounded test: its integral is exactly $\sum_x \mathbf{m}(x)$. On the other hand, every lower semicomputable test can be presented in terms of an increase of weights, and the limits of these weights, multiplied by $P(x)$, form a lower semicomputable semimeasure. (Note that the latter transformation is not unique: we can redistribute the weights among a string and its continuations without altering the sum over the infinite sequences.) □

Note that we used that both P (in the second part of the proof) and $1/P$ (in the first part) are lower semicomputable.

In Proposition 2.21, we can replace the sum with a least upper bound. This way, the following theorem connects three quantities, $\mathbf{t}_P$, the supremum and the sum, all of which are equal within a multiplicative constant.

Theorem 2.22. *We have* $\mathbf{t}_P(\omega) \stackrel{*}{=} \sup_{x \sqsubseteq \omega} \frac{\mathbf{m}(x)}{P(x)} \stackrel{*}{=} \sum_{x \sqsubseteq \omega} \frac{\mathbf{m}(x)}{P(x)}$, *or in logarithmic notation*

$$\mathbf{d}_P(\omega) \stackrel{+}{=} \sup_{x \sqsubseteq \omega} (-\log P(x) - Kp(x)). \tag{3}$$

Proof. The supremum is now smaller, so only the second part of the proof of Proposition 2.21 should be reconsidered.

The lower semicomputable function $\lceil \mathbf{d}_P(\omega) \rceil$ can be obtained as the supremum of a sequence of integer-valued basic functions of the form $k_i g_{x_i}(\omega)$, where $g_x(\omega) = 1_{x\Omega}(\omega) = 1$ if $x \sqsubseteq \omega$ and 0 otherwise. We can also require that if $i \neq j$, $x_i \sqsubseteq x_j$ then $k_i \neq k_j$: indeed, suppose $k_i = k_j$. If $i < j$ then we can delete the jth element, and if $i > j$, then we can replace $2^{k_i} g_{x_i}$ with the sequence of all functions $2^{k_i} g_z$ where z has the same length as x_j but differs from it. We have

$$2\mathbf{t}_P(\omega) \geqslant 2^{\lceil \mathbf{d}_P(\omega) \rceil} = \sup_i 2^{k_i} g_{x_i}(\omega) = \sup_{x_i \sqsubseteq \omega} 2^{k_i} \geqslant 2^{-1} \sum_{i : x_i \sqsubseteq \omega} 2^{k_i} = 2^{-1} \sum_i 2^{k_i} g_{x_i}(\omega).$$

The last inequality holds since according to our assumption, all the values k_i belonging to prefixes x_i of the same sequence ω are different, and the sum of different powers of 2 is at most twice larger than its largest element. Integrating by P, we obtain $4 \geqslant \sum_i 2^{k_i} P(x_i)$, hence $2^{k_i} P(x_i) \stackrel{*}{<} \mathbf{m}(x_i)$ by the maximality of $\mathbf{m}(x)$, so $2^{k_i} \stackrel{*}{<} \frac{\mathbf{m}(x_i)}{P(x_i)}$. We found

$$\mathbf{t}_P(\omega) \stackrel{*}{<} \sup_{i : x_i \sqsubseteq \omega} \frac{\mathbf{m}(x_i)}{P(x_i)} \leqslant \sup_{x \sqsubseteq \omega} \frac{\mathbf{m}(x)}{P(x)}.$$

□

Here is a reformulation:

$$\mathbf{d}_P(\omega) \stackrel{+}{=} \sup_n (-\log P(\omega(1:n)) - Kp(\omega(1:n))).$$

This reformulation can be generalized:

Theorem 2.23. *Let $n_1 < n_2 < \cdots$ be an arbitrary computable sequence of natural numbers. Then*

$$\mathbf{d}_P(\omega) \stackrel{+}{=} \sup_k (-\log P(\omega(1:n_k)) - Kp(\omega(1:n_k))).$$

The constant in the $\stackrel{+}{=}$ depends on the sequence n_k.

Proof. Every step of the proof of Theorem 2.22 generalizes to this case straightforwardly. □

This theorem has interesting implications of the case when instead of a sequence ω we consider an infinite two-dimensional array of bits. Then for the randomness deficiency, it is sufficient to compare complexity and probability of squares starting at the origin.

Historical digression

The above formula for randomness deficiency is a quantitative refinement of the following criterion.

Theorem 2.24 (Criterion of randomness in terms of prefix complexity)**.** *A sequence ω is random with respect to a computable measure P if and only if the difference $-\log P(x) - Kp(x)$ is bounded above for its prefixes.*

(Indeed, the last theorem says that the maximum value of this difference over all prefixes is exactly the average-bounded randomness deficiency.) This characterization of randomness was announced first, without proof, in [4], with the proof attributed to Schnorr. The first proof, for the case of a computable measure, appeared in [8].

The historically first clean characterizations of randomness in terms of complexity, by Levin and Schnorr independently in [15] and [22] have a similar form, but use complexity and a priori probability coming from a different kind of interpreter called "monotonic". (In the cited work, Schnorr uses a slightly different form of complexity, but later, he also adopted the version introduced by Levin.)

Definition 2.25 (Monotonic complexity)**.** Let us call to strings *compatible* if one is the prefix of the other. An enumerable subset $A \subseteq \{0,1\}^* \times \{0,1\}^*$ is called a *monotonic interpreter* if for every p, p', q, q', if $(p,q) \in A$ and $(p',q') \in A$ and p is compatible with p' then q is compatible with q'. For an arbitrary finite or infinite $p \in \{0,1\}^* \cup \Omega$, we define

$$A(p) = \sup\{\, x : \exists p' \sqsubseteq p \ (p', x) \in A \,\}.$$

The monotonicity property implies that this limit, also in $\{0,1\}^* \cup \Omega$, is well defined.

We define the (monotonic) complexity $Km_A(x)$ of a string x with respect to A as the length of a shortest string p with $A(p) \sqsupseteq x$. It is known that there is an *optimal* monotonic interpreter, where optimality has the same sense as above, for prefix complexity. We fix an optimal monotonic interpreter V and denote $Km(x) = Km_V(x)$. ⌟

Remark 2.26 (Oracle computation). A monotonic interpreter is a slightly generalized version of what can be accomplished by a Turing machine with a one-way read-only input tape containing the finite or infinite string p. The machine also has a working tape and a one-way output tape. In the process of work, on this

tape appears a finite or infinite sequence $T(p)$. The work may stop, if the machine halts or passes beyond the limit of the input word; it may continue forever otherwise. It is easy to check that the map $p \mapsto T(p)$ is a monotonic interpreter (though not all monotonic interpreters correspond to such machines, resulting in a somewhat narrower class of mappings).

These machines can be viewed as the definition of what we will later call *oracle computation*: namely, a computation that uses p as an oracle.

In our applications, such a machine would have the form $T(p,\omega)$ where the machine works on both infinite strings p and ω as input, but considers p the oracle and ω the string it is testing for randomness.

The class of mappings is narrower indeed. Let S be an undecidable recursively enumerable set of integers. Set $T(0^n1) = 0$ for all $n \in S$, and $T(0^n10) = 0$ for all n. Now after reading 0^n1, the machine T has to decide whether to output a 0 before reading the next bit, which is deciding the undecidable set S. It is unknown to us whether this class of mappings yields also a different monotonic complexity. ⌟

A monotonic interpreter will also give rise to something like a distribution over the set of finite and infinite strings.

Definition 2.27. Let us feed a monotonic interpreter A a sequence of independent random bits and consider the output distribution on the finite and infinite sequences. Denote $M_A(x)$ the probability that the output sequence begins with x. Denote $KM_V(x) = -\log M_V(x)$.

Recall that Λ denotes the empty string. A function $\mu : \{0,1\}^* \to [0,1]$ is called a *continous semimeasure* over the Cantor space Ω if $\mu(\Lambda) \leqslant 1$ and $\mu(x) \geqslant \mu(x0) + \mu(x1)$ for all $x \in \{0,1\}^*$. ⌟

It is easy to check that $M_V(x)$ is a lower semicomputable continuous semimeasure. The proposition below is similar in form to the Coding Theorem (Proposition 2.20) above, only weaker, since it does not connect to the complexity $Km(x)$ defined in terms of shortest programs. (It cannot, as shown in [9].)

Proposition 2.28. *(see [29])*

(a) *Every lower semicomputable continuous semimeasure is the output distribution of some monotonic interpreter.*

(b) *Among lower semicomputable continuous semimeasures, there is one that is maximal within a multiplicative constant.*

Definition 2.29 (Continuous a priori probability)**.** Let us fix a maximal lower semicomputable continuous semimeasure and denote it $M(x)$. We call $M(x)$ sometimes the *continuous a priori probability*, or *apriori probability on a tree*. ⌟

Now, the characterization by Levin (and a similar one by Schnorr) is the following. Its proof, technically not difficult, can be found in [6, 18, 25].

Proposition 2.30. *Let P be a computable measure over Ω. Then the following properties of an infinite sequence ω are equivalent.*

(i) *ω is random with respect to P.*

(ii) $\limsup_{x\sqsubset\omega} -\log P(x) - Km(x) < \infty$.

(iii) $\liminf_{x\sqsubset\omega} -\log P(x) - Km(x) < \infty$.

(iv) $\limsup_{x\sqsubset\omega} -\log P(x) - KM(x) < \infty$.

(v) $\liminf_{x\sqsubset\omega} -\log P(x) - KM(x) < \infty$.

Theorem 2.24 proved above adds to this a next equivalent characterization, namely that $-\log P(x) - Kp(x)$ is bounded above. It is different in nature from the one in Proposition 2.30: indeed, the expressions $-\log P(x) - Km(x)$ and $-\log P(x) - KM(x)$ are *always bounded from below* by a constant depending only on the measure P (and not on x or ω), while $-\log P(x) - Kp(x)$ is not.

Moreover, in the latter we cannot replace lim sup with lim inf, as the following example shows. Note that we can add to every word x some bits to achieve $Kp(y) \geqslant |y|$ (where $|y|$ is the length of word y). Indeed, if this was not so, then for the continutations of the word we would have $\mathbf{m}(y) \geqslant 2^{-|y|}$, and the sum $\sum_y \mathbf{m}(y)$ would be infinite. Let us build a sequence, adding alternatingly long stretches of zeros to make the complexity substantially less than the length, then bits that again bring the complexity up to the length (as shown, this is always possible). Such a sequence will not be random with respect to the uniform measure (since the lim sup of the difference is infinite), but has infinitely many prefixes for which the complexity is not less than the length, making the lim inf finite.

The following statement is interesting since no direct proof of it is known: the proof goes through Theorem 2.23, and noting that since the permutation of terms of the sequence does not change the coin-tossing distribution, it does not change the notion of randomness. More general theorems of this type, under the name of *randomness conservation*, can be found in [16, 17, 10].

Corollary 2.31. *Consider the uniform distribution (coin-tossing) P over binary sequences. The maximal difference between $|x|$ and $Kp(x)$ for prefixes x of a random sequence is invariant (up to a constant) under any computable permutation of the sequence terms. (The constant depends on the permutation, but not on the sequence.)*

Here is another corollary, a reformulation of Proposition 2.21:

Corollary 2.32 (Miller-Yu "ample excess" lemma)**.** *A sequence ω is random with respect to a computable measure P if and only if*

$$\sum_{x \sqsubset \omega} 2^{-\log P(x) - Kp(x)} < \infty.$$

This corollary also implies the fact mentioned above already:

Corollary 2.33. *Every finite sequence x has an extension y with $Kp(y) > |y|$.*

Proof. Take ω random, then $x\omega$ is random, and therefore by the Miller-Yu lemma $x\omega$ has arbitrarily long prefixes whose complexity is larger than the length. □

2.5 Game interpretation

The formula for the average-bounded deficiency can be interpreted in terms of the following game. Alice and Bob make their moves having no information about the opponent's move. Alice chooses an infinite binary sequence ω, Bob chooses a finite string x. If x turns out to be a prefix of ω, then Alice pays Bob 2^n where n is the length of x. (This version of the game corresponds to the uniform Bernoulli measure, in the general case Alice pays $1/P(x)$.) Recall the game-theoretic notions of *pure* strategy, as a deterministic choice by a player, and *mixed* strategy, as a probability distribution over deterministic choices.

Bob has a trivial strategy (choosing the empty string) that guarantees him 1 whatever Alice does. Also Alice has a mixed strategy (the uniform distribution, or, in general case, P) that guarantees her the average loss 1 whatever Bob does. Bob can devise a strategy that will benefit him in case (for whatever reason) Alice brings a nonrandom sequence.

A randomized algorithm that has no input and produces a string (or nothing) can be considered a mixed strategy for Bob (if the algorithm does not produce anything, Bob gets no money). For any such algorithm D the expected payment

(if Alice produces ω according to distribution P) does not exceed 1. Therefore, the set of sequences ω where the expected payment (averaged over Bob's random bits) is infinite, is a null set. Observe the following:

(i) For every probabilistic strategy of Bob, his expected gain (as a function of Alice's sequence) is an average-bounded test. (From here already follows that this expected value will be finite, if Alice's sequence is random in the sense of Martin-Löf.)

(ii) If $m(x)$ is the probability of x as Bob's move with algorithm D, his expected gain against ω is equal to

$$\sum_{x \sqsubseteq \omega} m(x)/P(x).$$

(iii) Therefore if we take the algorithm outputting the discrete apriori probability $\mathbf{m}(x)$, then Bob's expected gain will be a universal test (by the proved formula for the universal test).

Using the apriori probability as a mixed strategy enables Bob to punish Alice with an infinite penalty for any non-randomness in her sequence.

One can consider more general strategies for Bob: he can give for a pure strategy, not only a string x, but some basic function f on Ω with non-negative values. Then his gain for the sequence ω brought by Alice is set to $f(\omega)/\int f(\omega)\,dP$. (The denominator makes the expected return equal to 1.) To the move x corresponds the basic function that assigns $2^{|x|}$ to extensions of x and zero elsewhere. This extension does not change anything, since this move is a mixed strategy and we allow Bob to mix his strategies anyway. (After producing f, Bob can make one more randomized step and choose some of the intervals on which f is constant, with an appropriate probability.) In this way we get another formula for the universal test:

$$\mathbf{t}_P(\omega) \stackrel{*}{=} \sum_f \frac{\mathbf{m}(f) f(\omega)}{\int f(\omega)\,dP},$$

where the sum is taken over all basic functions f. This formula might be useful in more general situations (not Cantor space) where we do not work with intervals and consider some class of basic functions instead.

On concluding this part let us point to a similar game-theoretical interpretation of probability theory developed in the book [24] of Shafer and Vovk. There, the randomness of an object is not its property but, roughly speaking, a kind of guarantee with which it is being sold.

3 From tests to complexities

Formula (3) expresses the randomness deficiency (the logarithm of the universal test) of an infinite sequence in terms of complexities of its finite prefixes. A natural question arises: can we go in the other direction? Is it possible to express the complexity of a finite string x, or some kind of "randomness deficiency" of x, in terms of the deficiencies of x's infinite extensions? Proposition 2.6 and the discussion following it already brought us from infinite sequences to finite ones. This can also be done for the universal test:

Definition 3.1. Fix some computable measure P, and let t be any (average-bounded) test for P. For any finite string x let $\bar{t}(x)$ be the minimal deficiency of all infinite extensions of x:

$$\bar{t}(x) = \inf_{\omega \sqsupseteq x} t(\omega).$$

⌟

By Proposition 2.7, $\bar{t}$ is a lower semicomputable function defined on finite strings, and the function t can be reconstructed back from $\bar{t}$; so if $\mathbf{t}_P$ is our fixed universal test then $\bar{\mathbf{t}}_P$ can be considered as a version of randomness deficiency for finite strings.

The intuitive meaning is clear: a finite sequence z looks non-random if *all* infinite sequences that have prefix z look non-random.

Question 2. *Kolmogorov [13] had a somewhat similar suggestion: for a given sequence z we may consider the minimal deficiency (with respect to the uniform distribution, defined as a difference between length and complexity) of all its* finite *extensions. Are there any formal connections?*

Let us spell out what we found, in more general terms.

Definition 3.2 (Extended test for a computable measure)**.** A lower semicomputable, monotonic (with respect to the prefix relation) function $T : \{0,1\}^* \to [0,\infty]$ is called an *extended test* for computable measure P if for all N the average over words of length N is bounded by 1:

$$\sum_{x:|x|=N} P(x)T(x) \leqslant 1.$$

⌟

Monotonicity guarantees that the sum over words of a given length can be replaced by the sum over an arbitrary finite (or even infinite) prefix-free set S:

$$\sum_{x\in S} P(x)T(x) \leqslant 1. \tag{4}$$

(Indeed, extend the words of S to some common greater length.)

Proposition 3.3. *Every extended test generates (in the sense of Definition 2.5) some averge-bounded test on the infinite strings. Conversely, every average-bounded test on the infinite sequences is generated by some extended test.*

Proof. The first part follows immediately from the definition (and the theorem of monotone convergence under the integral sign). In the opposite direction, we can set for example $T(x) = \bar{t}(x)$, or refer to Proposition 2.4 if we do not want to rely on compactness. □

The existence of a universal extended test is proved by the usual methods:

Proposition 3.4. *Among the extended tests $T(x)$ for a computable measure $P(x)$ there is a maximal one, up to a multiplicative constant.*

Definition 3.5. Let us fix some dominating extended test and call it the *universal* extended test. ⌟

Proposition 3.6. *The universal extended test coincides with $\bar{\mathbf{t}}_P(x)$ to within a bounded factor.*

Proof. Since $\bar{\mathbf{t}}_P$ is an extended test, it is not greater than the universal test (to within a bounded factor). On the other hand, the universal extended test generates a test on the infinite sequences, it just remains to compare it with the maximal one. □

If our space is not compact (say, it is the set of infinite sequences of integers), then $\bar{\mathbf{t}}_P(x)$ is not defined, but there is still a universal extended test, which we will denote by $\mathbf{t}_P(x)$.

Warning: not all extended tests generating $\mathbf{t}_P(\omega)$ are maximal. (For example, one can make the test equal to zero on all short words, transferring its values to its extensions.)

The advantage of the function $\mathbf{t}_P(x)$ is that it is defined on finite strings, the condition (4) (for finite sets S) imposed on it is also more elementary than the integral condition, but clearly implies that it generates a test.

The method just shown is not the only way to move to tests on prefixes from tests on infinite sequences:

Definition 3.7. Assume that the computable measure P is positive on all intervals: $P(x) > 0$ for all x. Let $\hat{\mathbf{t}}_P(x)$ be the conditional expected value of $\mathbf{t}_P(\omega)$ if a random variable $\omega \in \Omega$ has distribution P and the condition is $\omega \sqsupseteq x$. In other terms: let $\hat{\mathbf{t}}_P(x)$ be the average of $\mathbf{t}_P$ on the interval $x\Omega$, that is let $\hat{\mathbf{t}}_P(x) = U(x)/P(x)$ where

$$U(x) = \int_{x\Omega} \mathbf{t}_P(\omega)\, dP(\omega).$$

⌟

The function U is a lower semicomputable semimeasure. (It is even a measure, but the measure is not guaranteed to be computable and the measure of the entire space Ω is not necessarily 1. In other words, we get a measure on Ω that has density $\mathbf{t}_P$ with respect to P.) This implies that the function $\hat{\mathbf{t}}_P(x)$ is a martingale, according to the following definition.

Definition 3.8. A function $g : \{0,1\}^* \to \mathbb{R}$ is called a *martingale* with respect to the probability measure P if

$$P(x)g(x) = P(x0)g(x0) + P(x1)g(x1).$$

It is a *supermartingale* if at least the inequality $\geqslant$ holds here. ⌟

Note that, as a martingale, the function $\hat{\mathbf{t}}_P(x)$ is *not* monotonically increasing with respect to the prefix relation.

Theorem 3.9.

$$\frac{\mathbf{m}(x)}{P(x)} \stackrel{*}{<} \mathbf{t}_P(x) \stackrel{*}{<} \hat{\mathbf{t}}_P(x) \stackrel{*}{<} \frac{M(x)}{P(x)}, \tag{5}$$

where $\mathbf{m}$ *is the a priori probability on strings as isolated objects (whose logarithm is minus prefix complexity) and* M *is the a continuous priori probability as introduced in Definition 2.29.*

Proof. In fact, the first inequality can be made stronger: we can replace $\mathbf{m}(x)/P(x)$ by $\sum_{t \sqsubseteq x} \mathbf{m}(t)/P(t)$. Indeed, this sum is a part of the expression for $\mathbf{t}_P(\omega)$ for every ω that starts with x.

The second inequality uses Proposition 3.6 and relates the minimal and average values of a random variable. The third inequality just compares the lower semicomputable semimeasure $U(x)$ and the maximal semimeasure $M(x)$. □

Note that while $\hat{\mathbf{t}}_P(x)$ is a martingale, $\frac{M(x)}{P(x)}$ is a supermartingale: it is actually maximal within multiplicative constant, among the lower semicomputable supermartingales for P.

Remarks 3.10. 1. We may insert

$$\stackrel{*}{<} \max_{t \sqsubseteq x} \frac{\mathbf{m}(t)}{P(t)} \stackrel{*}{<} \sum_{t \sqsubseteq x} \frac{\mathbf{m}(t)}{P(t)} \stackrel{*}{<} \tag{6}$$

between the first and the second terms of (5).

2. Using the logarithmic scale, we get

$$-\log P(x) - Kp(x) \stackrel{+}{<} \log \mathbf{t}_P(x) \stackrel{+}{<} \log \hat{\mathbf{t}}_P(x) \stackrel{+}{<} -\log P(x) - KM(x).$$

3. The Measure U depends on P (recall that U is a maximal measure that has density with respect to P), so for different P's, for example with different supports, like the Bernoulli measures with different parameters, we get different measures. But this dependence is bounded by the inequality above: it shows that the possible variations do not exceed the difference between $Kp(x)$ and $KM(x)$.
4. The rightmost inequality cannot be replaced by an equality. For example, let P be the uniform (coin-tossing) measure. Then the value of $U(x)$ tends to 0 when x is an increasing prefix of a computable sequence (we integrate over decreasing intervals whose intersection is a singleton that has zero uniform measure). On the other hand, the value $M(x)$ is bounded by a positive constant for all these x.
5. We used compactness (the finiteness of the alphabet $\{0,1\}$) in proving Proposition 2.7. But we could have used Proposition 2.6 and the discussion following it for a starting point, obtaining analogous results for the Baire space of infinite sequences of natural numbers.

⌟

All quantities listed in Theorem 3.9 can be used to characterize randomness: a sequence ω is random if the values of the quantity in question are bounded for its prefixes. Indeed, the Levin-Schnorr theorem guarantees that for a random sequence the right-hand side is bounded, and for a non-random one the left-hand side is unbounded. The monotonicity of the second term guarantees that all expressions except the first one tend to infinity. As we already mentioned above, one cannot say this about the first quantity.

Question 3. *Some quantities used in the theorem ($\mathbf{t}_P(x)$ and two added ones in (6)) are monotonic (with respect to the prefix partial order of x) by definition. We have seen that $\hat{\mathbf{t}}_P(x)$, as a martingale, is not monotonic. What can be said about $\frac{M(x)}{P(x)}$?*

All these quantities are "almost monotonic" since they do not differ much from the monotonic ones.

4 Bernoulli sequences

One can try to define randomness not only with respect to some fixed measure but also with respect to some family of measures. Intuitively a sequence is random if we can believe that it is obtained by a random process that respects *one of* these measures. As we show later, this definition can be given for any *effectively compact* class of measures. But to make it more intuitive, we start with a specific example: *Bernoulli measures*.

4.1 Tests for Bernoulli sequences

The Bernoulli measure B_p arises from independent tossing of a non-symmetric coin, where the probability of success p is some real number in $[0,1]$ (the same for all trials). Note that we do not require p to be computable.

Definition 4.1 (Average-bounded Bernoulli test)**.** A lower semicomputable function t on infinite binary sequences is a *Bernoulli test* if its integral with respect to any B_p does not exceed 1. ⌟

Proposition 4.2 (Universal Bernoulli test)**.** *There exists a universal (maximal up to a constant factor) Bernoulli test.*

Proof. A lower semicomputable function is the monotonic limit of basic functions. If the integral of a given basic function with respect to every B_p is less or equal than 1 for all p, this fact can be established effectively (indeed, the integral is a polynomial in p with rational coefficients). This allows us to eliminate all functions unfit to be tests, and to list all Bernoulli tests. Adding these up with appropriate coefficients, we obtain a universal one. □

Definition 4.3. We fix a universal Bernoulli test and denote it $\mathbf{t}_{\mathscr{B}}(\omega)$. Its logarithm will be called *Bernoulli deficiency* $\mathbf{d}_{\mathscr{B}}(\omega)$. A sequence is called a *Bernoulli sequence* if its Bernoulli deficiency is finite. ⌟

Again, we may modify the definition to within an additive constant, to make it nonnegative and integer.

The informal motivation is the following: ω is a Bernoulli sequence if the claim that it is obtained by independent coin tossing (coin symmetry is not required) looks plausible. And this statement is not plausible if one can formulate some property that is true for ω but defines an "effectively Bernoulli null set" (we did not formally introduce this notion, but could, analogously to effective null sets).

Analogously to the case of computable measures, we can extend the class test to finite sequences:

Definition 4.4 (Extended Bernoulli test)**.** A lower semicomputable monotonic function $T : \{0,1\}^* \to [0,\infty]$ is called an *extended Bernoulli tests* if for all natural numbers N and for all $p \in [0,1]$ the inequality $\sum_{x:|x|=N} B_p(x)T(x) \leqslant 1$ holds. ⌟

As for computable measures, there is a connection between tests for finite and tests for infinite sequences:

Proposition 4.5. *Every extended Bernoulli test generates a Bernoulli test over* Ω*. On the other hand, every Bernoulli test over* Ω *is generated by some extended Bernoulli test.*

There is a dominating universal extended Bernoulli test: it generats a universal Bernoulli test on Ω. As earlier, we wil use the same notation $\mathbf{t}_{\mathscr{B}}$ for the maximal tests on the finite and on the infinite sequences. Of course, it generates a universal Bernoulli test.

4.2 Other characterizations of the Bernoulli property

Just as for the randomness with respect to computable measures, several equivalent definitions exist. One may consider probability-bounded tests (the probability of the event $t(\omega) > N$ on any of the measures B_p must be not greater than $1/N$). One may call a test, following Martin-Löf's definition for the computable measures, any computable sequence of effectively open sets U_i with

$B_p(U_i) \leqslant 2^{-i}$ for all i and all $p \in [0,1]$. All these variant definitions are equivalent (and this is proved just as for randomness with respect to a computable measures).

Notation 4.6. Let $\mathbb{B}(n,k)$ denote the set of binary strings of length n with k ones (and $n-k$ zeroes). ⌟

Martin-Löf defined a Bernoulli test as a family of sets of words $U_1 \supseteq U_2 \supseteq U_3 \supseteq \cdots$; each of these sets is hereditary upward, that is for every word contains all of its extensions. The following restriction is made on these sets: consider arbitrary integer $n \geqslant 0$ and k from 0 to n; it is required that for all i the share of words in $\mathbb{B}(n,k)$ belonging to U_i is not greater than 2^{-i}.

For convenience of comparison let us replace the sets U_i with an integer-valued lower semicomputable function d for which $U_i = \{\, x : d(i) \geqslant i \,\}$. The hereditary property of the sets U_i implies the monotonicity of this function d with respect to the prefix relation. Besides this, it is required that the event $d \geqslant i$ within each set $\mathbb{B}(n,k)$ is not greater than 2^{-i}. Clearly, these requirements correspond to probability-bounded extended tests (in the logarithmic scale), only in place of the class B_p on words of length n another set of measures is considered, those concentrated on words of a given length with a given number of ones. The measures in the class B_p take equal values on words of equal lengths with equal number of ones, and are therefore representable by a mixture of uniform measures on $\mathbb{B}(n,k)$ with some coefficients. Replacing B_p with these measures, the condition becomes stronger.

Let us show that nonetheless, the set of Bernoulli sequences does not change from such a replacement; moreover, the universal test (as a function on infinite sequences) does not change (as usual, to within a bounded factor). We will show this for the average-bounded variant of tests (changing Martin-Löf's definition accordingly); this does not change the class of Bernoulli sequences. The reasoning is analogous for the probability-bounded tests.

Definition 4.7. A *combinatorial Bernoulli test* is a function $f : \{0,1\}^* \to [0,\infty]$ with the following constraints:

(a) It is lower semicomputable.

(b) It is monotonic with respect to the prefix relation.

(c) For all integer n,k with $0 \leqslant k \leqslant n$ the average of the function f on the set $\mathbb{B}(n,k)$ remains below 1:

$$|\mathbb{B}(n,k)|^{-1} \sum_{x \in \mathbb{B}(n,k)} f(x) \leqslant 1. \tag{7}$$

⌟

The last condition says that not only is the average of $f(x)$ bounded by 1 over the set $\{0,1\}^n$, as in extended tests for the unbiased coin-tossing measure, but its average is bounded by 1 separately in each set $\mathbb{B}(n,k)$ whose union is $\{0,1\}^n$.

Having such a test for words of bounded length, it can be continued by monotonicity:

Proposition 4.8. *If a combinatorial Bernoulli test $f(x)$ is given on strings x of length less than n, then extending it to longer strings using monotonicity we get a function that is still a combinatorial Bernoulli test.*

Proof. We extend f to words of length n, setting $f(x0) = f(x1) = f(x)$ for words x of length $n-1$. The set $\mathbb{B}(n,k)$ consists of two parts: words ending on zero and words ending on one. The first ones are in a one-to-one correspondence with $\mathbb{B}(n-1,k)$, the second ones with $\mathbb{B}(n-1,k-1)$. The function conserves the values in this correspondence, therefore the average in both parts is not greater than 1. Hence, the average over the whole $\mathbb{B}(n,k)$ is not greater than 1. □

The following is obtained by standard methods:

Proposition 4.9 (Universal combinatorial Bernoulli test)**.** *Among combinatorial Bernoulli tests, there is one that is maximal to within a bounded factor.*

Definition 4.10. Let us fix a universal combinatorial Bernoulli test $\mathbf{b}(x)$ and extend it to infinite sequences ω by

$$\mathbf{b}(\omega) = \sup_{x \sqsubseteq \omega} \mathbf{b}(x).$$

We will call the function obtained this way a universal combinatorial test on Ω and will denote it also by $\mathbf{b}$. ⌟

(By monotonicity, the least upper bound in this definition can be replaced with a limit.) Let us show that the this test coincides (to within a bounded factor) with the Bernoulli tests introduced earlier in Definition 4.3.

Theorem 4.11. $\mathbf{b}(\omega) \stackrel{*}{=} \mathbf{t}_{\mathscr{B}}(\omega)$.

Proof. We have already seen that $\mathbf{b}(x)$ is an extended Bernoulli test (from the bounds on the average on each part $\mathbb{B}(n,k)$ follows the bound on the expected value by the measure B_p, since this measure is constant on each part). Consequently $\mathbf{b}(\omega) \stackrel{*}{<} \mathbf{t}_{\mathscr{B}}(\omega)$.

The converse is not true: an extended Bernoulli test may not be a combinatorial test. But it is possible to construct a combinatorial test that takes the same values (to within a bounded factor) on the infinite sequences, and only this is asserted in the theorem.

Here is the idea. Consider an extended Bernoulli test t on words of length n and transfer it to words of much greater length N (applying the old test to its beginnings of length n). We obtain a certain function t'. We have to show that t' is close to some combinatorial test (that is only exceeds it by a constant factor). For this, t' must be averaged over the set $\mathbb{B}(N,K)$ for an arbitrary K between 0 and N. In other words, we must average t by the probability distribution on the n-bit prefixes of sequences of length N containing K ones. With $N \gg n$ this distribution will be close to the Bernoulli one with distribution $p = K/N$.

In terms of elementary probability theory, we have an urn with N balls, K of which is black, and take out from it n balls. We must compare the probability distribution with the Bernoulli one that would have been obtained at sampling with replacement. Let us show that

> *for $N = n^2$ the distribution without replacement does not exceed the one with replacement more than $O(1)$ times.*

(The inequality does not hold in the other direction: for $K = 1$ without replacement we cannot obtain a word with two ones, and with replacement we can. But we only need the inequality in the given direction.)

Indeed, in sampling without replacement the probability that a ball of a given color will be drawn is equal to the quotient

$$\frac{\text{the number of remaining balls of this color}}{\text{the number of all remaining balls}}.$$

The number of balls of this color is not more than in the case with replacement, on the other hand the denominator is at least $N-n$. Therefore the probability of any combination during sampling with replacement is at most the probability of the same combination with replacement, multiplied by $N/(N-n)$ to the power n. For $N = n^2$ the multiplier $(1+O(1/n))^n = O(1)$ is obtained.

This way, taking the extended Bernoulli test t and then defining $t'(x)$ on a word x of length N as t on the prefix of x of length $\lfloor\sqrt{N}\rfloor$, the obtained function t' will be a combinatorial test to within a bounded factor. (Note that its monotonicity follows from that of t.) □

4.3 Criterion for Bernoulli sequences

It is natural to compare the notion of Bernoulli sequence (those sequences for which the Bernoulli test is finite) with the notion of a sequence random with respect to the measure B_p. But Martin-Löf definition of randomness assumes that the measure is computable. Therefore it cannot be applied directly to B_p if p is non-computable. But this definition can be relativized, and if (the binary expansion of) p is given as an oracle (see Remark 2.26), then the measure B_p becomes computable and randomness is well defined. The following theorem supports an intuitive idea of Bernoulli sequence as a sequence that is random with respect to some Bernoulli measure:

Theorem 4.12. *A sequence ω is a Bernoulli sequence if and only if it is random with respect to some measure B_p, with oracle $p \in [0,1]$.*

By "with oracle p", we understand the possiblity to obtain from each i the ith bit in the binary expansion of the real number p (which is essentially unique, except in those cases when p is binary-rational, and in these cases both expansions are computable, and the oracle is trivial).

Before proving the theorem (even in a stronger quantitative form), we introduce a new notion, of a test depending explicitly on the parameter p of the Bernoulli measure B_p, which later will be extended to arbitrary (not just Bernoulli) measures. The required result will be obtained as the combination of the following claims:

(a) Among the "uniform" randomness tests, there exists a maximal test $\mathbf{t}(\omega, p)$.

(b) The function $\omega \mapsto \inf_p \mathbf{t}(\omega, p)$ coincides (as usual, to within a bounded factor) with the universal Bernoulli test.

(c) For a fixed p, the function $\omega \mapsto \mathbf{t}(\omega, p)$ coincides (to the same precision) with the maximal randomness test for the (p-computable) measure B_p, relativized to p.

These three assertions imply Theorem 4.12 easily: sequence ω is Bernoulli, if the Bernoulli test is finite; the latter is equal to the greatest lower bound of $\mathbf{t}(\omega, p)$,

hence its finiteness means $\mathbf{t}(\omega, p) < \infty$ for some p, which is equivalent to the relativized randomness with respect to the measure B_p.

We need some technical preparation. The randomness tests (as functions of two variables) will also be lower semicomputable, but the definition of this concept needs to be extended, since an additional real parameter is involved. (In what follows we will also consider a more general situation, in which the second argument is a measure.)

Definition 4.13. In the space $\Omega \times [0,1]$, let us call *basic rectangles* all sets of the form $x\Omega \times (u,v)$, where $u < v$ are rational numbers. (A technical point: we allow u, v to be outside $[0,1]$, but in this case the rectangle we mean is $x\Omega \times ([0,1] \cap (u,v))$.)

A function $f : \Omega \times [0,1] \to [-\infty, \infty]$ is called *lower semicomputable* if there is an algorithm that, given a rational r on its input, enumerates a sequence of basic rectangles whose union is the set of all pairs (ω, p) with $f(\omega, p) > r$.

The notion of *upper semicomputability* is defined analogously, and is equivalent to the lower semicomputablity of $(-f)$.

A function with finite real values is called *computable* if it is both upper and lower semicomputable. ⌟

This definition, as earlier, requires that the preimage of $(-\infty, r)$ be an effective open set uniformly in r, only now we consider effectively open sets in $\Omega \times [0,1]$, defined in a natural way.

Since the intersection of effective open sets is effective open, the following—more intuitive—formulation is obtained for computability:

Proposition 4.14. *A real function $f : \Omega \times [0,1] \to \mathbb{R}$ is computable if and only if for every rational interval (u,v) its preimage is the union of a sequence of basic rectangles that are effectively enumerated, uniformly in u and v.*

The intuitive meaning of this characterization will become clearer after observing that to "give approximations to α with any given precision" is equivalent to "enumerate all intervals containing α". Therefore for a computable function f we can find approximations to $f(\omega, p)$, if we are given appropriate approximations to ω and p.

We can reformulate the definition of (non-negative) lower semicomputable function, introducing the notion of basic functions. It is important for us that the basic functions are continuous, therefore the dependence on the real argument will be piecewise linear, without jumps.

Definition 4.15 (Basic functions, Bernoulli case)**.** We define an enumerated list of *basic* functions $\mathscr{E} = \{e_1, e_2, \dots\}$ over the set $\Omega \times [0,1]$ as follows. For $x \in \{0,1\}^*$, positive integer k and rational numbers u, v with $u + 2^{-k} < v - 2^{-k}$ define the function $g_{x,u,v,k}(\omega, p)$ as follows. If $x \not\sqsubseteq \omega$, then it is 0. Otherwise, its value does not depend on ω and depends piecewise linearly on p: it is 0 if $p \notin (u,v)$ and 1 if $u + 2^{-k} \leqslant p \leqslant v - 2^{-k}$, and varies linearly in between. Now $\mathscr{E}$ is the smallest set of functions containing all $g_{x,u,v,k}$, and closed under maxima, minima and rational linear combination. ⌟

Now lower semicomputable functions admit the following equivalent characterization:

Proposition 4.16. *A function $f : \Omega \times [0,1] \to [0,\infty]$ is lower semicomputable if and only if it is the pointwise limit of an increasing computable sequence of basic functions. (It follows that basic functions are computable.)*

Proof. This would be completely clear if for basic functions we also allowed the indicator functions of basic rectangles and the maxima of such functions. But we want the basic functions to be continuous (this will be important in what follows). One must note therefore that for $k \to \infty$ the function $g_{x,u,v,k}$ converges to the indicator function of a rectangle. □

The continuity of the basic functions guarantees the following important property:

Proposition 4.17. *Let $f : \Omega \times [0,1] \to \mathbb{R}$ be a basic function. The integral $\int f(\omega, p)\, B_p(d\omega)$ is a computable function of the parameter p, uniformly in the code of the basic function f.*

(Computability is understood in the above described sense; we remark that every computable function is continuous. An analogous statement holds for an arbitrary computable function f, not only for basic functions, but we do not need this.)

The following fact, proved in [12], will be used in the present paper a number of times, also in generalizations, but with essentially the same proof.

Proposition 4.18 (Trimming)**.** *Let $\varphi : \Omega \times [0,1] \to [0,\infty]$ be a lower semicomputable function. There is a lower semicomputable function $\varphi'(\omega, p)$ not exceeding $\varphi(\omega, p)$ with the property that for all p:*

(a) $\int \varphi'(\omega, p) B_p(d\omega) \leqslant 2$;

(b) *If* $\int \varphi(\omega,p)B_p(d\omega) \leqslant 1$ *then* $\varphi'(\omega,p) = \varphi(\omega,p)$ *for all* ω.

Proof. By Proposition 4.16, we can represent $\varphi(\omega,p)$ as a sum of a series of basic functions $\varphi(\omega,p) = \sum_n h_n(\omega,p)$. The integral $\int \sum_{i\leqslant n} h_i(\omega,p)B_p(d\omega)$ is computable by Proposition 4.17, as a function of p (uniformly in n), therefore the set S_n of all p where this integral is less than 2 is effectively open, uniformly in n.

Define now $h'_n(\omega,p)$ as $h_n(\omega,p)$ for all $p \in S_n$, and 0 otherwise. The function $h'_n(\omega,p)$ is lower semicomputable, and the integral $\int \sum_{i\leqslant n} h'_i(\omega,p)B_p(d\omega)$ will be less than 2 for all p. Defining $\varphi' = \sum_n h'_n$ we obtain a lower semicomputable function, and the theorem on the integral of monotonic limits gives that $\int \varphi'(\omega,p)B_p(d\omega)$ is less than 2 for all p.

It remains to note that if for some p the integral $\int \varphi(\omega,p)B_p(d\omega)$ does not exceed 1, then this p enters all sets S_n, and the change from h_n to h'_n as well as the change from φ to φ' does not change it. □

Now we are ready to introduce tests depending explicitly on p:

Definition 4.19. A *uniform test for Bernoulli measures* is a function t of two arguments $\omega \in \Omega$ and $p \in [0,1]$; informally, $t(\omega,p)$ measures the amount of nonrandomness ("regularity") in the sequence ω with respect to distribution B_p. We require the following:

(a) $t(\omega,p)$ is lower semicomputable jointly as a function of the pair (ω,p).

(b) For every $p \in [0,1]$ the expected value of $t(\omega,p)$ (that is $\int t(\omega,p)B_p(d\omega)$) does not exceed 1.

⌟

It remains to prove the three assertions promised earlier:

Lemma 4.20. *There exists a universal uniform test* $\mathbf{t}(\omega,p)$*, that is a test that multiplicatively dominates all uniform tests for Bernoulli measures.*

Lemma 4.21. *For the universal uniform test* $\mathbf{t}$ *of lemma 4.20, the function* $\mathbf{t}'(\omega) = \inf_p \mathbf{t}(\omega,p)$ *coincides (to within a bounded factor in both directions) with the universal Bernoulli test of Definition 4.3.*

This lemma implies that ω is a Bernoulli sequence iff $\mathbf{t}'(\omega)$ is finite, that is $\mathbf{t}(\omega,p)$ is finite for some $p \in [0,1]$.

Lemma 4.22. *For a fixed p the function $\mathbf{t}_p(\omega) = \mathbf{t}(\omega, p)$ coincides (to within a bounded factor) with the universal randomness test with respect to B_p relativized with oracle p.*

Proof of Lemma 4.20. Generate all lower semicomputable functions; using Proposition 4.18, they can be then trimmed to guarantee that all expectations do not exceed, say, 2, and all uniform tests should get through unchanged. Sum up all the trimmed functions with coefficients whose sum is less than $1/2$. □

Proof of Lemma 4.21. Let us show that $\mathbf{t}'(\omega)$ is a universal Bernoulli test. The integral of this function with respect to B_p does not exceed 1 since this function does not exceed $\mathbf{t}(\omega, p)$ for that p. The statement that this function is lower semicomputable (as a function of ω) is analogous to Proposition 2.7, and the proof is also analogous, relying on compactness. Both are special cases of the general theorem given in Proposition 7.20.

Therefore the function $\inf_p \mathbf{t}(\omega, p)$ is a Bernoulli test. The universality (maximality) follows obviously, since any Bernoulli test can be considered a uniform Bernoulli test of two variables that does not depend on variable p. □

Proof of Lemma 4.22. Consider first the case when p is a computable real number. Then the function $\mathbf{t}_p\colon \omega \mapsto \mathbf{t}(\omega, p)$ (where $\mathbf{t}$ is a uniform randomness test for Bernoulli measures) is lower semicomputable (we can enumerate all intervals that contain p and combine then with an algorithm for $\mathbf{t}$; in this way we represent $\mathbf{t}_p$ as the least upper bound of the computable sequence of basic functions).

A similar argument works for an arbitary p and shows that $\mathbf{t}_p$ is lower semicomputable with a p-oracle. Thus, $\mathbf{t}_p$ does not exceed the universal relativized test with respect to B_p.

The reverse implication is a bit more difficult. Assume that t is a lower semicomputable (with oracle p) randomness test with respect to B_p. We need to find a uniform Bernoulli test t' that majorizes it (for a given p). This t' must be lower semicomputable, now (a subtle but important point) using p as an argument of the function t', not as an oracle. In other words, one has to extend a function defined initially only for a single p, to all values of p, while also guaranteeing the bound on the integral.

As a warmup consider the case of computable p. Then no oracle is needed, and t is lower semicomputable. Adding dummy variable p we get a lower semicomputable function of two arguments. But this function may not be a uniform test since its expectation with respect to B_q may be arbitrary if $q \neq p$. However, Proposition 4.18 helps transform it into a t' (which will now really depend on

q) with $\int t'(\omega,q)B_q(d\omega) \leqslant 2$ for all q and $t'(\cdot,p) = t(\cdot,p)$. Dividing t' into half provides a uniform test.

Now consider the case of noncomputable p. In this case p is irrational, so the bits of its binary expansion can be obtained from any sequence of decreasing rational intervals that converge to p. Therefore an oracle machine that enumerates approximations for t from below (having p as an oracle) can be transformed into a machine that enumerates from below some function $\tilde{t}(\omega,q)$, that coincides with $t(\omega)$ if $q = p$. The function $\tilde{t}$ may not be a uniform Bernoulli test (its expectations for $q \neq p$ can be arbitrary); but it again can be trimmed with the help of Proposition 4.18. □

5 Arbitrary measures over binary sequences

In this section, we generalize the theory to arbitrary measures, not only Bernoulli ones, but still stay in the space Ω of binary sequences.

Notation 5.1. The set of all probability measures over the space Ω is denoted by $\mathscr{M}(\Omega)$. (Recall that the measure of the whole space Ω is equal to 1.) ⌟

5.1 Uniform randomness tests

Definition 5.2 (Uniform tests)**.** A *uniform* test is a lower semicomputable function $t(\omega,P)$ of two arguments (ω is a sequence, P is a measure on Ω) with

$$\int t(\omega,P)\,P(d\omega) \leqslant 1$$

for every measure P. ⌟

However, we have to define carefully the notion of a lower semicomputability in this case. The set $\mathscr{M}(\Omega)$ of all measures is a closed subset of the infinite (countable) product

$$\Xi = [0,1] \times [0,1] \times [0,1] \times \cdots \tag{8}$$

(the measure is defined by the values $P(x)$ for all strings x; these values should satisfy the equations (2), so we get a closed subset).

Let us introduce basic open sets and computability notions for the set $\Omega \times \mathscr{M}(\Omega)$.

Definition 5.3. An (open) *interval* (basic open set) in the space of measures is given by a finite set of conditions of type $u < P(y) < v$ where y is some binary string and u, v are some rational numbers; the basic open set consists of the measures P that satisfy these conditions. A *basic open set* in $\Omega \times \mathscr{M}(\Omega)$ has the form $x\Omega \times \beta$, (product of intervals in Ω and $\mathscr{M}(\Omega)$) where β is a basic open set of measures. Now lower and upper semicomputability and computability are defined in terms of these basic open sets just as they were defined for $\Omega \times [0,1]$ in Definition 4.13. ⌟

In much of what follows, we will exploit the fact that, due to the finiteness of the alphabet $\{0,1\}$, the space Ω of infinite binary sequences is compact, and also the set of measures $\mathscr{M}(\Omega)$ is compact. Recall that a set C is compact if every cover of C by open sets contains a finite subcover. We need, however, an effective version of compactness:

Definition 5.4 (Effective compactness)**.** A compact subset C of $\mathscr{M}(\Omega)$ is called *effectively compact* if the set

$$\{S : S \text{ is a finite set of basic open sets and } \bigcup_{E \in S} E \supseteq C\}$$

is enumerable. ⌟

The set $\mathscr{M}(\Omega)$ itself is, as it is easy to see, compact and effectively compact. It is compact, as said above, as a closed set in the product of compact spaces, and the effectivity follows from the fact that we can check whether some given basic sets cover the whole space (we are dealing with linear equations and inequalities in a finite number of variables, where everything is algorithmically decidable). From here, it also follows:

Proposition 5.5. *Every effectively closed subset of $\mathscr{M}(\Omega)$ is effectively compact.*

Proof. Let an effectively closed subset C of $\mathscr{M}(\Omega)$. be the complement of the union of a list $B_1, B_2, \ldots$ of basic open sets. Then a finite set S of basic open sets covers C if and only if together with a finite set of the B_i, it covers the whole space. And this property is decidable. □

Effective compactness implies effective closedness. This follows from the following two properties of our space and our basic open sets:

(a) For every closed set F and every point x outside F there are two disjoint open sets containing F and x.

(b) For every pair of basic open sets, it is uniformly decidable whether they are disjoint.

Let F be an effectively compact set. We call a basic open set B *manifestly disjoint* of F, if there is a finite set of basic open sets S disjoint of B covering F. Due to the effective compactness of F and property (b), the set of all basic open sets manifestly disjoint of F is enumerable. Property (a) implies that it covers the complement of F.

In view of later generalization to cases where the space itself may not be compact, we will refer to some effectively closed sets of $\mathscr{M}(\Omega)$ as effectively compact.

Now we introduce a dense set of computable functions called basic functions on the set $\Omega \times \mathscr{M}(\Omega)$, similarly to Definition 4.15. Their specific form is not too important.

Definition 5.6 (Basic functions for binary sequences and arbitrary measures)**.** The set of *basic* functions over the set $\Omega \times \mathscr{M}(\Omega)$ is defined analogously to Definition 4.15, starting from the functions

$$g_{x,y,u,v,k} : \Omega \times \mathscr{M}(\Omega) \to [0,1]$$

with $x, y \in \{0,1\}^*$ defined as follows. If $x \not\sqsubseteq \omega$, then $g_{x,y,u,v,k}(\omega, P) = 0$. Otherwise, its value does not depend on ω and depends piecewise linearly on $P(y)$ in a way that it is 0 if $P(y) \notin (u,v)$ and 1 if $u + 2^{-k} \leqslant P(y) \leqslant v - 2^{-k}$. ⌟

The analogue of Proposition 4.16 holds again: a lower semicomputable function is the monotonic limit of a computable sequence of basic functions (which themselves are computable).

The analogue of Proposition 4.17 holds also: the integral $\int f(\omega, P) P(d\omega)$ of a basic function is computable as a function of the measure P, uniformly in the number of the basic function.

Finally, the analogue of Proposition 4.18 holds again:

Theorem 5.7 (Trimming)**.** *Let $\varphi(\omega, P)$ be a lower semicomputable function. Then there exists a lower semicomputable function $\varphi'(\omega, P)$ such that for all P:*

(a) $\int \varphi'(\omega, P) P(d\omega) \leqslant 2$,

(b) *if* $\int \varphi(\omega, P) P(d\omega) \leqslant 1$ *then* $\varphi'(\omega, P) = t(\omega, P)$ *for all* ω.

The proof is completely analogous to the proof we gave for Proposition 4.18.

This allows the construction of a universal test as a function of a sequence and an arbitrary measure over Ω:

Theorem 5.8. *There exists a maximal (maximal to within a bounded factor) uniform randomness test.*

Proof. We use the same approach as before: we trim a lower semicomputable function in such a way that it becomes a test (or almost a test) and remains untouched if it were a test in the first place. □

Definition 5.9. Let us fix a universal uniform randomness test $\mathbf{t}(\omega, P)$.

We call a sequence ω *uniformly random* with respect to a (not necessarily computable) measure P if $\mathbf{t}(\omega, P) < \infty$. ⌟

Let us show that for computable measures, the new definition coincides with the old one.

Proposition 5.10. *Let P be a computable measure, let $\mathbf{t}_P(\omega)$ be a universal (average-bounded) randomness test for P as, and $\mathbf{t}(\omega, P)$ the universal uniform test defined above. Then there are constants $c_1, c_2 > 0$ such that $c_1\mathbf{t}_P(\omega) \leqslant \mathbf{t}(\omega, P) \leqslant c_2\mathbf{t}_P(\omega)$.*

The constants c_1, c_2 here depend on the choice of measure P and of the choice of the test $\mathbf{t}_P$ for this measure (this choice was done in an arbitrary way for each computable measure).

This proposition shows, that in the case of the computable measures, uniform randomness coincides with randomness in the sense of Martin-Löf.

Proof. Let us show $\mathbf{t}(\omega, P) \leqslant c_2\mathbf{t}_P(\omega)$ first. The function $\omega \mapsto \mathbf{t}(\omega, P)$ is lower semicomputable since we can effectively enumerate all intervals in the space of measures that contain P; therefore it is dominated by $\mathbf{t}_P(\omega)$.

To prove $\mathbf{t}(\omega, P) \geqslant c_1\mathbf{t}_P(\omega)$, consider the lower semicomputable function

$$t(\omega, Q) = \mathbf{t}_P(\omega).$$

The function $(\omega, Q) \mapsto t(\omega)$ is not guaranteed to be a uniform randomness test, since its integral can be greater than 1 if $Q \neq P$. However, it can be trimmed without changing it at P, and then it still remains (almost) a test. □

We are also interested in tests defined just for one, not necessarily computable, measure P:

Definition 5.11. We will call a function $f : \Omega \to [0,\infty]$ *lower semicomputable* relatively to measure P if it is obtained from a lower semicomputable function on the set $\Omega \times \mathscr{M}(\Omega)$ after fixing the second argument at P.

For a measure $P \in \mathscr{M}(\Omega)$, a *$P$-test of randomness* is a function $f : \Omega \to [0,\infty]$ lower semicomputable from P with the property $\int f(\omega)\, dP \leqslant 1$. ⌟

It seems as if a P-test may capture some nonrandomnesses that uniform tests cannot—however, this is not so, since trimming (see Theorem 5.7) generalizes:

Theorem 5.12. *Let P_0 be some measure along with some P_0-test $t_{P_0}(\omega)$. There is a uniform test $t'(\cdot,\cdot)$ with $t_{P_0}(\omega) \leqslant 2t'(\omega, P_0)$. On the other hand, the restriction of any uniform test to the measure P is a P-test.*

The notion of extended text can be generalized to uniform tests:

Definition 5.13 (Extended uniform test)**.** A lower semicomputable function $T : \{0,1\}^* \times \mathscr{M}(\Omega) \to [0,1]$ monotonic with respect to the prefix relation is called an *extended uniform test* if for all n and all distributions P we have $\sum_{x:|x|=n} T(x,P)P(x) \leqslant 1$. ⌟

As earlier, due to monotonicity, we could sum not only over words of a given length, but over an arbitrary prefix-free set.

The following follows from the analogue of Proposition 4.16 (representing a nonnegative lower semicomputable function as a sum of nonnegative basic functions):

Proposition 5.14. *Every uniform test $t(\omega,P)$ can be generated by an extended uniform test in the sense of $t(\omega,P) = \sup_{x \sqsubset \omega} T(x,P)$. Conversely, every extended uniform test T generates a uniform test t.*

Among the uniform extended tests, it is also possible to select a maximal one (using an analogous trimming method and summing the results). We fix an extended uniform test and denote it $\mathbf{t}(x,P)$ (where $x \in \{0,1\}^*$, and P is a measure over Ω). It generates a maximal uniform test $\mathbf{t}(\omega,P)$ (to within a bounded factor).

Remark 5.15. Much of the theory worked out at the beginning of this paper for 0-1 sequences holds also for sequences whose elements are arbitrary natural numbers. The extended tests of Definition 5.13 generalize, and the existence of a uniform universal extended test is proven in the same way. But it becomes important to define extended tests directly, and not via tests for infinite sequences, since compactness may not hold. ⌟

Proposition 5.10 allows us to generalize a result about Bernoulli measures:

Theorem 5.16. *Let P be a measure computable with some oracle A. Assume also that A can be effectively reconstructed as the values of the measure are provided with more and more precision. Then a sequence ω is uniformly random with respect to P if and only if it is random with respect to P with oracle A.*

(Since the oracle A makes P computable, the notion of Martin-Löf randomness is well defined.)

Proof. Assume that $\mathbf{t}(\omega, P) = \infty$ for the universal uniform test $\mathbf{t}$. Note that $\mathbf{t}(\cdot, P)$ is an A-lower semicomputable function and is a P-test, so ω is nonrandom with respect to P with oracle A.

On the other hand, let $t(\omega, A)$ be some A-lower semicomputable P-test with $t(\omega, A) = \infty$. That A can be reconstructed from P means that there is a computable mapping f from measures to binary sequences (oracles) defined at least over P, with $A = f(P)$. But then $(\omega, P) \mapsto t(\omega, f(P))$ is a P-test. The uniformization theorem 5.12 converts it into a uniform test that is infinite on (ω, P). □

Let us note that not all measures P satisfy the condition of the theorem (it means that the mass problem of "show approximations to the values of P" is equivalent to the decision problem of some set; on the degrees of such mass problems, see [21]). Later, in Theorem 5.36, we show a characterization of uniform randomness for arbitrary measures (in terms of Martin-Löf randomness with oracle).

Another application of the trimming technique: let us show that the notion of uniform randomness test is indeed a generalization of the notion of an uniform Bernoulli test we introduced earlier in Definition 4.1.

Theorem 5.17. *Let $\mathbf{t}(\omega, P)$ be the universal uniform test and let $\mathbf{t}(\omega, p)$ be the universal uniform Bernouli test defined in Lemma 4.20. Then $\mathbf{t}(\omega, B_p) \stackrel{*}{=} \mathbf{t}(\omega, p)$.*

(Here B_p is the Bernoulli measure with parameter p.)

Proof. For the inequality $\stackrel{*}{<}$ note that the function $(\omega, p) \mapsto \mathbf{t}(\omega, B_p)$ is an uniform Bernoulli test, since the mapping $p \mapsto B_p$ is computable mapping (in a natural sense).

For the other direction, there exists a computable function on measures that maps B_p to p (just take the probability of the one-bit string). Combining this function with $\mathbf{t}(\omega, p)$, we get a lower semicomputable function $f(\omega, P)$ on general measures P with $f(\omega, B_p) = \mathbf{t}(\omega, p)$. The function $f(\omega, p)$ is not a uniform

test yet, but again the trimming technique given by Theorem 4.18 yields the desired result. □

5.2 Apriori probability with an oracle, and uniform tests

For a computable measure, we had an expression for the universal test via apriori probability in Proposition 2.21. An analogous expression exists also for the universal uniform test:

Theorem 5.18.

$$\mathbf{t}(\omega, P) \stackrel{*}{=} \sum_{x \sqsubseteq \omega} \frac{\mathbf{m}(x \mid P)}{P(x)}.$$

To be honest, we still owe the reader the definition of the concept of apriori probability with respect to a measure, that is the quantity $\mathbf{m}(x \mid P)$. We do this right away, before returning to the proof.

Definition 5.19. A nonnegative function $t(x, P)$ whose arguments are the binary word x and the measure P will be called a *uniform lower semicomputable semimeasure*, if it is lower semicomputable and $\sum_x t(x, P) \leqslant 1$ for all measures P over Ω. ⌟

Proposition 5.20. *Among the uniform lower semicomputable semimeasures, there is a largest one to within a multiplicative constant.*

This is proved by the same method as the existence of a universal test (and even simpler, since the constraints on the values of the test do not depend on the measure).

Definition 5.21. We will fix one such largest semimeasure, and call it the *apriori probability with respect to P*. We will denote it by $\mathbf{m}(x \mid P)$. ⌟

(The vertical bar in place of a comma emphasizes the similarity to the conditional apriori probability normally considered.)

Proof of Proposition 5.18. We need to check two things. First we need to convince ourselves that the right-hand side of the formula defines a uniform test. Every member of the sum can be considered to be a function of two arguments, equal to 0 outside the cone of extensions of x, and equal to $\mathbf{m}(x \mid P)/P(x)$ inside

the cone. For every x, the functions $\mathbf{m}(x \mid P)$ and $1/P(x)$ are lower semicomputable (uniformly in x), and the sum gives a lower semicomputable function. The integral of this function by any measure P is equal to the sum of the integrals of the members, that is $\sum_x \mathbf{m}(x \mid P)$, and therefore does not exceed 1.

There is a special case, when $P(x) = 0$ for some x. In this case the corresponding member of the sum becomes infinite for any ω extending x. But since the measure of this cone is zero, the integral by this measure is by definition zero, and therefore the additive term, if is not equal to $\mathbf{m}(x \mid P)$, is simply smaller. This way, the right-hand side of the formula is a uniform test, and therefore does not exceed the universal uniform test: we proved the inequality $\stackrel{*}{>}$.

The second part of the proof is not so simple: observing the increase of the values of the uniform test, we must distribute this increase among the different members of the sum of the right-hand side, while preserving lower semicomputability. The difficulty is that if, say, the lower semicomputable function was 1 on some effectively open set A, and outside it was zero, and then this set was changed to a larger set B, then the difference (the characteristic function of $B \setminus A$) will not in general be lower semicomputable since in the set of measures (as also on a segment) the difference of two intervals will not be an open The.

This problem is solved by moving to continuous functions. Let us be given an arbitrary uniform test $t(\omega, P)$. Since it is lower semicomputable, it can be represented as the limit of a nondecreasing sequence of basic functions, or—passing to differences—in the form of a sum of a series of nonnegative basic functions: $t(\omega, P) = \sum_i t_i(\omega, P)$.

Being basic, the function t_i of ω depends only on a finite prefix of the sequence ω; denote the length of this prefix by n_i. For every word x of length n_i we get some lower semicomputable function $t_{i,x}(P)$, where $t_i(\omega, P) = t_{i,x}(P)$ if ω begins by x. Now define $m_i(x, P) = t_{i,x}(P) \cdot P(x)$, if x has length n_i (for the other lengths, zero). The function m_i is lower semicomputable (as the product of two lower semicomputable functions) uniformly in i, and therefore the sum $m(x, P) = \sum_i m_i(x, P)$ will be lower semicomputable.

Let us show that m is a semimeasure, that is $\sum_x m(x, P) \leqslant 1$ for all P. Indeed, in $\sum_i m_i(x, P)$ the nonzero terms correspond to words of length n_i, and this sum is equal to $\sum_x t_{i,x}(P) \cdot P(x)$, that is exactly the integral $\int t_i(\omega, P)\, P(d\omega)$, and the sum of these integrals does not exceed 1 by our condition.

Moreover, if for all prefixes x of the sequence ω the measure $P(x)$ is not

equal to zero, then

$$\sum_{x \sqsubseteq \omega} \frac{m_i(x,P)}{P(x)} = \frac{t_{i,x_i}(P) \cdot P(x_i)}{P(x_i)} = t_i(\omega,P)$$

(here x_i is the prefix of length n_i of ω), hence after summing over i

$$\sum_{x \sqsubseteq \omega} \frac{m(x,P)}{P(x)} = t(\omega,P),$$

and it just remains to apply the maximality of the apriori probability to obtain the $\overset{*}{<}$-inequality for the case that all prefixes of ω have nonzero P-measure. On the other hand, if one of these has zero P-measure, then the right-hand side is infinite, and so here the inequality is also satisfied. □

Question 4. *For the universal randomness test with respect to a computable measure, in this formula one could replace the sum with a maximum. Is this possible for uniform tests? (The reasoning applied there encounters difficulties in the uniform case.) Can one define apriori probabilithy on the tree in a reasonable way, and prove a uniform variant of the Levin-Schnorr theorem?*

5.3 Effectively compact classes of measures

We have considered Bernoulli tests, that is lower semicomputable functions $t(\omega)$ that are tests with respect to all Bernoulli measures. In this definition, in place of Bernoulli measures, an arbitrary effectively compact class can be taken:

Definition 5.22. Let $\mathscr{C}$ be an effectively compact class of measures over Ω. We say that lower semicomputable function t on Ω is a *$\mathscr{C}$-test* if $\int t(\omega)\,dP \leqslant 1$ for every $P \in \mathscr{C}$. ⌟

Theorem 5.23. *Let $\mathscr{C}$ be an effectively compact class of measures.*

(a) *There exists a universal $\mathscr{C}$-test $\mathbf{t}_{\mathscr{C}}(\cdot)$.*

(b) $\mathbf{t}_{\mathscr{C}}(\omega) = \inf_{P \in \mathscr{C}} \mathbf{t}(\omega,P)$.

Proof. Both of these statements are proved analogously to Lemmas 4.20 and 4.21. □

Remark 5.24. Since $\mathscr{C}$ is compact and the function $\mathbf{t}(\omega,P)$ is lower semicomputable, the inf-operation can be replaced by the min-operation. ⌟

Question 5. *Can we give criteria for randomness with respect to natural closed classes of measures (for example in terms of complexity)? How can we describe Bernoulli sequences in terms of complexities of their initial segments? It is known that the main term of the randomness deficiency is*

$$\log \binom{n}{k} - Kp(x \mid n,k).$$

The lecture notes [6] contains a characterization Bernoulli sequences, but it is rather messy.

What about Markov measures? Shift-invariant measures?

5.4 Sparse sequences

There are several situations closely related to some intuitive understanding of randomness, but not fitting directly into the framework of the question of a randomness of a given outcome ω to a given model (measure P). Our example is here a natural notion of sparsity, introduced in [3], but another example, online tests, will be considered in Section 9.

It is natural to call "p-sparse" a sequence ω, when its 1's come from some p-random sequence ω', but we allow some of its 0's to also come from the 1's of ω'. For example, the 1's of ω' may be a sequence of miracles, and ω is the sequence of those miracles that have been reported. The tacit hypothesis is, of course, that all reported miracles actually happened.

Definition 5.25 (Sparse sequences)**.** Let us introduce a coordinate-wise order between infinite binary sequences (or binary sequences of the same length): we say $\omega \leqslant \omega'$ if this is true coordinate-wise, that is $\omega(i) \leqslant \omega'(i)$ for all i: in other words, ω' is obtained from ω replacing some 0's with 1s.

Let B_p be a Bernoulli measure with some computable p. We say that a binary sequence ω is *p-sparse* if $\omega \leqslant \omega'$ for some B_p-random sequence ω'. (In terms of sets, p-sparse sets are subsets of p-random sets). ⌟

We will show that in the definition of sparsity, the existential quantifier can be eliminated, giving a criterion in terms of monotonic tests.

Definition 5.26. A real function f on Ω will be called *monotonic* if $\omega' \geqslant \omega$ implies $f(\omega') \geqslant f(\omega)$.

A monotonic lower semicomputable function $t : \Omega \to [0,\infty]$ is a *p-sparsity test* if $\int t(\omega)\, dB_p \leqslant 1$. A p-sparsity test is *universal* if it multiplicatively dominates all other sparsity tests for p. ⌟

The monotonicity of tests guarantees, informally speaking, that only the presence of some 1s is counted as regularity, not their absence. (Note that earlier we spoke of an entirely different kind of monotonicity, while defining extended tests: there we compared the values of a function on a finite word and its extension.)

Proposition 5.27. *Consider the universal test* $\mathbf{t}(\omega, P)$. *The expression*

$$r_p(\omega) = \min_{\omega' \geqslant \omega} \mathbf{t}(\omega', B_p)$$

defines a universal p-sparsity test.

Proof. Each p-sparsity test is by definition a test with respect to the measure B_p. Using its monotonicity and comparing it with the universal test we obtain that no sparsity test exceeds r_p (to within a bounded factor).

In the other direction it must be shown that the minimum in the expression for r_p is achieved, and that this function is a p-sparsity test. The lower semicomputability is proved usin that the property $\omega \leqslant \omega'$ gives an effectively closed set of the effectively compact space $\Omega \times \Omega$. The monotonicity and the integral inequality follow immediately from the definition. □

From this follows the following characterization in terms of tests:

Theorem 5.28. *A sequence* ω *is p-sparse (is obtained from a p-random by replacing some* 1*s with zeros) if and only if the universal sparsity test* $r_p(\omega)$ *is finite.*

Sparsity is equivalent to randomness with respect to a certain class of measures. To define this class, we introduce the notion of coupling of measures.

Definition 5.29. For measures P, Q we say $P \preceq Q$, or that P can be *coupled below* Q if there exists a probability distribution R on pairs of sequences (ω, ω') such that

(a) The first projection (marginal distribution) is P and the second one is Q.

(b) Measure R is entirely concentrated on pairs (ω, ω') with $\omega \leqslant \omega'$ (the probability of this event by the measure R is 1.

⌟

The following characterization of coupling is well known: it has many proofs, but all seem to go back to [27] (Theorem 11, p. 436). A proof can be found in [3].

Proposition 5.30. *The property $P \preceq Q$ is equivalent to the following: for all monotonic basic functions f the following inequality holds:*

$$\int f(\omega)\, dP \leqslant \int f(\omega)\, dQ.$$

In this characterization, we could have said "all monotonic integrable functions" as well.

Definition 5.31. Let $\mathscr{S}_p$ be the set of measures that can be coupled below B_p. ⌟

Proposition 5.32. *The set $\mathscr{S}_p$ of measures is effectively closed (and thus effectively compact).*

Proof. For each function f in Proposition 5.30, the condition defines an effectively closed set, and their intersection will also be effectively closed. □

Theorem 5.33. *The universal p-test $r_p(\omega)$ is a universal class test for class $\mathscr{S}_p$.*

Thus, a sequence is p-sparse if and only if it is random with respect to some measure that can be coupled below B_p.

The following lemma will be key to the proof.

Lemma 5.34 (Monotonization)**.** *Let $t : \Omega \to \mathbb{R}$ be a basic function with $\int t(\omega)\, dQ \leqslant 1$ for all $Q \in \mathscr{S}_p$. Define the monotonic function $\hat{t}(\omega) = \max_{\omega' \leqslant \omega} t(\omega')$ (the maximum is achieved since $t(\omega)$ depends only on finitely many positions of ω). Then $\int \hat{t}(\omega)\, dB_p \leqslant 1$.*

Proof. Let function t depend only on the first n coordinates. For each $x \in \{0,1\}^n$ fix $x' \leqslant x$ for which $t(x')$ reaches the maximum (among all such x'). Besides the distribution B_p consider a distribution Q in which the Bernoulli measure of x is tranferred to x' (the measures of several x may be transferred to the same x' and then be added). We described the behavior of Q on the first n bits; the following bits are chosen independently, and the probability of 1 in each position is equal to p. Note also that for the expected values of the functions t and $\hat{t}$ only the first n bits count.

By the construction, $Q \preceq B_p$ (essentially, we described a measure on pairs), therefore $\int t(\omega)\, dQ \leqslant 1$. But this integral is equal to $\int \hat{t}(\omega)\, dB_p$. □

Let us return to the theorem.

Proof of Theorem 5.33. Every p-sparsity test t is a class test for $\mathscr{S}_p$. Indeed, its integral by a measure in the class $\mathscr{S}_p$ does not exceed its integral by the measure B_p, by the monotonicity of the test and the possibility of coupling.

On the other hand, let us show that for every test t for the class $\mathscr{S}_p$, there is a a p-sparsity test that is not smaller. Indeed, the test t is the limit of an increasing sequence t_n of basic functions. Applying to them the monotonization lemma 5.34, we obtain a sequence of basic functions $\hat{t}_n$ that are everywhere greater or equal to t_n and have integrals bounded by 1 with respect to the measure B_p. Their limit is the needed p-sparsity test. □

5.5 Different kinds of randomness

There are several ways to define randomness with respect to an arbitrary (not necessarily computable) measure. We have already defined uniform randomness. Here are some other ways.

Oracles We can use the Martin-Löf definition (or its average-bounded version) with oracles. We would call a sequence ω random with respect to P, if there exists an oracle A that makes P computable such that ω is ML-random with respect to P with oracle A. (We say "there exists an oracle that makes P computable" but not "for all oracles that make P computable": indeed, some powerful oracle can always make ω computable and therefore non-random, unless ω is an atom of P.) As Adam Day and Joseph Miller have shown, this definition turns out to be equivalent to uniform randomness. The proof of this equivalence needs some preparation.

First let us look into why is it not possible to take for oracle the measure itself (as was done for the Bernoulli measures, where for oracle we chose a binary expansion of the number p). Well, the choice of such a representation is not unique ($0.01111\cdots = 0.10000\ldots$). When all we have is a single number p then this is not important, as the non-uniqueness arises only for rational p, and in this case both representations are computable. But for measures this is not so: a measure is represented by a countable number of reals (say, the probabilities of individual words, or the conditional probabilities), and the arbitrariness in the choice of representation is not reduced to a finite number of variants.

Definition 5.35. Fix some representation of measures by infinite binary sequences, that is a computable (and therefore continuous) mapping $\pi \mapsto R_\pi$ of Ω onto the space of measures. For example, we may split the binary sequence

π into countably many parts and use these parts as binary representations of the probability that the sequence continues with 1 after a certain prefix.

Define the notion of an *r-test* (representation-test, test of randomness relative to a given representation of the measure) as a lower semicomputable function $t(\omega,\pi)$ with $\int t(\omega,\pi)R_\pi(d\omega) \leqslant 1$ for all π. ⌟

This notion of r-test depends on the representation method chosen; there are no intuitive reasons to choose one specific representation and declare it to be "natural", but any representation is good for the argument below and we assume some representation fixed. The following statements can be proven just as similar statements before:

(a) Every lower semicomputable function $t(\omega,\pi)$ can be trimmed to make it not greater than twice an r-test (not changing it for those π where it already was a r-test).

(b) There exists an universal (maximal to within a bounded factor) r-test $\mathbf{t}(\omega,\pi)$.

For a fixed π, the function $\mathbf{t}(\cdot,\pi)$ is universal among the π-computable average-bounded tests with respect to the measure R_π. Indeed, it is such a test; on the other hand, any such test can be lower semicomputed by the oracle machine. This machine is applicable to any oracle (though may not give a test), giving a lower semicomputable function $t'(\omega,\pi)$ that is equal to the starting test for the given π. It remains to apply property (a).

As a consequence of this simple reasoning we obtain that the quantity $\mathbf{t}(\omega,\pi)$ is finite if and only if the sequence ω is random relative to the oracle π, with respect to measure R_π.

Theorem 5.36 (Day-Miller)**.** *A sequence ω is uniformly random with respect to measure P if and only if there is an oracle computing P that makes ω random (in the original Martin-Löf sense). More precisely,*

$$\mathbf{t}(\omega,P) \stackrel{*}{=} \inf_{R_\pi=P} \mathbf{t}(\omega,\pi). \tag{9}$$

Proof. Let us prove the equality shown in the theorem. Note that if t is a uniform test, then $t(\omega,R_\pi)$ as a function of ω and π is an r-test, and is therefore dominated by the universal r-test.

The other direction is somewhat more difficult. We have to show that the function on the right-hand side is lower semicomputable as a function of the sequence ω and the measure P. (The integral condition is obtained easily afterwards, as the measure P has at least one representation π.) This can be proved

using the effective compactness of the set of those pairs (P,π) with $P = R_\pi$. In the general form (for constructive metric spaces) this statement forms the content of Lemma 7.21.

It remains to explain the connection between the given equality and randomness relative to an oracle. If $\mathbf{t}(\omega, P)$ is finite, then by the proved equality a π exists with $R_\pi = P$ and finite $\mathbf{t}(\omega,\pi)$. As we have seen, this in turn means that ω is random with respect to the measure P, with an oracle π that makes P computable. Conversely, if $\mathbf{t}(\omega, P)$ is infinite, and some oracle A makes P computable, then the function $\mathbf{t}(\cdot, P)$ becomes A-lower semicomputable, and its integral by measure P does not exceed 1, hence the sequence ω will not be random relative to oracle A and with respect to measure P. □

Blind (oracle-free) tests We can define the notion of an effectively null set as before, even if the measure is not computable. The maximal effectively null set may not exist. For example, if measure P may be concentrated on some non-computable sequence π, then all intervals not containing π will be effective null sets, and their union (the complement of the singleton $\{\pi\}$) will not be, otherwise π would be computable.

However, we still can define random sequence as a sequence that does not belong to *any* effectively null set. Kjos-Hanssen suggested the name "Hippocratic randomness" for this definition (referring to a certain legend about the doctor Hippocrates), but we prefer the more neutral name "blind randomness".

Definition 5.37 (Blind tests)**.** A lower semicomputable function $t(\omega)$ with integral bounded by 1 will be called a *blind, or oracle-free, test* for measure P. A sequence ω is *blindly random* iff $t(\omega) < \infty$ for all blind tests. ⌟

As seen, there may not exist a maximal blind test.

This oracle-free notion of randomness can be characterized in the terms introduced earlier:

Theorem 5.38. *Sequence ω is blindly random with respect to measure P if and only if ω is random with respect to any effectively compact class of measures that contains P.*

Proof. Assume first that ω is not random with respect to some effectively compact class of measures that contains P. Then the universal test with respect to this class is a blind test that shows that ω is not blindly random with respect to P.

Now assume that there exists some blind test t for measure P with $t(\omega) = \infty$. Then just consider the class $\mathscr{C}$ of measures Q with $\int t(\omega)\, dQ \leqslant 1$. This class is effectively closed, (and thus effectively compact). Indeed, t be the supremum of the computable sequence of basic functions t_n. The class of measures Q with $\int t_n(\omega)\, dQ > 1$ is effectively open, uniformly in n, and $\mathscr{C}$ is the complement of the union of these sets. □

It is easy to see from the definition (or from the last theorem) that uniform randomness implies blind randomness (either directly or using the last theorem). The reverse statement is not true:

Theorem 5.39. *There exists a sequence ω and measure P such that ω is blindly random with respect to P but not uniformly random.*

Proof. Indeed, oblivous randomness does not change if we change the measure slightly (up to $O(1)$-factor). On the other hand, the changed measure may have much more oracle power that makes a sequence non-random. For example, we may start with uniform Bernoulli random measure $B_{1/2}$ (coin tosses with probabilities $1/2, 1/2, 1/2, \ldots$ and fix some random sequence $\omega = \omega(1)\omega(2)\ldots$. Then consider a (slightly) different measure B' with probabilities $1/2 + \omega(1)\varepsilon_1, 1/2 + \omega(2)\varepsilon_2, \ldots$ where $\varepsilon_1, \varepsilon_2, \ldots$ are so small and converge to zero so fast that they do not change the measure more than by $O(1)$-factor while being all positive. Then B' encodes ω, which makes it easy to construct a uniform test t with $t(\omega, B') = \infty$. □

However, there are some special cases (including Bernoulli measures) where uniform and blind randomness are equivalent. In order to formulate the sufficient conditions for such a coincidence, let us start with some definitions.

Definition 5.40 (Effective orthogonality)**.** For a probability measure P, let $\mathrm{Randoms}(P)$ denote the set of sequences uniformly random with respect to P. A class of measures is called *effectively orthogonal* if $\mathrm{Randoms}(P) \cap \mathrm{Randoms}(Q) = \emptyset$ for any two different measures in it. ⌟

Theorem 5.41. *Let $\mathscr{C}$ be an effectively compact, effectively orthogonal class of measures. Then for every measure P in $\mathscr{C}$ the uniform randomness with respect to P is equivalent to blind randomness with respect to P.*

The statement looks strange: we claim something about randomness with respect to measure P, but the condition of the claim is that P can be included

into a class of measures with some properties. (It would be natural to have a more direct requirement for P instead.) The theorem implies that the measures of Theorem 5.39 do not belong to any such class.

Proof. We have noted already that in one direction the statement is obviously true. Let us prove the converse. Assume that sequence ω is blindly random with respect to measure P. By Theorem 5.38, it is random with respect to the class $\mathscr{C}$. So, ω is uniformly random with respect to some measure P' from the class $\mathscr{C}$. It remains to show $P = P'$.

Imagine that this is not the case. Then we can construct an effectively compact class of measures $\mathscr{C}'$ that contains P but not P'. Indeed, since P and P' are different, they assign different measures to some finite string, and this fact can be used, in form of a closed condition separating P from P', to construct $\mathscr{C}'$. Consider now the effectively compact class $\mathscr{C} \cap \mathscr{C}'$. It contains P, and therefore ω will be random with respect to this class. Hence the class contains some measure P'' with respect to which ω is uniformly random. But $P' \neq P''$ (one measure is in $\mathscr{C}'$, the other one is not), so we get a contradiction with the assumption with the effective orthogonality of the class $\mathscr{C}$. □

Remark 5.42. The proved theorem is applicable in particular to the class of Bernoulli measures. It is tempting to think that there is a simpler proof, at least for this case: if ω is random with respect to p we can compute p from ω as the limit of relative frequency, and no additional oracle is needed. This is not so: though p is *determined* by ω, it does not even depend continuously on ω. Indeed, no initial segment of the sequence guarantees that its limiting frequency is in some given interval. However, we can apply an analogous reasoning to those sequences ω with the randomness deficiency bounded by some constant. (See [11] which introduces the notion of *layerwise computability*.) In particular, it can be shown that if ω is random with respect to the measure B_p then p is computable with oracle ω. ⌟

6 Neutral measure

The following theorem, first published in [16] and then again in [10], points to a curious property of uniform randomness which distinguishes it from randomness using an oracle.

Definition 6.1. A measure is called *neutral* if every sequence is uniformly random with respect to it. ⌟

Theorem 6.2. *There exists a neutral measure; moreover, there is a measure N with $\mathbf{t}(\omega, N) \leqslant 1$ for all sequences ω.*

Note that a neutral measure cannot be computable. Indeed, for a computable measure there exists a computable sequence that is not an atom (adding bits sequentially, we choose the next bit in such a way that its conditional probability is at most $2/3$). Such a sequence cannot be random with respect to N. For the same reason a neutral measure cannot be equivalent to an oracle (for a neutral measure N one cannot find an oracle A that make it computable and at the same time can be uniformly reconstructed from every approximation of N). Indeed, in this case uniform randomness (as we have shown) is equivalent to randomness with respect to N with oracle A, and the same argument works.

A neutral measure cannot be lower or upper semicomputable either, but this statement does not seem interesting, since here a semicomputable measure over Ω is also computable. Some more meaningful (and less trivial) versions of this fact are proved in [10].

Proof. Consider the universal test $\mathbf{t}(\omega, P)$. We claim that there exists a measure N with $\mathbf{t}(\omega, N) \leqslant 1$ for every ω. In other terms, for every ω we have a condition on N saying that $\mathbf{t}(\omega, N) \leqslant 1$ and we need to prove that these conditions (there is continuum of them) have non-empty intersection. Each of these condition is a closed set in a compact space (recall that $\mathbf{t}$ is lower semicontinuous), so it is enough to show that finite intersections are non-empty.

So let $\omega_1, \ldots, \omega_k$ be k sequences. We want to prove that there exists a measure N such that $\mathbf{t}(\omega_i, N) \leqslant 1$ for every i. This measure will be a convex combination of measures concentrated on $\omega_1, \ldots, \omega_k$. So we need to prove that k closed subsets of a k-vertex simplex (corresponding to k inequalities) have a common point. It is a direct consequence of the following classical topology result formulated in Lemma 6.3 below (which is used in the standard proof of Brouwer's fixpoint theorem).

To show that the lemma gives us what we want, consider any point of some face. For example, let X be a measure that is a mixture of, say, ω_1, ω_5 and ω_7. We need to show that X belongs to $A_1 \cup A_5 \cup A_7$: in our terms, that one of the numbers $\mathbf{t}(\omega_1, X)$, $\mathbf{t}(\omega_5, X)$ and $\mathbf{t}(\omega_7, X)$ does not exceed 1. It is easy since we know $\int t(\omega, X)\, dX(\omega) \leqslant 1$ (by the definition of the test), and this integral is a convex combination of the above three numbers with some coefficients (the weights of ω_1, ω_5 and ω_7 in X. $\square$

Lemma 6.3. *Let a simplex with vertices* $1,\dots,n$ *be covered by closed sets* $A_1,\dots,A_k$ *in such a way that vertex* i *belongs to* A_i *(for every* i*), edge* i*-*j *is covered by* $A_i \cup A_j$*, and so on (formally, face* $(i_1,\dots,i_s)$ *of the simplex is a subset of* $A_{i_1} \cup \dots \cup A_{i_s}$*; in particular, the union* $A_1 \cup \dots \cup A_k$ *is the entire simplex). Then the intersection* $A_1 \cap \dots \cap A_k$ *is not empty.*

For completeness, let us reproduce the standard proof of this lemma.

Proof. Consider a disjoint division T of the simplex into smaller n-dimensional simplices (in such a way that every vertex in the division is a vertex of every simplex containing it). Let S be the set of vertices of T. A *Sperner-labeling* is a covering of S by sets $A_1,\dots,A_k$ such that the points of S belonging to each lower-dimensional simplex formed by some vertices $i_1 < i_2 < \dots < i_r \leqslant k$ are covered by $A_{i_1} \cup \dots \cup A_{i_r}$. (A point gets label i if it belongs to A_i.) Sperner's famous combinatorial lemma (see for example the Wikipedia) implies that in any Sperner labeling, there is a simplex whose vertices are labeled with all k colors.

To apply the Sperner's lemma, note that our closed sets A_i satisfy the rules of Sperner coloring. Sperner's lemma guarantees the existence of a simplex that has all possible labels on its vertices. In this way we can get arbitrarily small simplices with this property; compactness then shows that all A_i have a common point. □

7 Randomness in a metric space

Most of the theory presented above for infinite binary sequences generalizes to infinite sequences of natural numbers. Much of it generalizes even further, to an arbitrary metric space. In what follows below we not only generalize; some of the results are new also for the binary sequence case.

7.1 Constructive metric spaces

We rely on the definition of a constructive metric space, and the space of measures on it, as defined in [10] and [12] (the lecture notes [6] are also recommended).

Definition 7.1. A *constructive metric space* is a tuple $\mathbf{X} = (X,d,D,\alpha)$ where (X,d) is a complete separable metric space, with a countable dense subset D

and an enumeration α of D. It is assumed that the real function $d(\alpha(v),\alpha(w))$ is computable. Open balls with center in D and rational radius are called *ideal balls*, or *basic open sets*, or *basic balls*. The (countable) set of basic balls will also be called the *canonical basis* in the topology of the metric space.

An infinite sequence $s_1, s_2, \dots$ with $s_i \in D$ is called a *strong Cauchy* sequence if for all $m < n$ we have $d(s_m, s_n) \leqslant 2^{-m}$. Since the space is complete, such a sequence always has a (unique) limit, which we will say is *represented* by the sequence. ⌟

We will generally use the notational convention of this definition: if there is a constructive metric space with an underlying set X then the we will use $\mathbf{X}$ (boldface) to denote the whole structure (X,d,D,α). But frequently, we just use X when the structure is automatically understood.

Examples 7.2. 1. A set $X = \{s_1, s_2, \dots\}$ can be turned into a constructive *discrete* metric space by making the distance between any two different points equal to 1. The set D consists of all points $\alpha(i) = s_i$.

2. The set $\overline{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$ can be turned into a constructive metric space by making the distance between any two different points with the distance function $d(x,y) = |\frac{1}{x} - \frac{1}{y}|$, where of course, $\frac{1}{\infty} = 0$. The set D consists of all points of $\mathbb{N}$. This metric space is called the *one-point compactification*, in a topological sense, of the *discrete metric space* $\mathbb{N}$ of Example 1.

3. The real line $\mathbb{R}$ with the distance $d(x,y) = |x-y|$ is a constructive metric space, and so is $\mathbb{R}_+ = [0,\infty)$. We can add the element ∞ to get $\overline{\mathbb{R}}_+ = [0,\infty]$. This is not a metric space now, but is still equipped with a natural constructive topology (see Remark 7.4 below). It could be equipped with a new metric in a way that would not change this constructive topology.

4. If $\mathbf{X}, \mathbf{Y}$ are constructive metric spaces, then we can define a constructive metric space $\mathbf{Z} = \mathbf{X} \times \mathbf{Y}$ with one of its natural metrics, for example the sum of distances in both coordinates. In case when $\mathbf{X} = \mathbf{Y} = \mathbb{R}$, this is called the L_1 metric. Let $D_{\mathbf{Z}}$ be the product $= D_{\mathbf{X}} \times D_{\mathbf{Y}}$.

5. Let X be a finite or countable (enumerated) alphabet, with a fixed numbering, and let $X^{\mathbb{N}}$ be the set of infinite sequences $x = (x(1), x(2), \dots)$ with distance function $d^{\mathbb{N}}(x,y) = 2^{-n}$ where n is the first i with $x(i) \neq y(i)$. This space generalizes the binary Cantor space of Definition 2.1, to the case mentioned in Remark 5.15. The balls in it are cylinder sets: for a given finite sequence z, we take all continuations of z.

⌟

Remark 7.3. Each point x of a constructive metric space $\mathbf{X}$ can be viewed as an "approximation mass problem": the set of total functions that for any given rational $\varepsilon > 0$ produce a ε-approximation to x by a point of the canonical dense set D. This is a mass problem in the sense of [20]. One can also note that this mass problem is Medvedev equivalent to the enumeration problem: enumerate all basic balls that contain x. ⌟

Remark 7.4. A constructive metric space is special case of a more general concept, which is often useful: a constructive topological space.

A *constructive topological space* $\mathbf{X} = (X, \tau, \nu)$ is a topological space over a set X with a basis τ effectively enumerated (not necessarily without repetitions) as a list $\tau = \{\nu(1), \nu(2), \ldots\}$.

For every nonempty subset Z of the space X, we can equip Z with a constructive topology: we intersect all basic sets with Z, without changing their numbering. On the other hand, not every subset of a constructive metric space naturally has the structure of a constructive metric space (the everywhere dense set D is not inherited).

But instead of introducing constructive topological spaces formally, we prefer not to burden the present paper with more abstractions, and will speak about some concepts like effective open sets and continuous functions, as defined on an arbitrary subset Z of the constructive metric space X. ⌟

Definition 7.5. An open subset of a constructive metric space is *lower semicomputable open* (or r.e. open, or c.e. open), or *effectively open* if it is the union of an enumerable set of elements of the canonical basis. It is *upper semicomputable closed*, or *effectively closed* if its complement is effectively open. Given any set $A \subseteq X$, a set U is *effectively open on* A if there is an effective open set V such that $U \cap A = V \cap A$. ⌟

Note that in the last definition, U is not necessarily part of A, but only its intersection with A matters.

Computable functions can be defined in terms of effectively open sets.

Definition 7.6 (Computable function)**.** Let X, Y be constructive metric spaces and $f : X \to Y$ a function. Then f is *continuous* if for each element U of the canonical basis of Y the set $f^{-1}(U)$ is an open set. It is *computable* if $f^{-1}(U)$ is also an effectively open set, uniformly in U. A partial function $f : X \to Y$ defined at least on a set A is *computable* if for each element U of the canonical basis of Y the set $f^{-1}(U)$ is effectively open on A, uniformly in U.

An element $x \in X$ is called *computable* if the function $f : \{0\} \to X$ with $f(0) = x$ is computable.

When $f(x)$ is defined only in a single point x_0 then we say that the element $y_0 = f(x_0)$ is x_0-*computable*. When $f : X \times Z \to Y$, defined on $X \times \{z_0\}$, is computable, then we say that the function $g : X \to Y$ defined by $g(x) = f(y, z_0)$ is z_0-*computable*, or computable *from* z_0. ⌟

There are several alternative characterizations of a computable element.

Proposition 7.7. *The following statements are equivalent for an element x of a constructive metric space $\mathbf{X} = (X, d, D, \alpha)$.*

(i) *x is computable.*

(ii) *the set of basic balls containing x is enumerable.*

(iii) *There is a computable sequence $z_1, z_2, \ldots$ of elements of D with $d(x, z_n) \leqslant 2^{-n}$.*

The following proposition connects computability with a more intuitive concept based on representation by strong Cauchy sequences.

Proposition 7.8. *Let $\mathbf{X}, \mathbf{Y}$ be constructive metric spaces and $f : X \to Y$ a function. Then f is computable if and only if there is a computable transformation that turns each strong Cauchy sequence $s_1, s_2, \ldots$ with $s_i \in D_{\mathbf{X}}$ converging to a point $x \in X$ into a strong Cauchy sequence $t_1, t_2, \ldots$ with $t_i \in D_{\mathbf{Y}}$ converging to $f(x)$.*

If f is a partial function with domain Z then f is computable if and only if there is a computable transformation that turns each strong Cauchy sequence $s_1, s_2, \ldots$ with $s_i \in D_{\mathbf{X}}$ converging to some point $x \in Z$ into a strong Cauchy sequence $t_1, t_2, \ldots$ with $t_i \in D_{\mathbf{Y}}$ converging to $f(x)$.

We omit the—not difficult—proof of this statement.

Remark 7.9. Though x_0-computability means computability from a strong Cauchy sequence $s_1, s_2, \ldots$ converging to x_0, it should not be considered the same as computability using a machine that treats this sequence as an "oracle". In case of x_0-computability, the resulting output must be independent of the strong Cauchy sequence $s_1, s_2, \ldots$ representing x_0. ⌟

The following definition of lower semicomputability is also a straightforward generalization of the special case in Definition 2.2.

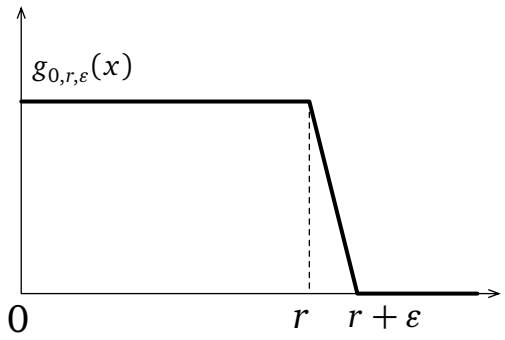

Figure 1: A hat function

Definition 7.10 (Lower semicomputability)**.** Let $\mathbf{X} = (X, d, D, \alpha)$ be a constructive metric space. A function $f : X \to [-\infty, \infty]$ is *lower semicontinuous* if the sets $\{x : f(x) > r\}$ are open, for every rational number r (from here it follows that they are open for all r, not only rational).

It is *lower semicomputable* if these sets are effectively open, uniformly in the rational number r. It is *upper semicomputable* if $-f$ is lower semicomputable.

A partial function $f : X \to Y$ defined at least on a set A is *lower semicomputable* on A if the sets $\{x : f(x) > r\}$ are effectively open in A, uniformly for every rational number r. ⌟

It is easy to check that a real function over a constructive metric space is computable if and only if it is lower and upper semicomputable. As before, one can define semicomputability equivalently with the help of basic functions.

Let us introduce an everywhere dense set of simple functions.

Definition 7.11 (Hat functions, basic functions)**.** We define an enumerated list of *basic* functions $\mathscr{E} = \{e_1, e_2, \dots\}$ in the constructive metric space $\mathbf{X} = (X, d, D, \alpha)$ as follows. For each point $u \in D$ and positive rational numbers r, ε let us define the *hat function* $g_{u,r,\varepsilon}$: its value in point x is determined by the distance of x to u and is equal to 1, if this distance is at most r, equal to zero, if the distance is not less than $r + \varepsilon$, and varies linearly as the distance runs through the segment $[r, r + \varepsilon]$: see Figure 1. Let $\mathscr{E}$ be the smallest set of functions containing all hat functions that is closed under min, max and rational linear combinations. ⌟

Proposition 7.12. *A function $f : X \to [0,\infty]$ defined on a constructive metric space is lower semicomputable if and only if it is the limit of a computable increasing sequence of basic functions.*

Note that the above characterization holds also for lower semicontinous functions, if we just omit the requirement that the sequence g_n be computable.

Definition 7.13. We can introduce the notion of lower semicomputability *from* z_0, or z_0*-lower semicomputability*, similarly to the z_0-computability of Definition 7.6, as lower semicomputability of a function defined on the set $X \times \{z_0\}$. ⌟

Sometimes two metrics on a space are equivalent from the point of view of computability questions. Let us formalize this notion.

Definition 7.14 (Uniform continuity, equivalence)**.** Let X, Y be two metric spaces, and $f : X \to Y$ a function. We say that f is *uniformly continuous* if for each $\varepsilon > 0$ there is a $\delta > 0$ such that $d_X(x,y) \leqslant \delta$ implies $d_Y(f(x), f(y)) \leqslant \varepsilon$.

If $\mathbf{X}, \mathbf{Y}$ are constructive metric spaces and function f is computable, we will call it *effectively uniformly continuous* if δ can be computed from ϵ effectively.

Two metrics d_1, d_2 over the same space are *(effectively) equivalent* if the identity map is (effectively) continuous in both directions. ⌟

For example, the Euclidean metric and the L_1 metric introduced in Example 7.2.4 are equivalent in the space $\mathbb{R}^2$.

Effective compactness was introduced in Definition 5.4: this generalizes immediately to arbitrary metric spaces. A weaker notion, local compactness, also has an effective version.

Definition 7.15 (Effective compactness and local compactness)**.** A compact subset C of a constructive metric space $\mathbf{X} = (X, d, D, \alpha)$ is called *effectively compact* if the set

$$\{\, S : S \text{ is a finite set of basic open sets and } \bigcup_{E \in S} E \supseteq C \,\}$$

is enumerable.

A subset C of a metric space is called *locally compact* if it is covered by the union of a set of balls B such that $\overline{B} \cap C$ is compact. Here $\overline{B}$ is the closure of B. It is *effectively locally compact* if it is covered by the union of an enumerated sequence of basic balls B_k such that $\overline{B}_k \cap C$ is effectively compact, uniformly in k. ⌟

Examples 7.16. 1. The countable discrete space of Example 7.2.1 is effectively compact if it is finite, and effectively locally compact otherwise.

2. The segment $[0,1]$ is effectively compact. The line $\mathbb{R}$ is effectively locally compact.

3. If the alphabet X is finite then the space $X^{\mathbb{N}}$ of infinite sequences is effectively compact. Otherwise it is not even locally compact.

4. Let $\alpha \in [0,1]$ be a lower semicomputable real number that is not computable. (It is known that there are such numbers, for example $\sum_{x\in\mathbb{N}} 2^{-Kp(x)}$.) The lower semicomputability of α allows to enumerate the rationals less than α and allows for the segment $[0,\alpha]$ to inherit the constructive metric (and topology) from the real line. This space is compact, but not effectively so.

⌟

The following is a useful characerization of effective compactness.

Proposition 7.17. (a) *A compact subset C of a constructive metric space $\mathbf{X} = (X,d,D,\alpha)$ is effectively compact if and only if from each (rational) ε one can compute a finite set of ε-balls covering C.*

(b) *For an effectively compact subset C of a constructive metric space, in every enumerable set of basic open sets covering C one can effectively find a finite covering.*

Proof. Assume that for all ε we can show a finite covering S_ε of the set C by balls of radius ε. Along with such a covering, we can enumerate all coverings with *guaranteedly* large balls (this means that for all balls $B(x,\varepsilon)$ from the covering S_ε there is a ball $B(y,\sigma)$ from the new covering with $\sigma > \varepsilon + d(x,y)$). The compactness of C guarantees that while S_ε runs through all ε-coverings of C, this way all coverings of C will be enumerated. (Indeed, if there is some covering S' not falling into the enumeration, then for all ε there is a ball of the covering S_ε not guaranteedly contained in any ball of S'. Applying compactness and taking a limit point of the centers of these non-contained balls, we obtain contradiction.)

The remaining statements are proved quite easily. □

The following statement generalizes Proposition 5.5, with the same proof.

Proposition 7.18. *Every effectively closed subset E of an effectively compact set C is also effectively compact.*

As earlier, the converse also holds: every effectively compact subset of a constructive metric space is effectively closed. Indeed, we can consider all possible coverings of this set by basic balls, and also outside balls that manifestly (by the relation of the distances of their centerse and their radiuses) are disjoint from the balls of the covering. The union of all these outside balls provide the complement of our effectively compact set.

It is known that a continuous function maps compact sets into compact ones. This statement also has a constructive counterpart, also provable by a standard argument:

Proposition 7.19. *Let C be an effectively compact subset of a constructive metric space X, and f a computable function from X into another constructive metric space Y. Then $f(C)$ is effectively compact.*

The statement that a lower semicontinuous function on a compact set reaches its minimum has also a computable analog (we provide a parametrized variant):

Proposition 7.20 (Parametrized minimum)**.** *Let $\mathbf{Y},\mathbf{Z}$ be constructive metric spaces, let $f : Y \times Z \to [0,\infty]$ be a lower semicomputable function, and C an effectively closed subset of $Y \times Z$. If it is also effectively compact, then the function*

$$g(y) = \inf_{z:(y,z)\in C} f(y,z)$$

is lower semicomputable from below (and the inf *can be replaced with* min *due to compactness).*

Instead of effective compactness of C, it is sufficient to require that its projection $C_Y = \{\, y : \exists z\,(y,z) \in C \,\}$ is effectively closed and covered by an enumerated sequence of basic balls B_k such that $\overline{B}_k \times Z \cap C$ is effectively compact, uniformly in k.

The weaker condition formulated at the end holds for example if Y is effectively locally compact and Z is effectively compact.

Proof. For start, we reproduce the classical proof of lower semicontinuity. One needs to check that the set $\{\, y : r < g(y) \,\}$ is open for all r. This set can be represented in the form of a union, noting that the condition $r < g(y)$ is equivalent to the condition

$$(\exists r' > r)\forall z\,[(y,z) \in C \Rightarrow f(y,z) > r'],$$

and it is sufficient to check the openness of the set

$$U = \{\, y : \forall z\, [(y,z) \in C \Rightarrow f(y,z) > r'] \,\}.$$

Now, $U = (Y \setminus C_Y) \cup \bigcup_k (B_k \cap U)$. Since $Y \setminus C_Y$ is assumed to be open, it is sufficient to show that each $B_k \cap U$ is open. Let $F_k = \overline{B}_k \times Z$, then by the assumptions, $F_k \cap C$ is compact. The condition $f(y,z) > r'$ by the assumption defines a certain open set V of pairs, hence $F_k \cap C \setminus V$ is closed, and as a subset of a compact set, compact. It follows that its projection $\{\, y \in \overline{B}_k : \exists z\, (y,z) \in F_k \cap C \setminus V \,\}$, as a continuous image of a compact set, is also compact, and so closed. Its complement in B_k, which is $B_k \cap U$, is then open.

Now this argument must be translated to an effective language. First of all note that it is sufficient to consider rational r and r'. Then the set V is effectively open, the set $F_k \cap C \setminus V$ is effectively closed, and as a subset of an effectively compact set, also effectively compact. Its projection, as a computable image of an effectively compact set, is also effectively compact, and as such, effectively closed. The complement of the projection is then effectively open. □

The following lemma is an application:

Lemma 7.21. *Let X, Z, Z' be metric spaces, where X is locally compact and Z is compact. Let $f : Z \to Z'$ be continuous and surjective, and $t : X \times Z \to [0,\infty]$ a lower semicontinuous function. Then the function $t_f : X \times Z' \to [0,\infty]$ defined by the formula*

$$t_f(x,z') = \inf_{z : f(z) = z'} t(x,z)$$

is lower semicontinuous.

If X, Z, Z' are constructive metric spaces, X is effectively locally compact, Z is effectively compact and f is computable, further t is lower semicomputable, then t_f is lower semicomputable.

Proof. We will prove just the effective version. We will apply Proposition 7.20 with $Y = X \times Z'$, and $C = X \times \{\, (f(z), z) : z \in Z \,\}$. Then $t_f(x,z') = \inf_{(x,z',z) \in C} t(x,z)$. The set Y is effectively locally compact, as the product of an effectively locally compact set and an effectively compact set. The projection of the set C onto Y is the whole set Y, and hence it is closed. Hence the proposition is applicable, according to the remark following it. □

7.2 Measures over a constructive metric space

On a metric space, the *Borel sets* are the smallest σ-algebra containing the open sets. We can define measures on Borel sets. These measures have the following *regularity* property:

Proposition 7.22 (Regularity)**.** *Let P be a measure over a complete separable metric space. Then every measureable set A can be approximated by large open sets: $P(A) = \inf_{G \supseteq A} P(G)$, where G is open.*

It is possible to introduce a metric over measures:

Definition 7.23 (Prokhorov distance)**.** For a set A and point x let us define the distance of x from A as $d(x,A) = \inf_{y \in A} d(x,y)$. The ε-neighborhood of a set A is defined as $A^\varepsilon = \{\, x : d(x,A) < \varepsilon \,\}$.

The *Prokhorov distance* $\rho(P,Q)$ of two measures is the greatest lower bound of all those ε for which, for all Borel sets A we have $P(A) \leqslant Q(A^\varepsilon) + \varepsilon$ and $Q(A) \leqslant P(A^\varepsilon) + \varepsilon$. ⌟

It is known that $\rho(P,Q)$ is indeed a metric, and it turns the set of probability measures over metric space X into a metric space. There is a number of other metrics for measures that are equivalent, in the sense of Definition 7.14.

Definition 7.24 (Space of measures)**.** For a constructive metric space, $\mathbf{X}$, let $\mathbf{M} = \mathscr{M}(\mathbf{X})$ define the metric space of the set of probability measures over $\mathbf{X}$, with the metric $\rho(P,Q)$. The dense set $D_{\mathbf{M}}$ is the set of those probability measures that are concentrated on finitely many points of $D_{\mathbf{X}}$ and assign rational values to them. Let $\alpha_{\mathbf{M}}$ be a natural enumeration of $D_{\mathbf{M}}$, this turns $\mathbf{M}$ into a constructive metric space, too.

A probability measure is called *computable* when it is a computable element of the space $\mathbf{M}$. ⌟

Computability of measures is a particularly simple property for the Cantor space of binary sequences in Definition 2.8 (which is easily shown to be equivalent to the definition given here); it is just as simple for the Baire space of sequences over a countable alphabet.

The analogue of Proposition 4.17 holds again: the integral $\int f(\omega,P)P(d\omega)$ of a basic function is computable as a function of the measure P, uniformly in the code of the basic function. Here is a closely related result:

Proposition 7.25. *If f is a bounded, effectively uniformly continuous function then its integral by the measure P is an effectively uniformly continuous function of P.*

Proof. It can be assumed without loss of generality that f is nonnegative (add a constant). Let measures P and P' be close. Then $P'(A) \leqslant P(A_\varepsilon) + \varepsilon$, where A_ε denotes the ε-neighborhood of A. Then

$$\int f\,dP' \leqslant \int f_\varepsilon\,dP + \varepsilon,$$

where $f_\varepsilon(x)$ is the least upper bound of f on the ε-neighborhood of x. (The integral of a nonnegative function g is defined by the measures of the sets $G_t = \{x : g(x) \geqslant t\}$; by Fubini's theorem on the change of the order of integration, this measure must be integrated by t as a function of t. Now, if $f(x) \geqslant t$ then $f_\varepsilon(x) \geqslant t$ in the ε-neighborhood of point x.) It remains to apply the effective uniform continuity of f to find out the precision by which the measure must be given in order to obtain a given precision in the integral. □

On the other hand, the measure of $P(B)$ of a basic ball B is not necessarily computable, only lower semicomputable. It is shown in [12] that this property also characterizes the computability of measures: P is computable if and only if $P(B)$ is lower semicomputable, uniformly in the basic ball B.

It is known that if a complete separable metric space is compact then so is the set of measures with the described metric. The following constructive version is proved by standard means:

Proposition 7.26. *If a constructive metric space* $\mathbf{X}$ *is effectively compact then its space of probability measures* $\mathscr{M}(\mathbf{X})$ *is also effectively compact.*

For the binary Cantor space, this was proved in Proposition 5.5. There, the topology of the space of measures was simply derived from the topology of the space $[0,1] \times [0,1] \times \cdots$. It can be seen that the Prokhorov metric leads to the same topology.

Example 7.27. Another interesting simple metric space is the infinite discrete space, say on the set of natural numbers $\mathbb{N}$. This is not a compact space, and the set of measures, namely the set of all functions $P(x) \geqslant 0$ with $\sum_{x\in\mathbb{N}} P(x) = 1$, is not compact either.

On the other hand, the set of semimeasures (see Definition 2.19) is compact. Indeed, recall that the space $[0,1] \times [0,1] \times \cdots$, of functions $P : \mathbb{N} \to [0,1]$ is compact. Hence also for each n the subset F_n of this set of consisting of functions P

obeying the restriction $P(0)+P(1)+\cdots+P(n) \leqslant 1$ is compact, as the product of a compact finite-dimensional set $\{\,(P(0),P(1),\ldots,P(n)) \in [0,1]^n : P(0)+\cdots+P(n) \leqslant 1\,\}$ and the compact infinite product set $\{\,(P(n+1),P(n+1),\ldots) : 0 \leqslant P(x) \leqslant 1 \text{ for } x > n\,\}$. The intersection of all sets F_n is then also compact, and is equal to the set of semimeasures.

Equivalently, we can consider the one-point compactification $\overline{\mathbb{N}}$ of $\mathbb{N}$ given in Example 7.2.2. Measures P on this space can be identified with semimeasures over $\mathbb{N}$: we simply set $P(\infty) = 1 - \sum_{n<\infty} P(n)$. ⌟

7.3 Randomness in a metric space

In the Cantor space Ω of infinite binary sequences we defined

- randomness with respect to computable measures (in the sense of Martin-Löf); see Definition 2.9;
- uniform randomness with respect to arbitrary measures (when the test is a function of the sequence and the measure), Definition 5.2;
- Randomness with respect to an effectively compact class of measures, Definition 5.22;
- Blind (oracle-free) randomness in Definition 5.37;

All these notions carry over with minor changes to an arbitrary constructive metric space. In the present section we discuss these generalizations and their properties, and then consider in more detail randomness with respect to an orthogonal class of measures.

For computable measures, a test is defined as a lower semicomputable function on a constructive metric space, whose integral is bounded by 1. Among such tests, there is a maximal one to within a multiplicative constant. As earlier, this is proved with the help of trimming: we list all lower semicomputable functions, forcing them into tests or almost tests, and then add them up with coefficients from a converging series.

This is done as before, by considering lower semicomputable functions as monotonic limits of basic ones. It is used that the integral of a basic function by a measure is computable as a function of the measure: see Propositions 7.25 and the discussion preceding it.

The uniform tests introduced in Definition 5.2 generalize immediately to the case of constructive metric spaces. Such a test is a lower semicomputable function of two arguments $t(x,P)$, where x is a point of our metric space, and P is

a measure over this space. The integral condition has the same form as earlier: $\int t(x,P)\,P(dx) \leqslant 1$.

As earlier, there exists a universal test, and this can be proved by the technique of trimming:

Theorem 7.28 (Trimming in metric spaces)**.** *Let $u(x,P)$ be a lower semicomputable function whose first argument is a point of a constructive metric space, and the second one is measure over this space. Then there exists a uniform tests $t(x,P)$ satisfying $u(x,Q) \leqslant 2t(x,Q)$ for all Q such that the function $u_Q : x \mapsto u(x,Q)$ is a test by the measure Q, that is $\int u(x,Q)\,Q(dx) \leqslant 1$.*

The proof repeats the reasoning of the proof of Theorem 5.7, while using the fact that for a basic function $b(x,P)$ on the product space the integral $\int b(x,P)\,P(dx)$ is a computable (continuous) function of P (which is proved analogously to our above argument on the computability of the integral).

We will denote the universal uniform test again by $\mathbf{t}(x,P)$. Strictly speaking, it depends also on the constructive metric space on which it is defined, but in general it is evident, which space is being considered, therefore it is not shown in the notation.

Definition 5.11 and Proposition 5.12 extend without difficulty.

Definition 7.29 (Tests for arbitrary measures)**.** Let $\mathbf{X} = (X,d,D,\alpha)$ be a constructive metric space. For a measure $P \in \mathscr{M}(\mathbf{X})$, a *$P$-test of randomness* is a function $f : X \to [0,\infty]$ lower semicomputable from P with the property $\int f(x)\,dP \leqslant 1$. ⌟

It seems as if a P-test may capture some nonrandomnesses that uniform tests cannot—however, this is not so, since trimming (see Theorem 5.7) generalizes:

Theorem 7.30 (Uniformization)**.** *Let P be some measure over a constructive metric space X, along with some P-test $t_P(x)$. There is a uniform test $t'(\cdot,\cdot)$ with $t_P(x) \leqslant 2t'(x,P)$.*

Theorem 5.36 generalizes to the case of constructive metric spaces. Let us mention one of the facts that generalize to uniform tests.

Proposition 7.31 (Kurtz tests, uniformly)**.** *Let S be an effectively open subset of the space $X \times \mathscr{M}(X)$. If the set $S_P = \{\, x : (x,P) \in S \,\}$, has P-measure 1 for some measure P, then the set $S(P)$ contains all uniformly P-random points.*

Proof. The indicator function $1_S(x,P)$ of the set S, that is equal to unity on S and to zero outside, is lower semicomputable. According to Proposition 7.12, it can be written as the limit of a computable increasing sequence of basic functions $0 \leqslant g_n(x,P) \leqslant 1$. The sequence $G_n : P \mapsto \int g_n(x,P)\,dP$ is an increasing sequence of functions computable uniformly in n. The motonone convergence theorem implies $G_n(P) \to 1$ for all $P \in \mathscr{C}$. Let us define for each measure P the numbers $n_K(P)$ as the minimal values of n for which $G_n(P) > 1 - 2^k$. These numbers are upper semicomputable as functions of P (in a natural sense; for measures P with $P(S_P) < 1$, some of these $n_k(P)$ are infinite). Correspondingly, the functions $1 - g_{n_k(P)}(x,P)$, as functions of x and P (define such a function to be zero for infinite $n_k(P)$, independently of x) are lower semicomputable, uniformly in k. Then $t(x,P) = \sum_{k>0}(1 - g_{n_k(P)}(x,P))$ is a uniform test, since at a given P, if its kth addend is zero if $n_k(P)$ is infinite, and is not greater than 2^{-k} for finite $n_k(P)$.

The conditions of the theorem talk about a measures P with $P(S_P) = 1$. Then all numbers $n_k(P)$ are finite. Consider an x outside S_P: then $g_{n_k(P)}(x,P) = 0$ by definition. Therefore all addends of the test sum are equal to unity, thus x is is not P-random point. Consequently, S_P includes all uniformly P-random points. □

7.4 Apriori probability, with an oracle

In Section 5.2 we defined apriori probability with a condition whose role was played by a measure over the Cantor space Ω. Now, having introduced the notion of a constructive metric space, we can note that this definition extends naturally to an arbitrary such space $\mathbf{X}$: we consider nonnegative lower semicomputable functions $m : \mathbb{N} \times X \to [0,\infty]$ for which $\sum_i m(i,x) \leqslant 1$, for all $x \in X$.

Among such functions, there is a maximal one to within a multiplicative constant. This is proved by the method of trimming: the lower semicomputable function $m(i,x)$ can be obtained as a sum of a series of basic functions each of which differs form zero only for one i; these basic functions must be multiplied by correcting coefficients that depend on the sum over all i. (In each stage, this sum has only finitely many members.)

We will call the maximal function of this kind *apriori probability with condition* x, and denote it $\mathbf{m}(i \mid x)$. We consider the first argument a natural number, but this is not essential: it is possible to consider words (or any other discrete constructive objects). As a special case we obtain the definition of apriori probability conditioned on a measure (Section 5.2), and also the standard notions of apriori probability with an oracle (which corresponds to $\mathbf{X} = \Omega$, the Cantor space

of infinite sequences), and the conditional apriori probability (corresponding to $\mathbf{X} = \mathbb{N}$).

In analogy with Martin-Löf's theorem, the apriori probability with a condition is expressible, in an arbitrary *effectively compact* constructive metric space $\mathbf{X}$ by apriori probability with an oracle.

Proposition 7.32. *Let $F : \Omega \to X$ be a computable map whose image is the whole space X. Then*

$$\mathbf{m}(i \mid x) \stackrel{*}{=} \min_{\pi : F(\pi) = x} \mathbf{m}(i \mid \pi).$$

Proof. We reason as in the proof of Theorem 5.36. The function $(i, \pi) \mapsto \mathbf{m}(i \mid F(\pi))$ is lower semicomputable on $\mathbb{N} \times \Omega$, hence the $\stackrel{*}{<}$-inequality.

In order to obtain the reverse inequality, we use Lemma 7.21 and note that the function on the right-hand side is correctly defined (the minimum is achieved) and is lower semicomputable. □

Note that the apriori probability with an oracle on the right-hand side of Proposition 7.32 is expressible by prefix complexity with an oracle. For the case of prefix complexity with condition in metric spaces it is not clear, how to define prefix complexity with such a condition (one can speak of functions whose graph is enumerable with respect to x, but it is not clear how to build a universal one). But one can define formally $Kp(i \mid x)$ as $\max_{\pi : F(\pi) = x} Kp(i \mid \pi)$, and then $Kp(i \mid x) \stackrel{+}{=} -\log \mathbf{m}(i \mid x)$, but it is questionable whether this can be considered a satisfactory definition of prefix complexity (say, the usual arguments using the self-delimiting property of programs are not applicable at such a definition). It is more honest to simply speak of the logarithm of apriori probability. Many results still stay true: for example the formula $Kp(i, j \mid x) \stackrel{+}{<} Kp(i \mid x) + Kp(j \mid x)$ can be proved, without introducing self-delimiting programs, just reasoning about probabilities.

Remark 7.33. Analogously, it is possible to supply points in constructive metric spaces as conditions in some of our other definitions. For example, we can consider uniform tests over the Cantor space Ω of infinite binary sequences, with condition in an arbitrary constructive metric space X: these will be lower semicomputable functions $t(\omega, P, x)$ with $\int t(\omega, P, x)\, P(d\omega) \leqslant 1$ for all P, x. It is also possible to fix a computable measure P, say the uniform one, and define tests with respect to this measure with conditions in X. ⌟

8 Classes of orthogonal measures

The definition of a class test for an effectively compact class of measures, as well as Theorem 5.23 about the expression of a class test, generalizes, with the same proof.

The set of Bernoulli measures has an important property shared by many classes considered in practice: namely that a random sequence determines the measure to which it belongs. A consequence of this was spelled out in Theorem 5.41. This section explores the topic in a more general setting.

There are some examples naturally generalizing the Bernoulli case: finite or infinite ergodic Markov chains, and ergodic stationary processes. Below, we will dwell a little more on the latter, since it brings up a rich complex of new questions.

We will consider orthogonal classes in the general setting of metric spaces: from now on, our measureable space is the one obtained from a constructive metric space $\mathbf{X} = (X, d, D, \alpha)$. The following classical concept is analogous to effective orthogonality, introduced in Definition 5.40.

Definition 8.1 (Orthogonal measures)**.** Let P, Q be two measures over a measureable space $(X, \mathscr{A})$, that is a space X with a σ-algebra $\mathscr{A}$ of measureable sets on it. We say that they are *orthogonal* if the space can be partitioned into measureable sets U, V with the property $P(V) = Q(U) = 0$.

Let $\mathscr{C}$ be a class of measures. We say that $\mathscr{C}$ is *orthogonal* if there is a measureable function $\varphi : X \to \mathscr{C}$ with the property $P(\varphi^{-1}(P)) = 1$. ⌟

Note that the space $\mathscr{M}(X)$, as a metric space, also allows the definition of Borel sets, and it is in this sense that we can talk about f being measureable.

Examples 8.2. 1. In an orthogonal class, any two (different) measures P and Q are orthogonal. Indeed, the sets $\{P\}$ and $\{Q\}$ are Borel (since closed), hence their preimages are measureable (and obviously disjoint). The converse statement is false: A class $\mathscr{C}$ of mutually orthogonal probability measures is not necessarily orthogonal, even if the class is effectively compact. For example, let λ be the uniform distribution over the interval $[0,1]$, and let for each $x \in [0,1]$ the probability measure δ_x be concentrated on x. Then the class $\{\lambda\} \cup \{\delta_x : x \in [0,1]\}$ is effectively compact, and its elements are mutually orthogonal. But the whole class is not orthogonal: the orthogonality condition requires $\phi(x) = \delta_x$, but then $\phi^{-1}(\lambda)$ will be empty.

2. Let P, Q be two probability measures. Of course, if Randoms(P) and Randoms(Q) are disjoint, then P and Q are orthogonal. The converse is not always true: for example it fails if λ, δ_x are as above, where x is random with respect to λ.

⌟

The following definition introduces the important example of stationary ergodic processes.

Definition 8.3. The Cantor space Ω of infinite binary sequences is equipped with an operation $T : \omega(1)\omega(2)\omega(3)\ldots \mapsto \omega(2)\omega(3)\omega(4)\ldots$ called the *shift*. A probability distribution P over Ω is *stationary* if for every Borel subset A of Ω we have $P(A) = P(T^{-1}(A))$. It is easy to see that this property is equivalent to requiring

$$P(x) = P(0x) + P(1x)$$

for every binary string x.

A Borel set $A \subseteq \Omega$ is called *invariant* with respect to the shift operation if $T(A) \subseteq A$. For example the set of all sequences in which the relative frequency converges to $1/2$ is an invariant set. A stationary distribution is called *ergodic* if every invariant Borel set has measure 0 or 1. ⌟

Here is a new example of a stationary process (all Bernoulli measures and stationary Markov chains are also examples).

Example 8.4. Let $Z_1, Z_2, \ldots$ be a sequence of independent, identically distributed random variables taking values $0, 1$ with probabilities 0.9 an 0.1 respectively. Let $X_0, X_1, X_2, \ldots$ be defined as follows: X_0 takes values $0, 1, 2$ with equal probabilities, and independently of all Z_i, further $X_n = X_0 + \sum_{i=1}^{n} Z_i \bmod 3$. Finally, let $Y_n = 0$ if $X_n = 0$ and 1 otherwise. The process $Y_0, Y_1, \ldots$ is clearly stationary, and can also be proved to be ergodic. As a function of the Markov chain $X_0, X_1, \ldots$, it is also called a *hidden Markov chain*. ⌟

The following theorem is a consequence of Birkhoff's pointwise ergodic theorem. For each binary string x let

$$g_x(\omega) = 1_{x\Omega}(\omega)$$

be the indicator function of the set $x\Omega$: it is 1 if and only if x is a prefix of ω.

Proposition 8.5. *Let P be a stationary process over the Cantor space Ω.*

(a) *With probability* 1*, the average*

$$A_{x,n}(\omega) = \frac{1}{n}(g_x(\omega) + g_x(T\omega) + \cdots + g_x(T^{n-1}\omega)) \tag{10}$$

converges.

(b) *If the process is ergodic then the sequence converges to* $P(x)$.

(For non-ergodic processes, the limit may depend on ω.) Birkhoff's theorem is more general, talking about more general spaces and measure-preserving transformations T, arbitrary integrable functions in place of g_x, and convergence to the expected value in the ergodic case. But the proposition captures its essence (and can also be used in the derivation of the more general versions).

Part (b) of Proposition 8.5 implies that the class $\mathscr{C}$ of ergodic measures is an orthogonal class. Indeed, let us call a sequence ω "stable" if for all strings x, the averages $A_{x,n}(\omega)$ of (10) converge. It is easy to see that in this case, the numbers $P(x)$ determine some probability measure Q_ω. Now, let $\varphi : \Omega \to \mathscr{C}$ be a function that assigns to each stable sequence ω the measure Q_ω provided Q_ω is ergodic. If the sequence is not stable or Q_ω is not ergodic, then let $\varphi(\omega)$ be some arbitrary fixed ergodic measure. It can be shown that φ is a measureable function: here, we use the fact that the set of stable sequences is a Borel set. By part (b) of Proposition 8.5, the relation $P(\varphi^{-1}(P)) = 1$ holds for all ergodic measures.

Note that the class of all ergodic measures is not closed, but we did not rely on the closedness of this class in the definition.

Example 8.2.2 shows that two measures can be orthogonal and still have common random sequences. But, for computable measures, as we will show right away, this is not possible.

We called a class of measures P effectively orthogonal in Definition 5.40, if all sets of random sequences $\mathrm{Randoms}(P)$ for measures P in the class are disjoint from each other.

Theorem 8.6. *Two computable probability measures on a constructive metric space are orthogonal if and only they are effectively orthogonal.*

Speaking of the effective orthogonality of two measures, we mean that they have no common (uniform) random sequences. In the effective case, pairwise orthogonality within the class and the orthogonality of the whole class are equivalent by definition.

Proof. We only need to prove one direction. Assume that P, Q are orthogonal, that is there is a measureable set A with $P(A) = 1$, $Q(A) = 0$. By Proposition 7.22, these measures are regular, so there is a sequence $G_n \supseteq A$ of open sets with $Q(G_n) < 2^{-n}$. Then for every n there is also a finite union H_n of basic balls with $P(H_n) > 1 - 2^{-n}$ and $Q(H_n) < 2^{-n}$; moreover, there is a computable sequence H_n with this property. Let $U_m = \bigcup_{n>m} H_n$. By Proposition 7.31, $\bigcap_m U_m$ contains all random points of P. On this other hand, the sets U_m form a Martin-Löf test for measure Q, so the intersection contains no random points of Q. □

We have shown above that ergodic measures form an orthogonal class. Careful analysis shows that this is also true effectively.

Theorem 8.7. *The set of ergodic measures over the Cantor set Ω forms an effectively orthogonal class.*

Proof. The paper [28] (more precisely, an analysis of it that will create uniform tests) shows that

(a) Sequences uniformly random with respect to some stationary measure are stable (in the sense that the above indicated limit of averages exists for them).

(b) Uniformly random sequences with respect to an ergodic measure are "typical" in the sense that these averages converge to $P(x)$.

To show (a), the paper introduces the function

$$\sigma(\omega, \alpha, \beta)$$

for rationals $0 < \alpha < \beta$, which is the maximum number of times that $A_{x,n}(\omega)$ crosses from below α to above β. This function is lower semicomputable, uniformly in the rationals α, β. Then it shows

$$(1 + \alpha^{-1})(\beta - \alpha) \int \sigma(\omega, \alpha, \beta)\, dP \leqslant 1,$$

that is that $(1 + \alpha^{-1})(\beta - \alpha)\sigma(\omega, \alpha, \beta)$ is an average-bounded test, implying that for Martin-Löf-random sequences, the average $A_{x,n}(\omega)$ crosses from below α to above β only a finite number of times. Now one can combine all these tests, for all strings x and all rational $0 < \alpha < \beta$, into a single test. This test is uniform in P: we did not rely on the computability of P.

To express (b), in view of part (a), it is sufficient, for each x, to prove

$$\liminf_n A_{x,n}(\omega) \leqslant P(x) \leqslant \limsup_n A_{x,n}(\omega) \tag{11}$$

for random ω. Take for example the statement for the lim inf. It is sufficient to show for each k,m that $\inf_{n\geqslant m} A_{x,n}(\omega) \leqslant P(x)+2^{-k}$ for a random ω. The set

$$S_{x,k,m} = \{\,(\omega,P) : \exists n \geqslant m\; A_{x,i}(\omega) < P(x)+2^{-k}\,\}$$

is effectively open, and the Birkhoff theorem implies $P(S_{x,k,m}(P)) = 1$ for for all ergodic measures P, for the set $S_{x,k,m}(P) = \{\,x : (x,P) \in S_{x,k,m}\,\}$. Proposition 7.31 implies that then for each P, the set $S_{x,k,m}(P)$ contains all P-random points.

Another approach is a proof that just shows (b) for computable ergodic measures (in a relativizable way), without an explicit test, as done in [2]. Then a reference to Theorem 5.16 allows us to conclude the same about uniformly random sequences. □

It is convenient to treat orthogonality of a class in terms of separator functions. For this, note that by a measureable real function we mean a Borel-measureable real function, that is a function with the property that the inverse images of Borel sets are Borel sets.

Definition 8.8 (Separator function)**.** Let $\mathscr{C}$ be a class of measures over the metric space X. A measureable function $s : X \times \mathscr{M}(X) \to [0,\infty]$, is called a *separator function* for the class $\mathscr{C}$ if for all measures P we have $\int s(x,P)\,dP \leqslant 1$, further for $P,Q \in \mathscr{C}$, $P \neq Q$ implies that only one of the values $s(x,P)$, $s(x,Q)$ is finite.

In case we have a constructive metric space $\mathbf{X}$, a separator function $s(x,P)$ is called a *separator test* if it is lower semicomputable in (x,P). ⌟

We could have required the integral to be bounded only for measures on the class, since trimming allows the extension of the boundedness property to all measures, just as in the remark after Definition 7.29.

The following observation connects orthogonality with separator functions and also shows that in case of effective orthogonality, each measure can be effectively reconstructed from any of its random elements.

Theorem 8.9. *Let $\mathscr{C}$ be a class of measures.*

(a) *If class $\mathscr{C}$ is Borel and orthogonal then there is a separator function for it.*

(b) *Class $\mathscr{C}$ is effectively orthogonal if and only if there is a separator test for it.*

The converse of part (a) might not hold: this needs further investigation.

Proof. Let us prove (a). If $\varphi(x)$ is a measureable function assigning measure $P \in \mathscr{C}$ to each element $x \in X$ as required in the definition of orthogonality, then by a general theorem of topological measure theory (see [14]), its graph is measureable. This allows the following definition: for $P \notin \mathscr{C}$ set $s(x,P) = 1$, further for $P \in \mathscr{C}$, set $s(x,P) = 1$ if $\varphi(x) = P$, and $s(x,P) = \infty$ otherwise.

Let us prove now (b). If $\mathscr{C}$ is effectively orthogonal then the uniform test $\mathbf{t}(x,P)$ is a separator test for the class $\mathscr{C}$. Suppose now that there is a separator test s for the class $\mathscr{C}$, and let $P,Q \in \mathscr{C}$, $P \neq Q$, $x \in \mathrm{Randoms}(P)$. Since s is a randomness test, $s(x,P) < \infty$, which implies $s(x,Q) = \infty$, hence $x \notin \mathrm{Randoms}(Q)$. □

The following result is less expected: it shows that if the class of measures is effectively compact then the existence of a lower semicontinuous separator function implies the existence of a lower semicomputable one (that is a separator test).

Theorem 8.10. *If for an effectively compact class of measures there is a lower semicontinuous separator function $s(x,P)$, then this class is effectively orthogonal.*

Proof. Let $\mathscr{C}$ be an effectively compact class of measures on a constructive metric space. We need to show that under the conditions of the theorem, for any two distinct measures P_1, P_2 in $\mathscr{C}$, the sets of random sequences are disjoint:

$$\mathrm{Randoms}(P_1) \cap \mathrm{Randoms}(P_2) = \emptyset.$$

Take two disjoint closed basic balls B_1 and B_2 in the constructive metric space $\mathbf{M}$ of measures, containing the measures P_1, P_2. The classes $\mathscr{C}_i = \mathscr{C} \cap B_i$, $i = 1,2$ of measures are disjoint effectively compact classes of measures, containing P_1 and P_2. Consider the functions

$$t_i(x) = \inf_{P \in \mathscr{C}_i} s(x,P).$$

For all x at least one of the values $t_1(x)$, $t_2(x)$ is infinite. By (a version of) Proposition 7.20, the functions $t_i(x)$ are lower semicontinuous, and hence $\mathscr{C}_1$- and $\mathscr{C}_2$-tests respectively.

Now we follow some of the reasoning of the proof of Proposition 7.31. For integer $k > 1$, consider the open set $S_k = \{x : t_1(x) > 2^k\}$. Since t_1 is a $\mathscr{C}_1$-test, then $P(S_k) < 2^{-k}$ for all $P \in \mathscr{C}_1$. On the other hand, since for all x one of

the two values $t_1(x)$, $t_2(x)$ is infinite, $P(S_k) = 1$ for all $P \in \mathscr{C}_2$. The indicator function $1_{S_k}(x)$ of the set S_k is lower semicontinuous, therefore it can be written as the limit of an increasing sequence (now not necessarily computable!) of basic functions $g_{k,n}(x)$. We conclude as in the proof of Proposition 7.31, that for each P there is an $n = n_k(P)$ with $\int g_{k,n}(x)\, dP > 1 - 2^{-k}$ for all $P \in \mathscr{C}_2$. The effective compactness of $\mathscr{C}$ implies then that there is an n independent of P with the same property. In summary, for each $k > 0$ a basic function h_k is found with

$$\int h_k\, dP < 2^{-k} \text{ for all } P \in \mathscr{C}_1,$$
$$\int h_k\, dP > 1 - 2^{-k} \text{ for all } P \in \mathscr{C}_2.$$

Such a basic function h_k can be found effectively from k, by complete enumeration. Now we can construct a lower semicomputble function

$$t_1'(x) = \sum_k h_k(x).$$

It is a test for the class $\mathscr{C}_1$, while $t_2'(x) = \sum_k (1 - h_k(x))$ is a test for all $P \in \mathscr{C}_2$ for the same reasons. These tests must be finite for elements random for P_1 and P_2, and this cannot happen simultaneously for both tests. □

The meaning of separator tests introduced above introduced notion of can be clarified as follows. Due to effective orthogonality of $\mathscr{C}$, the universal uniform test $\mathbf{t}(\omega, P)$ allows to separate the sequences into random ones according to different measures of the class $\mathscr{C}$: looking at a sequence ω, random with respect to some measure of this class (=random with respect to the class), we are looking for a $P \in \mathscr{C}$ for which $\mathbf{t}(\omega, P)$ is finite. This measure is unique in the class $\mathscr{C}$ (by the definition of effective orthogonality).

This separation property, however, can be satisfied also by a non-universal test, and we called such tests separator tests. The non-universal test is less demanding about the idea of randomness, giving it, so to say, a "first approximation": it might accept a sequence as random that will be rejected by a more serious test. (The converse is impossible, since the universal test is maximal.) What matters is only that this preliminary crude triage separates the measures of the class $\mathscr{C}$, that is that no sequence should appear "random" even "in first approximation", with respect to two measures at the same time.

For brevity, just for the purposes of the present paper, we will call "typicality" this "randomness in first approximation":

Definition 8.11. Given a separator test $s(x,P)$ we call an element x *typical* for $P \in \mathscr{C}$ (with respect to the test s) if $s(x,P) < \infty$. ⌟

A typical element determines uniquely the measure P for which it is typical.

For an example, consider the class of $\mathscr{B}$ of Bernoulli measures. For a test in "first approximation", we may recall von Mises, who called the first property of a random sequence ("Kollektiv" in his words) the stability of its relative frequencies. The stability of relative frequencies (strong law of large numbers in today's terminology) means $S_n(\omega)/n \to p$. Here $S_n(\omega)$ is the number of ones in the initial segment of length n of the sequence ω, and p is the parameter of the Bernoulli measure B_p.

There are several requirements close to this in this spirit:

(1) $S_n(\omega)/n \to p$ with a certain convergence speed.

(2) $S_n(\omega)/n \to p$.

(3) For the case when $\mathscr{C}$ is the class of all ergodic stationary measures over the Cantor space Ω, convert the proof of Theorem 8.7 into a test, implying $A_{x,n}(\omega) \to P(x)$ for all x.

Among these requirements, the one that seems most natural to a mathematician, namely (2), is not expressible in a semicomputable way. Requirement (1) has many possible formulations, depending on the convergence speed: we will show an example below.

Requirement (3) is significantly more complicated to understand, but is still much simpler than a universal test. It *does not* imply a computable convergence speed directly; indeed, as Vyugin showed in [28], a computable convergence speed does not exist for the case of computable non-ergodic measures. But later works, starting with [1], have shown that the the convergence for ergodic measures has a speed computable from P.

Here is an example of a test expressing requirement (1). (For simplicity, we obtain the convergence of relative frequencies not on all segments, only on lengths that are powers of two. With more care, one could obtain similar bounds on all initial segments.) By Chebyshev's inequality

$$B_p(\{\, x \in \{0,1\}^n : |\sum_i x(i) - np| \geqslant \lambda n^{1/2}(p(1-p))^{1/2}\,\}) \leqslant \lambda^{-2}.$$

Since $p(1-p) \leqslant 1/4$, this implies

$$B_p(\{\, x \in \{0,1\}^n : |\sum_i x(i) - np > \lambda n^{1/2}/2\,\}) < \lambda^{-2}.$$

Setting $\lambda = n^{0.1}$ and ignoring the factor $1/2$ gives

$$B_p(\{\, x \in \{0,1\}^n : |\sum_i x(i) - np| > n^{0.6} \,\}) < n^{-0.2}.$$

Setting $n = 2^k$:

$$B_p(\{\, x \in \{0,1\}^{2^k} : |\sum_i x(i) - 2^k p| > 2^{0.6k} \,\}) < 2^{-0.2k}. \tag{12}$$

Now, for a sequence ω in $\mathbf{B}^{\mathbb{N}}$, and for $p \in [0,1]$ let

$$g(\omega, B_p) = \sup\{\, k : |\sum_{i=1}^{2^k} \omega(k) - 2^k p| > 2^{0.6k} \,\}.$$

Then

$$\int g(\omega, B_p)\, B_p(d\omega) \leqslant \sum_k k \cdot 2^{-0.2k} = c < \infty.$$

Dividing by c, we obtain a test. This is a separator test, since $g(\omega, B_p) < \infty$ implies that $2^{-k} S_{2^k}(\omega)$ converges to p, and this cannot happen for two different p.

Theorem 5.41 generalizes, with essentially the same proof (using basic balls instead of initial sequences): it says that in an effectively compact, effectively orthogonal class of measures, blind randomness is the same as uniform Martin-Löf randomness. This raises the question whether every ergodic measure belongs to some effectively compact class. The answer is negative:

Theorem 8.12. *Consider stationary measures over Ω (with the shift transformation). Among these, there are some ergodic measures that do not belong to any effectively compact class of ergodic measures.*

Before proving the theorem, let us prove some preparatory statements.

Proposition 8.13. *Both the ergodic measures and the nonergodic measures are dense in the set of stationary measures $\mathscr{M}(\Omega)$ over Ω.*

Proof. First we will show how to approximate an arbitrary stationary measure P by ergodic measures. Without loss of generality assume that all probabilities $P(x)$ for finite strings x are positive. (If not, then we can mix in a little of the

uniform measure.) For a fixed n, consider the values $P(x)$ on strings x of length at most n. There is a process that reproduces these probabilities and that is isomorphic to an ergodic Markov process on $\{0,1\}^{n-1}$. In this process, for an arbitrary $x \in \{0,1\}^{n-2}$, $b,b' \in \{0,1\}$ the transition probability from bx to xb' is $P(bxb')/P(bx)$. Since both transition probabilities are positive, this Markov process is ergodic.

Now we show how to approximate an arbitrary ergodic measure by nonergodic measures. Let P be ergodic. Let us fix some $n > 0$ and $\varepsilon > 0$. By the pointwise ergodic theorem, there is a sequence in which the limiting frequencies of all words converge to the measure (almost all sequences—with respect to this measure—are such). Taking a long piece of this sequence and repeating it leads to a periodic sequence in which the frequencies of words of length not exceeding n differ from the measure P by at most ε (for any given n and $\varepsilon > 0$). (The repetition forms new words on the boundaries, but at a large length, this effect is negligible.) Consider now the measure concentrated on the shifts of this sequence, assigning the same weight to each of them (their number is equal to the minimum period). This measure is not ergodic, but is close to P. □

Proposition 8.14. *The set of ergodic measures is a G_δ set in the metric space of all stationary measures over Ω.*

Proof. We can restrict attention to the (closed) set of stationary measures. Let P be a stationary probability measure over Ω. Consider the function $A_{x,n}$ over Ω, defining $A_{x,n}(\omega)$ to be equal to the average number of occurrences of the word x in the n first possible positions of ω. By the ergodic theorem, the sequence of functions $A_{x,1}, A_{x,2}, \ldots$ converges in the L_1 sense. Moreover, the stationary measure P is ergodic if and only if the limit of this convergence is the constant function with value $P(x)$.

Since the limit exists for all stationary measures, it is sufficient to check that the constant $P(x)$ is a limit point. For each x, N and each rational ε the set $S_{x,N,\varepsilon}$ of those P for which there is an $n \geqslant N$ with

$$\int |A_{x,n}(\omega) - P(x)| P(d\omega) < \varepsilon$$

is open, and set of ergodic stationary measures is the intersection of these sets for all x, N, ε. □

Proof of Theorem 8.12. The union of all effectively compact classes of ergodic measures is F_σ. Suppose that it is equal to the set of all ergodic measures.

Then the set of nonergodic measures is a G_δ set which is also dense by Proposition 8.13.

As shown in Propositions 8.13 and 8.14, the set of ergodic measures is a dense G_δ set. But by the Baire category theorem, two dense G_δ sets cannot have an empty intersection. This contradiction proves the theorem. □

The following question still remains open:

Question 6. *Is there an ergodic measure over Ω for which uniform and blind randomness are different?*

Returning to arbitrary effectively compact, effectively orthogonal classes, we can connect the universal tests with class tests of Theorem 5.23 and separator tests.

Theorem 8.15. *Let $\mathscr{C}$ be an effectively compact, effectively orthogonal class of measures, let $\mathbf{t}(x,P)$ be the universal uniform test and let $\mathbf{t}_{\mathscr{C}}(x)$ be a universal class test for $\mathscr{C}$. Assume that $s(x,P)$ is a separator test for $\mathscr{C}$. Then we have the representation*

$$\mathbf{t}(x,P) \stackrel{*}{=} \max(\mathbf{t}_{\mathscr{C}}(x), s(x,P))$$

for all $P \in \mathscr{C}$, $x \in X$.

Proof. Let is note first that $\mathbf{t}_{\mathscr{C}}(x)$ and $s(x,P)$ do not exceed the universal uniform test $\mathbf{t}(x,P)$. Indeed $s(x,P)$ is a uniform test by definition. Also by definition, the universal class test $\mathbf{t}_{\mathscr{C}}(x)$ is a uniform test.

On the other hand, let us show that if $\mathbf{t}_{\mathscr{C}}(x)$ and $s(x,P)$ are finite, then $\mathbf{t}(x,P)$ does not exceed the greater one of them (to within a multiplicative constant). The finiteness of the first test guarantees that $\min_{Q\in\mathscr{C}} \mathbf{t}(x,Q)$ is finite: this minimum is equal to $\mathbf{t}_{\mathscr{C}}(x)$ to within a constant factor. If this minimum was achieved on some measure $Q \neq P$, then both values $s(x,Q)$ and $s(x,P)$ would be finite, contradicting to the definition of a separator. (Note that we proved a statement slightly stronger than promised: in place of "greater of the two", one can write "the first of the two, if the second one is finite".) □

The above theorem separates the randomness test into two parts (points at two possible causes of non-randomness). First, we must convince ourselves that x is random with respect to the class $\mathscr{C}$. For example in the case of a measure B_p, in the class $\mathscr{B}$ of Bernoulli measures, we must first be convinced that $\mathbf{t}_{\mathscr{B}}(\omega)$

is finite. This encompasses all the irregularity criteria. If the independence of the sequence is taken for granted, we may assume that the class test is satisfied.

After this, we know that our sequence is Bernoulli, and some kind of simple test of the type of the law of large numbers is sufficient to find out, by just which Bernoulli measure is it random: B_p or some other one. This second part, typicality testing, is analogous to parameter testing in statistics.

Separation is the only requirement of the separator test: its numerical value is irrelevant. For example in the Bernoulli test case, no matter how crude the convergence criterion expressed by the separator test $s(x,P)$, the maximum is always (essentially) the same universal test.

9 Are uniform tests too strong?

9.1 Monotonicity and/or quasi-convexity

Uniform tests may seem too strong, in case P is a non-computable measure. In particular, randomness with respect to computable measures (in the sense of Martin-Löf or in the uniform sense, they are the same for computable measures) has certain intuitively desireable properties that uniform randomness lacks. One of these is monotonicity: roughly, if Q is greater than P then if x is random with respect to P, it should also be random with respect to Q.

Proposition 9.1. *For computable measures P,Q, for all rational $\lambda > 0$, if $\lambda P(A) \leqslant Q(A)$ for all A, then*

$$\mathbf{m}(\lambda) \cdot \lambda \mathbf{t}(x,Q) \stackrel{*}{<} \mathbf{t}(x,P). \tag{13}$$

Here $\mathbf{m}(\lambda)$ is the discrete apriori probability of the rational λ. To make the constant in $\stackrel{*}{<}$ independent of P,Q, one needs also to multiply the left-hand side by $\stackrel{*}{=} \mathbf{m}(P,Q)$.

Proof. We have $1 \geqslant \int \mathbf{t}(x,Q)\, dQ \geqslant \int \lambda \mathbf{t}(x,Q)\, dP$, hence $\lambda \mathbf{t}(x,Q)$ is a P-test. Using the trimming method of Theorem 7.28 in finding universal tests, one can show that the sum

$$\sum_{\lambda : \lambda \int \mathbf{t}(x,Q)\, dP < 2} \mathbf{m}(\lambda) \cdot \lambda \mathbf{t}(x,Q)$$

is a P-test, and hence $\stackrel{*}{<} \mathbf{t}(x,P)$. Therefore this is true of each member of the sum, which is just what the theorem claims. It is easy to see that the multiplicative constants depend here on P,Q only via inserting a factor $\mathbf{m}(P,Q)$. □

The intuitive motivation for monotonicity is this: if there are two devices with internal randomness generators, outputting numbers with distributions P and Q, and if $\lambda P \leqslant Q$, then it can be imagined that the second device simulates the first one with probability λ, and does its own thing otherwise. Then every outcome intuitively plausible as the outcome of the first device, must also be deemed a plausible outcome of the second one, since this could have simulated the first one by chance. (The numerical value of the randomness deficiency may be, of course, somewhat larger, since we must believe in addition that the λ-probability event occurred.)

Uniform randomness violates, alas, this property: if measure Q is larger, but computationally more complex, then the randomness tests with respect to Q can exploit this additional information, to make nonrandom some outcomes that were random with respect to P (see the proof of Theorem 5.39). This is just the reason of the difference between uniform and blind (oracle-free) randomness, for which the analogous monotonicity property is obviously satisfied.

Another situation for which we have some intuition on randomness is the mixture (convex combination) of measures. Imagine two devices with output measures P and Q, and an outer box which triggers one of them with some probabilities λ, $1-\lambda$. As a whole, we obtain a system whose outcome is distributed by the measure $\lambda P + (1-\lambda)Q$. About which outcomes can we assert that are obtained randomly as a result of this experiment? Clearly both the outcomes random with respect to P and those random with respect to Q must be accepted (with the understanding that if the coefficient is small then some additional, but finite suspicion is added). And there should not be any other outcomes. A quantitative elaboration of this result (which in one direction follows from monotonicity) is given below.

Proposition 9.2. *Let P and Q be two computable measures.*

(a) *For a rational $0 < \lambda < 1$,*

$$\mathbf{m}(\lambda) \cdot \mathbf{t}(x, \lambda P + (1-\lambda)Q) \stackrel{*}{<} \max(\mathbf{t}(x,P), \mathbf{t}(x,Q)).$$

(b) *For arbitrary $0 < \lambda < 1$,*

$$\mathbf{t}(x, \lambda P + (1-\lambda)Q) \stackrel{*}{>} \min(\mathbf{t}(x,P), \mathbf{t}(x,Q)).$$

The constants in $\stackrel{*}{<}$ depend on the length of the shortest programs defining P and Q (their complexities), but not on λ (or other aspects of P,Q).

Statement (a) could be called the *quasi-convexity* of randomness tests (to within a multiplicative constant). For a test with an exact quasi-convexity property (without any multiplicative constants) there is a lower semicomputable semimeasure that is neutral (after extending tests to semimeasures see [16, 8]).

Statement (b) implies that no other random outcomes exist for the mixture of P and Q. This could be called the *quasi-concavity* of randomness tests (to within a multiplicative constant).

Proof. Part (a) follows from Proposition 9.1. Indeed, if $\lambda \geqslant 1/2$ then Proposition 9.1 implies $\mathbf{m}(\lambda)\cdot\mathbf{t}(x,\lambda P+(1-\lambda)Q) \stackrel{*}{<} \mathbf{t}(x,P)$ (absorbing $1/2$ into the $\stackrel{*}{<}$). If $\lambda < 1/2$ then it implies $\mathbf{m}(1-\lambda)\cdot\mathbf{t}(x,\lambda P+(1-\lambda)Q) \stackrel{*}{<} \mathbf{t}(x,Q)$ similarly, and we just recall $\mathbf{m}(\lambda) \stackrel{*}{=} \mathbf{m}(1-\lambda)$.

Part (b) follows from the fact that the right-hand side is a test with respect to an arbitrary mixture of the measures P and Q, and trimming can convert it into uniform test. □

It is easy to see that all these statements exploit the computability of the measures and the mixing coefficients in an essential way. The corresponding counterexamples are easy to build once it is recognized that the mixture of measures can be stronger from an oracle-computational point of view than any of them, as well as in the other way. For example, let us divide the segment $[0,1]$ into two halves and consider the measures P and Q that are uniformly distributed over these halves. Their mixture with coefficients λ and $1-\lambda$ will make the number λ obviously non-random (since it can be computed from this measure), though with respect to one of the measures in can very well be random. Taking instead of P and Q their mixtures, say, with coefficients $1/3$ and $2/3$ and then reversed, one can make λ random with respect to both measures.

In this example the mixture contains more information than each of the original measures. It can also be the other way: bend the interval $[0,1]$ with the uniform measure into a circle, and cut it into two half-circles by the points p and $p+1/2$. Then the uniform measures on these half-circles make p computable with respect to them and thus non-random, while the average of these measures is the uniform measure on the circle, with respect to which p can very well be random.

Let us note that for blind (oracle-free) randomness, we can guarantee without any restrictions that the set of points random with respect to the mixture of P and

Q is the union of points random with respect to P and Q. (In one direction this follows from monotonicity, which we already mentioned. In the other one: if an outcome is not random with respect to P and not random with respect to Q, then there are two tests proving this, and their minimum will a lower semicomputable test proving its non-randomness with respect to the mixture.)

These are strong motives to modify the concept of randomness test in order to reproduce these properties, while conserving other desireable properties (say the existence of a universal test and with it the notion of a deficiency of randomness). Some such modifications can be seen in [16, 8, 17].

9.2 Locality

Imagine that some sequence ω is uniformly random with respect to measure P and starts with 0. Change the values of the measure on sequences that start with 1. It is not guaranteed that ω remains uniformly random since now the measure may become stronger as an oracle (allowing to compute more). But this looks strange since the changes in measure are in the part of the universe that does not touch ω.

For blind (oracle-free) randomness, specifically this example is impossible (one can force the test to zero on sequences beginning with unity), but in principle the concept of test depends not only on the measure along the sequence (not only on the probabilities of occurrences of nulls and ones after its start).

For randomness with respect to computable measures, the situation is again better.

Proposition 9.3 (Prequentiality)**.** *Let P, Q be two computable measures on the space Ω of binary sequences, coinciding on all initial segments of some sequence ω. Then this sequence is simultaneously random or non-random with respect to P and Q.*

Proof. This follows immediately from the randomness criterion in terms of the complexity of the inital segments (Levin-Schnorr Theorem) in any of its variants (Theorem 2.24, Proposition 2.30, Corollary 2.32). □

On the other hand, it is easy to modify one of the counterexamples in 9.1 to violate prequentiality as well.

In case of an arbitrary constructive metric space an analogous statement holds, though with a stronger requirement: we assume that two computable measures are equal on all sets contained in some neighborhood of the outcome ω. (In

this case it is possible to multiply the test by a basic function without changing it in ω, and making it zero outside the neighborhood of coincidence).

Here is yet another way to obtain a clearly prequential definition of randomness, in which the randomness deficiency is a function of the sequence itself and the measures of its initial segments. For a given sequence ω and a given sequence $\{q(i)\}$ of real numbers with $1 = q(0) \geqslant q(1) \geqslant q(2) \geqslant \cdots \geqslant 0$, let

$$\mathbf{t}'(\omega, q) = \inf \mathbf{t}(\omega, P),$$

where the minimum is taken over all measures P with $P(\omega(1:n)) = q(n)$. The corresponding sets are effectively compact, so that this minimum will be a lower semicomputable function of ω and the sequence q. If for the sequence ω and the measures $q(i)$ of its initial segments, the value $\mathbf{t}'(\omega, q)$ is finite, then the sequence ω can be called *prequentially random*.

In other words, sequence ω is prequentially random with respect to measure P if there is a (in general different) measure Q with respect to which ω is random and which coincides with P on all initial segments of ω.

The requirement of prequentiality has been invoked in connection with a theory that extends probability theory and statistics to models of forecasting: see for example [5] and [26]. An example situation is the following. Let $\omega(n) = 1$ mean that there is rain on day n and 0 otherwise. Suppose that a forecasting office makes daily forecasts $p(1), p(2), \ldots$ of the probability of rain. It is not necessarily proposing a coherent probability model of global weather (a global probability distribution). It just provides forecasts for the conditional probabilities along the path corresponding to the weather that actually takes place.

Is it possible to estimate the quality of the forecast? It seems that in some situations, yes: if say, all forecasts are close to zero (say, less than 10%), and the majority of days (say more than 90%) is rainy. (It is said that the forecast is poorly *calibrated*.) Naturally, there are other possible inconsistencies, not related to the frequencies: the general question is whether the given sequence can be accepted as randomly obtained with the predicted probabilities. (Such a question arises also in the situation of estimating the quality of a random number generator each of whose output values is claimed to occur with whatever distribution the customer requires at that time of the process, for that particular bit.)

An additional circumstance to consider at the estimation of the quality of forecasts is that the forecaster can use a variety of information accessible to her at the moment of prediction (say, the evening of the preceding day), and not only

the members of the sequence ω. The presence of such information must also be taken into account at the estimation of the quality of the forecast.

The paper [26] proposes several different approaches to this question, which turn out to be equivalent. One involves a generalization of the notion of martingale (see Definition 3.8). It would be interesting to establish a connection with uniform randomness tests in the spirit of the above defined prequential deficiency. (Admittedly, in place of probabilities of initial segments, one must deal here with conditional probabilities, which is not quite the same, if these are not separated from zero.)

10 Questions for future discussion

We have already noted some questions that (in our view) would be interesting to study. In this section we collected a few more such questions.

1. Consider the following method for generating a sequence $\omega \in \Omega$ using an arbitrary distribution P on Ω in which the probabilities of all words are positive. Take a random sequence ρ of independent reals $\rho(1),\rho(2),\dots$ uniformly distributed over $[0,1]$. At stage n, after outputting $\xi(1:n-1)$, set $\xi(n)=1$ if

$$\rho(n) < P(\xi(1:n-1)1)/P(\xi(1:n-1)).$$

   Considering this as a random process, the output distribution will be exactly P. What sequences can be obtained on the ouput, from a Martin-Löf-random sequence of real numbers on the input? (It can be verified that for computable measures P one gets exactly the sequences that are Martin-Löf-random with respect to P.)

2. Recall the formula for the deficiency for computable measures:

$$\mathbf{t}(\omega,P) \stackrel{*}{=} \sum_{x \sqsubseteq \omega} \frac{\mathbf{m}(x)}{P(x)}. \tag{14}$$

   Both sides make sense for non-computable P, but this formula is no more true. Indeed, the right-hand side does not change significantly if a measure P is replaced by some other one that is close to P but is much more powerful as an oracle; and the left-hand side can become infinite while it was finite for P. Denote the righ-hand side by $t'(\omega,P)$. Does it make sense to take the finiteness of $t'(\omega,P)$ as a definition of randomness by a non-computable measure?

It will be at least monotonic (an increase of the measure will only increase randomness). With respect to mixtures of measures, we can say that it is quasi-convex; moreover, it is proved in [7] that $1/t'(\omega, P)$ is a concave function of P.

Another possibility is to define the randomness deficiency for an infinite sequence ω as $\log \sup_{x \sqsubset \omega} M(x)/P(x)$ (and consider the corresponding definition of randomness). For computable measures we obtain a definition equivalent to Martin-Löf's standard one. Paper [10] shows that the uniform tests defined by this expression (whether to use $\mathbf{m}(x)$ or $M(x)$) do not obey randomness conservation, while the universal uniform test does. The work [7] shows that, on the other hand, an expression related to the right-hand side of (14), whith the summation running over all positive basic functions instead of only the functions $1_{x\Omega}(\omega)$, obeys randomness conservation.

3. Can we define a reasonable class of tests with the property in Proposition 9.1 holding for all measures P (or some stronger version of it) so that there exists an universal class? For example, one may require

$$P \leqslant c \cdot Q \Rightarrow t(\omega, P) \geqslant t(\omega, Q)/c$$

(motivation: this is true for the right-hand side of formula (14). Could one also require the quasi-convexity, as in Proposition 9.2? Papers [16] and [8] provide some such examples, as well as [17].

How about the quasi-concavity of Proposition 9.2? A uniform test with this property seems less likely, since our counterexample seems more robust.

4. Relativization in recursion theory means that we take some set A and artificially declare it "decidable" by adding some oracle that tells us whether $x \in A$ for any given x. Almost all the theorems of classical recursion theory can be relativized. It is more delicate to declare some set E "enumerable". This means that we have some enumeration-oracle that enumerates the set E. The problem is, of course, that there are many enumerations. Still we can give the definition of an E-enumerable set. Let W be a set of pairs of the form (x, S) where x is an integer and S is a finite set of integers; assume W to be enumerable in the classical sense. Then consider the set $S(E, W)$ of all x such that $(x, S) \in W$ for some $S \subset E$. The sets $S(E, W)$ (for fixed E and all enumerable W) are called *enumerable with respect to the enumeration-oracle* E. (The relation $(x, S) \in E$ means that we add x to the E-enumeration as soon as we see all elements of S in E.) A standard (decision) oracle for a set A

can be considered a special case of an enumeration oracle (say, for the set $\{2n : n \in A\} \cup \{2n+1 : n \notin A\}$.

For some purposes, an enumeration oracle is as meaningful as a decision oracle: for example, we can speak about a lower semicomputable function with respect to enumeration oracle E, since it can be defined in terms of enumerable sets. But what can be proved for this kind of relativized notions?

For example, is there (for an arbitrary E) a maximal lower E-semicomputable semimeasure? Can one define prefix complexity with oracle E, and will it coincide with the logarithm of the maximal semimeasure lower semicomputable relative to E (if the latter exists)? What if we assume, in addition, that E is the set of all basic balls in a constructive metric space, containing a given point?

(For comparison: we could define an E-computable function as a function whose graph is E-enumerable. Then some familiar properties will hold; say, the composition of E-computable functions is again E-computable. On the other hand, we cannot guarantee that every non-empty E-enumerable set is the range of a total E-computable function: for some E this is not so.)

5. We may try do extend the definition of randomness in a different direction: to lower semicomputable semimeasures (that is output distributions of probabilistic machines that generate output sequence bit by bit). Levin's motivation for his definition was his goal to define the independence of the pair (x,η) of infinite sequences as randomness with respect to the semimeasure $M \times M$. Correspondingly, the the deficiency of randomness of the pair (ξ,η) with respect to $M \times M$ could be called the quantity of mutual information between the sequences ξ and η. This is motivated by the fact that the algorithmic mutual information

$$Kp(x) + Kp(y) - Kp(x,y) = -\log(\mathbf{m}(x) \times \mathbf{m}(y)) - Kp(x,y)$$

between finite objects x,y indeed looks like deficiency of randomness with respect to $\mathbf{m} \times \mathbf{m}$.

One possibility is to require that $M(z)/Q(z)$ is bounded, where M is a priori probability on the tree and Q is the semimeasure in question. The other possibility is to use random sequences for unbiased coin tossing and consider the output sequences in all these cases. It is not clear whether these two definitions coincide or if the second notion is well-defined (that is for two different machines with the same output distribution the image of the set of random sequences is the same). For *computable measures* it is indeed the case.

6. (Steven Simpson) Can we use uniform tests (modified in a proper way) for defining, say, 2-randomness? (The standard definition uses non-semicontinuous tests, but maybe it can be reformulated.)

Acknowledgements

The authors are thankful to their colleagues with them they have discussed the questions considered in the paper: first to L. Levin with whom many of the concepts of the paper originate, to A. Bufetov and A. Klimenko, and also to V. V'yugin and other participants of the Kolmogorov seminar (at the Mechanico-Mathematical school of Moscow State University). The paper was written with the financial support of the grants NAFIT ANR-08- EMER-008-01, RFBR 0901-00709-a, ...

Bibliography

[1] Jeremy Avigad, Philipp Gerhardy, and Henry Towsner. Local stability of ergodic averages. *Transactions of the American Mathematical Society*, 362(1):261–288, 2010. 8

[2] Laurent Bienvenu, Adam Dauy, Mathieu Hoyrup, Ilya Mezhirov, and Alexander Shen. A constructive version of Birkhoff's ergodic theorem for Martin-Löf random points. Technical report, 2010. arXiv.org:1007.5249. 8

[3] Laurent Bienvenu, Andrei Romashchenko, and Alexander Kh. Shen. Sparse sequences. In *Journees Automates Cellulares (Uzes)*, pages 18–28, Moscow, 2008. MCCME publishers. http://hal.archives-ouvertes.fr/hal-00274010/en. 5.4, 5.4

[4] Gregory J. Chaitin. A theory of program size formally identical to information theory. *J. Assoc. Comput. Mach.*, 22:329–340, 1975. 2.4

[5] Alexey Chernov, Alexander Kh. Shen, Nikolai Vereshchagin, and Vladimir G. Vovk. On-line probability, complexity and randomness. In Yoav Freund, Laszlo Gyorfi, Gyorgy Turan, and Thomas Zeugmann, editors, *Proceedings of the nineteenth international conference on algorithmic learning theory*, pages 138–153, Tokyo, 2008. 9.2

[6] Peter Gács. Lecture notes on descriptional complexity and randomness. Technical report, Boston University, Computer Science Dept., Boston, MA 02215. www.cs.bu.edu/~gacs/papers/ait-notes.pdf. 2.4, 5, 7.1

[7] Peter Gács. *Complexity and Randomness*. PhD thesis, J.W. Goethe University, Frankfurt, W.Germany, 1978. In German. 2

[8] Peter Gács. Exact expressions for some randomness tests. *Z. Math. Log. Grdl. M.*, 26:385–394, 1980. Short version: Springer Lecture Notes in Computer Science 67 (1979) 124-131. 2.4, 9.1, 3

[9] Peter Gács. On the relation between descriptional complexity and algorithmic probability. *Theoretical Computer Science*, 22:71–93, 1983. Short version: Proc. 22nd IEEE FOCS (1981) 296-303. 2.4

[10] Peter Gács. Uniform test of algorithmic randomness over a general space. *Theoretical Computer Science*, 341(1-3):91–137, 2005. 1, 2.4, 6, 6, 7.1, 2

[11] Mathieu Hoyrup and Cristóbal Rojas. An application of Martin-Löf randomness to effective probability. In *Cie2009, LNCS 5635*, pages 260–269, 2009. 5.42

[12] Mathieu Hoyrup and Cristóbal Rojas. Computability of probability measures and Martin-Löf randomness over metric spaces. *Information and Computation*, 207(7):830–847, 2009. 1, 4.3, 7.1, 7.2

[13] Andrei N. Kolmogorov. On the logical foundations of information theory and probability theory. *Problems of Information Transmission*, 5(3):1–4, 1969. 2

[14] K. Kuratowski. *Topology.* Academic Press, New York, 1966. 8

[15] Leonid A. Levin. On the notion of a random sequence. *Soviet Math. Dokl.*, 14(5):1413–1416, 1973. 1, 2.4

[16] Leonid A. Levin. Uniform tests of randomness. *Soviet Math. Dokl.*, 17(2):337–340, 1976. 2.4, 6, 9.1, 3

[17] Leonid A. Levin. Randomness conservation inequalities: Information and independence in mathematical theories. *Information and Control*, 61(1):15–37, 1984. 2.4, 9.1, 3

[18] Ming Li and Paul M. B. Vitányi. *Introduction to Kolmogorov Complexity and its Applications (Third edition)*. Springer Verlag, New York, 2008. 2.2, 2.3, 2.4, 2.4

[19] Per Martin-Löf. The definition of random sequences. *Information and Control*, 9:602–619, 1966. 1

[20] Y. T. Medvedev. Degrees of difficulty of mass problems. *Doklady Akademii Nauk SSSR. N.S.*, 104:501–504, 1955. In Russian. Mathematical Reviews (MathSciNet): MR0073542. 7.3

[21] Joseph S. Miller. Degrees of unsolvability of continuous functions. *The Journal of Symbolic Logic*, 62(2):555–584, 2004. 5.1

[22] Claus Peter Schnorr. Process complexity and effective random tests. *J. Comput. Syst. Sci*, 7(4):376–388, 1973. Conference version: STOC 1972, pp. 168-176. 2.4

[23] Glenn Shafer, Alexander Kh. Shen, Nikolai Vereshchagin, and Vladimir Vovk. Test martingales, Bayes factors and p-values. arXiv:0912.4269v2 [math.ST], 15pp, 2009. 2.3

[24] Glenn Shafer and Vladimir G. Vovk. *Probability and Finace: It's Only a Game!* Wiley, New York, 2001. ISBN: 978-0-471-40226-8. 2.5

[25] Alexander Kh. Shen. Algorithmic information theory and Kolmogorov complexity. Technical report, Uppsala University, 2000. TR2000-34, 31pp. Available at http://www.it.uu.se/research/publications/reports/2000-034/. 2.3, 2.4, 2.4

[26] Alexander Kh. Shen and Vladimir G. Vovk. Prequential randomness and probability. *Theoretical Computer Science*, 411:2632–2646, 2010. 9.2

[27] Volker Strassen. The existence of probability measures with given marginals. *Annals of Mathematical Statistics*, 36:423–439, 1965. 5.4

[28] V. V. V'yugin. Ergodic theorems for individual random sequences. *Theoretical Computer Science*, 207(2):343–361, 1998. 8, 8

[29] Alexander K. Zvonkin and Leonid A. Levin. The complexity of finite objects and the development of the concepts of information and randomness by means of the theory of algorithms. *Russian Math. Surveys*, 25(6):83–124, 1970. 1, 2.28

Алгоритмические тесты и случайность относительно классов мер

Л. Биенвеню[*], П. Гач[†], К. Рохас[‡], М. Хойруп[§], А. Шень[¶]

Аннотация

В этой работе приводятся некоторые новые результаты об алгоритмической случайности по отношению к классам мер, а также подробно излагаются известные (но не опубликованные подробно) результаты об алгоритмических тестах случайности.

Мы начинаем с переформулировки определения случайности по Мартин-Лёфу в терминах тестов случайности (функций, измеряющих степень "неслучайности" последовательностей). Приводится формула, выражающая значение универсального теста в терминах префиксной сложности. Рассматриваются также варианты определения дефекта случайности для конечных слов, связанные с универсальным тестом.

Далее рассматривается (введённое ещё Мартин-Лёфом) понятие бернуллиевой последовательности (как последовательности, не противоречащей гипотезе о том, что все испытания независимы и имеют одинаковую вероятность успеха). Показано, что определение с помощью универсального теста эквивалентно первоначальному определению Мартин-Лёфа и что последовательность является бернуллиевой тогда и только тогда, когда она случайна по Мартин-Лёфу относительно бернуллиевой меры B_p при некотором p (с оракулом для p).

Затем этот же вопрос (о сравнении тестов относительно классов мер и тестов как функции двух аргументов — последовательности и меры) применяется к произвольным эффективно замкнутым классам мер в канторовском пространстве. Изучаются свойства ортогональных классов мер и указываются предположения, в которых два понятия случайности (равномерная и безоракульная) совпадают.

В заключение рассматриваются обобщения некоторых из указанных результатов на случай произвольных метрических пространств.

1 Введение

Эта работа может рассматриваться как продолжение [10] (которая в свою очередь является развитием давних идей Л. Левина) и [12].

[*]Laurent Bienvenu, LIAFA, CNRS & Université Paris Diderot, Paris 7, Case 7014, 75205 Paris Cedex 13, France, e-mail: `Laurent dot Bienvenu at liafa dot jussieu dot fr`

[†]Peter Gács, Department of Computer Science, Boston University, 111 Cummington st., Room 138, Boston, MA 02215, e-mail: `gacs at bu dot edu`

[‡]Cristobal Rojas, Department of Mathematics, University of Toronto, Bahen Centre, 40 St. George St., Toronto, Ontario, Canada, M5S 2E4, e-mail: `crojas at math dot utoronto dot ca`

[§]Mathieu Hoyrup, LORIA – B248, 615, rue du Jardin Botanique, BP 239, 54506 Vandœuvre-lès-Nancy, France, e-mail: `Mathieu dot Hoyrup at loria dot fr`

[¶]Alexander Shen, LIF, Universitè Aix – Marseille, CNRS, 39, rue Joliot-Curie, 13453 Marseille cedex 13, France, on leave from ИППИ РАН, Б. Каретный, 19, Москва. Supported by NAFIT ANR-08-EMER-008-01, RFBR 0901-00709-a grants. e-mail: `sasha dot shen at gmail dot com`.

Хорошо известны различные варианты определения понятия случайной последовательности нулей и единиц, соответствующие равномерному распределению (бросанию честной монеты). Большинство этих результатов естественно переносится на случай произвольного вычислимого распределения вероятностей на пространстве Ω бесконечных последовательностей нулей и единиц.

Наша цель — исследовать возможности определения случайности в более общей ситуации, когда распределение на Ω не является вычислимым (или когда рассматривается случайность в других пространствах, не только в Ω). Для этой цели мы рассматриваем тест случайности $\mathbf{t}(\omega, P)$ как функцию двух переменных, последовательности ω и меры P. Большие значения такого теста, интуитивно говоря, соответствуют ситуациям, когда гипотеза о том, что последовательность ω получилась в результате случайного выбора по мере P, неправдоподобна.

Кроме того, следуя [15], мы будем рассматривать тесты относительно классов мер, обладающих свойством типа компактности. Такой тест, $t_{\mathcal{C}}(\omega)$, измеряет, насколько неправдоподобным кажется появление последовательности ω в результате случайного процесса, распределение вероятностей которого (нам неизвестное) принадлежит классу $\mathcal{C}$. Мы покажем, что для класса бернуллиевых мер (независимые испытания с одинаковой вероятностью успеха) возникающее понятие случайности относительно этого класса совпадает с введённым Мартин-Лёфом в [19].

Для классов, меры в которых попарно ортогональны (в некотором эффективном смысле), мы получаем разложение теста случайности по данной мере на два: один проверяет случайность относительно класса мер, а второй проверяет (достаточно грубо) соответствие последовательности конкретной мере. Для случая бернуллиевых мер в качестве второго теста можно взять просто закон больших чисел и проверять, что предельная частота действительно равна декларируемой вероятности успеха. Аналогичное разбиение возможно и для других классов, соответствующих эргодическим стационарным процессам.

Определение случайности с помощью равномерных тестов $\mathbf{t}(\omega, P)$, вообще говоря, не обладает некоторыми интуитивно желательными свойствами (скажем, не монотонно по P в естественном смысле). Но для случая эффективно ортогональных классов оно равносильно другому, "слепому" определению случайности, в котором рассматриваются лишь тесты, вычисление которых не использует меру P как оракул.

Статья начинается с переформулировки определения случайности по Мартин-Лёфу (относительно вычислимых мер) в терминах тестов. Значения теста мы рассматриваем как количественную характеристику "неслучайности" последовательности, и считаем случайными последовательностями те, для которых тест конечен. Мы рассматриваем два вида тестов (ограниченные в среднем и ограниченные по вероятности) и показываем, что они близки друг к другу.

Затем мы приводим формулу, которая выражает значение (ограниченного в среднем) теста через префиксную сложность (и даже два варианта такой формулы — с максимумом и с суммой). Эта формула является количественным уточнением критерия случайности Левина – Шнорра (в форме с префиксной сложностью, как в статье Чейтина). Далее мы обсуждаем некоторые варианты движения в обратную сторону: как от дефекта случайности для бесконечных последовательностей перейти к дефекту случайности конечных.

Далее мы определяем понятие теста бернуллиевости (частный случай случайности относительно класса мер, в данном случае — класса бернуллиевых мер). Мы показываем, что множество бернуллиевых последовательностей, для которых этот тест конечен, совпадает с объединением по всем $p \in [0, 1]$ множеств последовательностей, случайных в смысле Мартин-Лёфа относительно бернуллиевой меры B_p, при этом в определении случайности добавляется оракул для p. Для этого мы вводим понятие равномерного бернуллиева теста и устанавливаем

количественный вариант указанного результата: дефект бернуллиевости равен точной нижней грани (по p) дефектов случайности относительно каждой из мер B_p.

После этого мы вводим понятие равномерного теста (уже не ограничиваясь конкретным классом мер) и соответствующее ему понятие равномерной случайности (которое для случая вычислимых мер совпадает с определением Мартин-Лёфа).

Бернуллиевы меры обладают тем свойством, что видя случайную по одной из этих мер последовательность, можно восстановить значение p как предельную частоту единиц (закон больших чисел). Мы показываем, что для подобных классов мер различные определения случайности (равномерное и "слепое", когда тест не использует меру) равносильны. Это утверждение обобщается и на меры в произвольных конструктивных метрических пространствах.

Наконец, введём некоторые полезные обозначения.

Мы будем писать $f(x) \stackrel{\cdot}{<} g(x)$ для положительных функций f и g, если указанное неравенство выполняется с точностью до мультипликативной константы, то есть $f(x) \leqslant cg(x)$ для некоторого c и для всех x.

Запись $f(x) \stackrel{\cdot}{=} g(x)$ означает $f(x) \stackrel{\cdot}{<} g(x)$ и $g(x) \stackrel{\cdot}{<} f(x)$.

Обозначения $f(x) \stackrel{+}{<} g(x)$ и $f(x) \stackrel{+}{=} g(x)$ имеют аналогичный смысл (неравенство с точностью до аддитивной константы).

Через Λ мы обозначаем пустое слово (строку нулевой длины). Длина слова x обозначается $|x|$. Запись $x \sqsubseteq y$ или $y \sqsupseteq x$ означает, что слово x является началом (префиксом) слова y. Элементы бесконечной последовательности x (а также буквы слова x) обозначаются $x(1), x(2), \ldots$; её начало длины n обозначается $x(1:n)$.

Часто мы рассматриваем функции со значениям в множестве $\overline{\mathbb{R}}_+ = [0, +\infty]$ (неотрицательные функции, возможно, бесконечные в некоторых точках). Множества натуральных и действительных чисел обозначаются $\mathbb{N}$ и $\mathbb{Z}$; через $\mathbb{B}$ иногда обозначается множество $\{0, 1\}$.

Логарифмы, если не указано иное, берутся по основанию 2.

2 Случайность последовательностей относительно вычислимых мер

Мы начнём с определения случайности бесконечных двоичных последовательностей относительно вычислимых мер.

2.1 Перечислимые снизу функции на Ω

Определение 2.1 (Канторовское пространство)**.** *Множество $\{0,1\}^{\mathbb{N}}$ бесконечных двоичных последовательностей мы называем* двоичным канторовским пространством *и обозначаем Ω. Для каждого конечного двоичного слова x мы рассматриваем* интервал $x\Omega$*, состоящий из всех последовательностей, начинающихся на x. Интервалы являются* базисными открытыми множествами *стандартной топологии канторовского пространства;* открытыми *являются произвольные объединения интервалов.*

Понятие открытого множества, как и другие топологические понятия, имеет эффективный аналог.

Определение 2.2. Эффективно открытыми *множествами называют объединения перечислимых семейств интервалов.* Эффективно замкнутыми *называются дополнения эффективно открытых множеств.*

Далее можно определить эффективные G_δ *множества как счётные пересечения $\cap_i U_i$ последовательности эффективно открытых множеств U_i; при этом требуется, чтобы U_i*

было эффективно открыто равномерно по i (алгоритм получает на вход i и перечисляет интервалы, образующие U_i).

Будем называть функцию $t\colon \Omega \to [0,\infty]$ перечислимой снизу, *если*

(а) *для любого рационального r множество $U_r = \{\omega \mid r < t(\omega)\}$ открыто,*

(б) *и, более того, U_r эффективно открыто равномерно по r (существует алгоритм, который получает r и перечисляет интервалы, образующие U_r).*

Условие (а) означает, что функция t полунепрерывна снизу, так что перечислимость снизу является эффективизацией понятия полунепрерывности.

Понятие перечислимой снизу функции в дальнейшем играет важную роль. Его можно определить различными (эквивалентными) способами. Вот одна из таких переформулировок.

Определение 2.3. *Функция с рациональными значениями, определённая на Ω, называется* базисной, *если её значение на последовательности ω определяется конечным началом ω.*

Если это начало имеет длину N, то функция может принимать до 2^N значений, и её можно задать таблицей из 2^N строк, в которой для каждого варианта начала (двоичного слова длины N) указано рациональное значение функции. Поэтому базисные функции можно считать конструктивными объектами.

Следующее предложение легко следует из определений:

Предложение 2.4. *Перечислимые функции и только они являются поточечными пределами вычислимых возрастающих последовательностей базисных функций.*

Разность двух базисных функций тоже является базисной функцией, поэтому вместо пределов возрастающих функций можно говорить о суммах рядов, составленных из неотрицательных базисных функций.

Вот ещё один вариант определения перечислимых снизу функций на Ω.

Определение 2.5 (Порождающие функции)**.** *Будем говорить, что определённая на двоичных словах функция T со значениями в $[0,+\infty]$ является* перечислимой снизу, *если множество пар $\langle x, r\rangle$, где x — двоичное слово, а r — рациональное число, меньшее $T(x)$, перечислимо.*

Для каждой такой функции T определим функцию t на бесконечных последовательностях, положив

$$t(\omega) = \sup_{x \sqsubseteq \omega} T(x);$$

будем говорить, что функция T порождает *функцию t.*

Предложение 2.6. *При этом порождаются все перечислимые снизу функции на Ω и только они.*

Можно наложить дополнительные ограничения на порождающую функцию T, сохранив возможность порождать любую перечислимую снизу функцию на Ω. Например, можно требовать, чтобы функция T была монотонной (это значит, что $T(x) \leqslant T(y)$ при $x \sqsubseteq y$). В самом деле, от любой функции можно перейти к монотонной, положив $T'(x) = \max_{z \sqsubseteq x} T(z)$. Можно также потребовать, чтобы функция T принимала рациональные значения и была бы вычислимой (а не только перечислимой снизу). В самом деле, поскольку в определении участвует $\sup T(x)$ по всем x, являющимся началом ω, вместо увеличения $T(x)$ для некоторого x можно увеличить значения функции T для всех его продолжений достаточно большой длины, и эта задержка позволяет сделать функцию T вычислимой.

Следующее наблюдение использует компактность канторовского пространства. Среди всех функций T, порождающих данную функцию t, можно выбрать максимальную, положив

$$T(x) = \inf_{\omega \sqsupseteq x} t(\omega).$$

Предложение 2.7. *Определённая таким образом функция T перечислима снизу и порождает t. В её определении можно заменить* inf *на* min.

Доказательство. Очевидно, что порождаемая функция не превосходит t. С другой стороны, если $t(\omega) > r$, то в силу полунепрерывности снизу это верно в некоторой окрестности ω, и потому $T(x) \geqslant r$ для некоторого начала $x \sqsubseteq \omega$. Таким образом, порождаемая функция совпадает с t.

Остаётся убедиться, что T перечислима снизу. В самом деле, $r < \inf_{\omega \sqsupseteq x} t(\omega)$ тогда и только тогда, когда существует $r' > r$, для которого $r' < t(\omega)$ для всех $\omega \sqsupseteq x$. Последнее условие может быть переформулировано так: открытое множество тех последовательностей ω, для которых $t(\omega) > r'$, покрывает интервал $x\Omega$. Это открытое множество (по определению перечислимости снизу) есть объединение перечислимого семейства интервалов, и в силу компактности уже конечное число интервалов образует подпокрытие. Поскольку это в какой-то момент обнаруживается, указанное свойство перечислимо, и квантор существования по r' сохраняет перечислимость.

Полунепрерывность снизу также гарантирует, что минимум на компактном множестве достигается, так что inf можно заменить на min.

2.2 Тесты случайности

Мы предполагаем, что читатель знаком с основными понятиями теории меры (хотя бы для канторовского пространства Ω). Напомним, что мера (распределение вероятностей) P на Ω задаётся своими значениями на цилиндрах $x\Omega$. Эти значения задают неотрицательную действительную функцию на двоичных словах, которую мы обозначаем той же буквой, что и саму меру:

$$P(x) = P(x\Omega).$$

При этом

$$P(\Lambda) = 1, \quad P(x) = P(x0) + P(x1),$$

и любая неотрицательная функция на двоичных словах, обладающая этими двумя свойствами, соответствует мере на Ω.

Среди всех мер выделяются вычислимые.

Определение 2.8 (Вычислимые меры)**.** *Действительное число x называется* вычислимым*, если существует алгоритм, который по любому рациональному $\varepsilon > 0$ указывает рациональное приближение к x с абсолютной погрешностью не более ε.*

Вычислимые действительные числа можно определять также как пределы последовательностей $x_1, x_2, \ldots$, для которых $|x_n - x_{n+k}| \leqslant 2^{-n}$.

Функция, определённая на словах (или иных конструктивных объектах) и принимающая действительные значения, называется вычислимой*, если её значения вычислимы равномерно по входу, то есть существует алгоритм, который по входу и по $\varepsilon > 0$ указывает ε-приближение к значению функции на этом входе.*

Мера на Ω называется вычислимой*, если вычислима функция $P\colon \{0,1\}^* \to [0,1]$, соответствующая этой мере.*

Пусть фиксирована вычислимая (вероятностная) мера на Ω.

Определение 2.9 (Тест случайности по вычислимой мере)**.** *Перечислимая функция* $t\colon \Omega \to [0, +\infty]$ *называется* (ограниченным в среднем) тестом *относительно меры* P (P*-тестом*), *если её интеграл* (*математическое ожидание*) *по мере* P *не превосходит* 1*:*

$$\int t(\omega)\, dP(\omega) \leqslant 1.$$

Последовательность ω проходит *тест* t*, если* $t(\omega)$ *конечно* (*напомним, что мы рассматриваем перечислимые снизу функции, которые могут принимать бесконечные значения*).

Последовательность ω *называется* случайной *по мере* P*, если она проходит все* P*-тесты.*

Интуитивный смысл этого определения можно описать так: $t(\omega)$ отражает "количество закономерностей" в ω. Строя тест, мы можем объявить "закономерностью" любое (эффективно обнаруживаемое) свойство последовательности, надо только следить, чтобы их было не слишком много, иначе интеграл превысит границу.

Это определение эквивалентно (даёт тот же класс случайных последовательностей) классическому определению Мартин-Лёфа (см. ниже). Но сначала отметим, что среди тестов существует универсальный (максимальный):

Теорема 2.10. *Для любой вычислимой меры* P *существует универсальный* (*максимальный*) *тест* u*: это означает, что для любого* P*-теста* t *найдётся константа* c*, при которой*

$$t(\omega) \leqslant c \cdot u(\omega)$$

при всех $\omega \in \Omega$*.*

В частности, универсальность гарантирует, что всякая проходящая тест u последовательность проходит все другие тесты. Тем самым множество последовательностей, проходящих тест u, совпадает с множеством случайных последовательностей.

Доказательство. Будем перечислять все алгоритмы, задающие перечислимые снизу функции. (Такой алгоритм порождает возрастающую последовательность базисных функций.) Не все эти перечислимые функции будут тестами (интеграл может превысить единицу), но мы можем их фильтровать и не пропускать очередную функцию, пока не будет установлено, что её интеграл меньше (скажем) 2. (Напомним, что мера P вычислима, поэтому если интеграл меньше 2, то мы сможем в этом убедиться.) Такая фильтрация пропустит все тесты и ещё некоторые функции, которые превосходят тесты не более чем вдвое. Остаётся сложить все профильтрованные функции с коэффициентами, сумма которых не превосходит $1/2$, скажем, $1/2^{i+2}$.

В такой форме тесты случайности фигурировали в [8].

Убедимся, что это определение эквивалентно классическому определению Мартин-Лёфа:

Определение 2.11. *Пусть* P *— вычислимое распределение вероятностей на* Ω*. Последовательность открытых множеств* $U_1, U_2, \ldots$ *называется* тестом Мартин-Лёфа*, если множество* U_i *эффективно открыто* (*равномерно по* i) *и его мера не превосходит* 2^{-i}*.*

Последовательность ω проходит *этот тест, если она не принадлежит пересечению* $\cap_i U_i$*. Такие пересечения* (*а также все их подмножества*) *называют* эффективно нулевыми множествами*.*

Можно было бы рассматривать только эти пересечения (а не все их подмножества): такие множества было бы логично называть *эффективными нулевыми множествами.* Они являются эффективными G_δ-множествами (пересечениями последовательности равномерно эффективно открытых множеств).

Как мы уже говорили, это определение равносильно приведённому выше:

Теорема 2.12. *Последовательность проходит все тесты Мартин-Лёфа тогда и только тогда, когда она проходит все ограниченные в среднем тесты.*

Доказательство. Если t — ограниченный в среднем тест, то множество U_i тех ω, для которых $t(\omega) > 2^i$, эффективно открыто и имеет меру не более 2^{-i}, так что получается тест Мартин-Лёфа. Поэтому если ω проходит все тесты Мартин-Лёфа, то $t(\omega)$ конечно.

С другой стороны, из любого теста Мартип-Лёфа $\{U_i\}$ легко сделать ограниченный в среднем тест. Положим $t_i(\omega)$ равным 2^i внутри U_i и нулю вне U_i; функция t_i перечислима снизу и имеет среднее не больше 1, то есть представляет собой тест. Остаётся сложить, скажем, t_{2i} с весами 2^{-i}: если ω лежит в U_{2i}, то такая сумма будет не меньше 2^i.

В дальнейшем, говоря о случайности, мы будем иметь в виду случайность в смысле (любого из) этих определений определений, если не оговорено противное.

Ограниченные в среднем тесты не только отделяют случайные последовательности от неслучайных, но и классифицируют случайные последовательности: чем больше значение теста, тем ближе последовательность к неслучайным. Удобно перейти при этом к логарифмической шкале:

Определение 2.13. *Фиксируем некоторый универсальный (ограниченный в среднем) P-тест $\mathbf{t}_P(\omega)$. Через $\mathbf{d}_P(\omega)$ обозначим логарифм этого теста:*

$$\mathbf{t}_P(\omega) = 2^{\mathbf{d}(\omega)}.$$

Можно сказать, что $\mathbf{d}_P(\omega)$ измеряет в битах "дефект случайности" последовательности ω (количество закономерностей в ω).

При нашем определении дефект бывает отрицательным (и даже может быть равным $-\infty$): интеграл от теста не больше 1, и потому тест имеет значения, меньшие единицы. Можно изменить универсальный тест (взять его полусумму с постоянным тестом, везде равным единице) и добиться того, чтобы дефект был всегда не меньше -1. Можно также сделать дефект целочисленным (заменив каждое значение теста на максимальную степень двойки, меньшую его). Чтобы избавиться от отрицательных дефектов, можно разрешить тестам иметь любые конечные средние (не обязательно меньше единицы):

Предложение 2.14. *Функция $\mathbf{d}_P$ является максимальной (с точностью до константы) перечислимой снизу функцией на Ω, для которой P-среднее от $2^{\mathbf{d}_P(\cdot)}$ конечно.*

Замечание 2.15.

1. *Оригинальное определение Мартин-Лёфа также может быть использовано для измерения дефекта случайности. Именно, можно считать, что элементы множества U_i имеют дефект i или больше. Этот способ измерения дефекта, использованный в* [29]*, эквивалентен ограниченным по вероятности тестам (см. следующий раздел).*

2. *Мы определили функцию $\mathbf{d}_P(x)$ отдельно для каждой меры P (с точностью до константы). В дальнейшем мы определим (также с точностью до константы) функцию $\mathbf{d}(\omega, P)$ двух аргументов, которая будет для каждой вычислимой меры P совпадать с $\mathbf{d}_P$ (с той же точностью).*

2.3 Тесты, ограниченные по вероятности и в среднем

Приведённое выше определение ограниченного в среднем теста в каком-то смысле аналогично определению префиксной колмогоровской сложности; есть и другой вариант определения,

который больше похож на обычную сложность. (Определение префиксной и обычной сложности можно найти, например, в [25, 18]; мы используем эти понятия лишь как образец для аналогий, и потому не обсуждаем их подробно.)

Ослабим требования на тесты: вместо условия $\int t(\omega)\,dP(\omega) \leqslant 1$ будем требовать, чтобы для любого $c > 0$ множество последовательностей ω, для которых $t(\omega) > c$, имело бы меру не больше $1/c$. (Это условие следует из прежнего согласно неравенству Чебышёва.) Такие тесты будем называть *ограниченными по вероятности*.

В логарифмической шкале это определение может быть переформулировано так: P-мера множества последовательностей, имеющих дефект больше n, не превосходит 2^{-n}. Если ограничиться целыми значениями n, то мы приходим к классическому определению Мартин-Лёфа (см. замечание 2.15).

Легко видеть, что и при этом определении среди всех тестов существует максимальный (с точностью до умножения на константу). Ему соответствует максимальная (с точностью до аддитивной константы) функция дефекта. В самом деле, будем перечислять все тесты (и почти-тесты, где условие на меру вдвое ослаблено) и соответствующие им функции дефекта d_i. Затем возьмём их максимум (с аддитивными добавками, соответствующими весам):

$$\mathbf{d}(\omega) = \max_i [d_i(\omega) - i] - c.$$

Этот максимум может быть меньше d_i только на $i + c$; с другой стороны, множество тех ω, для которых $\mathbf{d}(\omega) > k$, представляет собой объединение множеств $\{\omega \mid d_i(\omega) > k + i + c\}$. Меры этих множеств не превосходят $O(2^{-k-i-c})$, и при подходящем c их объединение имеет меру не больше 2^{-k}, как и требуется.

Возникает естественный вопрос: как связаны значения универсального ограниченного в среднем теста $\mathbf{t}^{\mathrm{aver}}$ и универсального ограниченного по вероятности теста $\mathbf{t}^{\mathrm{prob}}$? Как мы видели, они оба бесконечны на одних и тех же последовательностях; более того, и конечные значения их близки:

Предложение 2.16.

$$\mathbf{d}^{\mathrm{aver}}(\omega) \stackrel{+}{<} \mathbf{d}^{\mathrm{prob}}(\omega) \stackrel{+}{<} \mathbf{d}^{\mathrm{aver}}(\omega) + 2\log \mathbf{d}^{\mathrm{aver}}(\omega)$$

Доказательство. Как мы видели, ограниченные в среднем тесты автоматически ограничены по вероятности, откуда следует первое неравенство. Чтобы доказать второе неравенство, рассмотрим произвольный ограниченный по вероятности тест и его логарифм $d(\omega)$. Покажем, что $d - 2\log d$ ограничен в среднем (в логарифмической шкале). В самом деле, событие "$d(\omega)$ находится между $i-1$ и i" имеет вероятность не более $1/2^{i-1}$, интеграл от $2^{d-2\log d}$ по этому множеству не превосходит $2^{-i+1}2^{i-2\log i} = O(1/i^2)$, и потому интеграл по всему пространству конечен.

Остаётся заметить, что неравенство $a \stackrel{+}{<} b + 2\log b$ следует из $b \stackrel{+}{>} a - 2\log a$. В самом деле, из $b \geqslant a - 2\log a$ следует $b \geqslant a/2$ (при достаточно больших a) и потому $\log a \leqslant \log b + 1$, так что $a \stackrel{+}{<} b + 2\log a \stackrel{+}{<} b + 2\log b$.

В общем случае вопрос о том, как связана ограниченность в среднем и ограниченность по вероятности, разбирается в статье [23]. Там показано (и это несложно), что если $u\colon [1, +\infty] \to [0, +\infty]$ — монотонная непрерывная функция, для которой $\int_1^\infty u(t)/t^2\,dt \leqslant 1$, то $u(t(\omega))$ является ограниченным в среднем тестом для любого ограниченного по вероятности теста t, и что это условие на u нельзя улучшить. (Наша оценка получается при $u(x) \sim x/\log^2 x$.)

Замечание 2.17. *Последнее предложение напоминает соотношение между простой и префиксной сложностями (как и с точки зрения соотношения между определениями — в одном ограничивается интеграл, в другом количество объектов, — так и по результатам). Важно иметь в виду, что сейчас разница между двумя величинами ограничена логарифмом* дефекта*, и потому мала, если последовательность близка к случайной, в то время как для разница между префиксной и обычной сложностями оценивается через логарифм самих этих величин (который велик для случайных объектов).*

Вопрос. Интересно было бы понять, отличаются ли два вида тестов лишь некоторым сдвигом шкалы или более существенным образом. Подтверждением такого более существенного различия могло бы служить семейство последовательностей ω_i и ω'_i, для которых

$$\mathbf{d}^{\mathrm{aver}}(\omega_i) - \mathbf{d}^{\mathrm{aver}}(\omega'_i) \to +\infty$$

при $i \to \infty$, но

$$\mathbf{d}^{\mathrm{prob}}(\omega_i) - \mathbf{d}^{\mathrm{prob}}(\omega'_i) \to -\infty.$$

Авторы не знают, существует ли такое семейство.

2.4 Формула для ограниченного в среднем дефекта

Эта формула использует понятие априорной вероятности (или префиксную сложность); напомним соответствующие определения (подробнее см. в [25, 18]).

Определение 2.18. *Множество двоичных слов называется* беспрефиксным*, если ни один из его элементов не является началом другого. Вычислимая частичная функция T из множества двоичных слов в себя называется* самоограниченным декомпрессором*, если её область определения является беспрефиксным множеством. Мы определяем сложность $KP_D(x)$ слова x относительно декомпрессора D как минимальную длину слова p, для которого $D(p) = x$. Среди всех самоограниченных декомпрессоров существует* оптимальный*, для которого функция KP_D минимальна с точностью до аддитивной константы. Эта минимальная функция (для некоторого фиксированного оптимального декомпрессора) называется* префиксной сложностью *и обозначается $KP(x)$.*

Величина $\mathbf{m}(x) = 2^{-KP(x)}$ называется дискретной априорной вероятностью *слова x.*

Название “априорная вероятность” связано с тем, что эта функция является максимальной (с точностью до постоянного множителя) в некотором классе вероятностных распределений. Мы приведём соответствующие определения и формулировки без доказательства.

Определение 2.19. *Функция $f\colon \{0,1\}^* \to [0,\infty)$ называется* дискретной полумерой*, если $\sum_x f(x) \leqslant 1$.*

Перечислимые снизу дискретные полумеры можно описать как выходные распределения вероятностных алгоритмов, использующих датчик случайных чисел и выдающих на выход некоторое слово (если алгоритм останавливается; с некоторой вероятностью он может и не остановиться).

Предложение 2.20. *Функция $\mathbf{m}(x)$ является перечислимой снизу дискретной полумерой, максимальной в этом классе с точностью до константы: для любой перечислимой снизу дискретной полумеры f найдётся такая константа c, что $c \cdot \mathbf{m}(x) \geqslant f(x)$ при всех x.*

Теперь можно указать явную формулу для универсального ограниченного в среднем теста случайности:

Предложение 2.21. *Для данной вычислимой меры P универсальный ограниченный в среднем тест $\mathbf{t}_P$ задаётся формулой:*

$$\mathbf{t}_P(\omega) \doteq \sum_{x \sqsubseteq \omega} \frac{\mathbf{m}(x)}{P(x)}.$$

(*Если $P(x) = 0$, соответствующая дробь считается бесконечной.*)

Доказательство. Перечислимая снизу функция на бесконечных последовательностях определяется как предел возрастающей последовательности базисных функций. Можно представлять себе это возрастание так: в каждый момент каждое слово x имеет некоторый неотрицательный рациональный "вес" $w(x)$, а значение функции на последовательности равно сумме весов всех её начал. Постепенно веса (изначально равные нулю) увеличиваются; в каждый момент лишь конечное число весов не равны нулю.

В терминах весов условие ограниченности в среднем записывается как

$$\sum_x P(x)w(x) \leqslant 1,$$

поэтому при умножении весов на $P(x)$ оно в точности соответствует определению дискретной полумеры. Заметим, что вычислимость меры P гарантирует, что перечислимость снизу сохраняется в обе стороны (при умножении и делении на P).

Более формально, функция

$$\sum_{x \sqsubseteq \omega} \frac{\mathbf{m}(x)}{P(x)}$$

является перечислимым снизу ограниченным в среднем тестом; её интеграл в точности равен $\sum_x \mathbf{m}(x)$. С другой стороны, любой перечислимый снизу тест может быть представлен в терминах увеличения весов, и предельные значения этих весов, умноженные на P, образуют перечислимую снизу полумеру.

(Заметим, что второе преобразование не однозначно: веса можно перераспределять между двоичным словом и его продолжениями без изменения функции на бесконечных последовательностях.)

В этом рассуждении нам было важно, что P (во второй части рассуждения) и $1/P$ (в первой) перечислимы снизу.

Оказывается, что в этом предложении можно заменить сумму на точную верхнюю грань:

Теорема 2.22.

$$\mathbf{t}_P(\omega) \doteq \sup_{x \sqsubseteq \omega} \frac{\mathbf{m}(x)}{P(x)} \doteq \sum_{x \sqsubseteq \omega} \frac{\mathbf{m}(x)}{P(x)} \tag{1}$$

Первое из равенств можно переписать в логарифмической шкале:

$$\mathbf{d}_P(\omega) \stackrel{+}{=} \sup_{x \sqsubseteq \omega} [-\log P(x) - KP(x)]$$

Доказательство. Поскольку верхняя грань не превосходит суммы, требует доказательства только неравенство в одну сторону: надо объяснить, почему верхняя грань не сильно меньше суммы.

Для данного теста t рассмотрим функции t_i (для всех $i \in \mathbb{Z}$), определённые так: $t_i(\omega) = 2^i$, если $t(\omega) > 2^i$, и равно нулю в противном случае. Все они перечислимы снизу, и их сумма отличается от t не более чем вдвое (в ту или другую сторону). Кроме того, для любой точки ω величина $\sum_i t_i(\omega)$ превосходит $\sup_i t_i(\omega)$ не более чем вдвое.

Преобразуем каждое t_i в сумму весов, как описано выше. При этом, поскольку t_i имеет только два значения (нулевое и ненулевое), можно считать, что вершины ненулевого веса образуют беспрефиксное множество (на каждой ветви есть максимум одна такая вершина).

Складывая веса вдоль каждой ветви ω, мы получим $\sum_i t_i(\omega)$, то есть универсальный тест $t(\omega)$ (с точностью до константы). Если же вместо суммы весов брать максимум, то мы получим нечто меньшее, но уменьшение будет не более чем в два раза, поскольку мы складываем различные степени двойки. (При этом важно, что для каждого t_i в отдельности переход от суммы к максимуму ничего не меняет, поскольку вдоль каждой ветви только один член ненулевой.)

Это рассуждение остаётся в силе, если разрешить ненулевые веса не для всех вершин, а только для слов определённых длин. Пусть у нас имеется некоторая вычислимая возрастающая последовательность длин $n_1 < n_2 < n_3 < \ldots$.

Теорема 2.23.

$$\mathbf{d}_P(\omega) \stackrel{+}{=} \sup_k[-\log P(\omega(1:n_k)) - KP(\omega(1:n_k))].$$

(Здесь $\omega(1:n)$ означает начало последовательности ω длины n.)

Доказательство. Переходя от перечислимых функций на последовательностях к суммам весов, можно выбирать веса только разрешённых длин.

Эта теорема позволяет дать естественную характеризацию дефекта случайности двумерных массивов (которые с точки зрения топологии и меры ничем не отличаются от одномерных, и потому определение ограниченного в среднем дефекта случайности на них очевидно переносится). А именно, достаточно сравнивать вероятность и сложность, скажем, для квадратов с центром в начале координат. (В самом деле, можно расположить клетки плоскости в последовательность таким образом, чтобы эти квадраты соответствовали началам последовательности, и сослаться на предыдущую теорему.)

Историческое отступление

Формула для дефекта случайности является количественным уточнением следующего критерия:

Теорема 2.24 (Критерий случайности в терминах префиксной сложности)**.** *Последовательность ω случайна по вычислимой мере P тогда и только тогда, когда разность $-\log P(x) - KP(x)$ ограничена сверху для всех её начал.*

Этот критерий был впервые сформулирован в [4] со ссылкой на Шнорра; доказательство (для произвольной меры) было опубликовано впервые в [8]. Ещё до этого Шнорр и Левин (независимо в [22] и [15]) сформулировали близкий критерий случайности, использующий несколько другой вид сложности ("монотонную сложность"). Приведём её определение и соответствующую формулировку критерия. (В цитированной работе Шнорра используется несколько другой вид сложности, но позже Шнорр также использовал вариант сложности, введённый Левиным.)

Определение 2.25 (Монотонная сложность)**.** *Будем называть два слова* совместными*, если одно из них является началом другого. Рассмотрим перечислимое множество A пар слов $\langle x, y\rangle$, обладающее таким свойством: если $\langle p, q\rangle \in A$, $\langle p', q'\rangle \in A$ и p совместно с p', то q*

совместно с q'. Такое множество ("монотонный декомпрессор") задаёт отображение множества конечных и бесконечных последовательностей в себя, определяемое такой формулой (и обозначаемое той же буквой A):

$$A(p) = \sum\{x \mid (\exists p' \sqsubseteq p)\langle p', x\rangle \in A\}.$$

Здесь p — конечная или бесконечная последовательность, p' и x — двоичные слова, а sup *понимается как наименьшее общее продолжение, которое может быть конечным или бесконечным. (Условие на A гарантирует, что общее продолжение существует.)*

Далее мы определяем монотонную сложность $KM_A(x)$ слова x относительно A как минимальную длину слова p, для которого $A(p) \sqsupseteq x$. Среди всех монотонных декомпрессоров существует оптимальный, сложность относительно него минимальна (с точностью до константы). Фиксируем оптимальный декомпрессор V и положим $KM(x) = KM_V(x)$.

Замечание 2.26. *Частным случаем монотонных декомпрессоров являются отображения, задаваемые* машинами Тьюринга с оракулом. *Представим себе машину M со односторонней входной лентой (только для чтения), на которой написана конечная или бесконечная последовательность p. Машина также имеет рабочую ленту, а также одностороннюю выходную ленту (только для записи). В процессе работы на этой ленте появляется конечная или бесконечная последовательность $M(p)$ (работа может закончиться, если машина придёт в заключительное состояние или выйдет за границу входного слова, или продолжаться бесконечно, если не будет ни того, ни другого). Легко убедиться, что отображение $p \mapsto M(p)$ будет монотонным декомпрессором (однако не все монотонные декомпрессоры соответствуют таким машинам, так что получается несколько более узкий класс отображений — что, впрочем, само по себе не гарантирует, что получится существенно другая функция сложности).*

Монотонные декомпрессоры (или машины с оракулом описанного вида) могут быть использованы для определения другого вида априорной вероятности: *априорной вероятности на дереве* (которую можно также назвать *непрерывной априорной вероятностью*).

Определение 2.27. *Подадим на вход монотонного декомпрессора A последовательность независимых случайных битов и посмотрим на выходное распределение на конечных и бесконечных последовательностях. Обозначим через $M_A(x)$ вероятность того, что выходная последовательность будет иметь начало x.*

Легко видеть, что функция M_A принимает неотрицательные значения, перечислима снизу, $M_A(\Lambda) = 1$ (здесь Λ — пустое слово) и что $M_A(x) \geqslant M_A(x0) + M_A(x1)$.

Функции, обладающие указанными свойствами, называются перечислимыми снизу полумерами на дереве (*или* непрерывными полумерами).

Используя ту же конструкцию, что и для оптимального декомпрессора, можно доказать такое утверждение [29]:

Предложение 2.28. (а) *Всякая перечислимая снизу полумера на дереве является выходным распределением M_A для некоторого монотонного декомпрессора A.*

(б) *Среди всех перечислимых снизу полумер на дереве существует максимальная (с точностью до умножения на константу).*

Определение 2.29. *Фиксируем некоторую максимальную перечислимую снизу полумеру на дереве и назовём её* априорной вероятностью на дереве, *или* непрерывной априорной вероятностью. *Обозначение:* $\mathbf{a}(x)$.

Соотношение между априорной вероятностью на дереве и монотонной сложностью отчасти напоминает соотношение между дискретной априорной вероятностью и префиксной сложностью. Однако в этом случае $2^{-KM(x)}$, хотя и является перечислимой снизу полумерой на дереве, не является максимальной [9]. Другими словами, $KA(x) = -\log \mathbf{a}(x)$ не превосходит монотонной сложности, но может быть меньше её (и разница не ограничена).

Теперь можно сформулировать упомянутый критерий случайности; его доказательство, технически не сложное, можно найти в [18, 6, 25].

Предложение 2.30. *Для вычислимой меры P на Ω и последовательности $\omega \in \Omega$ следующие свойства равносильны:*

(i) *ω случайна по мере P;*
(ii) $\limsup_{x \sqsubseteq \omega}[-\log P(x) - KM(x)] < \infty$;
(iii) $\liminf_{x \sqsubseteq \omega}[-\log P(x) - KM(x)] < \infty$;
(iv) $\limsup_{x \sqsubseteq \omega}[-\log P(x) - KA(x)] < \infty$;
(v) $\liminf_{x \sqsubseteq \omega}[-\log P(x) - KA(x)] < \infty$;

Критерий случайности с префиксной сложностью имеет два отличия: в нём разность (ограниченная сверху для случайных последовательностей) не всегда ограничена снизу (в отличие от последнего критерия); кроме того, в нём $\limsup$ нельзя заменить на $\liminf$.

В последнем можно убедиться на таком примере. Заметим, что к всякому слову x можно дописать некоторые биты, получив слово y с $KP(y) \geqslant |y|$ (где $|y|$ — длина слова y). В самом деле, если бы это было не так, то для продолжений слова x мы имели бы $\mathbf{m}(y) \geqslant 2^{-|y|}$ и сумма $\sum_y \mathbf{m}(y)$ была бы бесконечной. Построим последовательность, по очереди дописывая длинные участки из нулей, чтобы сделать сложность существенно меньше длины, а потом биты, которые вновь доводят сложность до длины (как мы только что видели, это всегда возможно). Такая последовательность не будет случайной по равномерной мере (поскольку $\limsup$ разности бесконечен), но имеет бесконечно много начал, у которых сложность не меньше длины, так что $\liminf$ конечен.

Формула для (ограниченного в среднем) дефекта случайности имеет любопытное следствие. Рассмотрим равномерную меру на последовательностях (соответствующую независимым бросаниям честной монеты). Эта мера инвариантна относительно перестановок, и отсюда легко следует, что вычислимые перестановки членов последовательности сохраняют случайность. Более того, они сохраняют и дефект случайности (с точностью до константы). Отсюда получаем такое следствие:

Предложение 2.31. *Максимальная разность $|x| - KP(x)$ для начал случайной последовательности ω изменяется при вычислимой перестановке членов последовательности не более чем на константу (зависящую от перестановки, но не от последовательности).*

Некоторые более общие результаты такого типа можно найти в [15, 16, 10].

Другое следствие известно под названием “леммы Миллера – Ю” (Miller–Yu ample access lemma):

Следствие 2.32. *Последовательность ω случайна относительно вычислимой меры P тогда и только тогда, когда*

$$\sum_{x \sqsubseteq \omega} 2^{-\log P(x) - KP(x)} < \infty.$$

Отсюда, кстати, можно получить другое доказательство уже упомянутого факта:

Следствие 2.33. *Для всякого слова x найдётся его продолжение y, у которого $KP(y) > |y|$.*

Доказательство. В самом деле, x является началом некоторой случайной последовательности, и у неё по лемме Миллера–Ю есть сколь угодно длинные начала, сложность которых больше длины.

2.5 Игровая интерпретация

Формула для дефекта случайности может быть интерпретирована в игровых терминах. Рассмотрим игру Алисы и Боба с неполной информацией. Алиса выбирает бесконечную последовательность нулей и единиц. Боб выбирает (не видя последовательности Алисы) слово x. Они встречаются и одновременно открывают свои ходы. После этого, если x является началом ω, то Алиса платит Бобу $2^{|x|}$ рублей. (Эта версия игры соответствует равномерной мере, то есть независимым бросаниям честной монеты; в общем случае Алиса платит Бобу $1/P(x)$.)

Как обычно для игр с неполной информацией, будем рассматривать *чистые* стратегии (возможности игроков, согласно правилам игры), и *смешанные стратегии* (распределения вероятностей на чистых стратегиях). Легко видеть, что *цена* этой игры (в смысле смешанных стратегий, как это обычно понимается для игр с неполной информацией) равна 1. В самом деле, Боб может указать пустое слово и получить 1 в любом случае. С другой стороны, если Алиса честно получает свою последовательность бросанием монеты, то математическое ожидание её проигрыша равно 1, как бы ни пошёл Боб.

Оказывается, что Боб может построить вероятностную стратегию, которая принесёт ему успех, если Алиса поленится бросать монеты и принесёт неслучайную последовательность. Рассмотрим вероятностный алгоритм D, который даёт на выходе двоичные слова (а может и ничего не дать с положительной вероятностью). Такой алгоритм является смешанной стратегией для Боба (если на выходе не появляется никакого слова, то Боб пропускает игру и ничего не получает).

Теперь можно заметить следующее:

(i) Для любой вероятностной стратегии Боба математическое ожидание её выигрыша (как функция от последовательности Алисы) является ограниченным в среднем тестом. (Отсюда уже следует, что это математическое ожидание будет конечным, если последовательность Алисы случайна в смысле Мартин-Лёфа.)

(ii) Если $m(x)$ — вероятность получить x на выходе алгоритма D, то математическое ожидание выигрыша Боба на ω равно

$$\sum_{x \sqsubseteq \omega} \frac{m(x)}{P(x)}.$$

(iii) Поэтому, если взять алгоритм, порождающий на выходе дискретную априорную вероятность $\mathbf{m}(x)$, то математическое ожидание выигрыша Боба будет универсальным тестом (по доказанной формуле для универсального теста).

Таким образом, использование априорной вероятности как смешанной стратегии позволяет Бобу (в среднем) наказать Алису бесконечным штрафом за любую неслучайность в её последовательности.

Можно рассматривать немного более общую игру и разрешить Бобу указывать (в качестве чистых стратегий) не одно слово x, а некоторую базисную функцию f с неотрицательными значениями. При этом его выигрыш (для последовательности ω, принесённой Алисой), равен $f(\omega)/\int f(\omega)\, dP(\omega)$. (Знаменатель делает средний выигрыш равным единице.) Ходу x в старой игре при этом соответствует базисная функция, равная $2^{|x|}$ на продолжениях x и нулю в остальных местах.

Такое обобщение не даёт по существу ничего нового: мы и так разрешаем смешанные стратегии, а базисную функцию можно представить смесью нескольких ходов. (Получив функцию

f, Боб может сделать ещё один вероятностный шаг и выбрать один из интервалов, на которых f постоянна, с соответствующей вероятностью.) Таким образом мы приходим к другой формуле для универсального теста:

$$\mathbf{t}_P(\omega) \doteq \sum_f \frac{\mathbf{m}(f) f(\omega)}{\int f(\omega)\, dP(\omega)}.$$

Преимущество этой формулы в том, что она сохраняет смысл в более общих случаях, чем канторовское пространство, когда никаких выделенных интервалов нет и мы работаем прямо с каким-то классом базисных функций.

Отметим в заключение, что игровая интерпретация теории вероятностей, согласно которой случайность объекта есть не его свойство, а, грубо говоря, тип гарантии, с которой этот объект продаётся, развита в книге Шейфера и Вовка [24].

3 От тестов к сложностям

Формула (1) выражает дефект случайности бесконечной последовательности (значение универсального ограниченного в среднем теста) через сложность её конечных начал. Возникает естественный вопрос: можем ли мы действовать в обратном направлении и связать сложность конечного слова с дефектом случайности его бесконечных продолжений?

Мы уже переходили от бесконечных последовательностей к конечным в предложении 2.7. Это можно сделать и для универсального теста:

Определение 3.1. *Фиксируем вычислимую меру P. Пусть t — ограниченный в среднем тест на Ω. Определим для любого конечного слова z значение $\bar{t}(z)$ как минимум значений t на всех продолжениях:*

$$\bar{t}(z) = \inf_{\omega \sqsupseteq x} t(\omega).$$

Функция $\bar{t}$ однозначно определяется по t, и, напротив, позволяет восстановить t, поэтому её можно считать конечной версией теста t. Интуитивно говоря, слово выглядит неслучайным, если все его бесконечные продолжения имеют большой дефект случайности с точки зрения t.

Вопрос. Колмогоров [13] предлагал аналогичный подход к конечным словам: для каждого слова z можно рассмотреть минимальный дефект случайности (относительно равномерного распределения, понимаемый как разность между длиной и сложностью) его *конечных* продолжений. Есть ли тут какая-то связь с функцией $\bar{t}$?

Покажем, каким образом можно определить функцию $\bar{\mathbf{t}}_P$, соответствующую универсальному тесту, не обращаясь к бесконечным последовательностям.

Определение 3.2 (расширенный тест для вычислимой меры)**.** *Будем называть неотрицательную монотонную перечислимую снизу функцию $T\colon \{0,1\}^* \to [0,+\infty]$* расширенным тестом *для вычислимой меры P, если для любого N среднее значение T на словах длины N не превосходит 1:*

$$\sum_{\{x\colon |x|=N\}} P(x)T(x) \leqslant 1.$$

Монотонность означает, что $T(x) \leqslant T(y)$ при $x \sqsubseteq y$. Она гарантирует, что сумму по всем словам данной длины можно заменить на сумму по произвольному конечному (или даже бесконечному) беспрефиксному множеству S:

$$\sum_{x\in S} P(x)T(x) \leqslant 1.$$

(В самом деле, продолжим слова из S до какой-то большой общей длины.)

Предложение 3.3. *Всякий расширенный тест порождает (в смысле определения* 2.5*) некоторый ограниченный в среднем тест на бесконечных последовательностях. Обратно, всякие ограниченный в в среднем тест на бесконечных последовательностях порождается некоторым расширенным тестом.*

Доказательство. Первая часть непосредственно следует из определения (и теоремы о монотонной сходимости под знаком интеграла). В обратную сторону можно положить $T = \bar{t}$ или сослаться на предложение 2.4, если не хотеть использовать компактность.

Но можно рассматривать расширенные тесты и не упоминая бесконечные последовательности. Обычным образом можно доказать, что среди них существует максимальный:

Предложение 3.4. *Пусть P — вычислимая мера. Среди всех расширенных тестов для меры P существует максимальный (с точностью до умножения на константу).*

Определение 3.5. *Будем называть этот максимальный тест* универсальным расширенным тестом *для меры P.*

Предложение 3.6. *Универсальный расширенный тест для меры P совпадает с $\overline{\mathbf{t}}_P$ с точностью до ограниченного множителя.*

Доказательство. Поскольку $\overline{\mathbf{t}}_P$ является расширенным тестом, то он не превосходит универсального (с точностью до константы). С другой стороны, универсальный расширенный тест задаёт тест на бесконечных последовательностях, и остаётся сравнить его с максимальным.

Это построение по существу использует компактность пространства Ω (и потому, например, не проходит для последовательностей натуральных чисел), но и без этого можно построить максимальный расширенный тест, который будем обозначать $\mathbf{t}_P(x)$; использование одного и того же обозначения $\mathbf{t}_P$ не вызовет путаницы, так как в одном случае аргументом являются бесконечные последовательности, а в другом — конечные слова.

Определение расширенного теста позволяет изгнать бесконечные последовательности, сохранив по существу то же понятие универсального теста и даже немного обогатив его: отметим, что не всякий расширенный тест, порождающий универсальный ограниченный в среднем тест, является универсальным расширенным тестом (его значение на каком-то слове может быть малым, что не мешает универсальности на уровне бесконечных последовательностей, поскольку значения на всех продолжениях большие).

Описанный способ перехода от тестов на бесконечных последовательностях к тестам на словах не является единственно возможным.

Определение 3.7. *Предположим, что вычислимая мера P положительна на всех интервалах: $P(x) > 0$ для любого слова x. Обозначим через $\hat{\mathbf{t}}_P(x)$ условное математическое ожидание $\mathbf{t}_P(\omega)$ при условии, что ω начинается на x. Другими словами, $\hat{\mathbf{t}}_P(x)$ есть среднее значение t на интервале $x\Omega$, то есть отношение интеграла*

$$U(x) = \int\limits_{x\Omega} \mathbf{t}(\omega)\, dP(\omega)$$

к $P(x)$.

Функция U является перечислимой снизу полумерой. Более того, она обладает свойствами меры, за исключением того, что мера всего Ω не равна единице (отметим также, что $U(x)$ не обязано быть вычислимым). Эта мера имеет плотность $\hat{\mathbf{t}}$ относительно P. Отсюда следует, что функция $\hat{\mathbf{t}}_P$ является мартингалом в смысле следующего определения:

Определение 3.8. *Функция* $g\colon \{0,1\}^* \to \mathbb{R}$ *называется* мартингалом *относительно распределения вероятностей* P*, если*

$$P(x)g(x) = P(x0)g(x0) + P(x1)g(x1)$$

для любого слова x*. Если заменить знак "=" на "*$\geqslant$*", получим определение* супермартингала.

Будучи мартингалом, функция $\hat{\mathbf{t}}_P(x)$ не является монотонной по x.

Следующая теорема устанавливает соотношение между различными мерами неслучайности двоичных слов:

Теорема 3.9.

$$\frac{\mathbf{m}(x)}{P(x)} \stackrel{\cdot}{<} \mathbf{t}_P(x) \stackrel{\cdot}{<} \hat{\mathbf{t}}_P(x) \stackrel{\cdot}{<} \frac{\mathbf{a}(x)}{P(x)},$$

где $\mathbf{m}(x)$ *— дискретная априорная вероятность слова* x *(см. предложение* 2.20*),* $\mathbf{a}(x)$ *— непрерывная априорная вероятность (на дереве, см. предложение* 2.28*) того же слова.*

Доказательство. Первое неравенство можно даже усилить, заменив $\mathbf{m}(x)/P(x)$ на сумму $\sum_{t\sqsubseteq x} \mathbf{m}(t)/P(t)$: эта сумма является частью выражения для $\mathbf{t}_P(\omega)$ для любого продолжения ω слова x.

Второе неравенство связывает среднее и наименьшее значения случайной величины.

Последнее неравенство следует из сравнения перечислимой снизу полумеры на дереве U с максимальной.

Отметим ещё, что $\hat{\mathbf{t}}_P(x)$ является мартингалом, а $\mathbf{a}(x)/P(x)$ — лишь супермартингалом (максимальным среди супермартингалов относительно P, с точностью до мультипликативной константы).

Замечания 3.10.

1. *Между первым и вторым членом неравенства последней теоремы можно поместить ещё два:*

$$\stackrel{\cdot}{<} \max_{t\sqsubseteq x} \frac{\mathbf{m}(t)}{P(t)} \stackrel{\cdot}{<} \sum_{t\sqsubseteq x} \frac{\mathbf{m}(t)}{P(t)} \stackrel{\cdot}{<}$$

2. *В логарифмической шкале имеем*

$$-\log P(x) - KP(x) \stackrel{+}{<} \log \mathbf{t}_P(x) \stackrel{+}{<} \log \hat{\mathbf{t}}_P(x) \stackrel{+}{<} -\log P(x) - KA\,(x).$$

3. *Мера* U *зависит от* P *(напомним, что* U *— это максимальная перечислимая снизу мера, имеющая плотность относительно* P*), и для различных мер* P *(например, с различными носителями) меры* U *могут быть разными. Но зависимость эта не так велика: теорема показывает, что возможные колебания ограничены разностью между* $KP(x)$ *и* $KA\,(x)$*.*

4. *Последнее неравенство в теореме (*$\hat{\mathbf{t}}_P(x) \stackrel{\cdot}{<} \mathbf{a}(x)/P(x)$*) нельзя заменить на равенство. Пусть, например, мера* P *равномерна, а в качестве* x *берутся начала возрастающей длины какой-то вычислимой последовательности. Тогда* $U(x)$ *стремится к нулю (область интегрирования сходится к одноэлементному множеству, имеющему меру нуль),* а $\mathbf{a}(x)$ *отделено от нуля.*

5. *Мы использовали компактность (конечность алфавита* $\{0,1\}$*), доказывая предложение* 2.7. *Вместо этого можно было бы использовать предложение* 2.6 *и получить аналогичные результаты для бэровского пространства последовательностей натуральных чисел.*

Все перечисленные в теореме 3.9 величины могут быть использованы для характеризации случайности: последовательность случайна тогда и только тогда, когда любая из этих величин ограничена на её начальных отрезках. В самом деле, теорема Левина – Шнорра гарантирует, что для случайной последовательности последнее отношение ограничено, а первое нет. Поскольку вторая величина монотонна, то для неслучайной последовательности все величины, начиная со второй, стремятся к бесконечности. Как мы уже упоминали, про первую величину этого утверждать нельзя.

Вопрос. Некоторые из величин, упомянутых в теореме 3.9 (вторая слева, а также две промежуточные между первой и второй), монотонны. Первая величина (см. обсуждение критерия случайности), а также величина $\hat{\mathbf{t}}_P(x)$ (мартингал), не монотонны. Что можно сказать про последнюю?

Отметим, что все эти величины если и не монотонны, то близки к монотонным.

4 Бернуллиевы последовательности

Можно стараться определить случайность не относительно конкретной меры, а относительно класса мер. (Интуитивно это означает, что мы готовы поверить, что последовательность получена в результате вероятностного процесса с распределением в этом классе.) Впоследствии мы сделаем это для произвольного *эффективно замкнутого* класса мер, но для наглядности начнём с конкретного примера: класса *бернуллиевых* мер.

4.1 Тесты для бернуллиевых последовательностей

Бернуллиева мера B_p соответствует последовательности независимых бросаний не обязательно симметричной монеты; вероятность появления единицы в каждом испытании равна некоторому $p \in [0,1]$ (одному и тому же во всех испытаниях). Отметим, что p не обязано быть вычислимым.

Определение 4.1 (ограниченный в среднем бернуллиев тест)**.** *Перечислимая снизу функция на бесконечных последовательностях называется ограниченным в среднем бернуллиевым тестом, если её интеграл по любой мере* B_p *(при любом* $p \in [0,1]$*) не превосходит* 1.

Предложение 4.2 (универсальный бернуллиев тест)**.** *Среди всех таких тестов существует максимальный (с точностью до мультипликативной константы).*

Доказательство. Перечислимая снизу функция есть предел возрастающей последовательности базисных функций. Для каждой из этих базисных функций её интеграл по мере B_p представляет собой многочлен от p, и легко проверить, что он не больше 1 при всех p (если это так). Соответственно можно фильтровать все негодные функции и перечислять все бернуллиевы тесты. Складывая их с коэффициентами, получаем универсальный.

Определение 4.3. *Фиксируем универсальный бернуллиев тест и обозначим его* $\mathbf{t}_{\mathcal{B}}(\omega)$*. Его логарифм будем называть* дефектом бернуллиевости *и обозначать* $\mathbf{d}_{\mathcal{B}}(\omega)$*. Последовательность называется* бернуллиевой*, если её дефект конечен.*

Как и раньше, можно немного модифицировать определение, чтобы считать дефект неотрицательным целым числом.

Как и для вычислимых мер, можно перейти к конечным последовательностям:

Определение 4.4. *Будем называть монотонную перечислимую снизу неотрицательную функцию* $T\colon \{0,1\} \to [0,+\infty]$ расширенным бернуллиевым тестом*, если для любого натурального* N *и для любого* $p \in [0,1]$ *выполняется неравенство* $\sum_{\{x\colon |x|=N\}} B_p(x)T(x) \leqslant 1$.

Как и для вычислимых мер, тесты на конечных и бесконечных последовательностях связаны:

Предложение 4.5. *Всякий расширенный бернуллиев тест порождает бернуллиев тест на* Ω*. Напротив, всякий бернуллиев тест на* Ω *порождается некоторым расширенным бернуллиевым тестом.*

Среди расширенных бернуллиевых тестов существует максимальный; он порождает универсальный бернуллиев тест на Ω. Как и раньше, мы будем использовать одно и то же обозначение $\mathbf{t}_{\mathcal{B}}$ для максимальных тестов на конечных и бесконечных последовательностях.

4.2 Другие варианты определения бернуллиевости

Как и для случайности относительно вычислимых мер, есть разные эквивалентные варианты определения. Можно рассматривать ограниченные по вероятности тесты (вероятность события $t(\omega) > N$ по любой из мер B_p должна быть не больше $1/N$). Можно, следуя определению Мартин-Лёфа для вычислимых мер, назвать тестом вычислимую последовательность эффективно открытых множеств U_i, для которых $B_p(U_i) \leqslant 2^{-i}$ при любом i и при любом $p \in [0,1]$. Все эти варианты определения эквивалентны (и доказывается это точно так же, как для случайности по вычислимой мере).

Интересно, что первоначальное определение бернуллиевости, данное Мартин-Лёфом в [19], было немного другим. Сейчас мы покажем, что оно также эквивалентно остальным, но это несколько сложнее.

Обозначение 4.6. *Через* $\mathbb{B}(n,k)$ *мы обозначаем множество всех слов длины* n*, содержащих ровно* k *единиц.*

Мартин-Лёф определяет тест бернуллиевости как семейство перечислимых множеств слов $U_1 \supset U_2 \supset U_3 \supset \ldots$; каждое из множеств наследственно вверх, то есть вместе с любым словом содержит все его продолжения. Ограничение на эти множества такое: рассмотрим произвольные целые $n \geqslant 0$ и k от 0 до n; через $\mathbb{B}(n,k)$ обозначим множество всех слов длины n, содержащих k единиц (и $n-k$ нулей); требуется, чтобы при всех i доля слов в $\mathbb{B}(n,k)$, принадлежащих U_i, была бы не больше 2^{-i}.

Для удобства сравнения заменим множества U_i на перечислимую снизу функцию d с целыми значениями, для которой $U_i = \{x \mid d(i) \geqslant i\}$. Наследственность множеств означает монотонность этой функции; помимо этого, требуется, чтобы вероятность события $d \geqslant i$ внутри любого множества $\mathbb{B}(n,k)$ была бы не больше 2^{-i}. Видно, что эти требования соответствуют ограниченным по вероятности расширенным тестам (в логарифмической шкале), но только вместо класса мер B_p на словах длины n рассматривается другой класс мер, а именно класс мер, сосредоточенных на словах данной длины с данным числом единиц. Меры из класса B_p принимают равные значения на словах одинаковой длины с одинаковым числом единиц, поэтому представимы в виде смеси равномерных мер на $\mathbb{B}(n,k)$ с некоторыми коэффициентами, от замены B_p на эти меры условие становится более сильным.

Покажем, что тем не менее класс бернуллиевых последовательностей не меняется от такой замены и, более того, универсальный тест (как функция на бесконечных последовательностях) тоже не меняется (с точностью до ограниченного множителя, как обычно). Мы покажем это для ограниченных в среднем вариантов тестов (соответственно изменив определение Мартин-Лёфа); на класс бернуллиевых последовательностей это не влияет. Рассуждение для ограниченных по вероятности тестов аналогично.

Дадим соответствующие определения.

Определение 4.7. *Функцию* $f\colon \{0,1\}^* \to [0,+\infty]$ *назовём* комбинаторным бернуллиевым тестом*, если*

(а) *она перечислима снизу;*

(б) *она монотонна (увеличивается при добавлении битов в конец слова);*

(в) *для любых целых* n, k *с* $0 \leqslant k \leqslant n$ *среднее значение функции* f *на множестве* $\mathbb{B}(n,k)$ *не превосходит* 1*.*

Можно сравнить эти требования со случаем равномерной меры: тогда мы требовали, чтобы среднее по всему $\{0,1\}^n$ не превосходило единицы; теперь требование сильное: среднее по по каждой из его частей $\mathbb{B}(n,k)$ должно быть не больше 1.

Имея такой тест для слов ограниченной длины, можно продолжать его по монотонности:

Предложение 4.8. *Пусть имеется функция* f*, определённая на словах длины меньше* n *и удовлетворяющая требованиям* (а)–(в)*. Тогда её продолжение по монотонности на слова больших длин также удовлетворяет этим требованиям.*

Доказательство. Будем продолжать её на слова длины n, положив $f(x0)$ и $f(x1)$ равным $f(x)$ для слов x длины $n-1$. Множество $\mathbb{B}(n,k)$ состоит из двух частей: слов, оканчивающихся на нуль, и слов, оканчивающихся на единицу. Первые находятся во взаимно однозначном соответствии с $\mathbb{B}(n-1,k)$, вторые — с $\mathbb{B}(n-1,k-1)$. Функция сохраняет значения при этом соответствии, поэтому среднее по каждой из частей не больше 1. Следовательно, и среднее по всему $\mathbb{B}(n,k)$ не больше 1.

Как обычно, можно определить универсальный комбинаторный бернуллиев тест:

Предложение 4.9 (универсальный комбинаторный бернуллиев тест)**.** *Среди комбинаторных бернуллиевых тестов существует максимальный с точностью до мультипликативной константы.*

Определение 4.10. *Фиксируем универсальный комбинаторный тест* $\mathbf{b}(x)$ *и продолжим его на бесконечные последовательности, положив*

$$\mathbf{b}(\omega) = \sup_{x \sqsubseteq \omega} \mathbf{b}(x).$$

Полученную функцию будем называть универсальным комбинаторным тестом на Ω *и обозначать той же буквой* $\mathbf{b}$*.*

(В силу монотонности точную верхнюю грань в этом определении можно заменить на предел.)

Покажем, что этот тест совпадает (с точностью до ограниченного множителя) с введёнными ранее бернуллиевыми тестами в смысле определения 4.1.

Теорема 4.11.

$$\mathbf{b}(\omega) \doteq \mathbf{t}_{\mathcal{B}}(\omega).$$

Доказательство. Мы уже видели, что комбинаторный бернуллиев тест является расширенным бернуллиевым тестом (из ограничений на среднее по каждой части $\mathbb{B}(n,k)$ следует ограничение на математическое ожидание по мере B_p, так как эта мера постоянна на каждой части). Следовательно, $\mathbf{b}(\omega) \dot{<} \mathbf{t}_{\mathcal{B}}(\omega)$.

Обратное утверждение неверно: расширенный бернуллиев тест может не быть комбинаторным тестом. Однако можно построить комбинаторный тест, который принимает те же значения (с точностью до константы) на бесконечных последовательностях, а только это и утверждается в теореме.

Идея тут состоит в следующем. Рассмотрим расширенный бернуллиев тест t на словах длины n и перенесём его на слова существенно большей длины N (применяя старый тест к их началам длины n). Получим некоторую функцию t'. Нам нужно показать, что t' близка к комбинаторному тесту (превышает его не более чем в константу раз). Для этого надо усреднить t' по множеству $\mathbb{B}(N,K)$ для произвольного K между 0 и N. Другими словами, нам нужно усреднить t по распределению вероятностей на n-битовых началах последовательностей длины N, содержащих K единиц. При $N \gg n$ это распределение будет близко к бернуллиевому с вероятностью $p = K/N$.

В терминах теории вероятностей мы имеем урну с N шарами, из которых K чёрных, и вынимаем из неё (без возвращения) n шаров. Нам надо сравнить распределение вероятностей с бернуллиевым, которое получилось бы при выборке с возвращением. Покажем, что

> *при $N = n^2$ распределение без возвращения не более чем в $O(1)$ раз превосходит распределение с возвращением.*

(Кстати, обратное неравенство не верно: при $K = 1$ без возвращения бы не можем получить слово с двумя единицами, а с возвращением можем. Но нам достаточно неравенства в эту сторону.)

В самом деле, при выборке без возвращения вероятность вытащить шар данного цвета равна отношению

$$\frac{\text{число оставшихся шаров этого цвета}}{\text{число всех оставшихся шаров}}.$$

Оставшихся шаров этого цвета не больше, чем в случае с возвращением, а знаменатель не меньше $N - n$. Поэтому вероятность любой комбинации при выборке без возвращения не больше вероятности же комбинации с возвращением, умноженной на $N/(N-n)$ в степени n. При $N = n^2$ возникает множитель $(1 + O(1/n))^n = O(1)$.

Таким образом, если взять расширенный бернуллиев t и затем определить $t'(x)$ на слове x длины N как t на начале слова x длины $\lfloor\sqrt{N}\rfloor$, то полученная функция t' будет комбинаторным тестом с точностью до константы. (Отметим, что её монотонность следует из монотонности t.)

4.3 Критерий бернуллиевости

Естественно сравнивать понятие бернуллиевой последовательности (для которой тест бернуллиевости конечен) с понятием случайной по мере B_p последовательности. Однако определение случайности по Мартин-Лёфу предполагало вычислимость меры, и непосредственно не применимо к мере B_p при невычислимом p.

Можно, однако, релятивизировать определения Мартин-Лёфа, разрешив обращаться к оракулу для p. С таким оракулом мера B_p становится вычислимой и определение случайности по Мартин-Лёфу приобретает смысл.

Следующая теорема подтверждает интуитивный смысл бернуллиевых последовательностей как последовательностей, случайных по мере B_p при некотором p:

Теорема 4.12. *Последовательность ω является бернуллиевой тогда и только когда, когда она случайна по мере B_p с оракулом p для некоторого $p \in [0,1]$.*

Говоря об оракуле p, мы имеем в виду возможность получать по i значение i-го бита в двоичном разложении p (которое единственно, за исключением тех случаев, когда p двоично-рационально, а в этих случаях оба разложения вычислимы и оракул тривиален).

Мы будем доказывать эту теорему (и притом в более сильной количественной форме), введя понятие теста случайности по мерам B_p как функции двух аргументов (последовательности и p). Требуемый результат получится как комбинация следующих утверждений:

(а) Среди таких "равномерных" тестов случайности существует максимальный тест $\mathbf{t}(\omega, p)$.

(б) Функция $\omega \mapsto \inf_p \mathbf{t}(\omega, p)$ совпадает (как обычно, с точностью до ограниченного множителя) с универсальным бернуллиевым тестом.

(в) При фиксированном p функция $\omega \mapsto \mathbf{t}(\omega, p)$ совпадает (с той же точностью) с релятивизированным относительно p максимальным тестом случайности относительно (p-)вычислимой меры B_p.

Из этих трёх утверждений легко следует теорема 4.12: последовательность ω бернуллиева, если тест бернуллиевости на ω конечен; он равен точной нижней грани $\mathbf{t}(\omega, p)$, поэтому его конечность означает, что $\mathbf{t}(\omega, p) < \infty$ при некотором p, что равносильно p-релятивизованной случайности по мере B_p.

Нам понадобится некоторая техническая подготовка. Тесты случайности (как функции двух аргументов) тоже будут перечислимыми снизу, но это понятие требует уточнения, поскольку добавился второй аргумент, действительное число. (Впоследствии мы рассмотрим и более общую ситуацию, когда вторым аргументом является мера.) Дадим соответствующие определения.

Определение 4.13. *Назовём* базисными прямоугольниками *в пространстве $\Omega \times [0,1]$ множества вида $x\Omega \times (u, v)$, где x — двоичное слово, а u, v — рациональные числа, причём $u < v$. (Техническая оговорка: числа u, v могут лежать и вне $[0,1]$, в этом случае по второй координате берётся пересечение (u, v) с $[0,1]$.)*

Функция $f\colon \Omega \times [0,1] \to [-\infty, +\infty]$ называется перечислимой снизу, *если существует алгоритм, который получает на вход рациональное r и порождает прямоугольники, в объединении дающие всё множество пар $\langle \omega, p \rangle$ с $r < f(\omega, r)$.*

Это определение, как и раньше, требует, чтобы прообраз $(-\infty, r)$ был эффективно открытым множеством равномерно по r, но только теперь мы рассматриваем эффективно открытые множества в $\Omega \times [0,1]$, определённые естественным образом.

Аналогично определяется и перечислимость сверху, *равносильная перечислимости снизу функции $(-f)$.*

Функцию с конечными действительными значения называют вычислимой, *если она перечислима и снизу, и сверху.*

Поскольку пересечение эффективно открытых множеств эффективно открыто, получаем такую формулировку:

Предложение 4.14. *Функция $f\colon \Omega \times [0,1] \to \mathbb{R}$ вычислима тогда и только тогда, когда для каждого интервала (u, v) с рациональными концами его прообраз есть объединение последовательности базисных прямоугольников, эффективно порождаемой по u и v.*

Интуитивный смысл этого определения можно понять, если иметь в виду, что задача "указывать приближения к α с любой заданной точностью" равносильна задаче "перечислять все интервалы, содержащие α". Поэтому для вычислимой функции f мы можем находить приближения к $f(\omega, p)$, если нам дают приближения к ω и p.

Определение (неотрицательной) перечислимой снизу функции можно переформулировать, введя понятие базисной функции. Нам будет важно, что базисные функции непрерывны, поэтому зависимость от действительного аргумента будет кусочно-линейной, а не скачками.

Определение 4.15 (базисные функции, бернуллиев случай)**.** *Пусть x — двоичное слово, (u, v) — рациональный интервал, а k — натуральное число, для которого $u + 2^{-k} < v - 2^{-k}$. Определим функцию $g_{x,u,v,k}(\omega, p)$ так: если ω не начинается на x, то она равна нулю; если ω начинается на x, то зависимость от p будет кусочно-линейной, причём при $p \notin (u, v)$ функция равна нулю, внутри $(u + 2^{-k}, v - 2^{-k})$ функция равна 1, а в промежутке линейно меняется.*

Теперь рассмотрим наименьший класс функций, содержащий все функции $g_{x,u,v,k}$ и замкнутый относительно линейных комбинаций с рациональными коэффициентами, максимумов и минимумов. Это счётное множество функций, которые можно задавать конструктивно, и эти функции будем называть базисными*.*

Теперь можно дать эквивалентное описание перечислимости снизу:

Предложение 4.16. *Функция $f\colon \Omega \times [0,1] \to [0, +\infty]$ перечислима снизу тогда и только тогда, когда она представима в виде поточечного предела неубывающей последовательности базисных функций.*

Доказательство. Это было бы совсем ясно, если считать базисными функциями характеристические функции базисных прямоугольников и максимумы конечного числа таких функций. Но мы хотим, чтобы базисные функции были непрерывны по p (это будет важно в дальнейшем). Поэтому надо заметить, что при $k \to \infty$ функция $g_{x,u,v,k}$ стремится к характеристической функции прямоугольника.

Непрерывность базисных функций гарантирует такое важное свойство:

Предложение 4.17. *Пусть $f\colon \Omega \times [0,1] \to \mathbb{R}$ — базисная функция. Тогда значение интеграла $\int f(\omega, p)\, dB_p(\omega)$ является вычислимой функцией от p (и от базисной функции f).*

(Вычислимость понимается в описанном выше смысле; отметим, что всякая вычислимая функция непрерывна. Аналогичное утверждение верно для любой вычислимой функции f, не только базисной, но нам это не понадобится.)

Теперь мы готовы сформулировать и доказать важный технический факт (доказанный в [12]); он не раз нам понадобится (в том числе и в более общей ситуации).

Предложение 4.18 (усечение)**.** *Пусть $\varphi\colon \Omega \times [0,1] \to [0, \infty]$ — перечислимая снизу функция. Тогда можно построить другую перечислимую снизу функцию $\varphi'(\omega, p)$, не превосходящую $\varphi(\omega, p)$ в каждой точке, для которой при любом p:*

(а) *$\int \varphi'(\omega, p)\, dB_p(\omega) \leqslant 2$;*

(б) *если $\int \varphi(\omega, p)\, dB_p(\omega) \leqslant 1$, то $\varphi'(\omega, p) = \varphi(\omega, p)$ при всех ω.*

Доказательство. Согласно Предложению 4.16, можно представить φ в виде суммы ряда неотрицательных базисных функций: $\varphi(\omega, p) = \sum_n h_n(\omega, p)$. Предложение 4.17 гарантирует, что интеграл

$$\int \sum_{i \leqslant n} h_i(\omega, p)\, dB_p(\omega)$$

является вычислимой функцией от p (равномерно по n), и поэтому множество S_n тех p, где этот интеграл меньше 2, эффективно открыто (равномерно по n).

Теперь положим $h'_n(\omega, p) = h_n(\omega, p)$, если $p \in S_n$, и $h'_n(\omega, p) = 0$ в противном случае. Функция h'_n будет перечислимой снизу, и интеграл $\int \sum_{i \leqslant n} h'_i(\omega, p)\, dB_p(\omega)$ будет меньше 2 при всех p. Положив $\varphi' = \sum h'_n$, мы получим перечислимую снизу функцию, и по теореме о монотонной сходимости $\int \varphi'(\omega, p)\, dB_p(\omega)$ не больше 2 при всех p.

Остаётся заметить, что если при некотором p интеграл $\int \varphi(\omega, p)\, dB_p(\omega)$ не превосходит 1, то это p войдёт во все S_n и переход от h_n к h'_n, как и переход от φ к φ', ничего не изменит.

После этой подготовки мы можем определить равномерные тесты бернуллиевости и доказать их свойства:

Определение 4.19. *Функцию t от двух аргументов $\omega \in \Omega$ и $p \in [0, 1]$ назовём* равномерным тестом бернуллиевости*, если*

(а) *она перечислима снизу (в описанном выше смысле, как функция пары)*;

(б) *для любого $p \in [0, 1]$ математическое ожидание $t(\omega, p)$ по мере B_p (то есть интеграл $\int t(\omega, p)\, dB_p(\omega)$) не превосходит 1.*

Нам осталось доказать три обещанных утверждения:

Лемма 4.20. *Существует* универсальный *равномерный тест бернуллиевости $\mathbf{t}(\omega, p)$, который является максимальным в этом классе (с точностью до константы).*

Лемма 4.21. *Для этого теста функция $\mathbf{t}'(\omega) = \inf_p \mathbf{t}(\omega, p)$ совпадает (с точностью до ограниченного в обе стороны множителя) с универсальным тестом бернуллиевости $\mathbf{t}_{\mathcal{B}}(\omega)$ в смысле определения* 4.3.

Из этих двух лемм вытекает, что последовательность ω является бернуллиевой тогда и только тогда, когда $\mathbf{t}'(\omega) < \infty$, то есть $\mathbf{t}(\omega, p) < \infty$ при некотором p, и это позволяет завершить доказательство теоремы 4.12 ссылкой на такое утверждение:

Лемма 4.22. *Для фиксированного p функция $\mathbf{t}_p(\omega) = \mathbf{t}(\omega, p)$ совпадает (с точностью до ограниченного множителя) с релятивизованным относительно p универсальным тестом случайности относительно меры B_p*

Доказательство. (лемма 4.20) Будем перечислять все перечислимые снизу функции двух аргументов. К каждой из них применим предложение 4.18, и полученные суммы сложим с коэффициентами, образующими вычислимо сходящийся ряд с суммой меньше $1/2$.

Доказательство. (лемма 4.21) Покажем, что функция $\mathbf{t}'$ является универсальным бернуллиевым тестом. При любом p математическое ожидание этой функции по мере B_p не больше 1 (поскольку она не превосходит $\mathbf{t}(\omega, p)$ для этого конкретного p).

Кроме того, эта функция перечислима снизу. Это доказывается аналогично предложению 2.7 с использованием компактности. (Аналогичное утверждение в более общей ситуации будет доказано в предложении 7.20.)

Таким образом, $\mathbf{t}'$ является бернуллиевым тестом. Универсальность (максимальность) очевидно следует из того, что любой бернуллиев тест можно рассматривать как функцию двух переменных, которая будет равномерным бернуллиевым тестом.

Аналогичное рассуждение показывает, что для естественным образом определённого универсального расширенного равномерного бернуллиева теста $\mathbf{t}(x, p)$ (первым аргументом которого является двоичное слово) величина $\inf_p \mathbf{t}(x, p)$ будет универсальным расширенным бернуллиевым тестом.

Доказательство. (лемма 4.22) Предположим вначале, что p вычислимо. Тогда мы можем перечислять все интервалы, содержащие p, и функция $\mathbf{t}_p\colon \omega \to \mathbf{t}(\omega, p)$ перечислима снизу (чтобы перечислять те x, где $\mathbf{t}_p(\omega) < r$, мы перечисляем прямоугольники, в которых $\mathbf{t}(\omega, p)$, и отбираем из них те, где вторая проекция содержит p).

Аналогичное рассуждение можно провести для любого p и установить, что функция $\mathbf{t}_p$ перечислима снизу с p-оракулом. Таким образом, $\mathbf{t}_p$ не превосходит универсального релятивизованного теста для B_p.

Обратное рассуждение чуть сложнее. Пусть имеется некоторый тест t для B_p, перечислимый снизу с оракулом p. Мы должны найти равномерный тест $t'(\omega, p)$, который мажорирует t (при данном p). Другими словами, нужно продолжить функцию, первоначально определённую только для одного p, на все значения p, и при этом ещё и гарантировать оценку для интеграла.

Начнём с простого случая, когда p вычислимо. В этом случае оракул не нужен и функция t перечислима снизу. Добавив в неё фиктивный второй аргумент p, мы получим перечислимую снизу функцию двух аргументов. Но тестом эта функция, скорее всего, не будет, так как про её математическое ожидание по мере B_q при $q \neq p$ мы ничего не знаем. Тут нам помогает предложение 4.18: с его помощью мы преобразуем t в перечислимую снизу функцию $t'(\omega, q)$ (которая теперь уже реально зависит от q), для которой $\int t'(\omega, q)\, dB_q(\omega) \leqslant 2$ при всех q, а $t'(\cdot, p) = t(\cdot, p)$. Поделив t' пополам, получим равномерный тест.

Теперь рассмотрим случай невычислимого p. В этом случае p иррационально, поэтому биты его двоичного разложения можно получать, имея перечисление всех содержащих его интервалов (дождавшись, пока появится интервал, однозначно определяющий нужный нам бит). Поэтому машина, использующая оракул p, может быть преобразована в машину, которая перечисляет снизу некоторую функцию $\tilde{t}(\omega, q)$, совпадающую с $t(\omega)$ при $q = p$. Эта функция вовсе не обязана быть равномерным тестом бернуллиевости (поскольку условие на интеграл гарантировано только при $q = p$, но её опять же можно подвергнуть усечению с помощью предложения 4.18.

5 Произвольные меры на Ω

В этом разделе мы по-прежнему ограничиваемся двоичными последовательностями, но меры на Ω могут быть любыми, а не только бернуллиевыми.

Обозначение 5.1. *Будем обозначать множество всех вероятностных распределений на Ω через $\mathcal{M}(\Omega)$.*

(Напомним, что мера всего пространства Ω всегда равна 1.)

5.1 Равномерные тесты случайности

Определение 5.2. *Назовём* равномерным тестом *перечислимую снизу функцию $t(\omega, P)$ двух аргументов (последовательности ω и меры P на Ω), для которой*

$$\int t(\omega, P)\, dP(\omega) \leqslant 1$$

для любой меры P.

Здесь требует уточнения понятие перечислимой снизу функции. Пространство всех мер $\mathcal{M}(\Omega)$ можно рассматривать как замкнутое подмножество бесконечного произведения

$$\Xi = [0,1] \times [0,1] \times [0,1] \times \ldots$$

(мера задаётся своими значениями на интервалах, которых счётное число; эти значения должны удовлетворять соотношениям, выделяющим замкнутое множество). Теперь определим базисные множества, эффективно открытые множества и пр. для пространства мер:

Определение 5.3. *Базисное множество* (*открытый* интервал) *в пространстве мер задаётся конечным множеством условий вида $u < P(y) < v$, где y — двоичное слово, а u, v — рациональные числа. Оно состоит из всех мер P, удовлетворяющих этим условиям.* Базисное открытое множество *в пространстве $\Omega \times \mathcal{M}(\Omega)$ имеет вид $x\Omega \times \beta$ (произведение интервалов в Ω и в $\mathcal{M}(\Omega)$).*

Перечислимость снизу, сверху и вычислимость теперь определяются стандартным образом в терминах базисных открытых множеств, см. определение 4.13.

Мы будем использовать компактность пространств Ω (мы рассматриваем последовательности над конечным алфавитом $\{0,1\}$) и $\mathcal{M}(\Omega)$. Это свойство позволяет выбирать из любого открытого покрытия конечное подпокрытие. Нам понадобится эффективный вариант этого свойства:

Определение 5.4 (эффективная компактность)**.** *Компактное подмножество C пространства $\mathcal{M}$ называется* эффективно компактным*, если множество*

$$\{S \mid S \text{ — конечное семейство базисных множеств, покрывающее } C\}$$

перечислимо.

Само пространство $\mathcal{M}(\Omega)$, как легко видеть, компактно и эффективно компактно. Компактно оно как замкнутое множество в произведении компактных пространств, а эффективность следует из того, что мы можем проверить, что данные базисные множества покрывают всё пространство (речь идёт о линейных равенствах и неравенствах с конечным числом переменных, а там всё алгоритмически разрешимо). Отсюда легко следует такое утверждение:

Предложение 5.5. *Всякое эффективно замкнутое подмножество $\mathcal{M}(\Omega)$ эффективно компактно.*

Доказательство. Пусть эффективно замкнутое множество C имеет дополнение, являющееся объединением базисных открытых множеств $U_1, U_2, \ldots$; семейство S является покрытием C тогда и только тогда, когда вместе с некоторым конечным набором из U_i оно покрывает всё пространство. А это свойство перечислимо.

Верно и обратное — что эффективно компактное подмножество эффективно замкнуто. (Его дополнение есть объединение всех интервалов, которые не пересекаются с некоторым конечным покрытием множества, а такие ситуации можно перечислять.)

Теперь мы можем продолжить построение по аналогии с бернуллиевыми мерами. Определим понятие базисной функции (по аналогии с определением 4.15; конкретный вид базисных функций не имеет большого значения):

Определение 5.6 (базисные функции для равномерных тестов по произвольным мерам в Ω)**.** Базисные функции *на множестве $\Omega \times \mathcal{M}(\Omega)$ определяются аналогично определению* 4.15*, начиная с функций*

$$g_{x,y,u,v,k} \colon \Omega \times \mathcal{M}(\Omega) \to [0,1].$$

Здесь x, y — двоичные слова, u, v — рациональные числа, а k — натуральное число; значение $g_{x,y,u,v,k}(\omega, P)$ равно нулю, если ω не начинается на x; при $x \sqsubseteq \omega$ это значение кусочно-линейно зависит от $P(y)$, и равно 0 при $x \notin (u, v)$ и 1 при $x \in (u + 2^{-k}, v - 2^{-k})$.

Как и в предложении 4.16, всякая перечислимая снизу неотрицательная функция является пределом возрастающей последовательности базисных функций (заметим, что в $g_{x,y,u,v,k}(\omega, P)$ входит значение P только на слове y, но мы затем берём минимумы и максимумы).

Далее, как в предложении 4.17, можно заметить, что для базисной функции f интеграл $\int f(\omega, P)\, dP(\omega)$ является вычислимой функцией меры P (и базисной функции f).

Наконец, остаётся верным (с тем же доказательством) и аналог предложения 4.18:

Теорема 5.7 (усечение)**.** *Пусть $\varphi(\omega, P)$ — перечислимая снизу функция. Тогда существует перечислимая снизу функция $\varphi'(\omega, P)$, для которой для любого P*

(а) $\int \varphi'(\omega, P)\, dP(\omega) \leqslant 2$*;*

(б) *если* $\int \varphi(\omega, P)\, dP(\omega) \leqslant 1$*, то* $\varphi'(\omega, P) = \varphi(\omega, P)$ *при всех* ω*.*

Это позволяет построить универсальный тест как функцию последовательности и произвольной меры на Ω:

Теорема 5.8. *Существует универсальный (максимальный с точностью до постоянного множителя) равномерный тест.*

Доказательство. Как и раньше, будем перечислять все перечислимые снизу функции, подвергать каждую из них усечению (которое её не портит, если функция и так была тестом), и затем сложим получившиеся тесты (или почти-тесты) с подходящими коэффициентами.

Определение 5.9. *Фиксируем один из универсальных равномерных тестов и будем обозначать его $\mathbf{t}(\omega, P)$. Будем говорить, что последовательность является* равномерно случайной *по мере P (не обязательно вычислимой), если $\mathbf{t}(\omega, P) < \infty$.*

Покажем, что для вычислимых мер это определение согласуется с прежним (определение 2.13):

Предложение 5.10. *Пусть P — вычислимая мера, а $\mathbf{t}_P(\omega)$ — универсальный ограниченный в среднем тест для этой меры в смысле определения* 2.13*. Тогда $c_1\, \mathbf{t}_P(\omega) \leqslant \mathbf{t}(\omega, P) \leqslant c_2\, \mathbf{t}_P(\omega)$ для некоторых $c_1, c_2 > 0$ и для всех ω.*

Здесь константы c_1 и c_2 зависят от выбора меры P и от выбора теста $\mathbf{t}_P$ для этой меры (этот выбор был произвольно сделан для каждой вычислимой меры).

Это предложение показывает, в частности, что для вычислимых мер равномерная случайность совпадает со случайностью в смысле Мартин-Лёфа.

Доказательство. Для начала покажем, что $\mathbf{t}(\omega, P) \leqslant c_2\, \mathbf{t}_P(\omega)$. Заметим, что функция $\omega \mapsto \mathbf{t}(\omega, P)$ является перечислимой снизу: поскольку мера P вычислима, мы можем эффективно перечислять все интервалы в пространстве мер, её содержащие. Поэтому она мажорируется максимальным перечислимым снизу P-тестом $\mathbf{t}_P$.

Чтобы доказать обратное неравенство, добавим фиктивный аргумент и рассмотрим функцию

$$t(\omega, Q) = \mathbf{t}_P(\omega).$$

Эта функция, естественно, не является равномерным тестом, так как её интеграл по мере Q (при $Q \neq P$) может быть любым, но после усечения она становится (почти) тестом, не меняясь на P.

Можно пытаться определить тесты относительно некоторой одной (не обязательно вычислимой) меры. Будем говорить, что функция $f : \Omega \to [0, +\infty]$ *перечислима снизу относительно меры* P, если она получается из перечислимой снизу функции на $\Omega \times \mathcal{M}(\Omega)$ фиксацией второго аргумента равным P. Теперь можно дать такое определение:

Определение 5.11. *Пусть P — некоторая мера на Ω. Будем называть* тестом случайности относительно P *перечислимую снизу относительно P функцию f, для которой $\int f(\omega)\, dP(\omega)$ не превосходит единицы.*

Теорема 5.7 показывает, однако, что нового понятия случайности при этом не получается — мы приходим к тем же самым равномерным тестам:

Теорема 5.12. *Пусть P — некоторая мера, а $t_P(\omega)$ — тест относительно этой меры. Тогда существует равномерный тест $t'(\cdot, \cdot)$, для которого $t_P(\omega) \leqslant 2t(\omega, P)$. Напротив, сужение любого равномерного теста на меру P является P-тестом.*

Для равномерных тестов также ввести понятие расширенного теста:

Определение 5.13 (расширенные равномерные тесты)**.** *Функция $T\colon \{0,1\}^* \times \mathcal{M}(\Omega) \to [0,1]$, перечислимая снизу и монотонная по первому аргументу, называется* расширенным равномерным тестом*, если*

$$\sum_{|x|=n} T(x, P)P(x) \leqslant 1$$

для любого n и любой меры P.

Как и раньше, в силу монотонности можно суммировать не по словам данной длины, а по любому беспрефиксному множеству.

Следующее предложение легко доказывается с использованием аналога предложения 4.16 (представления неотрицательных перечислимых снизу функций как сумм рядов):

Предложение 5.14. *Любой равномерный тест $t(\omega, P)$ порождается некоторым расширенным равномерным тестом в следующем смысле:*

$$t(\omega, P) = \sup_{x \sqsubseteq \omega} T(x, P).$$

Напротив, эта формула по любому расширенному равномерному тесту T даёт равномерный тест t.

Среди расширенных равномерных тестов тоже можно выбрать максимальный (проводя аналогичное усечение и складывая результаты). Фиксируем один из таких тестов; будем обозначать его $\mathbf{t}(x, P)$ (где $x \in \{0,1\}*$, P — мера на Ω). Он порождает максимальный расширенный равномерный тест $\mathbf{t}(\omega, P)$ (с точностью до ограниченного множителя).

Замечание 5.15. *Если мы захотим перенести развитую нами теорию на случай некомпактного пространства последовательностей натуральных чисел (вместо компактного пространства последовательностей нулей и единиц), то можно и нужно определять расширенные тесты непосредственно, а не через тесты на бесконечных последовательностях. При этом можно доказать и существование максимального среди них.*

Предложение 5.10 позволяет обобщить результат, известный нам для бернуллиевых мер:

Теорема 5.16. *Пусть мера P вычислима относительно оракула A и, напротив, оракул A может быть эффективно восстановлен по известным приближения с произвольной точностью к значениям меры P. В этом случае последовательность ω равномерно случайна относительно меры P тогда и только тогда, когда она случайна по Мартин-Лёфу относительно меры P с оракулом A.*

(Поскольку добавление оракула A делает меру P вычислимой, случайность по Мартин-Лёфу имеет смысл.)

Доказательство. Пусть $\mathbf{t}(\omega, P)$ бесконечно. Заметим, что функция $\mathbf{t}(\cdot, P)$ является A-перечислимой снизу, так как мера P вычислима с оракулом A. Поэтому ω не случайна по мере P с оракулом A.

Напротив, пусть ω не случайна по мере P с оракулом A и $t(\cdot)$ — A-перечислимый снизу P-тест, для которого $t(\omega) = \infty$. Поскольку оракул A может быть восстановлен по приближениям к P, то существует перечислимая снизу функция $\bar{t}(\cdot, \cdot)$, для которой $\bar{t}(\cdot, P) = t(\cdot)$. Остаётся преобразовать $\bar{t}$ в равномерный тест с помощью теоремы 5.7.

Отметим, что не всякая мера P удовлетворяет условию теоремы (оно означает, что массовая проблема "указывать приближения к значениям меры P" равносильна проблеме разрешения некоторого множества; про степени таких массовых проблем см. в [21]). Впоследствии (теорема 5.36) мы покажем, как можно характеризовать равномерную случайность для произвольных мер (в терминах случайности по Мартин-Лёфу с оракулом).

Другое применение техники усечения: покажем, что равномерные тесты являются обобщением равномерных бернуллиевых тестов в смысле определения 4.19.

Теорема 5.17. *Пусть $\mathbf{t}(\omega, P)$ — универсальный равномерный тест и $\mathbf{t}(\omega, p)$ — универсальный равномерный тест бернуллиевости из леммы 4.20. Тогда $\mathbf{t}(\omega, B_p) \stackrel{+}{=} \mathbf{t}(\omega, p)$.*

Здесь B_p — бернуллиева мера с параметром p.

Доказательство. Для доказательства $\stackrel{+}{<}$-неравенства заметим, что функция $\langle \omega, p \rangle \mapsto \mathbf{t}(\omega, B_p)$ является равномерным бернуллиевым тестом, поскольку функция $p \mapsto B_p$ вычислима (в естественном смысле).

Чтобы доказать обратное неравенство, заметим, что существует вычислимое отображение из пространства мер в $[0, 1]$, которое переводит B_p в p (достаточно взять вероятность однобитового слова). Комбинируя эту функцию с $\mathbf{t}(\omega, p)$, мы получаем перечислимую снизу функцию $f(\omega, P)$, определённую на всех мерах и продолжающую наш тест на бернуллиевых мерах: $f(\omega, B_p) = \mathbf{t}(\omega, p)$. Функция f ещё не является равномерным тестом, но к ней можно применить усечение.

5.2 Априорная вероятность с оракулом и равномерные тесты

Для вычислимой меры у нас было выражение для универсального теста (предложение 2.21) через (дискретную) априорную вероятность. Аналогичное выражение существует и для универсального равномерного теста:

Теорема 5.18.

$$\mathbf{t}(\omega, P) \stackrel{+}{=} \sum_{x \sqsubseteq \omega} \frac{\mathbf{m}(x|P)}{P(x)}.$$

Здесь, правда, нам ещё предстоит определить понятие априорной вероятности относительно меры, то есть величину $\mathbf{m}(x|P)$. Мы сейчас это сделаем, после чего вернёмся к доказательству.

Определение 5.19. *Будем называть неотрицательную функцию $t(x, P)$, аргументами которой являются двоичное слово x и мера P,* равномерной перечислимой снизу полумерой, *если она перечислима снизу и $\sum_x t(x, P) \leqslant 1$ для любой меры P на Ω.*

Предложение 5.20. *Среди всех равномерных перечислимых снизу полумер существует наибольшая с точностью до умножения на константу.*

Это доказывается тем же способом, что и существование универсального теста (и даже немного проще, поскольку здесь ограничение на значения теста не зависит от меры).

Определение 5.21. *Фиксируем одну из таких наибольших полумер и назовём её* априорной вероятностью относительно P. *Будем обозначать её $\mathbf{m}(x|P)$.*

(Мы используем чёрточку вместо запятой, чтобы подчеркнуть родство с рассматриваемой обычно условной априорной вероятностью.)

Доказательство.(теоремы 5.18) Нам нужно проверить две вещи. Во-первых, мы должны убедиться, что правая часть формулы задаёт равномерный тест. Каждый из членов суммы можно рассматривать как функцию двух аргументов, равную 0 вне конуса продолжений x и равную $\mathbf{m}(x|P)/P(x)$ внутри этого конуса. Для данного x функции $\mathbf{m}(x|P)$ и $1/P(x)$ перечислимы снизу (равномерно по x), и их суммирование даёт перечислимую снизу функцию. Интеграл этой функции по какой-либо мере P равен сумме интегралов слагаемых, то есть $\sum_x \mathbf{m}(x|P)$, и потому не превосходит 1.

Здесь есть особый случай, когда $P(x) = 0$ для некоторого x. В этом случае соответствующее слагаемое формулы становится бесконечным для ω, продолжающих x. Но поскольку мера этого конуса равна нулю, то интеграл по нему равен нулю, и потому слагаемое хоть и не равно $\mathbf{m}(x|P)$, но только меньше. Таким образом, правая часть формулы есть равномерный тест и потому не превосходит универсального равномерного теста: мы доказали $\dot{>}$-неравенство.

Вторая часть доказательства не так проста: наблюдая за увеличением значений равномерного теста, мы должны распределить это увеличение между различными членами суммы в правой части, при этом сохранив перечислимость снизу. Трудность в том, что если, скажем, сначала перечислимая снизу функция была равна 1 на некотором эффективно открытом множестве A, а вне него равнялась нулю, а потом это множество заменилось на большее множество B, то разница (характеристическая функция $B \setminus A$), вообще говоря, не будет перечислимой снизу, так как в пространстве мер (как, например, и на отрезке) разность двух интервалов не будет открытым множеством.

Решение этой проблемы состоит в том, что мы переходим к непрерывным функциям. Пусть нам дан произвольный равномерный тест $t(\omega, P)$. Поскольку он перечислим снизу, его можно представить как предел неубывающей последовательности неотрицательных базисных функций, или — переходя к разностям — в виде суммы ряда из неотрицательных базисных функций: $t(\omega, P) = \sum t_i(\omega, P)$.

Будучи базисной, функция ω зависит лишь от некоторого конечного начала последовательности ω; обозначим длину этого начала n_i. Для каждого слова x длины n_i мы получаем некоторую перечислимую снизу функцию $t_{i,x}(P)$, при этом $t_i(\omega, P) = t_{i,x}(P)$, если ω начинается на x. Теперь положим $m_i(x, P) = t_{i,x}(P) \cdot P(x)$, если x имеет длину n_i (для остальных длин нуль). Функция m_i перечислима снизу (как произведение двух перечислимых снизу функций) равномерно по i, поэтому и сумма $m(x, P) = \sum m_i(x, P)$ будет перечислимой снизу.

Покажем, что m является полумерой, то есть что $\sum_x m(x,P) \leqslant 1$ при любом P. В самом деле, $\sum_x m_i(x,P)$ ненулевые члены соответствуют словам длины n_i, и эта сумма равна $\sum_x t_{i,x}(P)P(x)$, то есть в точности интегралу $\int t_i(\omega,P)\,dP(\omega)$, а сумма этих интегралов не превосходит 1 по условию.

Кроме того, если для всех начал x последовательности ω мера $P(x)$ не равна нулю, то

$$\sum_{x\sqsubseteq\omega} \frac{m_i(x,P)}{P(x)} = \frac{t_{i,x_i}(P)\cdot P(x)}{P(x)} = t_i(\omega,P)$$

(здесь x_i — начало ω длины n_i), поэтому после суммирования по i

$$\sum_{x\sqsubseteq\omega} \frac{m(x,P)}{P(x)} = t(\omega,P),$$

и остаётся воспользоваться максимальностью полумеры, чтобы получить $\dot{<}$-неравенство для случая, когда все начала ω имеют ненулевую P-меру. Если же одно из них имеет нулевую P-меру, то правая часть бесконечна, так что и тут неравенство выполнено.

Вопрос. Для универсального теста случайности относительно равномерной меры в этой формуле можно было заменить сумму на максимум. Можно ли это сделать для равномерных тестов? (Применённое тогда рассуждение встречает трудности.) Можно ли разумно определить априорную вероятность на дереве относительно меры, и доказать равномерный вариант теоремы Левина–Шнорра?

Мы вернёмся к определению априорной вероятности с оракулом (и её связи с префиксной сложностью) в разделе 7.4

5.3 Эффективно компактные классы мер

Мы рассматривали бернуллиевы тесты, то есть полунепрерывные снизу функции, интеграл от которых по любой бернуллиевой мере не превосходит 1. В этом определении вместо бернуллиевых мер можно рассматривать произвольный эффективно компактный класс:

Определение 5.22. *Пусть $\mathcal{C}$ — эффективно компактный класс мер на Ω. Неотрицательная полунепрерывная снизу функцию $t\colon \Omega \to [0,\infty]$ называется* $\mathcal{C}$-тестом, *если $\int t(\omega)\,dP(\omega) \leqslant 1$ для любой меры $P \in \mathcal{C}$.*

Теорема 5.23. *Пусть $\mathcal{C}$ — эффективно компактный класс мер.*
(а) *Существует универсальный $\mathcal{C}$-тест $\mathbf{t}_{\mathcal{C}}(\cdot)$.*
(б) $\mathbf{t}_{\mathcal{C}}(\omega) = \inf_{P\in\mathcal{C}} \mathbf{t}(\omega,P)$.

Доказательство. Оба утверждения теоремы доказываются аналогично леммам 4.20 и 4.21.

Замечание 5.24. *Поскольку класс $\mathcal{C}$ компактен, а функция $\mathbf{t}(\omega,P)$ полунепрерывна снизу, то* inf *в утверждении* (б) *можно заменить на* min.

Вопрос. Можно ли найти какие-то критерии случайности по отношению к естественным классам мер (в частности, в терминах сложности)? Например, можно ли охарактеризовать бернуллиевы последовательности в терминах сложности их начальных отрезков? Можно показать, что главный член дефекта бернуллиевости можно записать как

$$\log C_n^k - KP(x|n,k)$$

для начального отрезка x длины n, содержащего k единиц. Подобный критерий приведён в [6], но он выглядит довольно искусственно.

Аналогичные вопросы естественно задать и для других классов (марковские меры, инвариантные относительно сдвигов меры).

5.4 Разреженные последовательности

Бывают ситуации, в которых мы говорим о случайности, но это не сводится к стандартной постановке (случайность данного наблюдения ω относительно данной модели P). Сейчас мы рассмотрим один из таких случаев — понятие разреженной последовательности, введённое в [3]. Другой пример, который можно назвать онлайн-случайностью, рассмотрен в разделе 9.2.

Будем называть p-разреженной последовательность, в которой меньше единиц, чем в случайной по бернуллиевой мере B_p. Другими словами, будем брать произвольные B_p-случайные последовательности и заменять в них некоторые единицы на нули. Всё, что получится таким образом, будет p-разреженным.

Определение 5.25 (разреженные последовательности)**.** *Введём покоординатный порядок на бесконечных последовательностей нулей и единиц (или конечных последовательностей одной длины): $\omega \leqslant \omega'$, если $\omega(i) \leqslant \omega'(i)$ при всех i, то есть ω может быть получена из ω' заменой некоторых единиц на нули.*

Пусть B_p — бернуллиева мера для некоторого вычислимого p. Будем говорить, что последовательность ω является p-разреженной*, если $\omega \leqslant \omega'$ для некоторой B_p-случайной ω'. (В терминах множеств: p-разреженные множества — это подмножества p-случайных множеств.)*

Покажем, что в определении разреженности можно избавиться от квантора существования по ω' и дать критерий в терминах монотонных тестов.

Определение 5.26. *Будем говорить, что функция $f\colon \Omega \to [0,\infty]$ монотонна, если $f(\omega') \geqslant f(\omega)$ при $\omega' \geqslant \omega$.*

Монотонная перечислимая снизу функция $f\colon \Omega \to [0,\infty]$ называется тестом p-разреженности*, если $\int t(\omega)\, dB_p(\omega) \leqslant 1$. Тест разреженности называем* универсальным*, если он максимален среди всех таких тестов (с точностью до умножения на константу, как обычно).*

Монотонность тестов гарантирует, говоря неформально, что закономерностью является наличие единиц на каких-то местах, а не их отсутствие. (Отметим, что раньше мы говорили совсем о другой монотонности, определяя расширенные тесты: там сравнивались значения функции на конечном слове и его продолжении.)

Предложение 5.27. *Рассмотрим универсальный тест $\mathbf{t}(\omega, P)$. Тогда величина*

$$r_p(\omega) = \min_{\omega' \geqslant \omega} \mathbf{t}(\omega, B_p)$$

задаёт универсальный тест p-разреженности.

Доказательство. Тест p-разреженности по определению является тестом по мере B_p. Используя его монотонность и сравнивая с универсальным, получаем, что любой тест разреженности не превосходит r_p (с точностью до константы).

В обратную сторону нужно показать, что минимум в выражении для r_p достигается и что эта функция является тестом p-разреженности. Перечислимость снизу доказывается с использованием того, что свойство $\omega \leqslant \omega'$ задаёт эффективно замкнутое подмножество эффективно

компактного пространства $\Omega \times \Omega$ (ср. ниже предложение 7.20). Монотонность и неравенство для интеграла непосредственно следуют из определения.

Отсюда получаем критерий разреженности в терминах тестов:

Теорема 5.28. *Последовательность является p-разреженной (получается из p-случайной заменой некоторых единиц на нули) тогда и только тогда, когда универсальный тест разреженности $r_p(\omega)$ конечен.*

Разреженность эквивалентна случайности по некоторому классу мер. Чтобы описать этот класс, введём понятие спаривания (coupling) мер.

Определение 5.29. *Пусть P, Q — две меры на Ω. Будем говорить, что мера P может быть спарена с Q (обозначение: $P \preceq Q$), если существует мера R на $\Omega \times \Omega$, для которой:*

(а) *первая проекция R равна P, а вторая равна Q;*

(б) *мера R целиком сосредоточена на парах $\langle \omega, \omega' \rangle$, у которых $\omega \leqslant \omega'$ (вероятность этого события по мере R равна 1).*

Отметим, что отношение спаривания в этом определении несимметрично (хотя из названия этого не видно); более наглядно было бы говорить "P может быть помещена под Q", если $P \preceq Q$.

Следующий критерий спариваемости хорошо известен и восходит к [27]; доказательство можно найти в [3].

Предложение 5.30. *Свойство $P \preceq Q$ равносильно такому: для всякой монотонной базисной функции f выполнено неравенство*

$$\int f(\omega)\, dP(\omega) \leqslant \int f(\omega)\, dQ(\omega).$$

В этом критерии можно допустить произвольные монотонные функции, или, наоборот, ограничится характеристическими функциями множеств.

Определение 5.31. *Пусть $\mathcal{S}_p$ — класс всех мер P, для которых $P \preceq B_p$.*

Предложение 5.32. *Класс мер $\mathcal{S}_p$ является эффективно замкнутым (и, следовательно, эффективно компактным).*

Доказательство. Каждое из неравенств предыдущего предложения (для каждой базисной функции f) задаёт эффективно замкнутое множество, и их пересечение тоже будет эффективно замкнутым.

Теорема 5.33. *Универсальный тест r_p является универсальным тестом для класса мер $\mathcal{S}_p$.*

Отсюда вытекает, что последовательность является p-разреженной тогда и только тогда, когда она равномерно случайна относительно некоторой меры из класса $\mathcal{S}_p$.

Доказательство этой теоремы основано на таком утверждении:

Лемма 5.34 (монотонизация)**.** *Пусть $t\colon \Omega \to \mathbb{R}$ — базисная функция, и $\int t(\omega)\, dQ(\omega) \leqslant 1$ для любой меры $Q \in \mathcal{S}_p$. Определим монотонную базисную функцию $\hat{t}(\omega) = \max_{\omega' \leqslant \omega} t(\omega)$; это определение корректно, так как $t(\omega)$ зависит только от конечного числа позиций в ω. Тогда $\int \hat{t}(\omega)\, dB_p(\omega) \leqslant 1$.*

Доказательство. Пусть функция t зависит только от первых n координат. Для каждого $x \in \{0,1\}^n$ выберем $x' \leqslant x$, где $t(x')$ достигает максимума (среди таких x'). Помимо распределения B_p рассмотрим распределение Q, в котором бернуллиева мера x перенесена на x' (при этом меры из различных x могут быть отнесены к одному x' и тогда складываются). Мы описали поведение Q на первых n битах; следующие биты добавляются независимо и вероятность единицы в каждой позиции равна p; отметим также, что для математических ожиданий функций t и $\hat{t}$ важны только первые n битов.

По построению $Q \preceq B_p$ (мы по существу описали меру на парах), поэтому $\int t(\omega)\, dQ(\omega) \leqslant 1$. Но этот интеграл равен $\int \hat{t}(\omega)\, dB_p(\omega)$. Лемма доказана.

Вернёмся к теореме 5.33.

Доказательство. Всякий тест p-разреженности t является тестом для класса $\mathcal{S}_p$. В самом деле, интеграл t по мере из класса $\mathcal{S}_p$ не превосходит интеграла t по мере B_p в силу монотонности теста и возможности спаривания.

В другую сторону: покажем, что для любого теста t для класса $\mathcal{S}_p$ существует не меньший его тест p-разреженности. В самом деле, тест t может быть представлен в виде предела возрастающей последовательности базисных функций t_n. Применив к ним лемму о монотонизации, получим возрастающую последовательность базисных функций $\hat{t}_n$, которые всюду не меньше t_n и имеют интегралы не больше 1 по мере B_p. Их предел и будет требуемым тестом p-разреженности.

5.5 Варианты определений случайности

Мы уже определили равномерную случайность последовательности относительно произвольной (не обязательно вычислимой) меры. Однако есть и другие варианты такого рода определений.

Оракулы

Мы можем использовать определение случайности по Мартин-Лёфу, добавляя оракул, который делает меру вычислимой. А именно, назовём последовательность ω случайной относительно меры P, если существует оракул A, относительно которого P вычислима, и при этом ω случайна в смысле Мартин-Лёфа с оракулом A относительно P.

(Мы говорим "существует оракул A, делающий меру P вычислимой", а не "для любого оракула A, делающего P вычислимой", поскольку среди таких оракулов есть и оракул, делающий последовательность ω вычислимой. В этом случае она не может быть случайной, если только не является атомом меры P.)

Оказывается, что это определение (как доказали Адам Дей и Джозеф Миллер), этот вариант определения равносилен равномерной случайности. Доказательство этой эквивалентности требует некоторых приготовлений.

Прежде всего зададим себе вопрос, почему нельзя взять в качестве оракула саму меру (как это делалось для случая бернуллиевых мер, когда мы в качестве оракула брали двоичное разложение числа p). Дело в том, что выбор такого разложения не однозначен ($0.01111\ldots = 0.10000\ldots$). Когда речь идёт об одном числе p, то это не важно, поскольку неоднозначность возникает только для рациональных p, и в этом случае оба представления вычислимы. Однако для мер это уже не так: мера задаётся счётным количеством действительных чисел (скажем, вероятностями отдельных слов, или условными вероятностями), и произвол в выборе представления может не сводиться к конечному число вариантов.

Определение 5.35. *Зафиксируем некоторый способ кодирования мер на Ω двоичными последовательностями, то есть вычислимое отображение $\pi \mapsto R_\pi$ множества Ω в пространство мер. Например, можно разбить последовательность π на счётное число частей и каждую из них считать двоичной записью условной вероятности единицы после некоторого начала (начал тоже счётное число). При этом возникает неоднозначность (если вероятность какого-то начала равна нулю, то условные вероятности после него не играют роли), но она и так была.*

Определим теперь r-тест (*representation test, тест случайности по данному представлению меры*) *как перечислимую снизу неотрицательную функцию $t(\omega, \pi)$, для которой неравенство $\int t(\omega, \pi)\, dR_\pi(\omega) \leqslant 1$ выполняется при всех π.*

Как мы уже обсуждали, одна и та же мера P может иметь много представлений (может быть много различных π, для которых $R_\pi = P$), и значения теста для различных представлений одной и той же меры могут быть разными.

Как обычно, легко доказать, что

(а) всякая перечислимая снизу функция может быть эффективно усечена (сделана не более чем вдвое превосходящей r-тест), при этом если она уже была r-тестом, то она не изменится;

(б) существует универсальный (максимальный с точностью до константы) r-тест $\mathbf{t}(\omega, \pi)$.

При фиксированном π функция $\mathbf{t}(\cdot, \pi)$ совпадает с универсальным π-вычислимым ограниченным в среднем тестом случайности относительно меры R_π. В самом деле, она является таким тестом; с другой стороны, любой такой тест перечисляется снизу машиной с оракулом, и эта машина может быть применена к любому оракулу (но может не давать теста); мы получаем перечислимую снизу функцию $t'(\omega, \pi)$, которая совпадает с исходным тестом при данном π; остаётся применить свойство (а).

Как следствие этого простого рассуждения мы получаем, что величина $\mathbf{t}(\omega, \pi)$ конечна тогда и только тогда, когда последовательность ω случайна с оракулом π относительно меры R_π.

Теорема 5.36 (Дей–Миллер)**.** *Последовательность ω равномерно случайна по мере P тогда и только тогда, когда существует оракул π, делающий меру P вычислимой, а последовательность ω — случайной в смысле Мартин-Лёфа по мере P с оракулом π.*

Кроме того,

$$\mathbf{t}(\omega, P) \doteq \inf_{\{\pi | R_\pi = P\}} \mathbf{t}(\omega, \pi).$$

Доказательство. Докажем указанное в теореме равенство. Заметим, что если t — равномерный тест, то $t(\omega, R_\pi)$ как функция от ω и π представляет собой r-тест, и потому мажорируется универсальным r-тестом.

Обратное утверждение несколько сложнее. Нам нужно доказать, что функция в правой части перечислима снизу как функция последовательности ω и меры P. (Условие на интеграл после этого получается легко, поскольку мера P имеет хотя бы одно представление π.) Это можно доказать, используя эффективную компактность множества пар $\langle P, \pi \rangle$, для которых $P = R_\pi$. В общем виде (для произвольных конструктивных метрических пространств) это утверждение составит содержание леммы 7.21 на с. 45, и мы не будем приводить отдельного доказательства для рассматриваемого частного случая, поскольку оно ничем не отличается от общего.

Осталось объяснить, как связаны доказанное равенство и случайность с оракулом. Если $\mathbf{t}(\omega, P)$ конечно, то по доказанному равенству существует π, при котором $R_\pi = P$ и $\mathbf{t}(\omega, \pi)$ конечно. Как мы видели, это в свою очередь означает, что ω случайна по мере R_π, то есть по мере P, с оракулом π, который делает меру P вычислимой.

Напротив, если $t(\omega, P)$ бесконечно, а оракул A делает меру P вычислимой, то функция $t(\cdot, P)$ будет A-перечислимой снизу, и её интеграл не превосходит 1 по мере P, так что последовательность ω не будет случайной с оракулом A по мере P.

Слепая (безоракульная) случайность

Можно использовать определение эффективно нулевого множества (или перечислимого снизу теста) и в ситуации невычислимой меры. При этом может не существовать максимального эффективно нулевого множества. Например, если мера P сосредоточена на единственной невычислимой последовательности π, то все интервалы, не содержащие π, будут эффективно нулевыми множествами, а их объединение (дополнение к синглетону $\{\pi\}$) таковым не будет, иначе π была бы вычислимой.

Тем не менее мы можем определить понятие случайной последовательности как последовательности, не лежащей *ни в одном* эффективно нулевом множестве (что эквивалентно тому, что все тесты на ней конечны). Кьёс-Хансен предложил называть такую случайность "гиппократовой" (ссылаясь на легенду о враче Гиппократе), но мы предпочитаем говорить о "слепой" (blind) или "безоракульной" случайности.

Определение 5.37 (слепые тесты)**.** *Перечислимые снизу (без оракула) функции $t(\omega)$, для которых $\int t(\omega)\, dP(\omega) \leqslant 1$, будем называть* слепыми*, или* безоракульными*, тестами для меры P. Последовательность ω будем называть* безоракульно случайной *по мере P, если $t(\omega)$ конечно для любого такого теста t.*

Как мы видели, может не существовать максимального слепого теста.

Это понятие безоракульной случайности можно характеризовать во введённых ранее терминах:

Теорема 5.38. *Последовательность ω является безоракульно случайной относительно меры P тогда и только тогда, когда она случайна относительно любого эффективно компактного класса мер, содержащего меру P.*

Доказательство. Предположим, что ω не случайна относительно некоторого эффективно компактного класса мер, содержащих меру P. Тогда перечислимый снизу (безо всякого оракула) тест для этого класса будет безоракульным тестом для P, так что ω не будет безоракульно случайной.

С другой стороны, предположим, что существует некоторый безоракульный тест t для меры P, для которого $t(\omega)$ бесконечно. Тогда можно попросту рассмотреть класс всех мер Q, для которых t является тестом, то есть для которых $\int t(\omega)\, dQ(\omega) \leqslant 1$. Этот класс эффективно замкнут, и потому эффективно компактен. В самом деле, если для некоторой меры Q интеграл больше 1, то уже для некоторого базисного приближения t_n к t (снизу) этот интеграл больше 1, а последнее свойство задаёт эффективно открытое множество в пространстве мер. Перечисляя все t_n и объединяя все эти множества, получаем эффективно открытое множество.

Из определения (или из последней теоремы) легко вывести, что из равномерной случайности последовательности ω относительно P следует безоракульная случайность. Обратное утверждение неверно:

Теорема 5.39. *Существует последовательность ω, безоракульно случайная по некоторой мере P, но не являющаяся равномерно случайной по этой мере.*

Доказательство. Заметим, что безоракульная случайность не изменится, если мы чуть-чуть изменим меру P (так, чтобы мера любого множества изменилась не более чем в $O(1)$ раз). С другой стороны, с вычислительной точки зрения новая мера может быть гораздо сильнее. Например, начнём с равномерной бернуллиевой меры $B_{1/2}$, в которой все испытания независимы и имеют вероятность успеха $1/2$, и возьмём некоторую случайную по ней последовательность $\omega = \omega(1)\omega(2)\ldots$. Затем рассмотрим чуть сдвинутую меру B', в которой вероятности успеха равна $1/2 + \omega(1)\varepsilon_1, 1/2 + \omega(2)\varepsilon_2, \ldots$; здесь ε_i настолько малы и так быстро сходятся к нулю, что B' отличается от B на любом множестве не более чем в константу раз. Тогда B' содержит информацию об ω, и несложно построить равномерный тест t, для которого $t(\omega, B') = \infty$.

Однако бывают некоторые классы мер, для которых понятия равномерной и безоракульной случайности совпадают. (В частности, таковы бернуллиевы меры.) Чтобы сформулировать достаточные условия такого совпадения, начнём с определения.

Определение 5.40. *Обозначим через* $\mathrm{Randoms}(P)$ *множество последовательностей, равномерно случайных относительно меры* P. *Назовём класс мер* эффективно ортогональным, *если*

$$\mathrm{Randoms}(P) \cap \mathrm{Randoms}(Q) = \varnothing$$

для любых двух различных мер P *и* Q *из этого класса.*

Теорема 5.41. *Пусть* $\mathcal{C}$ *— эффективно компактный и эффективно ортогональный класс мер. Тогда для любой меры* P *из этого класса понятия равномерной и безоракульной случайности относительно* P *совпадают.*

Утверждение этой теоремы выглядит парадоксально: мы утверждаем нечто о случайности по одной мере P, а в условии стоит возможность вложить P в класс мер с некоторыми свойствами. (Было бы естественно найти более явные достаточные условия на P.)

Из этой теоремы следует, что построенная при доказательстве теоремы 5.39 мера не может быть вложена в эффективно замкнутый эффективно ортогональный класс.

Доказательство. Мы уже отмечали, что в одну сторону утверждение прямо следует из определения. Докажем обратное. Предположим, что последовательность ω безоракульно случайна относительно меры P. По теореме 5.38 она случайна относительно класса мер $\mathcal{C}$. Следовательно, она равномерно случайна относительно некоторой меры P' из класса $\mathcal{C}$. Остаётся доказать, что $P = P'$.

Пусть это не так. Покажем, что существует компактный класс мер $\mathcal{C}'$, который содержит P, но не содержит P'. В самом деле, $P \neq P'$ означает, что некоторое слово имеет различные меры относительно P и P', и можно найти замкнутое условие на меру этого слова, которое отделит P от P'. Теперь рассмотрим эффективно компактный класс $\mathcal{C} \cap \mathcal{C}'$. Он содержит P и потому последовательность ω будет случайной относительно этого класса. Значит, и в нём есть мера P'', относительно которой последовательность ω равномерно случайна. Но $P' \neq P''$ (одна мера лежит в $\mathcal{C}'$, а другая — нет), так что получаем противоречие с эффективной ортогональностью класса $\mathcal{C}$.

Замечание 5.42. *Доказанная теорема применима, в частности, к классу бернуллиевых мер. Может показаться, что её можно доказать проще: если последовательность* ω *случайна (безоракульно или тем более равномерно) по мере* B_p, *то предел частоты единиц в ней равен* p *и тем самым он определяется самой последовательностью (и дополнительный оракул для* p *ничего нового не даёт). Это рассуждение, однако, неправильно: хотя* p *и определяется*

последовательностью, но не является вычислимой (или хотя бы непрерывной) функцией от неё. В самом деле, никакой начальный отрезок последовательности не гарантирует, что её предельная частота будет в заданном интервале. Аналогичное рассуждение, однако, можно применить к последовательностям, у которых дефект случайности ограничен заранее известной константой. (См. подробнее в [11]*, где введено относящееся к этому понятие послойной вычислимости.) В частности, можно показать, что если последовательность ω безоракульно случайна по мере B_p, то двоичное разложение p вычислимо с оракулом ω.*

6 Нейтральная мера

Следующая теорема, опубликованная в [16] и затем в [10], указывает на парадоксальное свойство равномерной случайности, которая отличает её от случайности с оракулом.

Определение 6.1. *Назовём меру на Ω* нейтральной*, если всякая последовательность является равномерно случайной относительно этой меры.*

Теорема 6.2. *Существует нейтральная мера; более того, существует мера N, для которой $\mathbf{t}(\omega, N) \leqslant 1$ при всех $\omega \in \Omega$.*

Прежде чем доказывать эту теорему, отметим, что все вычислимые последовательности обязаны быть атомами нейтральной меры (иметь положительную вероятность). В самом деле, можно построить тест, который ищет длинные отрезки вычислимой последовательности, имеющие малую меру (этого можно дождаться, имея последовательность и меру в качестве аргументов), и присваивает им большое значение дефекта.

Отсюда следует, что нейтральная мера не может быть вычислимой. В самом деле, для вычислимой меры легко построить вычислимую последовательность, не являющуюся атомом (надо из двух продолжений слова выбирать то, которое имеет меньшую — или хотя бы не сильно бóльшую — меру). Аналогичное рассуждение показывает, нейтральная мера не эквивалентна никакому оракулу (нет оракула, который делал бы её вычислимой и, напротив, мог бы быть восстановлен по приближениям к ней). В самом деле, если A — такой оракул, то (как мы видели) равномерная случайность равносильна случайности с оракулом A, и можно повторить то же рассуждение.

Нейтральная мера не может быть также перечислимой сверху или снизу, но при нашем определении (когда мера всего пространства должна равняться единице) это не даёт ничего нового. Некоторые более осмысленные (и менее тривиальные) варианты этого утверждения доказаны в [17].

Доказательство. Рассмотрим универсальный тест $\mathbf{t}(\omega, P)$. Мы утверждаем, что существует мера N, для которой $\mathbf{t}(\omega, N) \leqslant 1$ для любой последовательности N. Другими словами, для каждой последовательности ω мы имеем условие на N, состоящее в том, что $\mathbf{t}(\omega, N) \leqslant 1$, и надо доказать, что все эти условия совместны (пересечение их непусто). Каждое условие задаёт замкнутое множество в компактном пространстве всех мер (вспомним, что $\mathbf{t}$ перечислимо снизу, и тем более полунепрерывно снизу), поэтому достаточно доказать совместность любого конечного числа условий .

Итак, возьмём k произвольных последовательностей $\omega_1, \ldots, \omega_k$. Нам надо доказать, что существует мера N, для которой $\mathbf{t}(\omega_i, N) \leqslant 1$ при всех $i = 1, \ldots, k$. Эту меру мы будем искать в виде выпуклой комбинации мер, сосредоточенных в $\omega_1, \ldots, \omega_k$. Таким образом, нам надо показать, что k замкнутых подмножеств k-мерного симплекса (соответствующих k условиям) имеют общую точку. Это делается с помощью известной топологической леммы (используемой в стандартном доказательстве теоремы Брауэра о неподвижной точке):

Лемма 6.3. *Пусть симплекс с вершинами $1, \ldots, n$ покрыт k замкнутыми множествами $A_1, \ldots, A_k$. Пусть при этом вершина i всегда принадлежит множеству A_i, ребро i–j целиком лежит в объединении $A_i \cup A_j$, и так далее (грань $(i_1, \ldots, i_s)$ целиком лежит в $A_{i_1} \cup \ldots \cup A_{i_s}$). Тогда пересечение $A_1 \ldots, A_k$ непусто.*

Приведём для полноты стандартное доказательство этой леммы. Рассмотрим симплициальное разбиение данного симплекса на мелкие симплексы и пометим каждую их вершину каким-то числом i от 1 до k, с тем условием, чтобы эта вершина лежала в A_i. Более того, можно предполагать что вершина i помечена числом i, вершины на отрезке i–j помечены либо числом i, либо числом j, и так далее. Комбинаторная лемма Шпернера говорит, что есть симплекс разбиения, у которого все вершины помечены по-разному. Устремляя размер максимального симплекса разбиения к нулю, и выбирая предельную точку последовательности получившихся разноцветных симплексов, находим искомую точку в пересечении всех A_i. Лемма доказана.

Применим теперь доказанную лемму. Согласно этой лемме, нам достаточно доказать, что любая точка на грани симплекса покрывается объединением соответствующих множеств. Пусть, скажем, есть точка (мера) X, являющаяся смесью вершин ω_1, ω_5 и ω_7; это значит, что мера X сосредоточена в множестве $\{\omega_1, \omega_5, \omega_7\}$. Нам нужно показать, что точка X покрыта объединением множеств A_1, A_5 и A_7, в нашем случае это означает, что одно из чисел $\mathbf{t}(\omega_1, X)$, $\mathbf{t}(\omega_3, X)$ и $\mathbf{t}(\omega_7, X)$ не превосходит единицы. Но мы знаем, что $\int \mathbf{t}(\omega, X)\, dX(\omega) \leqslant 1$ согласно определению теста, а этот интеграл является взвешенным средних этих трёх величин, так что хотя бы одна из них не превосходит 1.

7 Случайные точки метрического пространства

Большая часть сформулированных нами результатов о случайных последовательностях битов переносится на случай последовательностей натуральных чисел, а часто и на более общий случай метрических пространств. Мы сейчас изложим такие обобщения (а также и некоторые новые — даже и для пространства Ω — результаты).

7.1 Конструктивные метрическое пространства

Определяя конструктивные метрические пространства и перечислимые снизу функции на них, мы следуем [10, 12] (см. также[6]).

Определение 7.1. *Конструктивное метрическое пространство $\mathbf{X} = (X, d, D, \alpha)$ состоит из полного сепарабельного метрического пространства (X, d), в котором выделено счётное плотное множество D и его нумерация $\alpha\colon \mathbb{N} \to D$ (определённая на всём $\mathbb{N}$). Требуется, чтобы расстояние $d(\alpha(m), \alpha(n))$ было бы эффективно вычислимо (с любой требуемой точностью) по m и n.*

Открытые шары с центрами в точках из D и рациональными радиусами будем называть базисными шарами*; множество всех таких шаров образует* канонический базис *топологии X как метрического пространства.*

Будем называть последовательность $s_1, s_2, \ldots$ точек из D сильно фундаментальной*, если $d(s_m, s_n) \leqslant 2^{-m}$ при $n > m$. По предположению пространство X полно, поэтому всякая такая последовательность имеет единственный предел, и точки пространства можно отождествить с классами эквивалентности сильно фундаментальных последовательностей.*

Часто мы будем обозначать конструктивное метрическое пространство $\mathbf{X}$ просто X (если d, D и α ясны из контекста).

Примеры 7.2.

1. В *дискретном* метрическом пространстве $\Sigma = \{s_1, s_2, \ldots\}$ расстояние между любыми двумя различными точками равно 1; множество D содержит все точки и $\alpha(i) = s_i$.

2. Можно добавить к натуральным числам бесконечный элемент, положив $\overline{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$. Расстояние при этом можно определить как обычное расстояние между обратными величинами (при этом, естественно, $1/\infty = 0$). Это метрическое пространство можно назвать *одноточечной компактификацией* пространства натуральных чисел с дискретной метрикой предыдущего примера.

3. Вещественная прямая $\mathbb{R}$ с обычным расстоянием $d(x, y) = |x - y|$ также является конструктивным метрическим пространством (с каким-либо естественным выбором множества D и его нумерации). То же самое можно сказать о её положительной части $\mathbb{R}_+ = [0, \infty)$; можно добавить и бесконечный элемент $+\infty$, но тогда надо изменить метрику (например, перенеся её с отрезка).

4. Имея два конструктивных метрических пространства $\mathbf{X}$ и $\mathbf{Y}$, можно рассмотреть их произведение $\mathbf{Z} = \mathbf{X} \times \mathbf{Y}$ с одной из естественных метрик (например, сумма расстояний по обеим координатам); множество $D_{\mathbf{Z}}$ также является произведением $D_{\mathbf{X}} \times D_{\mathbf{Y}}$.

5. Пусть X — конечный или счётный алфавит (с фиксированной нумерацией). Тогда множество $X^{\mathbb{N}}$, состоящее из бесконечных последовательностей $x = (x(1), x(2), \ldots)$ с $x(i) \in X$, превращается в метрическое пространство, если положить $d(x, y) = 2^{-n}$, где n — минимальный индекс i, где $x(i)$ и $y(i)$ различаются. Это пространство является обобщением рассмотренного нами двоичного канторовского пространства; шары в нём являются цилиндрами: для данной конечной последовательности точек $z \in X^*$ мы берём все продолжения z.

Замечание 7.3. *Каждая точка x конструктивного метрического пространства $\mathbf{X}$ может рассматриваться как "массовая проблема" в смысле Медведева* [20]*: по данному рациональному $\varepsilon > 0$ указать номер точки из D, приближающей x с погрешностью не более ε. Легко проверить, что эта проблема эквивалентна (в смысле Медведева) проблеме перечисления всех базисных шаров, содержащих точку x.*

Замечание 7.4. *Конструктивное метрическое пространство является частным случаем более общего (и часто полезного) понятия конструктивного топологического пространства.*

Конструктивное топологическое пространство $\mathbf{X} = (X, \tau, \nu)$ *состоит из топологического пространства X, базиса открытых множеств τ и его нумерации ν: это значит, что $\tau = \{\nu(1), \nu(2), \ldots\}$ и что открытыми множествами в X являются объединения множеств из τ.*

Если Z является непустым подмножеством эффективного топологического пространства, то оно само становится эффективным топологическим пространством: мы пересекаем все базисные множества с Z, не меняя их нумерацию. В этом состоит важное преимущество понятия конструктивного топологического пространства (по сравнению с конструктивными метрическими пространствами): там мы можем перенести метрику на подмножество, но никакого естественного способа выделить в нём счётное плотное множество с нумерацией не видно.

В этой статье мы, однако, не будем стараться обобщить наши результаты на конструктивные топологические пространства (для чего нужно было бы сформулировать точно, какой класс конструктивных топологических пространств мы хотим рассматривать), а в качестве компромисса ограничимся подмножествами метрических пространств.

Определив структуру конструктивного топологического пространства, мы можем теперь определить некоторые эффективные варианты топологических понятий (для конструктивных метрических пространств):

Определение 7.5. *Открытое подмножество U конструктивного метрического пространства X называется* эффективно открытым*, если оно является объединением перечислимого семейства базисных шаров. Дополнение эффективно открытых множеств мы называем* эффективно замкнутыми.

Пусть A — некоторое подмножество X. Будем говорить, что множество $U \subseteq X$ открыто на A*, если найдётся эффективно открытое в X множество V, для которого $U \cap A = V \cap A$.*

Отметим, что в последнем определении U не обязано быть частью A, но реально играет роль лишь пересечение U с A.

Теперь можно определить вычислимость в терминах эффективно открытых множеств.

Определение 7.6 (вычислимые функции)**.** *Пусть $f\colon X \to Y$ — отображение метрических пространств, определённое на всём X. Функция f* непрерывна *тогда и только тогда, когда прообраз любого базисного открытого шара $B \subset Y$ является открытым подмножеством X; назовём функцию f* вычислимой*, если этот прообраз является эффективно открытым множеством (равномерно по B).*

Частичная функция f из X в Y, область определения которой содержит некоторое подмножество $A \subset X$, вычислима на A*, если прообраз любого базисного открытого шара B является эффективно открытым на A (равномерно по B). Из этого определения видно, что поведение функции вне A на вычислимость (на A) не влияет.*

Частным случаем вычислимости функций можно считать вычислимость точек: точку $x \in X$ будем называть вычислимой, если функция на одноэлементном пространстве $f\colon \{0\} \to X$ с $f(0) = x$ вычислима.

Если функция f, определённая в единственной точке $x_0 \in X$ и принимающая значение $y_0 \in Y$, вычислима на своей области определения, то мы говорим, что $y_0 = f(x_0)$ является x_0-вычислимым*. Если функция $f\colon Y \times Z \to Y$, определённая на $X \times \{z_0\}$, вычислима на своей области определения, мы называем функцию $g\colon X \to Y$, отображающую x в $g(x) = f(x, z_0)$,* z_0-вычислимой*, или* вычислимой относительно z_0.

Несложно проверить, что наше определение вычислимой точки эквивалентно более привычным:

Предложение 7.7. *Следующие свойства точки x конструктивного метрического пространства $\mathbf{X} = (X, d, D, \alpha)$ равносильны:*

(i) *x вычислима;*

(ii) *множество базисных шаров, содержащих x, перечислимо;*

(iii) *существует вычислимая последовательность $z_1, z_2, \ldots$ элементов D (заданных своими α-номерами), для которой $d(x, z_n) \leqslant 2^{-n}$ при всех n.*

Следующее предложение даёт более привычную переформулировку определения вычислимости:

Предложение 7.8. *Пусть $f\colon X \to Y$ — отображение метрических пространств. Функция f вычислима тогда и только тогда, когда существует вычислимое преобразование (задаваемое машиной с оракулом), которое переводит любую сильно фундаментальную последовательность точек из $D_{\mathbf{X}}$ с пределом x в сильно фундаментальную последовательность точек из $D_{\mathbf{Y}}$ с пределом $f(x)$.*

Если f — частичная функция с областью определения $Z \subset X$ и значениями в Y, то её вычислимость на Z равносильна существованию вычислимого преобразования, которое применимо к любой сильно фундаментальной последовательности с пределом $x \in Z$ и преобразует её в сильно фундаментальную последовательность с пределом $f(x)$.

Замечание 7.9. *В некотором смысле x_0-вычислимость аналогична вычислимости с оракулом (и в канторовском пространстве совпадает с ней), но в общем случае надо иметь в виду, что определение имеет более сложную природу: в этом определении машина имеет доступ к некоторой последовательности $s_1, s_2, \ldots$, сходящейся к x_0, но эта последовательность не фиксирована.*

Определение 7.10 (перечислимость снизу)**.** *Пусть дано конструктивное метрическое пространство $\mathbf{X} = (X, d, D, \alpha)$. Функция $f\colon X \to [-\infty, \infty]$* полунепрерывна снизу*, если множества $\{x \mid f(x) > r\}$ открыты при любом рациональном r (отсюда следует, что они открыты при любом r, не обязательно рациональном). Она называется* перечислимой снизу*, если эти множества эффективно открыты при любом рациональном r (равномерно по r). Частичная функция f из X в Y, определённая (по крайней мере) на некотором подмножестве A пространства X, называется* перечислимой снизу на A*, если множества $\{x \mid f(x) > r\}$ эффективно открыты на A равномерно по r.*

Аналогично определяется и перечислимость сверху; она равносильна перечислимости снизу функции $-f$.

Легко проверить, что функция $f\colon X \to \mathbb{R}$ вычислима тогда и только тогда, когда она перечислима сверху и снизу.

Как и раньше, можно дать эквивалентное определение перечислимости снизу с помощью базисных функций.

Определение 7.11 (базисные функции в конструктивном метрическом пространстве)**.** *Определим счётное множество* базисных *функций $\mathcal{E} = \{e_1, e_2, \ldots\}$ в конструктивном метрическом пространстве $\mathbf{X} = (X, d, D, \alpha)$ следующим образом. Для каждой точки $d \in D$ и для любых положительных рациональных чисел r и ε определим функцию $g_{d,r,\varepsilon}$: её значение в точке x определяется расстоянием от x до d и равно 1, если это расстояние не больше r, равно нулю, если расстояние не меньше $r + \varepsilon$, и линейно меняется, когда расстояние пробегает $[r, r + \varepsilon]$. См. рис.* 1.

Затем мы рассматриваем все функции, получаемые из семейства $g_{d,r,\varepsilon}$ замыканием относительно рациональных линейных комбинаций и операций максимума и минимума. Множество таких функций и обозначается $\mathcal{E}$; они имеют естественную нумерацию.

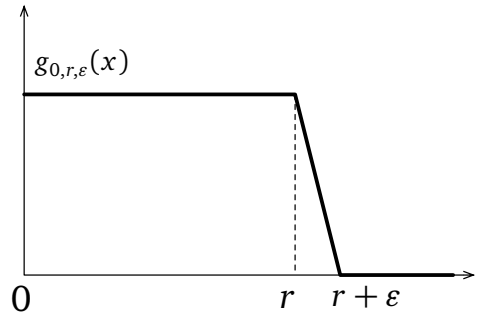

Figure 1: Функции, из которых строятся базисные.

Предложение 7.12. *Функция $f\colon X \to [0, +\infty]$, определённая на конструктивном метрическом пространстве, перечислима снизу тогда и только тогда, когда она является поточечным пределом неубывающей вычислимой последовательности базисных функций.*

Если в этом предложении отказаться от требования вычислимости, то вместо перечислимости снизу получится полунепрерывность снизу.

Определение 7.13. *Аналогичным образом определяется перечислимость снизу* относительно точки z_0 *некоторого метрического пространства* (*как перечислимость снизу на произведении области определения и* $\{z_0\}$).

Выбор метрики в конструктивном метрическом пространстве часто не влияет на понятие вычислимости. В частности, мы можем не различать эквивалентные метрики в смысле следующего определения (конструктивный вариант равномерной непрерывности тождественного отображения пространства в себя с другой метрикой):

Определение 7.14 (равномерная непрерывность, эквивалентность)**.** *Пусть* X *и* Y *— конструктивные метрические пространства, а* $f\colon X \to Y$ *— вычислимая функция. Мы говорим, что* f равномерно непрерывна*, если для любого рационального* $\varepsilon > 0$ *существует рациональное* $\delta > 0$*, для которого* $d_{\mathbf{X}}(x_1, x_2) \leqslant \delta$ *гарантирует* $d_{\mathbf{Y}}(f(x_1), f(x_2)) \leqslant \varepsilon$*. Мы говорим, что* f эффективно равномерно непрерывна*, если по* ε *можно эффективно найти соответствующее* δ*.*

Две метрики на одном и том же пространстве называются (эффективно) эквивалентными*, если тождественная функция, рассматриваемая как отображение пространства с одной метрикой в пространство с другой метрикой,* (*эффективно*) *равномерно непрерывна* (*в обе стороны*)*.*

Например, в $\mathbb{R}^2$ евклидова метрика и L_1-метрика эффективно эквивалентны.

Понятие эффективной компактности (определение 5.4) очевидно переносится на произвольные конструктивные метрические пространства. Есть эффективный аналог и у более слабого понятия локальной компактности.

Определение 7.15 (эффективная компактность и локальная компактность в метрических пространствах)**.** *Компактное подмножество* C *эффективного метрического пространства* X *называется* эффективно компактным*, если можно перечислять все конечные его покрытия базисными множествами пространства* X*.*

Подмножество C *метрического пространства называется* локально компактным*, если его можно покрыть шарами* B*, у которых пересечения* $\overline{B} \cap C$ *компактны.* (*Здесь* $\overline{B}$ *— замыкание шара* B*.*) *Подмножество* C *будем называть* эффективно локально компактным*, если существует вычислимая последовательность базовых шаров* B_k*, покрывающих* C*, для которых* $\overline{B}_k \cap C$ *эффективно компактны равномерно по* k*.*

Примеры 7.16.

1. Конечное дискретное пространство компактно, а бесконечное — локально компактно.

2. Отрезок $[0, 1]$ является эффективно компактным. Прямая $\mathbb{R}$ является эффективно локально компактным пространством.

3. Для конечного алфавита X пространство бесконечных последовательностей $X^{\mathbf{N}}$ является эффективно компактным. (Для бесконечного алфавита это пространство не будет локально компактным.)

4. Пусть $\alpha \in [0, 1]$ — перечислимое снизу действительное число, не являющееся вычислимым. (Такие числа существуют; например, число $\sum 2^{-KP(x)}$ является таковым.) Рассмотрим отрезок $[0, \alpha]$ как конструктивное метрическое пространство: перечислимость α снизу позволяет перенумеровать рациональные числа, меньшие α. Это конструктивное метрическое пространство будет компактным, но не эффективно компактным.

Следующее предложение даёт полезный критерий эффективной компактности в конструктивных метрических пространствах.

Предложение 7.17. (а) *Компактное подмножество C конструктивного метрического пространства X эффективно компактно тогда и только тогда, когда по любому рациональному $\varepsilon > 0$ можно эффективно указать конечное покрытие множества C базисными шарами радиуса ε.*

(б) *Пусть C — эффективно компактное подмножество конструктивного метрического пространства. Тогда из любого перечислимого семейства базисных шаров, покрывающих C, можно эффективно выбрать конечное покрытие.*

Доказательство. Пусть для каждого ε мы умеем указывать конечное покрытие S_ε множества C шарами радиуса ε. Вместе с таким покрытием будем перечислять и все покрытия *гарантированно* большими шарами (это значит, что для каждого шара $B(x, \varepsilon)$ из покрытия S_ε в этом новом покрытии найдётся шар $B(y, \sigma)$ с $\sigma > \varepsilon + d(x, y)$). Компактность C гарантирует, что при этом (если сделать это для всех ε) будут перечислены все покрытия C. (В самом деле, если есть какое-то покрытие S', которое в перечисление не попадёт, то для каждого ε есть один из шаров покрытия S_ε, которые не попадает гарантированно внутрь одного из шаров покрытия S'. Применив компактность и взяв предельную точку центров этих непопадающих шаров, получим противоречие.)

Остальные утверждения доказываются совсем просто.

Следующее предложение обобщает предложение 5.5 и доказывается аналогичным рассуждением.

Предложение 7.18. *Всякое эффективно замкнутое подмножество эффективно компактного множества эффективно компактно.*

(Вспоминая определения, это утверждение можно переформулировать так: пересечение эффективно компактного множества в пространстве X с эффективно замкнутым подмножеством пространства X является эффективно компактным.)

Как и раньше, верно и обратное: всякое эффективно компактное подмножество конструктивного метрического пространства эффективно замкнуто. В самом деле, мы можем рассмотреть всевозможные покрытия этого множества базисными шарами, а также шары, заведомо (по соотношению расстояния и радиусов) не пересекающиеся с множествами покрытия. Все такие шары вместе в объединении дадут дополнение нашего эффективно компактного множества.

Образ компактного пространства при непрерывном отображении компактен. Это утверждение имеет эффективный аналог (с аналогичным доказательством):

Предложение 7.19. *Пусть C — эффективно компактное подмножество конструктивного метрического пространства X, а f — вычислимое на C отображение C в другое конструктивное метрическое пространство. Тогда $f(C)$ эффективно компактно.*

Утверждение о том, что полунепрерывная снизу функция на компактном множестве достигает минимума, тоже имеет вычислимый аналог (мы приведём сразу параметрический вариант):

Предложение 7.20 (минимум с параметром)**.** *Пусть Y, Z — конструктивные метрические пространства, $f\colon Y \times Z \to [0, \infty]$ — перечислимая снизу функция, а C — эффективно компактное подмножество $Y \times Z$. Тогда функция*

$$g(y) = \inf_{\{z \mid (y,z) \in C\}} f(y, z)$$

(*где* $\inf$ *можно заменить на* $\min$ *в силу компактности, только надо считать, что минимум пустого множества равен* $+\infty$) *перечислима снизу.*

Вместо эффективной компактности C *достаточно предполагать, что проекция* $C_Y = \{y \mid \exists z\,(y,z) \in C\}$ *эффективно замкнута и покрыта вычислимой последовательностью шаров* B_k*, для которых* $(\overline{B}_k \times Z) \cap C$ *эффективно компактно равномерно по* k*.*

Последнее условие заведомо выполняется, если Y эффективно локально компактно, а Z эффективно компактно.

Доказательство. Для начала воспроизведём классическое доказательство полунепрерывности снизу. Нам надо проверить, что для любого r множество $\{y \mid r < g(y)\}$ открыто. Это множество можно представить в виде объединения, заметив, что условие $r < g(y)$ равносильно условию

$$(\exists r' > r)\,\forall z\left[(y,z) \in C \Rightarrow f(y,z) > r'\right],$$

и достаточно проверить, что множество

$$U = \left\{y \mid \forall z\left[(y,z) \in C \Rightarrow f(y,z) > r'\right]\right\}$$

открыто. Множество U можно представить в виде

$$U = (Y \setminus C_Y) \cup \bigcup_k (B_k \cap U).$$

Множество $Y \setminus C_Y$ открыто по условию, поэтому достаточно показать, что каждое из множеств $B_k \cap U$ открыто. Положим $F_k = \overline{B}_k \times Z$; по предположению, $F_k \cap C$ компактно. Условие $f(y,z) > r'$ в силу полунепрерывности задаёт некоторое открытое множество пар V, следовательно, $F_k \cap C \setminus V$ — замкнутое подмножество компактного множества и потому компактно. Поэтому его проекция

$$\{y \in \overline{B}_k \mid \exists z\,(y,z) \in F_k \cap C \setminus V\}$$

является непрерывным образом компактного множества и потому компактна (тем самым замкнута), а её дополнение в B_k (то есть $B_k \cap U$) открыто.

Теперь надо перевести это рассуждение на эффективный язык. Прежде всего заметим, что можно ограничиться рациональными r и r'. Затем надо заметить, что множество V эффективно открыто (равномерно по r'), а множества $F_k \cap C \setminus V$ равномерно эффективно замкнуты (и будучи подмножествами эффективно компактного множества, эффективно компактны). Поэтому их проекции (как образы) эффективно компактны и эффективно замкнуты, а дополнения эффективно открыты.

Следствием этого предложения является такая лемма:

Лемма 7.21. *Пусть* X, Z, Z' *— метрические пространства, причём* X *локально компактно, а* Z *компактно. Пусть* $f\colon Z \to Z'$ *— непрерывная функция, множество значений которой совпадает с* Z'*, а* $t\colon X \times Z \to [0, +\infty]$ *— полунепрерывная снизу функция. Тогда функция* $t_f\colon X \times Z' \to [0, +\infty]$*, определённая формулой*

$$t_f(x, z') = \inf_{\{z \mid f(z) = z'\}} t(x, z),$$

является полунепрерывной снизу.

Если X*,* Z*,* Z' *— конструктивные метрические пространства,* X *эффективно локально компактно,* Z *эффективно компактно, функция* f *вычислима, а функция* t *перечислима снизу, то функция* t_f *перечислима снизу.*

Доказательство. Приведём рассуждение сразу для эффективного варианта. Применим предыдущее предложение с $Y = X \times Z'$ и

$$C = X \times \{(f(z), z) \mid z \in Z\}.$$

Тогда

$$t_f(x, z') = \inf_{(x,z',z)\in C} t(x, z).$$

Множество Y эффективно локально компактно как произведение эффективно локально компактного и эффективно компактного множеств. Проекция C на Y совпадает со всем Y и потому замкнута. Поэтому можно применить предыдущее предложение.

7.2 Меры на конструктивном метрическом пространстве

В метрическом пространстве выделяются борелевские множества (минимальная σ-алгебра, содержащая открытые множества), и можно говорить о мерах на борелевских множествах. Они обладают следующим свойством *регулярности*:

Предложение 7.22 (регулярность)**.** *Пусть P — мера на полном сепарабельном метрическом пространстве. Тогда любое измеримое множество A можно приблизить большими открытыми множествами:*

$$P(A) = \inf_{G\supseteq A} P(G),$$

где G открыто.

На мерах можно ввести расстояние:

Определение 7.23 (расстояние Прохорова)**.** *Определим расстояние от точки x до множества A в метрическом пространстве как $d(x, A) = \inf_{y\in A} d(x, y)$. Определим ε-окрестность множества A как $A^\varepsilon = \{x \mid d(x, A) < \varepsilon\}$.*

Расстояние Прохорова $\rho(P, Q)$ *между двумя мерами P и Q определяется как точная нижняя грань тех $\varepsilon > 0$, для которых $P(A) \leqslant Q(A^\varepsilon) + \varepsilon$, а также $Q(A) \leqslant P(A^\varepsilon) + \varepsilon$, при всех борелевских A.*

Известно, что определённая таким образом функция расстояния действительно является метрикой; тем самым на множестве всех вероятностных мер в метрическом пространстве возникает структура метрического пространства. Есть и другие способы ввести расстояние на пространстве мер, дающие эквивалентные метрики (в том смысле, что тождественное отображение со сменой метрики равномерно непрерывно в обе стороны).

Определение 7.24 (пространство мер)**.** *Пусть $\mathbf{X}$ — конструктивное метрическое пространство. Введём в пространстве мер на нём структуру конструктивного метрического пространства $\mathbf{M} = \mathcal{M}(\mathbf{X})$. В качестве счётного всюду плотного множества $D_\mathbf{M}$ возьмём множество мер, сосредоточенных на некотором конечном подмножестве множества $D_\mathbf{X}$, и принимающих рациональные значения. Такие меры имеют естественное описание как конструктивные объекты, нужно указать номера элементов этого конечного подмножества и их меры. Таким образом мы получаем нумерацию $\alpha_\mathbf{M}$ точек в $D_\mathbf{M}$.*

Вычислимые точки этого конструктивного метрического пространства называют вычислимыми *мерами на $\mathbf{X}$.*

Определённое таким образом понятие вычислимости является обобщением введённого нами ранее понятия вычислимой меры на канторовском пространстве (а также естественного понятия вычислимой меры на бэровском пространстве последовательностей натуральных чисел).

Имеет место аналог предложения 4.17: интеграл $\int f(\omega, P)\, dP(\omega)$ базисной функции f по мере P является вычислимой функцией от P и f.

Вот ещё один родственный результат:

Предложение 7.25. *Пусть f — ограниченная эффективно равномерно непрерывная функция. Тогда её интеграл по мере P, рассматриваемый как функция от меры P, является эффективно равномерно непрерывной функцией.*

Доказательство. Без ограничения общности можно считать, что f неотрицательна (добавим константу). Пусть меры P и P' близки. Тогда $P'(A) \leqslant P(A_\varepsilon) + \varepsilon$, где A_ε обозначает ε-окрестность множества A. Тогда

$$\int f\, dP' \leqslant \int f_\varepsilon\, dP + \varepsilon,$$

где $f_\varepsilon(x)$ есть точная верхняя грань f на ε-окрестности точки x. (Интеграл неотрицательной функции g определяется мерами множеств $G_t = \{x \mid g(x) \geqslant t\}$, согласно теореме Фубини об изменении порядка интегрирования эту меру как функцию от t надо проинтегрировать по t. При этом если $f(x) \geqslant t$, то $f_\varepsilon(x) \geqslant t$ в ε-окрестности точки x.) Остаётся воспользоваться эффективной равномерной непрерывностью функции f, чтобы узнать, с какой точностью надо задавать меру, чтобы получить данную точность в интеграле.

С другой стороны, мера $P(B)$ базисного шара не обязана быть вычислимой, но она перечислима снизу (равномерно по B). Как показано в [12], это свойство (равномерная перечислимость снизу) также является критерием вычислимости меры P.

Известно, что для компактного сепарабельного метрического пространства X пространство мер на X с описанной метрикой также компактно. Это утверждение имеет конструктивный вариант, который доказывается стандартным образом:

Предложение 7.26. *Если конструктивное метрическое пространство $\mathbf{X}$ эффективно компактно, то и пространство $\mathcal{M}(X)$ вероятностных мер на X эффективно компактно.*

Для пространства Ω это упоминалось в предложении 5.5.

Примеры 7.27.

Бесконечное дискретное метрическое пространство ($\mathbb{N}$) не компактно, и множество мер на нём (которое можно отождествить с множеством функций $P\colon \mathbb{N} \to [0,1]$, для которых $\sum_i P(i) = 1$) тоже не компактно. С другой стороны, если перейти к полумерам, заменив условие на $\sum_i P(i) \leqslant 1$, то в естественной метрике получится компактное пространство. В самом деле, в отличие от равенства неравенства достаточно проверять для конечных сумм, и каждое неравенство задаёт замкнутое множество в компактном произведении $[0,1]^{\mathbb{N}}$, так что пересечение таких множеств тоже будет компактным. Легко понять, что оно будет и эффективно компактным.

Переход к полумере соответствует компактификации пространства $\mathbb{N}$: недостающая часть суммы ряда переносится на бесконечную точку.

7.3 Случайность в метрическом пространстве

В пространстве Ω мы определяли

- случайность относительно вычислимых мер (в смысле Мартин-Лёфа; см. определение 2.9 на языке тестов);
- равномерную случайность относительно произвольных мер (тест является функцией последовательности и меры, определение 5.2);
- случайность относительно эффективно компактного класса мер, определение 5.22;
- слепую (безоракульную) случайность, определение 5.37.

Все эти понятия с небольшими изменениями переносятся на произвольное конструктивное метрическое пространство. В этом разделе мы обсудим эти обобщения и их свойства, а затем более подробно рассмотрим случайность относительно ортогональных классов мер.

Для вычислимых мер тест определяется как перечислимая снизу функция на метрическом пространстве, интеграл от которой не превосходит 1. Среди таких тестов существует максимальный с точностью до константы. Как и раньше, это доказывается с помощью усечения: мы перечисляем все перечислимые снизу функции, принудительно превращая их в тесты или почти тесты, и затем складываем их с коэффициентами, образующими сходящийся ряд.

Это делается как и раньше, при этом мы рассматриваем перечислимые снизу функции как возрастающие пределы базисных. Важно, что интеграл от базисной функции по вычислимой мере вычислим. Более того, интеграл от базисной функции по произвольной мере вычислимо зависит от этой функции и от этой меры. Для базисных точек в пространстве мер это ясно, далее надо воспользоваться предложением 7.25.

Легко обобщить на случай конструктивных метрических пространств и понятие равномерного теста (см. определение 5.2 для случая канторовского пространства). Такой тест представляет собой перечислимую снизу функцию двух аргументов $t(x, P)$, где x — точка нашего метрического пространства, а P — мера на этом пространстве. Условие на интеграл, как и раньше, имеет вид $\int t(x, P)\, dP(x) \leqslant 1$.

Как и раньше, существует универсальный тест, и это можно доказать с помощью техники усечения:

Теорема 7.28 (усечение в метрических пространствах)**.** *Пусть $u(x, P)$ — перечислимая снизу функция, первый аргумент которой — точка конструктивного метрического пространства, а второй — мера на этом пространстве. Тогда существует равномерный тест $t(x, P)$, для которого $u(x, Q) \leqslant 2t(x, Q)$ при всех Q, для которых функция $u_Q\colon x \mapsto u(x, Q)$ является тестом по мере Q, то есть $\int u(x, Q)\, dQ(x) \leqslant 1$.*

Доказательство повторяет рассуждение из теоремы 5.7, при этом используется тот факт, что для базисной функции $b(x, P)$ на произведении пространств интеграл $\int b(x, P)\, dP(x)$ является вычислимой (непрерывной) функцией от P (что доказывается аналогично приведённому нами рассуждению про вычислимость интеграла).

Универсальный тест мы будем обозначать $\mathbf{t}(x, P)$. Вообще-то для каждого конструктивного метрического пространства он свой, но обычно понятно, какое пространство имеется в виду, так что в обозначение оно не входит.

Помимо существования универсального теста, из возможности усечения следует возможность "униформизации" в следующем смысле. Определим тест относительно меры P (не обязательно вычислимой) на конструктивном метрическом пространстве X:

Определение 7.29. *Пусть* $\mathbf{X} = (X, d, D, \alpha)$ *— конструктивное метрическое пространство, а* P *— мера на нём. Назовём* P-тестом случайности *функцию* $f\colon X \to [0, +\infty]$*, если она перечислима снизу относительно* P *и если* $\int f(x)\, dP(x) \leqslant 1$.

В этом определении фигурирует только мера P. Ясно, что из равномерного теста можно получить тест относительно P. Оказывается, что (с точностью до константы) так получаются все тесты относительно P:

Теорема 7.30 (униформизация)**.** *Пусть* P *— некоторая мера на конструктивном метрическом пространстве* X*, и дан некоторый* P*-тест* $t_P(x)$*. Тогда существует равномерный тест* $t'(\cdot, \cdot)$*, для которого* $t_P(x) \leqslant 2t'(x, P)$.

Доказательство. Из определения перечислимой снизу относительно P функции сразу же следует, что она является сужением некоторой перечислимой снизу функции двух аргументов. Остаётся применить предыдущую теорему к этому продолжению.

Многие результаты (например, теорема 5.36) обобщаются на произвольные метрические пространства. Вот ещё один пример такого обобщения (равномерный вариант так называемой "случайности по Курцу", Kurtz randomness):

Предложение 7.31. *Пусть* X *— конструктивное метрическое пространство, а* S *— эффективно открытое подмножество пространства* $X \times \mathcal{M}(X)$*. Если множество* $S_P = \{x \mid (x, P) \in S\}$ *имеет* P*-меру* 1 *для некоторой меры* $P \in \mathcal{M}(X)$*, то* S_P *содержит все равномерно* P*-случайные точки.*

Доказательство. Характеристическая функция $1_S(x, P)$ множества S, равная единице внутри множества и нулю снаружи, перечислима снизу и потому есть предел вычислимой возрастающей последовательности базовых функций $g_n(x, P)$ с $0 \leqslant g_n(x, P) \leqslant 1$. Последовательность функций $G_n\colon P \mapsto \int g_n(x, P)\, dP(x)$ представляет собой неубывающую последовательность непрерывных вычислимых (равномерно по n) функций. По теореме о монотонной сходимости значения $G_n(P)$ стремятся к единице для тех мер P, для которых $P(S_P) = 1$. Определим для каждой меры P числа $n_k(P)$ как минимальные значения n, для которых $G_n(P) > 1 - 2^{-k}$. Эти числа перечислимы сверху как функции от P (в естественном смысле; заметим, что для мер P, при которых $P(S_P) < 1$, некоторые из $n_k(P)$ бесконечны). Соответственно функции $1 - g_{n_k(P)}(x, P)$ как функции от x и P (такую функцию мы считаем нулём при бесконечном $n_k(P)$, независимо от x) перечислимы снизу, равномерно по k. Положим теперь $t(x, P) = \sum_{k>0}(1 - g_{n_k(P)}(x, P)$. Эта функция является равномерным тестом, поскольку при данном P её k-е слагаемое равно нулю, если $n_k(P)$ бесконечно, и имеет интеграл по мере P не больше 2^{-k} при конечном $n_k(P)$.

В условии теоремы говорится о мере P, для которой $P(S_P) = 1$. Тогда все $n_k(P)$ конечны, а $g_{n_k(P)}(x, P) = 0$ для любого x вне S_P. Поэтому все слагаемые в сумме, образующей тест, равны единице, и x не является равномерно P-случайной точкой. Следовательно, S_P включает в себя все равномерно P-случайные точки.

7.4 Априорная вероятность с оракулом

В разделе 5.2 мы определили априорную вероятность с условием, роль которого играла мера на Ω. Теперь, введя понятие конструктивного метрического пространства, мы можем заметить, что это определение естественно обобщается на любое пространство $\mathbf{X}$: мы рассматриваем неотрицательные перечислимые снизу функции $m\colon \mathbb{N} \times X \to [0, +\infty]$, для которых $\sum_i m(i, x) \leqslant 1$ при любом $x \in X$.

Среди таких функций существует максимальная с точностью до константы. Это доказывается методом усечения: мы не будем повторять рассуждение подробно, отметим лишь, что перечислимую снизу функцию $m(i,x)$ можно получить как сумму ряда из базисных функций, каждая из которых отлична от нуля только для одного i.

Максимальную из таких функций будем называть *априорной вероятностью с условием x* и обозначать $\mathbf{m}(i|x)$.

Мы считали первый аргумент натуральным числом, но это не существенно: можно рассматривать слова (или любые другие дискретные конструктивные объекты). Частным случаем этого определения является определение априорной вероятности относительно меры (раздел 5.2), а также стандартные понятия априорной вероятности с оракулом (что соответствует $\mathbf{X} = \Omega$) и условной априорной вероятности (что соответствует $\mathbf{X} = \mathbb{N}$).

По аналогии с теоремой Дея–Миллера, можно выразить априорную вероятность с условием в произвольном эффективно компактном метрическом пространстве $\mathbf{X}$ через априорную вероятность с оракулом.

Предложение 7.32. *Пусть $F\colon \Omega \to X$ — вычислимое отображение, образом которого является всё пространство X. Тогда*

$$\mathbf{m}(i|x) \mathrel{\dot=} \min_{\{\pi|F(\pi)=x\}} \mathbf{m}(i|\pi).$$

Доказательство. Рассуждаем как в доказательстве теоремы 5.36. Функция $(i,\pi) \mapsto \mathbf{m}(i|F(\pi))$ является перечислимой снизу на $\mathbb{N}\times\Omega$, откуда получается $\dot<$-неравенство.

Чтобы получить обратное неравенство, мы пользуемся 7.21 и замечаем, что функция в правой части корректно определена (минимум достигается) и перечислима снизу.

Заметим, что априорная вероятность (с оракулом) в правой части предложения 7.32 может быть выражена через префиксную сложность (с оракулом). Для случая условий в метрических пространствах не ясно, как определять префиксную сложность с таким условием (можно говорить о функциях с перечислимым относительно точки x графиком, но неясно, как строить универсальную). Можно формально определить $KP(i|x)$ как $\max_{\{\pi|F(\pi)=x\}} KP(i|\pi)$, тогда $KP(i|x) \stackrel{+}{=} -\log \mathbf{m}(i|x)$, но вряд ли это можно считать удовлетворительным определением префиксной сложности (скажем, обычные рассуждения, где используется самоограниченность программы, при таком определении уже не применимы, хотя многие результаты остаются верными; например, формулу $KP(i,j|x) \stackrel{+}{<} KP(i|x) + KP(j|x)$ можно доказать, не приписывая друг к другу самоограниченные программы, а рассуждая с вероятностями) — честнее просто говорить о логарифме априорной вероятности.

Замечание 7.33. *Аналогичным образом можно добавлять точки конструктивных метрических пространств в качестве условий и в другие наши определения. Например, можно рассматривать равномерные тесты на Ω с условиями в произвольном конструктивном метрическом пространстве X: это будут перечислимые снизу функции $t(\omega, P, x)$, для которых $\int t(\omega,P,x)\,dP(\omega) \leqslant 1$ при всех x. Можно также фиксировать вычислимую меру P, например, равномерную, и определить тесты относительно этой меры с условиями в X.*

8 Классы ортогональных мер

Как и в случае пространства Ω, для мер в произвольном метрическом пространстве можно определить понятие эффективно компактного класса и универсального теста случайности

относительно этого класса. Сохраняется (с тем же доказательством) и формула для универсального теста относительно класса (теорема 5.23).

Класс бернуллиевых мер (как и многие другие часто используемые классы) обладает важным свойством: случайная по одной из мер этого класса последовательность однозначно определяет меру, по которой она случайна. Именно это обстоятельство по существу было использовано в теореме 5.41. В этом разделе мы рассмотрим тот же вопрос в более общей ситуации, когда речь идёт о мерах на конструктивном метрическом пространстве $\mathbf{X} = (X, d, D, \alpha)$.

Это обобщение включает в себя естественные примеры: конечные и бесконечные марковские цепи, стационарные эргодические процессы (см. ниже).

Сначала приведём определение ортогональности мер (которое можно считать классическим аналогом эффективной ортогональности (определение 5.40).

Определение 8.1. *Пусть P, Q — две меры на $(X, \mathcal{A})$, где X — некоторое пространство, а $\mathcal{A}$ — некоторая σ-алгебра подмножеств X. Говорят, что меры P и Q* ортогональны, *если пространство можно разбить на два непересекающихся множества U и V из $\mathcal{A}$, для которых $P(V) = Q(U) = 0$.*

Говорят, что класс $\mathcal{C}$ является ортогональным, *если существует измеримая функция $\varphi\colon X \to \mathcal{C}$, для которой $P(\varphi^{-1}(P)) = 1$ для любой меры $P \in \mathcal{C}$.*

Когда мы говорим об измеримости функции φ, имеется в виду, что в метрическом пространстве $\mathcal{M}(X)$ определены борелевские множества.

Примеры 8.2.

1. В ортогональном классе мер любые две (различные) меры P и Q ортогональны. В самом деле, множества $\{P\}$ и $\{Q\}$ борелевские (замкнутые), и потому их прообразы измеримы (и, очевидно, не пересекаются). Обратное утверждение неверно: класс $\mathcal{C}$ попарно ортогональных мер не обязан быть ортогональным, даже если он эффективно компактен. Пусть λ — равномерная мера на отрезке $[0, 1]$. Для каждой точки $x \in [0, 1]$ рассмотрим меру δ_x, сосредоточенную в точке x. Тогда класс $\{\lambda\} \cup \{\delta_x \mid x \in [0, 1]\}$ эффективно компактен, и его элементы попарно ортогональны. Однако он не является ортогональным классом: условие ортогональности требует, чтобы мера δ_x была значением φ на x, а тогда $\varphi^{-1}(\lambda)$ будет пустым.

2. Пусть P и Q — две меры. Если $\mathrm{Randoms}(P)$ и $\mathrm{Randoms}(Q)$ не пересекаются, то эти меры ортогональны (в качестве U и V можно взять, скажем, случайные и неслучайные по мере P последовательности). Обратное, вообще говоря, неверно: меры λ и δ_x ортогональны, но множества случайных последовательностей пересекаются, если x взять случайным по мере λ.

В качестве примера рассмотрим стационарные эргодические процессы.

Определение 8.3. *Рассмотрим на пространстве Ω бесконечных двоичных последовательностей преобразование левого сдвига:*

$$T\colon \omega(1)\omega(2)\ldots \mapsto \omega(2)\omega(3)\ldots.$$

Распределение вероятностей P на Ω назовём стационарным, *если*

$$P(T^{-1}(A)) = P(A)$$

для любого борелевского множества A. Легко проверить, что это эквивалентно требованию

$$P(x) = P(0x) + P(1x)$$

для всех слов x.

Борелевское множество $A \subset \Omega$ назовём инвариантным *относительно сдвига, если $T(A) \subset A$. Например, множество последовательностей, в которых частота единиц стремится к $1/2$, является инвариантным. Стационарное распределение называется* эргодическим, *если любое инвариантное борелевское множество имеет меру 0 или 1.*

Вот пример стационарного процесса.

Пример 8.4. *Пусть $Z_1, Z_2, \ldots$ — последовательность независимых одинаково распределённых случайных величин, принимающих значения 0 и 1 с вероятностями соответственно 0.9 и 0.1. Определим $X_0, X_1, X_2, \ldots$ так: X_0 принимает значения $0, 1, 2$ с равными вероятностями и независима от всех Z_i, $X_n = X_0 + \sum_{i=1^n} Z_n \bmod 3$. Наконец, пусть $Y_n = 0$ при $X_n = 0$ и $Y_n = 1$ при $X_n \neq 0$. Легко видеть, что процесс $Y_0, Y_1, \ldots$ является стационарными; можно доказать, что он эргодический. Поскольку он является функцией марковской цепи X_n, его называют* скрытой марковской цепью (*hidden Markov chain*).

Следующее утверждение является следствием эргодической теоремы Биркгофа о поточечной сходимости. Через g_x будем обозначать индикатор события $x \sqsubseteq \omega$, то есть $g_x(\omega)$ равно 1 при $x \sqsubseteq \omega$ и 0 в противном случае.

Предложение 8.5. *Пусть P — стационарное распределение вероятностей на пространстве Ω.*

(а) *Для почти всех по мере P последовательностей ω последовательность*

$$A_{x,n}(\omega) = \tfrac{1}{n}(g_x(\omega) + g_x(T\omega) + \ldots + g_x(T^{n-1}\omega))$$

сходится.

(б) *Для эргодического процесса этот предел равен $P(x)$.*

(Для неэргодических процессов предел может зависеть от ω.)

Общая теорема Биркгофа касается произвольных пространств и сохраняющих меру преобразований, а в качестве g_x можно взять произвольную интегрируемую функцию, и гарантировать поточечную сходимость (в эргодическом случае — к математическому ожиданию).

Утверждение (б) показывает, что класс $\mathcal{C}$ эргодических мер является ортогональным. В самом деле, будем называть последовательность ω "стабильной", если для неё существуют пределы из п. (а) при любом x. Легко понять, что в этом случае эти пределы задают некоторую меру Q_ω. Определим функцию $\varphi\colon \Omega \to \mathcal{C}$, положив $\varphi(\omega) = Q_\omega$, если мера Q_ω является эргодической, и выбрав в качестве значения произвольную эргодическую меру, если Q_ω не является эргодической или ω не является стабильной. Пункт (б) гарантирует, что $P(\varphi^{-1}(P)) = 1$ для любой эргодической меры P.

Тут используется, что множество стабильных последовательностей борелевское. Заметим, что класс эргодических мер незамкнут, но это в определении не предполагается.

Мы видели (пример 8.2.2), что две меры могут быть ортогональны, но иметь общие случайные последовательности. Однако для вычислимых мер, как мы сейчас докажем, это невозможно.

Будем говорить, что две меры эффективно ортогональны, если классы равномерно случайных относительно них последовательностей не пересекаются. (Это позволяет переформулировать определение 5.40 так: класс мер эффективно ортогонален, если любые две меры в этом классе эффективно ортогональны.)

Теорема 8.6. *Две вычислимые меры на конструктивном метрическом пространстве ортогональны тогда и только тогда, когда они эффективно ортогональны.*

Доказательство. Как мы уже говорили, в одну сторону это верно для любых мер. Докажем обратное утверждение. Пусть даны две вычислимые ортогональные меры P, Q; по определению ортогональности существует измеримое множество A, для которого $P(A) = 1$, $Q(A) = 0$. В силу регулярности (предложение 7.22) найдётся последовательность открытых множеств G_n, содержащих A, для которых $Q(G_n) < 2^{-n}$. Поскольку G_n содержит A, то $P(G_n) = 1$. Множество G_n открыто, поэтому найдётся конечное объединение $H_n \subset G_n$ базисных шаров, для которого $P(H_n) > 1-2^{-n}$; для H_n мера Q тоже меньше 2^{-n}. Перебором можно найти вычислимую последовательность множеств H_n с такими свойствами (P-мера большая, Q-мера маленькая).

Рассмотрим теперь $\limsup H_n$, то есть множество $\bigcap_m U_m$, где $U_m = \bigcup_{n>m} H_n$. Согласно предложению 7.31, каждое из множеств U_m, а значит, и их пересечение, содержит все P-случайные точки. С другой стороны, множества U_n образуют тест в смысле Мартин-Лёфа относительно меры Q, поэтому это пересечение не содержит ни одной Q-случайной точки.

Мы видели, что эргодические меры образуют ортогональный класс. Более детальный анализ показывает, что они эффективно ортогональны.

Теорема 8.7. *Эргодические меры на канторовском пространстве образуют эффективно ортогональный класс.*

Доказательство. В статье [28] приведено доказательство эффективной эргодической теоремы, из которого следует, что

(а) Равномерно случайные последовательности по стационарной мере стабильны (в том смысле, что для них существует указанный выше предел частот);

(б) Для равномерно случайных по эргодической мере последовательностей этот предел совпадает с мерой $P(x)$.

Опишем коротко схему доказательства. Для любых рациональных чисел $0 < \alpha < \beta$ рассмотрим перечислимую снизу функцию $\omega \mapsto \sigma(\omega, \alpha, \beta)$, которая считает, сколько раз величина $A_{x,n}(\omega)$ с ростом n пересекла промежуток (α, β) слева направо (была меньше α и стала больше β). Затем можно доказать, что $(1 + \alpha^{-1})(\beta - \alpha) \int \sigma(\omega, \alpha, \beta)\, dP(\omega) \leqslant 1$, то есть функция $(1 + \alpha^{-1})(\beta - \alpha)\sigma(\alpha, \beta)$ является ограниченным в среднем тестом. Следовательно, для равномерно случайных (и даже для безоракульно случайных) последовательностей число таких пересечений интервала конечно.

Чтобы доказать (б), если (а) уже гарантировано, достаточно для каждого x установить, что

$$\liminf_n A_{x,n}(\omega) \leqslant P(x) \leqslant \limsup_n A_{x,n}(\omega)$$

для всех случайных ω. Рассмотрим, например, первое неравенство (второе аналогично). Достаточно показать для любых k и m, что

$$\inf_{n \geqslant m} A_{x,n}(\omega) \leqslant P(x) + 2^{-k}$$

для случайной ω. Множество

$$S_{x,k,m} = \{(\omega, P) \mid (\exists n \geqslant m) A_{x,i}(\omega) < P(x) + 2^{-k}\}$$

является эффективно открытым, и по теореме Биркгофа множество $S_{x,k,m}(P) = \{x \mid (x, P) \in S_{x,k,m}\}$ имеет P-меру 1, если мера P эргодическая. Предложение 7.31 гарантирует, что множество $S_{x,k,m}(P)$ содержит все равномерно P-случайные точки.

Другой подход к доказательству состоит в том, чтобы установить сходимость частот к $P(x)$ для случайных по Мартин-Лёфу последовательностей относительно вычислимых эргодических мер (при этом доказательство должно выдерживать релятивизацию), не используя явного теста, как это сделано в [2]. После этого можно сослаться на теорему 5.36 и получить сходимость для равномерно случайных последовательностей.

Для работы с ортогональными классами мер полезно понятие сепаратора. В этом определении, говоря об измеримости функций, мы имеем в виду их измеримость по Борелю (прообраз борелевского множества является борелевским); меры мы тоже считаем определёнными на борелевских множествах.

Определение 8.8 (функция-сепаратор)**.** *Пусть $\mathcal{C}$ — класс мер на конструктивном метрическом пространстве $\mathbf{X}$. Измеримую функцию*

$$s\colon X \times \mathcal{M}(\mathbf{X}) \to [0, +\infty]$$

назовём сепаратором *для класса $\mathcal{C}$, если $\int s(x,P)\,dP(x) \leqslant 1$ для любой меры P, а для любых двух различных мер $P, Q \in \mathcal{C}$ и для любой точки x хотя бы одно из значений $s(x,P)$ и $s(x,Q)$ бесконечно.*

Сепаратор называется тестом-сепаратором*, если он перечислим снизу как функция x и P.*

В определении сепаратора мы требуем $\int s(x,P)\,dP(x) \leqslant 1$ для всех мер (а не только для мер из класса P), но это не очень существенно, поскольку к тест-сепаратору можно применить усечение.

Следующая теорема связывает понятие ортогонального класса мер с сепараторами, а также устанавливает, что для случая эффективно ортогонального класса каждая мера может быть восстановлена по случайной (по этой мере) последовательности.

Теорема 8.9. *Пусть $\mathcal{C}$ — класс мер на конструктивном метрическом пространстве.*

(а) *Если борелевский класс мер $\mathcal{C}$ ортогонален, то для него существует сепаратор.*

(б) *Класс $\mathcal{C}$ является эффективно ортогональным тогда и только тогда, когда существует тест-сепаратор.*

(Что касается обратного к (а) утверждения, то авторы не знают, верно ли оно.)

Доказательство. Докажем сначала (а). Пусть $\varphi(x)$ — функция, которая для каждого $x \in X$ указывает меру в соответствии с определением ортогональности. По предположению эта функция борелевская, поэтому (см. [14]) её график является борелевским множеством. Положим $s(x,P) = 1$ при $P \notin \mathcal{C}$, а также при $P \in \mathcal{C}$ и $\varphi(x) = P$, и положим $s(x,P) = \infty$ при $P \in \mathcal{C}$ и $\varphi(x) \neq P$.

Докажем теперь утверждение (б). Если класс $\mathcal{C}$ эффективно ортогонален, то универсальный равномерный тест и будет тест-сепаратором для класса $\mathcal{C}$. С другой стороны, пусть имеется тест-сепаратор для класса $\mathcal{C}$. Пусть P и Q — две различные меры для класса $\mathcal{C}$, и точка x равномерно случайна по обеим мерам. Поскольку s является равномерным тестом случайности, то $s(x,P)$ и $s(x,Q)$ конечны, что противоречит определению теста-сепаратора.

Следующий результат менее ожидаем; он показывает, что для случая эффективно компактного класса мер из существования полунепрерывного снизу сепаратора следует существование и перечислимого снизу сепаратора (то есть теста-сепаратора).

Теорема 8.10. *Пусть для эффективно компактного класса мер существует полунепрерывный снизу сепаратор $s(x,P)$. Тогда этот класс эффективно ортогонален.*

Доказательство. Пусть $\mathcal{C}$ — эффективно компактный класс мер на конструктивном метрическом пространстве. Мы должны показать, что в предположениях теоремы для любых двух различных мер $P_1, P_2 \in \mathcal{C}$ множества случайных последовательностей не пересекаются:

$$\mathrm{Randoms}(P_1) \cap \mathrm{Randoms}(P_2) = \varnothing.$$

Возьмём в пространстве мер два непересекающихся базисных замкнутых шара B_1 и B_2, содержащих меры P_1 и P_2, и рассмотрим классы мер $\mathcal{C}_1 = \mathcal{C} \cap B_1$ и $\mathcal{C}_2 = \mathcal{C} \cap B_2$. Это непересекающиеся эффективно компактные классы мер, содержащие P_1 и P_2. Рассмотрим теперь функции

$$t_i(x) = \inf_{P \in \mathcal{C}_i} s(x, P).$$

Для любого x хотя бы одно из значений $t_1(x)$ и $t_2(x)$ бесконечно. Функции t_1 и t_2 полунепрерывны снизу (первая часть доказательства предложения 7.20) и являются $\mathcal{C}_1$- и $\mathcal{C}_2$-тестами.

Теперь мы можем применить рассуждение, аналогичное доказательству предложения 7.31. Пусть $k > 1$ — целое число. Рассмотрим открытое множество $S_k = \{x \mid t_1(x) > 2^k\}$. Поскольку t_1 является $\mathcal{C}_1$-тестом, то $P(S_k) < 2^{-k}$ для всех $P \in \mathcal{C}_1$. С другой стороны, поскольку для каждого x одно из значений $t_1(x)$ и $t_2(x)$ бесконечно, то $P(S_k) = 1$ для всех $P \in \mathcal{C}_2$. Характеристическая функция 1_{S_k} множества S_k полунепрерывна снизу, и потому может быть представлена как поточечный предел неубывающей последовательности (не обязательно вычислимой!) базисных функций $g_{k,n}$. Рассуждая как в предложении 7.31, мы заключаем, что найдётся $n = n_k(P)$, при котором $\int g_{k,n}\, dP > 1 - 2^{-k}$ для любого $P \in \mathcal{C}_2$. Эффективная компактность класса $\mathcal{C}_2$ позволяет выбрать n общим для всех $P \in \mathcal{C}_2$.

Зафиксируем достигнутое: для всякого k найдётся базисная функция h_k, для которой

$$\int h_k\, dP < 2^{-k} \text{ при всех } P \in \mathcal{C}_1;$$
$$\int h_k\, dP > 1 - 2^{-k} \text{ при всех } P \in \mathcal{C}_2.$$

Такую функцию можно найти эффективно по k перебором.

Теперь можно построить перечислимую снизу функцию

$$t'_1(x) = \sum_k h_k(x).$$

Она является тестом для класса $\mathcal{C}_1$. Функция $t'_2(x) = \sum_k (1 - h_k(x))$ по аналогичным причинам будет тестом для класса $\mathcal{C}_2$. Эти тесты должны быть конечны для случайных по мерам P_1 и P_2 последовательностей, а одновременно для обоих тестов это быть не может.

Смысл введённого нами понятия теста-сепаратора можно пояснить следующим образом. Универсальный тест $\mathbf{t}(\omega, P)$ в силу эффективной ортогональности позволяет разделить последовательности, случайные по разным мерам из класса $\mathcal{C}$: глядя на последовательность ω, равномерно случайную по одной из мер этого класса (=случайную относительно класса $\mathcal{C}$), мы ищем $P \in \mathcal{C}$, для которого $\mathbf{t}(\omega, P)$ конечно. Такая мера P в классе $\mathcal{C}$ единственна (согласно определению эффективной ортогональности).

Последнее, однако, может выполняться и для неуниверсального теста, и такие тесты мы назвали тестами-сепараторами. Неуниверсальный тест менее требователен к идее случайности, и описывает её, так сказать, в первом приближении: может оказаться, что та последовательность, которую он считает случайной (на которой значение $t(\omega, P)$ конечно), более серьёзный

тест уже отбракует. (Обратное невозможно, так как универсальный тест максимален.) Важно только, чтобы уже эта предварительная грубая отбраковка позволяла разделить меры из класса $\mathcal{C}$, то есть чтобы ни одна последовательность не казалась "в первом приближении случайной" сразу по двум мерам.

Определение 8.11. *Для данного тест-сепаратора $s(x, P)$ будем называть элемент x* случайным в первом приближении относительно P*, если значение этого тест-сепаратора конечно: $s(x, P) < \infty$.*

В качестве примера рассмотрим класс бернуллиевых мер. В качестве такого "теста в первом приближении" можно вспомнить слова фон Мизеса, который самым первым свойством случайной последовательности (*коллектива*, как он говорил) называл устойчивость частот. Свойство устойчивости частот (усиленный закон больших чисел в современной терминологии) состоит в том, что $S_n(\omega)/n \to p$. Здесь $S_n(\omega)$ — количество единиц в начальном отрезке последовательности ω длины n, а p — параметр бернуллиевой меры B_p.

Можно пытаться использовать это свойство для построения сепаратора разными способами, вот несколько возможных требований:

(1) $S_n(\omega)/n \to p$ с некоторой фиксированной скоростью сходимости.

(2) $S_n(\omega)/n \to p$ без указания конкретной скорости сходимости.

(3) Можно вспомнить доказательство теоремы 8.7 для класса всех эргодических стационарных мер на Ω, и получить тест, гарантирующий сходимость всех частот $A_{x,n}(\omega)$ к соответствующим вероятностям $P(x)$.

Наиболее простое и естественное (с математической точки зрения) требование (2) не записывается в виде перечислимого снизу теста, но чтобы поправить дело, можно перейти к (1) и фиксировать скорость сходимости. Вот один из возможных вариантов. (Для простоты мы будем использовать только неравенство Чебышёва, и получим сходимость частот не на всех отрезках, а только по степеням двойки. Более аккуратная оценка позволила бы получить сходимость частот по всем начальным отрезкам.)

Неравенство Чебышёва гарантирует, что

$$B_p(\{x \in \mathbb{B}^n \colon |S_n(x) - np| > \lambda n^{1/2}(p(1-p))^{1/2}\}) \leqslant \lambda^{-2}.$$

Здесь $S_n(x)$ — частота единиц в слове длины n. Поскольку $p(1-p) \leqslant 1/4$, отсюда следует, что

$$B_p(\{x \in \mathbb{B}^n \colon |S_n(x) - np| > \lambda n^{1/2}/2\}) \leqslant \lambda^{-2}.$$

Положив, скажем, $\lambda = n^{0.1}$ (и опуская множитель $1/2$, что лишь ослабляет утверждение), получаем

$$B_p(\{x \in \mathbb{B}^n \colon |S_n(x) - np| > n^{0.6}\}) \leqslant n^{-0.2}.$$

Чтобы ряд сходился, ограничимся лишь членами вида $n = 2^k$:

$$B_p(\{x \in \mathbb{B}^{2^k} \colon |S_{2^k}(x) - 2^k p| > 2^{0.6k}\}) \leqslant 2^{-0.2k}.$$

Теперь для бесконечной последовательности ω и для $p \in [0, 1]$ положим

$$g(\omega, B_p) = \sup\{k \colon |S_{2^k}(\omega) - 2^k p| > 2^{0.6k}\}.$$

При этом

$$\int g(\omega, B_p)\, dB_p(\omega) \leqslant \sum_k k \cdot 2^{-0.2k} = c < \infty$$

и поделив на c, получаем тест. Это тест-сепаратор, так как $g(\omega, B_p) < \infty$ влечёт сходимость последовательности $2^{-k}S_{2^k}(\omega)$ к p и для двух разных p такого случиться не может.

Теорема 5.41 обобщается на случай произвольного метрического пространства (доказательство остаётся практически тем же, надо использовать базисные шары вместо начальных отрезков): для всякого эффективно компактного эффективно ортогонального класса мер и всякой меры в этом классе слепая (безоракульная) случайность равносильна равномерной случайности. В связи с этим естественно спросить, нельзя ли произвольную эргодическую меру поместить в некоторый эффективно компактный класс. Оказывается, что нет.

Теорема 8.12. *Рассмотрим стационарные (инвариантные относительно сдвига) меры на пространстве Ω. Среди них существует эргодическая мера, не содержащаяся ни в каком эффективно компактном классе стационарных эргодических мер.*

Прежде чем доказывать эту теорему, приведём некоторые вспомогательные утверждения.

Предложение 8.13. *Как эргодические, так и неэргодические меры плотны в классе стационарных мер.*

Доказательство. Для начала покажем, что всякую стационарную меру можно приблизить эргодической. Без ограничения общности можно считать, что вероятность $P(x)$ появления любого слова x по этой мере строго положительна. (Если нет, можно подмешать немного равномерной меры.) Фиксируем какое-либо n и рассмотрим значения меры $P(x)$ на строках длины не более n. Существует марковский процесс с таким же распределением вероятностей, в котором вероятность следующего бита определяется $n-1$ предыдущими битами: для любого $x \in \mathbb{B}^{n-2}$ и любых битов b, b' вероятность перехода от bx к xb' равна $P(bxb')/P(bx)$. В этом процессе все вероятности перехода положительны, и поэтому он является эргодическим. С ростом n он стремится к исходной стационарной мере.

С другой стороны, всякую стационарную меру P можно приблизить и неэргодической мерой. Очевидно, достаточно рассмотреть случай, когда сама мера P эргодическая. Тогда, согласно эргодической теореме, можно найти последовательность, в которой предельные частоты всех подслов соответствуют мере. (Почти все — в смысле этой меры — последовательности таковы.) Взяв длинный кусок этой последовательности и зациклив его, можно найти периодическую последовательность, в которой частоты слов длины не больше n отличаются от меры P не более чем на ε (для любых данных n и $\varepsilon > 0$). (При зацикливании образуются новые слова на месте склейки, но при большой длине это не играет роли.) Теперь можно рассмотреть меру, соответствующую случайным сдвигам этой последовательности (она сосредоточена на конечном множестве последовательностей — их столько, каков минимальный период). Эта мера не эргодична, но близка к P.

Нам понадобится ещё одно утверждение:

Предложение 8.14. *Множество эргодических мер образует G_δ-подмножество в метрическом пространстве всех мер на Ω.*

Доказательство. Мы можем ограничиться (замкнутым) множеством стационарных мер. Рассмотрим функцию $A_{x,n}$ на Ω, положив $A_{x,n}(\omega)$ равным доле вхождений слова x среди первых n возможных позиций (мы прикладываем x к ω, начиная с первой, второй,..., n-ой позиции и смотрим долю совпадений). Эргодическая теорема гарантирует, что при каждом x последовательность функций $A_{x,1}, A_{x,2}, \ldots$ сходится в смысле L_1 (на самом деле имеет место даже и сходимость почти всюду). При этом стационарная мера P будет эргодической тогда и только тогда, когда пределом этой последовательности будет константа $P(x)$.

В силу существования предела для стационарных мер достаточно проверять, что константа $P(x)$ является предельной точкой. Для любых x, N и ε множество $S_{x,N,\varepsilon}$ тех P, для которых существует $n \geqslant N$ с

$$\int |A_{x,n}(\omega) - P(x)|\, dP(\omega) < \varepsilon,$$

является открытым, а пересечение этих множеств по всем x, N, ε и даёт указанный выше критерий эргодичности стационарной меры.

Теперь мы можем доказать теорему 8.12.

Доказательство. Объединение всех эффективно компактных классов эргодических мер является F_σ-множеством. Предположим, что оно включает в себя все эргодические меры. Тогда множество неэргодических мер является G_δ-множеством, которое плотно в силу предложения 8.13. С другой стороны, как мы видели в предложениях 8.14 и 8.13, множество неэргодических мер также является плотным G_δ-множеством. Но пересечение этих двух множеств пусто, что противоречит теореме Бэра о категории. Теорема 8.12 доказана.

Тем не менее вопрос, с которого мы начали, остаётся открытым:

Вопрос. Существует ли эргодическая мера, для которой понятия равномерной и слепой (безразличной) случайности не совпадают?

Возвращаясь к произвольным эффективно компактным эффективно ортогональным классам, мы можем связать универсальные тесты с тестами для класса (см. теорему 5.23) и тестами-сепараторами.

Теорема 8.15. *Пусть $\mathcal{C}$ — эффективно компактный класс эффективно ортогональных мер. Пусть $\mathbf{t}_\mathcal{C}(x)$ — универсальный тест случайности для этого класса, а $s(x,P)$ — некоторый тест-сепаратор для $\mathcal{C}$. Тогда универсальный равномерный тест $\mathbf{t}(x,P)$ для мер этого класса можно выразить так:*

$$\mathbf{t}(x,P) \doteq \max(\mathbf{t}_\mathcal{C}(x), s(x,P))$$

для всех $P \in \mathcal{C}$ и для всех x.

Доказательство. Заметим прежде всего, что $t_\mathcal{C}(x)$ и $s(x,P)$ не превосходят универсального равномерного теста $\mathbf{t}(x,P)$ (что следует из его универсальности).

С другой стороны, покажем, что если $\mathbf{t}_\mathcal{C}(x)$ и $s(x,P)$ конечны, то $\mathbf{t}(x,P)$ не превосходит наибольшего из них (с точностью до константы). Конечность первого теста гарантирует, что $\min_{Q\in\mathcal{C}} \mathbf{t}(x,Q)$ конечен: этот минимум равен $\mathbf{t}_\mathcal{C}(x)$ с точностью до константы. Если этот минимум достигался бы на какой-то мере $Q \neq P$, то оба значения $s(x,Q)$ и $s(x,P)$ были бы конечны, что противоречит определению сепаратора. (Заметим, что мы доказали чуть более сильное утверждение, чем обещали: вместо "наибольшего из них" можно написать "первого из них, если второй конечен".)

Утверждение этой теоремы позволяет разбить проверку случайности по некоторой мере P из класса $\mathcal{C}$ на две части (указывает две возможные причины неслучайности). Во-первых, мы должны убедиться, что x случайно относительно класса $\mathcal{C}$. Например, в случае меры B_p из класса $\mathcal{B}$ бернуллиевых мер мы вначале должны убедиться, что $\mathbf{t}_\mathcal{B}(\omega)$ конечно. После этого мы знаем, что наша последовательность бернуллиева и достаточно какой-то простой проверки типа закона больших чисел, чтобы выяснить, по какой именно бернуллиевой мере она случайна: B_p или какой-то другой. Вторую часть можно рассматривать как аналогичную параметрическому тестированию в статистике.

С количественной точки зрения (если нас интересует не просто случайность и неслучайность, но и значение теста) вторая часть тестирования не важна: про сепаратор нам надо знать лишь, конечно или бесконечно его значение.

9 Равномерные тесты: слишком сильные требования?

9.1 Монотонность и квази-выпуклость

С интуитивной точки зрения равномерные тесты случайности (в наиболее общей форме см. определение 7.29) могут казаться слишком сильными, если мера P не вычислима. И действительно, они не обладают некоторыми интуитивно желательными свойствами, которыми обладает понятие случайности относительно вычислимых мер (в смысле Мартин-Лёфа или равномерное, для вычислимых мер это одно и то же). Одним из таких свойств является монотонность: большая (с точностью до константы) мера имеет больше случайных объектов.

Предложение 9.1. *Пусть P и Q — две вычислимые меры, а $\lambda > 0$ — рациональное число, причём $\lambda P(A) \leqslant Q(A)$ для всех A. Тогда*

$$\mathbf{m}(\lambda) \cdot \lambda \cdot \mathbf{t}(x, Q) \stackrel{\cdot}{<} \mathbf{t}(x, P).$$

Здесь $\mathbf{m}(\cdot)$ — дискретная априорная вероятность рационального числа λ; константа в $\stackrel{\cdot}{<}$ определяется сложностью пары программ, задающих P и Q.

Доказательство. Функция $\lambda\, \mathbf{t}(\cdot, Q)$ является P-тестом, так как

$$\int \lambda\, \mathbf{t}(x, Q)\, dP(x) \leqslant \int \mathbf{t}(x, Q)\, dQ(x) \leqslant 1.$$

Используя усечение, мы заключаем, что сумма

$$\sum_{\{\lambda \mid \lambda \cdot \int \mathbf{t}(x,Q)\, dP(x) < 2\}} \mathbf{m}(\lambda) \cdot \lambda \cdot \mathbf{t}(x, Q)$$

с точностью до константы является P-тестом, и потому не превосходит $\mathbf{t}(x, P)$. Тем более это верно и для всех членов этой суммы. (Упомянутая константа обратно пропорциональна $\mathbf{m}(P, Q)$.)

Интуитивная мотивировка свойства монотонности такова: если есть два устройства с внутренними датчиками случайности, генерирующие объекты с выходным распределением P и Q, и $\lambda P \leqslant Q$, то можно представить себе, что с вероятностью λ второе устройство моделирует первое, а в остальных случаях делает что-то своё. Тогда всякий объект, который с интуитивной точки зрения правдоподобен на выходе первого устройства, должен считаться правдоподобным и на выходе второго: вдруг оно-таки промоделировало первое? (Численное значение дефекта, конечно, может быть немного больше, так как мы дополнительно должны поверить, что произошло событие с вероятностью λ.)

Для равномерной случайности, увы, это свойство не выполнено: если мера Q больше, но вычислительно сложнее, то тесты случайности относительно Q могут использовать эту дополнительную информацию, чтобы сделать неслучайными некоторые объекты, которые относительно P были случайными (см. доказательство теоремы 5.39). Именно в этом причина

отличия равномерной случайности от слепой (безоракульной), для которой аналогичное свойство выполнено по очевидным причинам.

Другая ситуация, в которой у нас есть некоторая интуиция случайности — это смесь (выпуклая комбинация) мер. Представим себе два устройства с выходными мерами P и Q, и внешнюю оболочку, которая с какими-то вероятностями λ и $1-\lambda$ запускает одно из них. В целом мы получаем систему, выход которой распределён по мере $\lambda P + (1-\lambda)Q$. Про какие объекты мы готовы поверить, что они случайно получены в результате такого эксперимента? ясно, что это должны быть случайные по мере P объекты, а также случайные по мере Q объекты (при этом если коэффициент мал, то должно добавляться дополнительное удивление, но конечное). И других объектов быть не должно. Количественное уточнение этого результата (который в одну сторону следует из монотонности) даётся в следующем предложении.

Предложение 9.2. *Пусть P и Q — две вычислимые меры.*

(а) $\mathbf{m}(\lambda) \cdot \mathbf{t}(x, \lambda P + (1-\lambda)Q) \mathrel{\dot<} \max(\mathbf{t}(x,P), \mathbf{t}(x,Q))$;

(б) $\mathbf{t}(x, \lambda P + (1-\lambda)Q) \mathrel{\dot>} \min(\mathbf{t}(x,P), \mathbf{t}(x,Q))$.

В первом утверждении λ — рациональное число в $(0,1)$, а $\mathbf{m}(\lambda)$ — его дискретная априорная вероятность. Во втором утверждении λ может быть любым. Константы в $\mathrel{\dot<}$ не зависит от λ (определяются сложностью пары мер P и Q).

Первое утверждение можно назвать *квази-выпуклостью* тестов случайности (с точностью до константы). Для тестов, обладающих свойством квази-выпуклости в уточнённом варианте, без умножения на константу, можно построить нейтральную перечислимую снизу полумеру (в некотором точном смысле этого слова, при надлежащем обобщении понятия теста на полумеры, см.[16, 8]).

Второе утверждение можно назвать *квази-вогнутостью*; оно показывает, что никаких новых случайных объектов относительно смеси P и Q не появляется.

Доказательство. Первое утверждение является ослаблением предложения 9.1. Если $\lambda \geqslant 1/2$, то из этого предложения следует, что $\mathbf{m}(\lambda) \cdot \mathbf{t}(x, \lambda P + (1-\lambda)Q) \mathrel{\dot<} \mathbf{t}(x,P)$ (множитель $1/2$ можно включить в $\mathrel{\dot<}$). При $\lambda \leqslant 1/2$ верно аналогичное неравенство $\mathbf{m}(1-\lambda) \cdot \mathbf{t}(x, \lambda P + (1-\lambda)Q) \mathrel{\dot<} \mathbf{t}(x,Q)$; при этом $\mathbf{m}(1-\lambda) \doteq \mathbf{m}(\lambda)$.

Второе утверждение следует из того, что правая часть (как функция от x) является тестом относительно любой смеси мер P и Q, и можно воспользоваться усечением, чтобы сделать её равномерным тестом.

Легко понять, что все эти утверждения существенно используют вычислимость мер и коэффициентов в смеси. Соответствующие контрпримеры легко построить, если осознать, что смесь мер может быть как более сильным с вычислительной точки зрения оракулом, чем каждая из них (если пропорции смешивания невычислимы), так и наоборот. Например, разделим отрезок $[0,1]$ на две половины и рассмотрим две меры P и Q, равномерно распределённые на этих половинах. Их смесь с коэффициентами λ и $1-\lambda$ делает число λ заведомо неслучайным (поскольку оно может быть вычислено относительно этой меры), хотя по одной из мер оно вполне может быть случайным. (Взяв вместо P и Q их смеси, скажем, с коэффициентами $1/3$ против $2/3$ и наоборот, можно сделать λ случайным по обеим мерам.)

В этом примере смесь содержит больше информации, чем каждая из мер. Может быть и наоборот: свернём отрезок $[0,1]$ с равномерной мерой в окружность и разобьём его на две полуокружности точками p и $p+1/2$. Тогда равномерные меры на этих полуокружностях делают p вычислимым относительно них и потому неслучайным, а среднее этих мер есть равномерная мера на окружности, относительно которой p вполне может быть случайным.

Заметим, что для слепой (безоракульной) случайности мы можем безо всяких ограничений гарантировать, что множество случайных относительно смеси P и Q точек будет объединением

множеств точек, случайных относительно P и относительно Q. (В одну сторону это следует из монотонности, которую мы уже отмечали. В другую: если точка не случайна относительно P и не случайна относительно Q, то есть два теста, это доказывающих, и их минимум будет перечислимым снизу тестом, доказывающим её неслучайность относительно смеси.) Было бы интересно модифицировать понятие теста случайности, чтобы восстановить эти свойства, сохранив другие желательные свойства (скажем, существование универсального теста и тем самым понятие дефекта случайности). Некоторые предложения такого рода имеются в [16, 8, 17].

9.2 Локальность

Представим себе, что последовательность ω случайна по равномерной мере и начинается с нуля. Теперь изменим эту меру на последовательностях, начинающихся с единицы. Может оказаться, что последовательность перестанет быть случайной, так как значения меры теперь могут быть использованы как оракул (например, последовательность может стать вычислимой относительно новой меры). Но это выглядит странным, так как изменение меры происходит не в той части, где лежит наша последовательность.

Для слепой (безоракульной) случайности конкретно этот пример, как легко видеть, невозможен (тест можно принудительно обнулить на последовательностях, начинающихся с единицы), но в принципе понятие теста зависит от меры не только вдоль последовательности (не только от вероятности появления нуля и единицы после её начал).

Опять же для вычислимых мер ситуация лучше.

Предложение 9.3 (преквенциальное свойство)**.** *Пусть P и Q — две вычислимые меры на пространстве Ω бесконечных последовательностей нулей и единиц, совпадающие на всех началах некоторой последовательности ω. Тогда эта последовательность одновременно случайна или не случайна по мерам P и Q.*

Доказательство. Это немедленно следует из критерия случайности в терминах сложности начальных отрезков (теорема Левина–Шнорра) в любом из его вариантов (теорема 2.24, предложение 2.30 и следствие 2.32).

Для невычислимых мер это (как показывают примеры, аналогичные рассмотренным в предыдущем разделе) неверно.

В случае вычислимых мер в произвольном пространстве имеет место аналогичное утверждение, правда, с более сильным требованием: мы предполагаем, что две меры совпадают на любых множествах, содержащихся в некоторой окрестности последовательности ω. (В этом случае можно умножить тест на базисную функцию, не изменив его в ω и сделав нулевым вне окрестности совпадения.)

Вот ещё один способ, позволяющий получить заведомо преквенциальное определения случайности, в котором дефект случайности является функцией от самой последовательности и от мер её начальных отрезков. Для данной последовательности ω и для данной последовательности $\{q(i)\}$ действительных чисел, для которых $1 = q(0) \geqslant q(1) \geqslant q(2) \geqslant \ldots \geqslant 0$, положим

$$\mathbf{t}'(\omega, q) = \inf \mathbf{t}(\omega, P),$$

где минимум берётся по всем мерам P, для которых $P(\omega(1 : n)) = q(n)$. Соответствующие множества (для случай двоичных последовательностей) эффективно компактны, так что этот минимум будет перечислимой снизу функцией от ω и последовательности q. Если для последовательности ω и мер $q(i)$ её начальных отрезков значение $\mathbf{t}'(\omega, q)$ конечно, то последовательность ω можно назвать *преквенциально случайной.*

Другими словами, последовательность ω преквенциально случайна по мере P, если существует (вообще говоря, другая) мера Q, относительно которой ω случайна и которая совпадает с P на всех начальных отрезках ω.

Требование преквенциальности связано с попытками перенести понятия теории вероятностей и статистики в ситуацию последовательных предсказаний членов последовательности, ср. [5, 26]. Рассмотрим, например, прогноз погоды, в котором $\omega(n)$ означает, что в день n идёт дождь. Метеобюро перед каждым днём указывает число $p(n)$, которое оно называет вероятностью дождя в день n. (При этом на следующие дни никакого распределения вероятностей не указывается. Другими словами, вместо глобального распределения вероятностей бюро прогнозов указывает лишь условные вероятности вдоль пути, соответствующего фактической погоде.)

Можно ли оценить качество прогноза? Кажется, что в некоторых ситуациях да: если, скажем, все предсказания близки к нулю (скажем, меньше 10%), а большинство дней (скажем, более 90%) были дождливые. (Говорят, что такой прогноз плохо *калиброван*.) Но, естественно, возможны и какие-то другие виды несоответствий, не только частотные: общий вопрос состоит в том, можно ли воспринимать данную последовательность как полученную случайно с предсказанными вероятностями. (Другая ситуация, где возникает такой вопрос, это оценка качества датчика случайных битов, который выдаёт бит с заказанным распределением, на каждом шаге своим.)

Дополнительным обстоятельством при оценке качества предсказания является то, что предсказатель может использовать разнообразную информацию, доступную на момент предсказания (скажем, вечер предыдущего дня), а не только предыдущие члены последовательности ω. Наличие такой информации должно учитываться и при оценке качества предсказания.

В статье [26] обсуждаются подобные вопросы и предлагаются различные варианты определений, в частности, связанные с понятием мартингала, и доказывается эквивалентность некоторых из них. Интересно было бы установить связь и с равномерными тестами случайности в духе приведённого выше преквенциального определения дефекта (правда, вместо вероятностей начальных отрезков тут возникают условные вероятности, что не совсем то же самое, если они не отделены от нуля).

10 Вопросы

Мы уже отмечали некоторые вопросы, которые (на наш взгляд) было бы интересно изучить. В этом разделе мы собрали ещё несколько таких вопросов.

1. Рассмотрим следующий метод порождения последовательности $\xi \in \Omega$, распределённой в соответствии с данным распределением P на Ω, при котором вероятности всех слов ненулевые. Возьмём случайную последовательность ρ независимых равномерно распределённых на $[0,1]$ случайных чисел. После того как $\xi(1:n-1)$ уже построена, мы полагаем $\xi(n)=1$ тогда и только тогда, когда

$$\rho(n) < P(\xi(1:n-1)1)/P(\xi(1:n-1)).$$

Если рассматривать это как вероятностный процесс, то выходное распределение будет в точности P. Спрашивается, какие последовательности можно получить на выходе, если начинать со случайных по Мартин-Лёфу последовательностей действительных чисел. (Можно проверить, что для вычислимых мер P получаются в точности случайные по Мартин-Лёфу относительно P последовательности.)

2. Вспомним формулу для дефекта случайности по вычислимой мере:

$$\mathbf{t}(\omega, P) \doteq \sum_{x \sqsubseteq \omega} \frac{\mathbf{m}(x)}{P(x)}.$$

Обе части имеют смысл при произвольном P, но они могут быть различны. Причину этого мы уже обсуждали: небольшое изменение меры почти не влияет на правую часть, но может изменить её вычислительную силу как оракула и существенно изменить левую.

Обозначим правую часть этого равенства через $t'(\omega, P)$. Может быть, имеет смысл считать конечность t' определением случайности по невычислимым мерам? По крайней мере она будет монотонной (от увеличения меры случайность будет только расти). Относительно смеси мер она будет квази-выпуклой, более того, в [7] доказано, что $1/t'(\omega, P)$ является вогнутой функцией от P.

Другое возможное определение дефекта случайности для бесконечной последовательности ω по мере P таково: $\log \sup_{x \prec \omega} [\mathbf{a}(x)/P(x)]$. Для вычислимых мер мы вновь получаем определение, равносильное стандартному определению Мартин-Лёфа. В работе [10] показано, что определённые таким образом тесты случайности (а также аналогичные, использующие монотонную сложность вместо априорной вероятности) не обладают некоторым естественным свойством (*сохранения случайности*) — в отличие от равномерных тестов. В [7] показано, что, с другой стороны, что если в определении t' в правой части рассмотреть сумму по всем вычислимым функциям с конечным числом рациональных значений, а не только характеристические функции множеств $x\Omega$, то свойство сохранения информации выполняется.

3. Можно ли разумно определить дефект случайности последовательности относительно произвольных мер, добившись его монотонности (в каком-нибудь естественном смысле)? Например, можно было бы потребовать

$$P \leqslant c \cdot Q \Rightarrow t(\omega, P) \geqslant t(\omega, Q)/c.$$

(отметим в качестве мотивировки, что правая часть приведённой выше формулы для дефекта обладает этим свойством). Можно ли рассчитывать при этом на свойство квази-выпуклости? Некоторые попытки такого рода предприняты в [16, 8], а также в [17]

Свойство квази-вогнутости, видимо, обеспечить труднее (в этой ситуации приведённые контрпримеры выглядят более устойчивыми).

4. Стандартной процедурой в теории вычислимости является релятивизация: некоторое множество A объявляется разрешимым по определению, и алгоритмам разрешается использовать "оракул" для этого множества (отвечающий на вопросы о принадлежности ему). Это увеличивает класс вычислимых функций, но большинство результатов теории вычислимости остаются верными. Более сложная ситуация возникает, когда мы объявляем некоторое множество E перечислимым по определению. Проблема тут в том, что его можно перечислять в разном порядке, и разные перечисляющие его "оракулы" могут дать разные результаты. Тем не менее существует естественное понятие *перечислимого относительно* E множества (как ещё говорят, множества, *сводящегося по перечислимости* к E). Приведём соответствующее определение. Пусть W есть некоторое множество пар вида $\langle x, S\rangle$, где x — натуральное число, а S — конечное множество натуральных чисел. Будем считать, что множество W перечислимо. Тогда для любого множества E можно рассмотреть множество $S(E, W)$, состоящее из всех x, при которых $\langle x, S\rangle \in W$ при некотором $S \subset E$. (Неформально говоря, пара $\langle x, S\rangle$ понимается как инструкция: выдавать на выход x, обнаружив в перечислении E все элементы из списка S.) Добавление стандартного разрешающего оракула для множества A можно рассматривать как частный случай такой сводимости, положив $E = \{2n \mid n \in A\} \cup \{2n+1 \mid n \notin A\}$.

В некоторых ситуациях можно пытаться обойтись такого рода оракулом. Скажем, вполне можно говорить о перечислимой снизу относительно E функции, поскольку её можно определить в терминах перечислимых множеств. Но не очевидно, что определённые таким образом понятия обладают привычными для нас свойствами.

Можно ли утверждать (для произвольного E), что существует максимальная перечислимая снизу относительно E полумера? Можно ли определить префиксную сложность с оракулом E и будет ли она совпадать с логарифмом максимальной полумеры (если таковая существует)? Что будет, если дополнительно предположить, что E есть множество всех базисных шаров в конструктивном метрическом пространстве, содержащих некоторую точку?

(Для сравнения напомним, что можно определить E-вычислимую функцию как функцию, график которой E-перечислим. При этом выполняются некоторые знакомые свойства, скажем, композиция двух E-вычислимых функций является E-вычислимой. Однако, скажем, утверждение о том, что всякое непустое E-перечислимое множество является областью значений всюду определённой E-вычислимой функции, уже не гарантировано: при некоторых E это не так.)

5. Можно пытаться обобщать понятие случайности в другом направлении, рассматривая не вычислимые меры, а перечислимые полумеры, то есть выходные распределения вероятностных машин, выдающих бит за битом (и, возможно, выдающих конечную последовательность с положительной вероятностью). Это предложил Левин, имея в виду определить независимость двух последовательностей α и β как случайность пары (α, β) относительно полумеры $\mathbf{a} \times \mathbf{a}$. (Такой подход предполагает, что все последовательности случайны относительно полумеры $\mathbf{a}$.) Соответственно дефект случайности пары (α, β) относительно $\mathbf{a} \times \mathbf{a}$ можно было бы назвать количеством общей информации в последовательностях α и β, по аналогии с конечными словами, где взаимная информация слов x и y, определяемая как

$$KP(x) + KP(y) - KP(x, y) = -\log(\mathbf{m}(x) \times \mathbf{m}(y)) - KP(x, y),$$

выглядит как дефект случайности относительно $\mathbf{m} \times \mathbf{m}$.

Одна из возможностей для определения случайности последовательности относительно полумеры Q такая: потребовать ограниченности отношения $\mathbf{a}(x)/Q(x)$ для начальных отрезков x последовательности ω. Другой вариант: рассматривать случайные по Мартин-Лёфу относительно равномерной меры последовательности случайных битов, использовать их как исходы датчика случайных битов в вероятностной машине и смотреть, какие последовательности могут получиться на выходе. Неизвестно, совпадают ли это определения. Неизвестно также, корректно ли второе из них (в том смысле, что двум вероятностным машинам с одним и тем же выходным распределением соответствует одно и то же множество образов случайных последовательностей). Для вычислимых мер (машин, выдающих бесконечные последовательности с вероятностью 1) это действительно так.

6. (Этот вопрос задал С. Симпсон) Можно ли предложить естественное понятие тестов случайности для, скажем, 2-случайных последовательностей? (Обычное определение на языке тестов соответствует тестам, не являющимся полунепрерывными.)

Благодарности

Авторы благодарны своим коллегам, с котороми они обсуждали рассматриваемые в статье вопросы, в первую очередь Л. Левину, к которому восходят многие из понятий этой статьи, А. Буфетову и А. Клименко, а также В. Вьюгину и другим участникам колмогоровского семинара (на мехмате МГУ в Москве). Статья написана при финансовой поддержке грантов NAFIT ANR-08-EMER-008-01, RFBR 0901-00709-а.

References

[1] Jeremy Avigad, Philipp Gerhardy, and Henry Towsner. Local stability of ergodic averages. *Transactions of the American Mathematical Society*, 362(1):261–288, 2010.

[2] Laurent Bienvenu, Adam Day, Mathieu Hoyrup, Ilya Mezhirov, and Alexander Shen. A constructive version of Birkhoff's ergodic theorem for Martin-Löf random points. http://arxiv.org/abs/1007.5249

[3] Laurent Bienvenu, Andrei Romashchenko, Alexander Shen. Sparse sequences. Journees Automates Cellulaires, 2008 (Uzes). Moscow: MCCME publishers, 2008. P.18–28. http://hal.archives-ouvertes.fr/hal-00274010/en.

[4] Gregory J. Chaitin. A theory of program size formally identical to information theory. *Journal of the ACM*, 22:329–340, 1975.

[5] Alexey Chernov, Alexander Kh. Shen, Nikolai Vereshchagin, and Vladimir G. Vovk. On-line probability, complexity and randomness. In Yoav Freund, Laszlo Gyorfi, Gyorgy Turan, and Thomas Zeugmann, editors, *Proceedings of the nineteenth international conference on algorithmic learning theory*, pages 138–153, Tokyo, 2008.

[6] Peter Gács. Lecture notes on descriptional complexity and randomness. Technical report, Boston University, Computer Science Dept., Boston, MA 02215. www.cs.bu.edu/~gacs/papers/ait-notes.pdf.

[7] Peter Gács. *Complexity and Randomness.* PhD thesis, J.W. Goethe University, Frankfurt, W.Germany, 1978. In German.

[8] Peter Gács. Exact expressions for some randomness tests. *Z. Math. Log. Grdl. M.*, 26:385–394, 1980. Short version: Springer Lecture Notes in Computer Science 67 (1979) 124-131.

[9] Peter Gács. On the relation between descriptional complexity and algorithmic probability. *Theoretical Computer Science*, 22:71–93, 1983. Short version: Proc. 22nd IEEE FOCS (1981) 296-303.

[10] Peter Gács. Uniform test of algorithmic randomness over a general space. *Theoretical Computer Science*, 341(1-3):91–137, 2005.

[11] Mathieu Hoyrup and Cristóbal Rojas. An application of Martin-Löf randomness to effective probability. In *Cie2009, LNCS 5635*, pages 260–269, 2009.

[12] Mathieu Hoyrup and Cristóbal Rojas. Computability of probability measures and Martin-Löf randomness over metric spaces. *Information and Computation*, 207(7):830–847, 2009.

[13] Andrei N. Kolmogorov. On the logical foundations of information theory and probability theory. *Problems of Information Transmission*, 5(3):1–4, 1969.

[14] K. Kuratowski. *Topology.* Academic Press, New York, 1966.

[15] Leonid A. Levin. On the notion of a random sequence. *Soviet Math. Dokl.*, 14(5):1413–1416, 1973.

[16] Leonid A. Levin. Uniform tests of randomness. *Soviet Math. Dokl.*, 17(2):337–340, 1976.

[17] Leonid A. Levin. Randomness conservation inequalities: Information and independence in mathematical theories. *Information and Control*, 61(1):15–37, 1984.

[18] Ming Li and Paul M. B. Vitányi. *Introduction to Kolmogorov Complexity and its Applications (Third edition)*. Springer Verlag, New York, 2008.

[19] Per Martin-Löf. The definition of random sequences. *Information and Control*, 9:602–619, 1966.

[20] Y. T. Medvedev. Degrees of difficulty of mass problems. *Doklady Akademii Nauk SSSR. N.S.*, 104:501–504, 1955. In Russian. Mathematical Reviews (MathSciNet): MR0073542.

[21] Joseph Miller. Degrees of unsolvabiility of continuous functions. *The Journal of Symbolic Logic*, 69(2), 555-584, 2004.

[22] Claus Peter Schnorr. Process complexity and effective random tests. *J. Comput. Syst. Sci*, 7(4):376–388, 1973. Conference version: STOC 1972, pp. 168-176.

[23] Glenn Shafer, Alexander Shen, Nikolai Vereshchagin, and Vladimir Vovk. Test martingales, Bayes factors, and p-values.
`arxiv.org`, 0912.4269v2.

[24] Glenn Shafer, Vladimir Vovk. Probability and Finance: It's Only a Game! Wiley, 2001. ISBN: 978-0-471-40226-8.

[25] Alexander Shen. Algorithmic information theory and Kolmogorov complexity. Technical Report TR2000-34, Uppsala University. 31pp. Available at
`http://www.it.uu.se/research/publications/reports/2000-034/`.

[26] Vladimir G. Vovk and Alexander Shen. Prequential randomness and probability. *Theoretical Computer Science*, 411:2632–2646, 2010.

[27] Volker Strassen. The existence of probability measures with given marginals. *Annals of Mathematical Statistics*, 36:423–439, 1965.

[28] V. V. V'yugin. Ergodic theorems for individual random sequences. *Theoretical Computer Science*, 207(2):343–361, 1998.

[29] Alexander K. Zvonkin and Leonid A. Levin. The complexity of finite objects and the development of the concepts of information and randomness by means of the theory of algorithms. *Russian Math. Surveys*, 25(6):83–124, 1970.