Randomness: Old and New Ideas

Dmitriy Klyushin

Taras Shevchenko National University of Kyiv, Volodymyrs'ka str. 64/13, Kyiv, 01601, Ukraine

Abstract
The survey of classical theories of randomness is provided, and an alternative model is proposed. Analysis of the classical models demonstrates that despite their mathematical rigor they are hardly useful in practice. The new model is based on the lattice theory, has the strong mathematical basis and easily used in practice.
.

Keywords
randomness, computational complexity, typicality, random sequence, chaotic sequence, lattice

1. Introduction

Randomness is one of the most important and difficult notions in computer science. The importance of randomness is justified by the fact that we face randomness in the simulation of real processes (physical, chemical, etc.), cryptography and many randomized algorithms. Difficulty of randomness lies in the fact that its nature is controversial. Some classics of computer science (e.g. Turing [1] and von Neumann [2]) considered randomness as a purely physical phenomenon (see citations in the excellent survey [3]). Thus, now there exist two parallel worlds: the world of physicists, engineers, computer scientists, and other investigators that work in the field of real applications and the world of pure mathematicians that attend to theoretical issues of randomness (e.g. consistency of axioms, interconnections between different definitions of randomness, etc.). We propose a strongly valid mathematical theory of randomness that is easily applicable in practice. Following to Vitanyi [4, 5] we divide the works on the concept of randomness into three categories: frequency approach, computational complexity and randomness as typicality.

2. Frequency approach (von Mises)

The model proposed by von Mises uses a concept of an infinite binary sequence $x_1, x_2, \ldots$ (collective) that meets the following conditions: 1) if h_n is the relative frequency of units in first n elements of a sequence, then $\lim_{n\to\infty} h_n(T, A) = \lim_{n\to\infty} \frac{1}{n}\sum_{k=1}^{n} x_k = p, 0 < p < 1$ (global regularity), and 2) every infinite subsequence $x_{i_1}, x_{i_2}, \ldots$ drawn from the sequence $x_1, x_2, \ldots$ using a rule of acceptable selection has the same limit p (local regularity).

Definition 1 (von Mises). A sequence is said to be random if it has two properties: 1) every sequence of relative frequencies of units in the collective has the same limit; 2) the relative frequencies are invariant under the procedure of so-called acceptable selection (the choice of a sequence in which the choice of an nth element does not depend on its value).

Objections to von Mises theory boil down to two aspects: 1) it uses too strict assumptions about the relative frequency and 2) the rule of admissible choice of elements of a subsequence is fuzzy. These objections became the subject of research by Wald [6] and Church [7]. Wald proposed to limit

IT&I-2020 Information Technology and Interactions, December 02–03, 2020, KNU Taras Shevchenko, Kyiv, Ukraine
EMAIL: dokmed5@gmail.com
ORCID: 0000-0003-4554-1049

the possible rules for selecting subsequences by any fixed countable set of functions and showed that such collectives exist. Church clarified that this set must be a set of recursive functions. Thus, the theory received due mathematical rigor. Such sequences are called random Mises–Wald–Church sequences. In 1939, a new counterexample was put forward against this theory. The construction of Ville [8] demonstrated the existence of random sequences of Mises–Wald–Church, in which the boundary of the sequences of relative frequencies is equal to 1/2, but $h_n \geq \frac{1}{2}$ for all *n*. Van Lambalgen [9–12] carefully conducted an analysis of Ville counterexamples and other objections to von Mises theory. In particular, van Lambalgen distinguishes three main objections to von Mises theory from Frechet [13] and Ville [8]: 1) von Mises theory is weaker than Kolmogorov theory [14, 15] because it does not follow the law of the repeated logarithm; 2) collectives do not always satisfy all asymptotic properties arising in the methods of measure theory (therefore they can not serve as satisfactory models for real phenomena), and 3) the von Mises formalization for game strategies using the rule of allowable choice of elements has disadvantages because there is possibility to win an unlimited sum.

The answer to the first objection put forward by Ville comes down to the fact that von Mises theory is purely frequency and does not provide the operation of passing to the limit in as in the measure theory [8]. In other words, von Mises model and Kolmogorov model are not equivalent. But the fact that they are different cannot be considered as a disadvantage of any of these models [16].

The second objection belonging to Frechet can be divided into two parts: 1) collectives cannot be satisfactory models for random phenomena, because one-sided convergence, which allows refuting Ville counterargument, is not observed in practice; 2) collectives do not satisfy the asymptotic laws arising from the theory of measure. Van Lambalgen refuted these objections, pointing out that in practice there are only finite sequences and collectives were invented precisely to describe their properties, and von Mises did not set himself the goal of describing infinite random phenomena. Note that this statement is contradictory, because von Mises axioms include the limit of an infinite sequence of relative frequencies. The second part of the counterargument is somewhat reminiscent of Ville first counterargument and it is similarly refuted: the fact that collectives do not satisfy the asymptotic laws arising from the theory of measure indicates only a fundamental difference between these models, but is not their shortcomings.

The third objection refers to the existence of a strategy invented by Ville, which allows the player to win an infinite amount of money in the endless continuation of the game with the coin. In other words, there is a collective describing a coin game in which a player wins an unlimited amount, although by definition collectives deny this possibility. However, as van Lambalgen notes, the notions of fair play according to Ville and von Mises are different, so this counterargument is not valid.

3. Randomness as computational complexity (Kolmogorov)

Concluding that von Mises–Wald–Church theory is too fuzzy, Kolmogorov improved it by proposing a new class of algorithms for selecting valid sequences.

Kolmogorov complexity of a sequence $x = (x_1, x_2, ..., x_N)$, or is algorithmic entropy, is the length $K(x)$ of its shortest description, constructed using a Turing machine. If there is some additional information y, then we can consider conditional Kolmogorov complexity $K(x|y)$. A sequence is called Bernoullian by Kolmogorov if its complexity is close to $\log_2 C_N^k$, i.e. $K(x|N,k) \approx \log_2 C_N^k$. Also, Kolmogorov introduced the notions of chaotic sequence that satisfies the condition $K(x|N,k) \geq \log_2 C_N^k - m$. If a set A contains finite number of elements $x_1, x_2, ..., x_N$, then the complexity of its element is less or equal to $log_2 N$. An element *x* of *A* is random if its complexity is close to maximal, i.e. $K(x|A) \approx log_2 N$. The difference $log_2 N - K(x|A)$ is a defect of randomness of an element x.

In the class of sequences random according to Kolmogorov, frequency stability is observed in all acceptable Kolmogorov subsequences. Thus, the class of sequences random according to Kolmogorov is a partial case of the class of random sequences von Mises-Wald-Church. But, according to Uspensky [17], today von Mises theory remains an incomplete imprint of the intuitive notion of chance. Its main feature is the insistence on the frequency stability of random sequences. The contribution of Kolmogorov in the development of the theory of chance is quite fully covered in the work of Vovk and Shafer [18].

Wolf and Shafer believe that the Kolmogorov theory of randomness is based on the principle of frequency stability of von Mises and on the principle of Cournot [19]. The von Mises principle states that the relative frequency of infinite sequence of outcomes of random tests has a limit, and the Cournot principle states that a very unlikely event in a single test will not occur. Accordingly, the works of Kolmogorov on this topic can be divided into two categories: those based on the principle of von Mises (1963-1965), and those based on the principle of Cournot (1965-1987).

In [15] Kolmogorov formulated two main shortcomings of von Mises theory: 1) a frequency approach that appeals to the concept of limit frequency that cannot have practical application, because in real applications researchers are dealing with finite sequences; 2) frequency approach can not be developed purely mathematically.

In 1965, Kolmogorov began to develop the theory of algorithmic randomness [20–22]. Within this theory, he introduced the concept of the Bernoullian sequence: a binary sequence $\left(x_1, x_2, ..., x_N\right)$ consisting of k ones and $N-k$ zeros, to describe which requires at least $\log_2 C_N^k$ bits. Therefore, the problem of randomness was reduced to the choice of a certain way of describing the sequences. The main invention that ensured the success of the proposed theory was a universal method of description, which generates descriptions that are shorter or slightly longer than the descriptions created by alternative methods. Regardless of Kolmogorov analogous methods were invented by Solomonoff [23–25] and Chaitin [26].

Kolmogorov proposed to consider an infinite binary sequence as random if there is a constant such that for all the entropy of the initial segment of the sequence exceeds.

Definition 2 (Kolmogorov). An infinite binary sequence $x_1, x_2, ..., x_n, ...$ is said to be random if there is a constant for an arbitrary natural number that satisfies the inequality $K\left(x_1, x_2, ..., x_n\right) \geq n-c$.

For a long time, the focus of Kolmogorov and his followers (Asarin [27, 28], Shen [29], Vyugin [30, 31] etc.) were finite sequences. Their research was aimed at the consistent removal from consideration of statistical models based on the concept of probability, and their replacement by models based on the concept of complexity.

Vovk and Schafer [18] note the following characteristic features of the theory of complexity proposed by Kolmogorov and his followers: 1) It considers only finite sequences and finite sets of constructive objects; 2) it is based on the assumption that an event that has a very low probability will not occur.

Thus, developing the theory of complexity, Kolmogorov abandoned the von Mises principle and based it on the Cournot principle. It should be noted that the complexity theory remains the subject of intensive theoretical research. In 2007 for a series of works "On clarification of estimates AN Kolmogorov relating to the theory of chance" Muchnik and Semenov [32] was awarded the prize named after Kolmogorov. In these works important results were obtained in the field of combinatorial theory of probabilities and the theory of frequency tests of randomness. Muchnik and Semenov proved that the lower estimate by Kolmogorov, which characterizes the maximum number of admissible selection rules, for which there is guaranteed to be a generator of random numbers, is accurate in order and even asymptotically accurate. Kolmogorov put it back in 1963, when work on complexity theory was just beginning.

An original approach to estimating the complexity of finite sequences of zeros and ones was proposed by Arnold [33]. The value of this work lies in the fact that it uses the ideas of various fields: computational mathematics, topology, graph theory, algebra. Despite the fact that a complete solution of the problem is not obtained in the work, the combination of methods of different branches of mathematics seems to be the most fruitful and promising approach.

4. Randomness as typicality (Martin-Löf)

Attempts to extend the theory of Kolmogorov complexity to infinite sequences have encountered the problem of oscillation of complexity. Consider a fixed finite binary sequence $(x_1, x_2, ..., x_n)$. Do inequalities $K(x_1, x_2, ..., x_m) \le K(x_1, x_2, ..., x_n)$ or $K(x_1, x_2, ..., x_m | m) \le K(x_1, x_2, ..., x_n | n)$ hold for all infinite binary sequences x and $m \le n$? As stated in [1], the answers to both questions are negative. As Vitanyi [1] points out, even for sequences of high complexity that satisfy the inequality $K(x_1, x_2, ..., x_n) \ge n - \log_2 n - 2\log_2 \log_2 n$ for all n, the value $\left(n - K(x_1, x_2, ..., x_n)\right) / \log_2 n$ varies from 0 to 1.

This problem was solved in 1966, when Martin-Löf [34] concluded that the randomness defect of an element of a finite set can be considered as a universal statistical test, and extended it to infinite sequences using constructive measure theory. In this case, Martin-Löf assumed that the random object is typical, i.e. belongs to the vast majority. Martin-Löf definition looks like this.

Definition 3 (Martin-Löf). An infinite binary sequence $x_1, x_2, ..., x_n, ...$ is said to be random with respect to uniform measure, if for an arbitrary natural n there is a constant c such that $K(x_1, x_2, ..., x_n) \ge n - c$.

Obviously, a sequence that is random by Martin-Löf is random by von Mises. From the other side, there are sequences that do not satisfy the conditions of Martin-Löf. A uniform measure of a set of sequences for which there is a constant c and an infinite number of numbers n, such $K(x_1, x_2, ..., x_n) \ge n - c$ is equal to one. Therefore, the uniform measure of the set of random sequences that do not satisfy the condition of Martin- Löf definition is equal to zero.

Independently of Martin-Löf and each other, Schnorr [35] and Levin [36, 37] worked on the problem of infinite binary random sequences. They showed that an infinite binary sequence is random according to Martin-Löf if and only if the randomness defect of its initial segments is of limited value, i.e. $|KM(x_1, x_2, ..., x_n) - n| = O(1)$ where $KM(x_1, x_2, ..., x_n)$ is the monotonic entropy.

It is obvious that the sequence, random according to Martin-Lö**ö**f, is also random according to Mises-Wald-Church. On the other hand, as Wald construction demonstrates, there are Mises–Wald–Church collectives in which the relative frequency of the unit goes to 1/2 and $K(x_1, x_2, ..., x_n) = O(f(n)\log_2 n)$ for any unlimited, non-decreasing, totally recursive function. Such sequences do not satisfy the conditions for the Martin-Löf.

As we can see, the models described above are purely theoretical and their application in practice is associated with great difficulties. We offer an alternative approach, which is both strictly mathematically grounded and easily implemented in practical applications.

5. Alternative model (Petunin–Klyushin)

Consider the trial T with two outcomes A and $\bar{A}$. Introduce the indicator x_k such that $x_k = 1$ if in kth repetition of T we observe A and 0 otherwise. The sequence of bits $x_1, x_2, ...$ is said to be Bernoullian sequence of order p, $0 \le p \le 1$, if $\lim\limits_{n \to \infty} h_n(T, A) = \lim\limits_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} x_k = p$, where $h_n(T, A)$ is the relative frequency of A under the n repetitions of T.

5.1. Basics of alternative approach

The key issue of this approach is that for correct definition of the randomness we must consider an infinite sequence of the results of series $X_1, X_2, ...$. For convenience, let arrange these series in an indefinite characteristic matrix $\Theta(T) = \{x_{ij}\}_{i,j=1}^{\infty}$. Denote rows of $\Theta(T)$ as $X_i = (x_{i1}, x_{i2}, ..., x_{in}, ...)$ and columns as $X_j^* = (x_{1j}, x_{2j}, ..., x_{nj}, ...)$. Every row X_n and every column X_n^* of the matrix $\Theta(T)$ can be considered as a binary representation of real numbers $\alpha_n = 0, x_{n1}x_{n2}...x_{nn}...$ and $\alpha_n^* = 0, x_{1n}x_{2n}...x_{nn}...$ in $[0,1]$ respectively. These numbers form the sets M and M^*, respectively.

Definition 4 (Petunin–Klyushin). A trial T is said to be random if 1) every row X_n and column X_n^* ($n = 1, 2, ...$) of $\Theta(T)$ is a Bernoullian sequence of the same order $p \in [0,1]$; 2) M and M^* are dense in $[0,1]$. A random experiment E is an infinite series of trials T. A random event R_E is an outcome of T occurring in a random experiment E. The probability $p_E(A)$ of R_E is the order $p \in [0,1]$ of the Bernoullian sequences of the outcomes generated in E.

In practice, we work with finite matrices. Thus, we propose the following useful clarification: T is said to be a random trial if 1) every row X_i and column X_i^* ($i = 1, 2, ... n$) of finite matrix $\Theta_n(T)$ are segments of Bernoullian sequences of the same order $p \in [0,1]$; and 2) if for an arbitrary $\varepsilon > 0$ there exists such n that the sets M_n and M_n^* generated by columns and rows of the finite characteristic matrix $\Theta_n(T) = \{x_{ij}\}_{i,j=1}^{n}$ form ε-net in $[0,1]$.

Theorem 1. The probability that the sets M and M^* generated of rows and columns of the characteristic matrix $\Theta(T)$ in the Bernoullian experiment are dense is equal to 1.

Proof. Consider the case M. Take a binary presentation $\alpha = 0, i_1 i_2 ... i_n ...$ of an arbitrary real number from $[0,1]$. Choose an arbitrary $\varepsilon > 0$ and a natural n_0, such that $\frac{1}{2^{n_0}} < \frac{\varepsilon}{2}$. Put $\tilde{\alpha} = 0, 0...0 i_{n_0+1} i_{n_0+2} ...$ and $\hat{\alpha} = \alpha - \tilde{\alpha} = 0, i_1 i_2 ... i_{n_0} 0...0...$ Let A be a random event that after n_0 independent repetitions of the random trial T we obtain a set $\{i_1, i_2, ..., i_{n_0}\}$. Suppose that in this set units occur k times, and zeros occur $n_0 - k$ times. Denote by T_A a random trial with outcomes A and $\bar{A}$. Then, $p(T_1 T_2, ..., T_{n_0}, A) = p^k (1-p)^{n_0-k} > 0$ and $p(T_1, T_2, ..., T_{n_0}, \bar{A}) = 1 - p(T_1, T_2, ..., T_{n_0}, A) = \delta < 1$. Let us prove, that the probability of at least one event A in a sequence of independent Bernoulli trials equals to 1. Indeed, the probability of $\bar{A}$ is less than δ^n for any n. Thus, it equals to zero. Therefore, the probability that there exists a row of $\Theta(T)$ such that its first n_0 elements are $i_1, i_2, ..., i_{n_0}$ is equal to 1. This row is a binary presentation of a number $\bar{\alpha}$ in M, such that $|\alpha - \bar{\alpha}| < \frac{\varepsilon}{2}$

Let $(\gamma, \eta) \subset [0,1]$ be an arbitrary interval. Put $\alpha = \frac{\gamma + \eta}{2}$. Then the probability that there exists some number $\bar{\alpha} \in M$ such that $|\alpha - \bar{\alpha}| < \frac{\varepsilon}{2}$ equals to 1, thus $\bar{\alpha} \in [\gamma, \eta]$. Therefore, in the Bernoulli model E the number set M represented by the rows $\Theta(E)$ is dense in $[0,1]$ with probability 1. The proof of the theorem for M^* is similar.

5.2. Field of events

Let T be a random trial, and $S(T)$ be a set of all outcomes of T. Define addition and multiplication on members of $S(T)$, and negation of an event. Then, we shall be able to determine the probability $p_E(A)$ of an event A in $S(T)$ transforming it into a field of events $S(E)$. Introduce partial order in $S(E)$ generated by the random experiment E: an event A implies an event B, i.e. $A \le B$, if the occurrence of A in E implies the occurrence of B. Therefore, $S(E)$ becomes a partially ordered set where $A+B=\sup(A,B)=A\vee B$ and $AB=\inf(A,B)=A\wedge B$. Addition and multiplication can be performed using the relation of partial order: $\sum_{i\in J}A_i=\sup_{i\in J}\{A_i\}$ and $\prod_{i\in J}A_i=\inf_{i\in J}\{A_i\}$. Since sum and product of the events always exist in $S(E)$, the field of events $S(E)$ is a complete distributive lattice.

As far as partial order is defined only for elements of $S(E)$, we may apply addition, multiplication and negation only to events of the same field. The complement to element A in a lattice with zero is such an element $A'\in S$ that $A\wedge A'=0$ and $A\vee A'=I$, and the lattice $S(E)$ is called a lattice with complement if every element has a complement. In the field of events, zero element O is the impossible event, the unit element I is the certain event, and the complement of an element A is its negation $\bar{A}$. Thus, the field of events $S(E)$ is a Boolean algebra with complement.

The complete lattice $S(E)$ is called totally distributive [39] if it satisfies duality laws: for an arbitrary non-empty family of index sets J_γ, $\gamma\in C$

$$\bigwedge_{\gamma\in C}\left[\bigvee_{\alpha\in J_\gamma}X_{\gamma,\alpha}\right]=\bigvee_{\varphi\in\Phi}\left[\bigwedge_{\gamma\in C}X_{\gamma,\varphi(\gamma)}\right],$$

$$\bigvee_{\gamma\in C}\left[\bigwedge_{\alpha\in J_\gamma}X_{\gamma,\alpha}\right]=\bigwedge_{\varphi\in\Phi}\left[\bigvee_{\gamma\in C}X_{\gamma,\varphi(\gamma)}\right],$$

where Φ is a set of all functions defined on C such that $\varphi(\gamma)\in J_\gamma$ and $X_{\gamma,\alpha}$, $X_{\gamma,\varphi(\gamma)}\in S(E)$, $\alpha\in J_\gamma$

Theorem 2 [39]. For an arbitrary random experiment E the field of events $S(E)$ is a totally distributive complete Boolean algebra.

Theorem 3 (Tarsky [39]). If complete Boolean algebra S is totally distributive then it is isomorphic to the algebra $2^{\aleph}$ consisting of all subsets of some set M with respect to the structures of partially ordered spaces (or Boolean algebras).

5.3. Random variables

Let us introduce the following useful definitions.

***Definition* 5.** *The set of events $B=\{B_i\}_{i\in J}$ from the field of events $S(E)$ is called base if the following conditions hold:*

1) all events B_i from B are mutually exclusive $B_iB_j=0$ if $i\neq j$;

2) an arbitrary event A from $S(E)$ can be represented as a sum of events B_i from B:

$$A=\sum_{k\in K}B_{i_k}.$$

A probability distribution $P_E(A)$ in the field of events $S(E)$ depends on a random experiment E and a random event A. Further we shall suppose that E is fixed, thus $P_E(A)$ depends only on $A\in S(E)$.

By definition, $P(A)=\lim_{n\to\infty}h_n(A)$, where $h_n(A)$ is a relative frequency of the event A. The probability $P(A)$ is a finitely additive function defined on $S(E)$, but it is not countably additive because the limit of the relative frequency in not interchangeable for a sequence of mutually exclusive events from $S(E)$.

Now, define a random variable x as a random experiment E with basic numerical set $B(E)\subset R^1$, or $B(E)\subset C$. Individual values of a random variable x in the partially ordered space $S(E)$ play the role of atoms of a lattice. Often, it is convenient to consider a random variable x as a function defined on a basic set of $S(E)$ and map every elementary event $B_i \in B(E)$ to a number $x = x(B_i)$. These definitions of a random variable are equivalent.

Consider a concept of probability distribution on a field of events generated by values of a random variable. At first, consider random variables taking on values in the set of rational numbers Q. Then, we shall extend this concept to random variables with real values.

Denote by $B_E(x)$ a set of all possible rational values of random variable x in a random experiment E. Suppose, $B_E(x) = Q$. Then $S(E) = 2^Q$.

Definition 6. A random variable x taking rational values is said to be continuous if its distribution function $F_x(u)$ is continuous in R^1. Respective distribution of probabilities is said to be continuous.

Definition 7. A random variable x with rational values is said to be singular if there exists such subset $\Psi = \{a_1, a_2, ..., a_n, ...\} \subset Q$ that $p(E, \{a_n\}) = p_n > 0 \quad \forall n \in N$ and $\sum_{n=1}^{\infty} p_n = 1$. Respective distribution of probabilities is said to be singular.

Theorem 4 [38]. Let $F(u)$ be an arbitrary continuous distribution function in R^1 then there exists a random experiment E with $B_E = Q$ and distribution of probability $p(E, A)$, $A \subset Q$ such that for every $u \in R^1$ $p\left(E, Q_{(-\infty,u]}\right) = F(u)$, where $Q_{(-\infty,u]} = Q \bigcap (-\infty, u]$.

Theorem 5 [38]. Let $F(u)$ be an arbitrary distribution function concentrated on the segment $[a,b]$:

$$F(u) = \begin{cases} 0, & if \quad u \le a, \\ 1, & if \quad u \ge b. \end{cases}$$

Then there exists a random experiment E with numerical base set $B_E = [a,b]$ generating a distribution of probabilities $p(E, A)$ on all subsets $A \subset [a,b]$ such that $p\big(E, (a,u]\big) = F(u)$ if $u \in (a,b)$.

Theorem 5 has the remarkable consequence: if the distribution function $F(u)$ is continuous then the distribution of probabilities generated by $F(u)$ is not a measure. If we suppose the opposite then we have a measure defined on all subsets of the segment $[a,b]$, which is equal to zero at every one-point set. This contradicts to classic Ulam's theorem [40], according to which the measure mentioned above is equal to zero everywhere.

The concept of independent events in the new theory is introduced in the following way. Let $p(E, A|B)$ be the conditional probability of the event A in the experiment E generated by the series of the trial T. Then, the event A does not depend on B if

$$p(E, A|B) = p(E, A|\overline{B}).$$

Theorem 6 [38]. *Let E be a random experiment, A and B be random events that can occur in the experiment E. The random event A does not depend on B if and only if*

$$p(E, A|B) = p(E, A).$$

5.4. Operations on random variables

Let us define multiplication by constant, addition, subtraction, multiplication and division of two random variables considering a random variable as a function $x(B)$, $B \in B_T$, defined on the set of elementary outcomes B_T of some random trial T. For example, suppose that a set of elementary outcomes of the random trials T_1 and T_2 belong to disjoint segments [a, b] and [c, d]. Let random variables x and y take on their values as a result of the random trials T_1 and T_2. Thus, we can interpret x as a function $x(B)$ defined on [*a*, *b*] and y as a function $y(B)$ defined on [*c*, *d*]. Since the segments are disjoint, the sets of elementary outcomes of these trials are disjoint also and sum $x+y$ is no valid.

Let us introduce a useful concept that we need in further.

Definition 8. *The random experiments* E_1 *and* E_2 *are said to be commutative if* $p((E_1,E_2),(A_1,A_2)) = p((E_2,E_1),(A_2,A_1))$. Let $T_c = \{T_1,T_2\}$ be a composite trial, then $B_{T_c} = B_{T_1} \times B_{T_2}$, where $\times$ denotes the Cartesian product of the sets B_{T_1} and B_{T_2}. The results of the random trial T_c is the random event $B_c = (B_1, B_2)$, where $B_1 \in B_{E_1}$ and $B_2 \in B_{E_2}$, so that x takes on value $x(B_1)$, and y takes on value $y(B_2)$. We would introduce arithmetic operations as $(x+y)(B_c) = x(B_1) + y(B_2)$, $(x-y)(B_c) = x(B_1) - y(B_2)$, $(xy)(B_c) = x(B_1)y(B_2)$, $\left(\frac{x}{y}\right)(B_c) = \frac{x(B_1)}{y(B_2)}$, but they are valid only if random experiments E_1 and E_2 are commutative. Let us consider the concept of isomorphic experiments and isomorphic random events. A function $\Psi : X \to Y$ defined on an ordered set X and taking on values in an ordered set Y is said to be an isotonic function**,** if $x \le y$ implies $\Psi(x) \le \Psi(y)$

An isotonic function that is invertible is said to be an isomorphism. Thus, an isomorphism between ordered sets is a single-valued mapping that satisfies these conditions. This is an inverse isotonic property of the mapping Ψ that is called a structural isomorphism of ordered sets X and Y.

Definition 9. Let E_1 and E_2 be two random experiment and let $S(E_1)$ and $S(E_2)$ be the fields of random events generated by E_1 and E_2, respectively. We shall call the fields of events $S(E_1)$ and $S(E_2)$ isomorphic, if between their elements there exists a one-to-one mapping Ψ, which is a structural isomorphism of Boolean algebras $S(E_1)$ and $S(E_2)$, such that the probability of random events is $p(E_1, A) = p(E_2, \Psi(A))$, where the experiments E_1 and E_2 are isomorphic.

That is, two fields of events $S(E_1)$ and $S(E_2)$ are isomorphic if there exists one-to-one mapping $\Psi: S(E_1) \to S(E_2)$, which is isotonic in respect with ordering of correspondent events $S(E_1)$ and $S(E_2)$ in the Boolean algebras and has the inverse isotonic property: $\forall A \in S(E_1)$ $p(E_1, A) = p(E_2, \Psi(A))$. This mapping Ψ is said to be a probabilistic isomorphism.

Theorem 7 [38]. The fields of events $S(E_c)$ and $S(\tilde{E}_c)$ generated by the composite experiments $E_c = \{E_1, E_2\}$ and $\tilde{E}_c = \{E_2, E_1\}$ are isomorphic if the random experiments E_1 and E_2 are commutative.

Using the above theorem we can introduce addition and multiplication of random variables x and y, produced in random experiments E_1 and E_2, respectively. The sum $x+y$ and the product xy take on their values in composite experiments $E_c = (E_1, E_2)$, and, $y+x$ and yx take on their values in composite experiment $\tilde{E}_c = (E_2, E_1)$. Let us consider the random value $x+y$ as a result of a random experiment E_c with numerical base $B_{E_c} = B_{E_1} \oplus B_{E_2} = \{x+y : x \in B_{E_1}, y \in B_{E_2}\}$, where $B_{E_i}, i = 1,2$ is the numerical bases of the random experiment E_i.

The random variable $y+x$ is identified with a random experiment $\tilde{E}_c$ with numerical base $B_{\tilde{E}_c} = B_{E_c} \oplus B_{E_2} = B_{E_1} \oplus B_{E_2} = B_{E_c}$. The field of events $S(E_c)$ and $S(\tilde{E}_c)$ are isomorphic when random experiments E_1 and E_2 are commutative.

Then, the random variables $x+y$ and $y+x$ are isomorphic. If isomorphic objects are identified, we can write $x+y = y+x$. The similar results is true for multiplication: $xy = yx$. Notice, that for the random variables $x+y$ and $y+x$ the fields of events $S(E_c)$ and $S(\tilde{E}_c)$ coincide, since they are sets of all possible subsets of numerical sets $B_{E_c} = B_{\tilde{E}_c}$, and therefore the random experiments E_c and $\tilde{E}_c$ generate the identical distributions of probabilities on these fields.

6. Conclusion

The new frequency-based approach based on the concept of a characteristic matrix of a random experiment eliminates the need to formalize the von Mises rule for acceptable collective selection. In the new model, rows and columns of the characteristic matrix automatically form collectives. Using the topological properties of the sets of numbers represented by the rows and columns of the characteristic matrix makes it easy to apply the new randomness criterion in practice. In addition, we propose correct way to define arithmetic operations on random variables in the frame of new model.

7. References

[1] A. Turing, Computing machinery and intelligence, Mind 236 (1950) 433–460. doi: 10.1093/mind/LIX.236.433.

[2] J. von Neumann, Various techniques used in connection with random digits, in: (Eds.) A. Householder, G.E. Forsythe, and H.H. Germond Monte Carlo Method. National Bureau of Standards Applied Mathematics Series 12 (1951): 36–38.

[3] R. Downey, Randomness, Computation and Mathematics, in: S.B. Cooper, A. Dawar, B. Löwe (Eds.), How the World Computes, CiE 2012, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, 2012, vol. 7318. doi: 10.1007/978-3-642-30870-3_17.

[4] P.M.B. Vitanyi Randomness, 2001, arXiv:math/0110086v2. URL: https://arxiv.org/abs/math/0110086.

[5] L. Li, P.M.B. Vitanyi, An Introduction to Kolmogorov Complexity and its Applications. Third Edition, Springer-Verlag, New York, 2008.

[6] A. Wald, Die Wiederspruchsfreiheit des Kollektivbegriffes der Wahrscheinlich-keitsrechnung, Ergebnisse eines Mathematischen Kolloquiums 8 (1937) 38-72.

[7] A. Church, On the concept of a random sequence, Bull. AMS, 46 (1940) 130–135. doi: 10.1090/S0002-9904-1940-07154-X.

[8] J. Ville Etude critique de la notion de collectif, Gauthiers-Villars, Paris, 1939.

[9] M. van Lambalgen, Randomness and foundations of probability: von Mises's axiomatisation of random sequences, in: T. Ferguson et al. (Eds.), Probability, Statistics and Game Theory: papers in honour of David Blackwell. Institute for Mathematical Statistics Monograph Series, 20 (1996) 347–367. doi: 10.1214/lnms/1215453582.

[10] M. van Lambalgen, Von Mises' definition of random sequences reconsidered, J. Symb. Logic 52 (1987) 725–755. doi: 10.1017/S0022481200029728 .

[11] M. van Lambalgen, The axiomatisation of randomness, J. Symb. Logic 55 (1987) 1143–1167. doi: 10.2307/2274480.

[12] M. van Lambalgen, Independence, randomness and the axiom of choice, J. Symb. Logic 57 (1992) 1274–1304. doi: 10.2307/2275368.

[13] M. Frechet, Expose et discussion de quelques recherches recentes sur les fondements du calcul des probabilities, in: Colloque consacre au calsul des probabilites. Proceedings of the conference held at the Universite de Geneve, 1937, pp. 22–55.

[14] A.N. Kolmogorov, Grundbegriffe der Wahrscheinlichkeitsrechnung. Ergebnisse der Mathematic und ihrer Grenzgebiete, Springer-Verlag, Berlin, Heidelberg, 1933. doi: 0.1007/978-3-642-49888-6.

[15] A.N. Kolmogorov, Basic concepts of probability theory, Moscow, Nauka, 1974 (In Russian).

[16] A.N. Kolmogorov, On tables of random numbers, Sankhya. Indian J. Statist. Ser. A. 25 (1963) 369–376. Reprinted: Theoretical Computer Science 207 (1998) 387-395. doi: 10.1016/S0304-3975(98)00075-9

[17] V.A. Uspensky, Four algorithmic faces of randomness, Math. Prosveschenie 10 (2006) 71–108 (in Russian).

[18] V.G. Vovk, G.R. Shafer, Kolmogorov's Contributions to the Foundations of Probability, Problems of Information Transmission, 39 (2003) 21–31. doi: 10.1023/A:1023674330295.

[19] R. von Mises, Wahrscheinlichkeitsrechnung und ihre Adwendung in der Statistik und theoretischen Physik, Springer-Verlag, Berlin, Heidelberg, 1928. doi: 0.1007/978-3-662-36230-3

[20] A.N. Kolmogoroff, On the Logical Foundations of Information Theory and Probability Theory, Problems Inform. Transmission 5 (1969) 1-4.

[21] A.N. Kolmogorov, Combinatorial foundations of information theory and the calculus of probabilities, Russian Math. Surveys 38 (1983) 29-40. .

[22] A.N. Kolmogorov, On logical foundation of probability theory, in: Probability Theory and Mathematical Statistics. Lecture Notes in Mathematics, vol. 1021, Springer–Verlag, Berlin, Heidelberg, 1983, pp. 1-5. doi: 10.1007/BFb0072897.

[23] R.J. Solomonoff, A preliminary report on a general theory of inductive inference, Technical Report ZTB–138. Zator Company, Cambridge, MA, USA, November 1960.

[24] R.J. Solomonoff, A formal theory of inductive inference, Part I, Inform. and Control 7 (1964) 1–22. doi: 10.1016/S0019-9958(64)90223-2.

[25] R.J. Solomonoff, A formal theory of inductive inference, Part II, Inform. and Control 7 (1964) 224–254. doi: 10.1016/S0019-9958(64)90131-7.

[26] G. Chaitin, On the length of programs for computing finite binary sequences: statistical considerations, J. Assoc. Comput. Mach. 16 (1969) 145–159. doi: 10.1145/321495.321506.

[27] E.A. Asarin, Some Properties of Kolmogorov Δ-Random Finite Sequences, Theory Probab. Appl. 32 (1987) 507–508. doi: 10.1137/1132070.

[28] E.A. Asarin, On the Equivalence of Being Typical and Chaotic for Finite Objects, Theory Probab. Appl., 35 (1991), 760–761. doi: 10.1137/1135108.

[29] A. Kh. Shen, The notion of (α,β)-stochasticity in Kolmogorov's sense and its properties, Dokl. Akad. Nauk SSSR 271 (1983) 1337–1340.

[30] V.V. Vyugin, On Nonstochastic Objects, Problems Inform. Transmission 21 (1985) 77–83.

[31] V.V. Vyugin, On Randomness Defect of a Finite Object Relative to Measures with Given Complexity Bounds, Theory Probab. Appl. 32 (1987) 508–512.

[32] A.L. Semenov, A.A. Muchnik, An Improvement of Kolmogorov's Estimates Related to Random Number Generators and a Definition of Randomness in terms of complexity, Dokl. Akad. Nauk 68 (2003) 132–134.

[33] V.I. Arnold, Topology and statistics of formulae of arithmetic, Russian Math. Surveys 58 (2003) 637–664. doi: 10.4213/rm641.

[34] P. Martin-Löf, The definition of random sequences, Inform. and Control 9 (1966) 602–619. doi: 10.1016/S0019-9958(66)80018-9.

[35] C.P. Schnorr, Process complexity and effective random tests, J. of Computer and System Sciences 7 (1973) 376–388. doi: 10.1016/S0022-0000(73)80030-3.

[36] L.A. Levin, The concept of a random sequence, Dokl. Akad. Nauk SSSR 212 (1976) 548–550.

[37] L.A. Levin, Uniform tests for randomness, Dokl. Akad. Nauk SSSR, 227 (1976) 33–35.

[38] Yu.I. Petunin. D.A. Klyushin D.A., A structural approach to solving the 6th Hilbert problem, Theor. Probability and Math. Statist. 71 (2005) 165-173. doi: 10.1090/S0094-9000-05-00656-3.

[39] G. Birkhoff, Lattice Theory. AMS Colloquium Publication, 3rd edition, 1967.

[40] J.C. Oxtoby, Measure and Category Springer-Verlag, New York, 1971. doi: 10.1007/978-1-4615-9964-7.