Preface

The notion of algorithmic complexity (also sometimes called algorithmic entropy) appeared in the 1960s in between the theory of computation, probability theory, and information theory.

The idea of A. N. Kolmogorov was to measure the amount of information in finite objects (and not in random variables, as it is done in classical Shannon information theory). His famous paper [78], published in 1965, explains how this can be done (up to a bounded additive term) using the algorithmic approach.

Similar ideas were suggested a few years earlier by R. Solomonoff (see [187] and his other papers; the historical account and reference can be found in [103]).

The motivation of Solomonoff was quite different. He tried to define the notion of a priori probability. Imagine there is some experiment (random process) and we know nothing about its internal structure. Can we say something about the probabilities of different outcomes in this situation? One can relate this to the complexity measures saying that simple objects have greater a priori probability than complex ones. (Unfortunately, Solomonoff’s work become popular only after Kolmogorov mentioned it in his paper.)

In 1965 G. Chaitin (then an 18-year-old undergraduate student) submitted two papers [28] and [29]; they were published in 1966 and 1969, respectively. In the second paper he proposed the same definition of algorithmic complexity as Kolmogorov.

The basic properties of Kolmogorov complexity were established in the 1970s. Working independently, C. P. Schnorr and L. Levin (who was a student of Kolmogorov) found a link between complexity and the notion of algorithmic randomness (introduced in 1966 by P. Martin-Löf [115]). To achieve this, they introduced a slightly different version of complexity, the so-called monotone complexity. Also Solomonoff’s ideas about a priori probability were formalized in the form of prefix complexity, introduced by Levin and later by Chaitin. The notions of complexity turned out to be useful both for theory of computation and probability theory.

Kolmogorov complexity became popular (and for a good reason: it is a basic and philosophically important notion of algorithm theory) after M. Li and P. Vitányi published a book on the subject [103] (first edition appeared in 1993). Almost everything about Kolmogorov complexity that was known at the moment was covered in the book or at least mentioned as an exercise. This book also provided a detailed historical account, references to first publications, etc. Then the books of C. Calude [25] and A. Nies [147] appeared, as well as the book of R. Downey and D. Hirschfeldt [49]. These books cover many interesting results obtained recently.

---

1Kolmogorov wrote in [79], “I came to a similar notion not knowing about Solomonoff’s work.”
Our book does not try to be comprehensive (in particular, we do not say much about the recent results mentioned above). Instead, we tried to select the most important topics and results (both from the technical and philosophical viewpoints) and to explain them clearly. We do not say much about the history of the topic: as is usually done in textbooks, we formulate most statements without references, but this does not mean (of course) any authorship claim.

We start the book with a section “What is this book about?” where we try to give a brief overview of the main ideas and topics related to Kolmogorov complexity and algorithmic randomness so the reader can browse this section to decide whether the book is worth reading.

As an appendix we reproduce the (English translation) of a small brochure written by one of the authors (V.U.), based on his talk for high school students and undergraduates (July 23, 2005) delivered during the “Modern Mathematics” Summer School (Dubna near Moscow); the brochure was published in 2006 by MCCME publishing house (Moscow). The lecture was devoted to different notions of algorithmic randomness, and the reader who has no time or incentive to study the corresponding chapters of the book in detail can still get some acquaintance with this topic.

Unfortunately, the notation and terminology related to Kolmogorov complexity is not very logical (and different people often use different notation). Even the same authors use different notation in different papers. For example, Kolmogorov used both the letters $K$ and $H$ in his two basic publications [78, 79]. In [78] he used the term “complexity” and denoted the complexity of a string $x$ by $K(x)$. Later in [79] he used the term “entropy” (borrowed from Shannon information theory) for the same notion that was called “complexity” in [78]. Shannon information theory is based on probability theory; Kolmogorov had an ambitious plan to construct a parallel theory that does not depend on the notion of probability. In [79] Kolmogorov wrote, using the same word entropy in this new sense:

The ordinary definition of entropy uses probability concepts, and thus does not pertain to individual values, but to random values, i.e., to probability distributions within a group of values. [...] By far, not all applications of information theory fit rationally into such an interpretation of its basic concepts. I believe that the need for attaching definite meanings to the expressions $H(x|y)$ and $I(x|y)$, in the case of individual values $x$ and $y$ that are not viewed as a result of random tests with a definite law of distribution, was realized long ago by many who dealt with information theory.

As far as I know, the first paper published on the idea of revising information theory so as to satisfy the above conditions was the article of Solomonoff [187]. I came to similar conclusions, before becoming aware of Solomonoff’s work in 1963–1964, and published my first article on the subject [78] in early 1965.
The meaning of the new definition is very simple. Entropy $H(x|y)$ is the minimal [bit] length of a [...] program $P$ that permits construction of the value of $x$, the value of $y$ being known,

$$H(x|y) = \min_{A(P,y,x)} I(P).$$

This concept is supported by the general theory of “computable” (partially recursive) functions, i.e., by theory of algorithms in general.

[...] The preceding rather superficial discourse should prove two general theses.

1) Basic information theory concepts must and can be founded without recourse to the probability theory, and in such a manner that “entropy” and “mutual information” concepts are applicable to individual values.

2) Thus introduced, information theory concepts can form the basis of the term random, which naturally suggests that randomness is the absence of regularities.\(^2\)

And earlier (April 23, 1965), giving a talk “The notion of information and the foundations of the probability theory” at the Institute of Philosophy of the USSR Academy of Sciences, Kolmogorov said:

So the two problems arise sequentially:

1. Is it possible to free the information theory (and the notion of the “amount of information”) from probabilities?

2. It is possible to develop the intuitive idea of randomness as incompressibility (the law describing the object cannot be shortened)?

(The transcript of his talk was published in [85] on p. 126).

So Kolmogorov uses the term “entropy” for the same notion that was named “complexity” in his first paper, and denotes it by letter $H$ instead of $K$.

Later the same notion was denoted by $C$ (see, e.g., [103]) while the letter $K$ is used for prefix complexity (denoted by $KP(x)$ in Levin’s papers where prefix complexity was introduced).

Unfortunately, attempts to unify the terminology and notation made by different people (including the authors) have lead mostly to increasing confusion. In the English version of this book we follow the terminology that is most used nowadays, with few exceptions, and we mention the other notation used. For the reader’s convenience, a list of notation used (p. xv) and index (p. 505) are provided.

Acknowledgments

In the beginning of the 1980s Kolmogorov (with the assistance of A. Semenov) initiated a seminar at the Mathematics and Mechanics Department of Moscow State (Lomonosov) University called “Description and computation complexity”; now the seminar (still active) is known as the “Kolmogorov seminar”. The authors are deeply grateful to their colleagues working in this seminar, including A. Zvonkin.

\(^2\)The published English version of this paper says “random is the absence of periodicity”, but this evidently is a translation error, and we correct the text following the Russian version.
E. Asarin, V. Vovk (they were Kolmogorov’s students), S. Soprunov, V. Vyun-
gin, A. Romashchenko, M. Vyalii, S. Tarasov, A. Chernov, M. Vyugin, S. Posit-

The authors express their gratitude to all the people who helped them to prepare the Russian edition, especially Marina Feigelman who made a drawing for its cover, Olga Lehtonen who performed the cover design, and Victor Shuvalov who helped a lot with typesetting.

The authors were supported by the International Science Foundation (Soros foundation), STINT (Sweden), Russian Fund for Basic Research (01-01-00493-
a, 01-01-01028-a, 06-01-00122-a, 09-01-00709-a, 12-01-00864-a), CNRS, and ANR (France, ANR-08-EMER-008 NAFIT and ANR-15-CE40-0016-01 RaCAF grants).

The book was made possible by the generous support of our colleagues, including Bruno Bauwens, Laurent Bienvenu, Harry Buhrman, Cris Calude, Bruno Durand, Péter Gács, Denis Hirschfeldt, Rupert Hölzl, Mathieu Hoyrup, Michal Koucký, Leonid Levin, Wolfgang Merkle, Joseph Miller, Andre Nies, Christopher Porter, Jan Reimann, Jason Rute, Michael Sipser, Steven Simpson, Paul Vitányi, Sergey Vorobyov, and many others.

We are thankful to American Mathematical Society (in particular, Sergei Gelfand) for the suggestion to submit the book for publication in their book program and for the kind permission to keep the book available freely in electronic form at our homepages. We thank the (anonymous) referees for their attention and suggestions, and Jennifer Wright Sharp for correcting our (numerous) English language errors.

For many years the authors had the privilege to work in a close professional and personal contact with Andrej Muchnik (1958–2007), an outstanding mathematician, a deep thinker, and an admirable person, who participated in the work of the Kolmogorov seminar and inspired a lot of work done in this seminar. We devote this book to his memory.

A. Shen, V. Uspensky, N. Vereshchagin
November 1, 2016