PREFACE

Mathematics and sciences, including political science have always involved many problems requiring large computations and sometimes, thousands of people. A century ago, the word "computer" meant a human being performing those computations. The top-level scientists, like Gottfried Leibniz, Lady Ada Lovelace, Alan Turing, and others were thinking how to automatize those computations. The breakthrough happened in the thirties-forties of the previous century, when Alan Turing proved the theorem about the universal program and John von Neumann developed the scheme of the universal computer machine, which all of us have used since then – see Chapter 23. The technology was ready, and the very first electronic computer "ENIAC" executed its initial programs in 1945. Since then, "computer" has meant an electronic device.

ENIAC declassifying in 1946 led to the explosive growth of the number of electronic computers, and correspondingly, to the growth of the number of people working with computers. Those people were mostly mathematicians, but very soon mathematics departments could not provide enough cadres, and the colleges and universities had to start teaching different courses to the new "computer scientists," whose first mathematical course was often called *Discrete Mathematics* or *Finite Mathematics*. Within a few years, discrete mathematics has become an independent mathematical discipline. Paul Halmos predicted [25, p. 19] that in the foreseeable future ". . . discrete mathematics will be an increasingly useful tool in the attempt to understand the world, and ... analysis will therefore play a proportionally smaller role."

Textbooks for the new discipline quickly followed, from concise lecture notes to Kenneth Rosen's monumental treatise [43], whose 8th edition (2019) amounts to more than 1000 pages. But every new generation meets their own challenges and requires new textbooks, see, e.g., [42], whatever good are the previous ones. A quarter century back, it was important to

emphasize the algorithmic nature of discrete mathematics [37]. Now the 20-30-year-old discussions – see, e.g., [36], are mostly forgotten. The Internet security issues are more important than ever before, and this textbook was written with strengthened attention to these topics. A short version of these lectures was initially taught in 1971 and has evolved during the following half-century, being greatly influenced by the times and people – by my students, friends, and colleagues on both sides of the Atlantic.

To describe the contents of this book in more detail, let us notice that our thoughts are initially appeared as electrical-chemical potentials in the "grey matter" in our brains. To communicate our thoughts to other people, those potentials must be converted into electrical potentials governing oscillations of our vocal cords, and the latter create the fluctuations of the air pressure, carrying our speech. When these acoustical oscillations reach our ears, all the transformations are done in the opposite direction. Thus, the information that we create and obtain, is to be encoded and decoded in many different ways. These transformations are studied by coding theory, which is an important part of the discrete mathematics. However, to perform those conversions, we must represent the signals in a suitable form, i.e., as Boolean functions, and the book starts with an exposition of elementary logic and Boolean calculus. What is more, we often do not want other people to know the outcomes of our dealings with information, hence giving rise to the cybersecurity issues.

Boolean functions are maps, and chapters devoted to the functions, sets, and relations follow. We also consider in more detail predicates and quantifiers, which are necessary in many applications. When it is appropriate, we include expositions of some applications of these mathematical questions to computer-related issues, such as, e.g., relational databases or hashing functions. Several classical discrete mathematics topics, namely combinatorics, graph theory, complete systems of functional elements, etc., and some applications like finite automata, necessary for the potential users of the book, are included. These developments are based upon some algebraic structures, like groups, rings, fields, and Boolean Algebras. That allowed us to consider certain cryptography issues, in particular, the Discrete Logarithm Problem.

The book also contains chapters about number theory and game theory. No discussion of cryptography is possible these days without number-theoretical issues, like clock arithmetic and CRT. That background allows us to consider affine ciphers and some procedures of sharing secrets. The book also includes a chapter about game theory, the topic, whose inclusion in a discrete mathematics text is long overdue.

It is not the first text, which uses cryptology to enhance the teaching of mathematics – see, e.g., an interesting note [7]. Due to the volume restrictions, specifically crypto-questions are not covered here as much as they deserve. If the discussion of crypto–issues would deviate too far from the discrete mathematics, we are to stop there. To proceed farther, we would recommend the excellent books [2, 13, 14, 40]. The table of contents shows in more detail, what is in the book.

Many sections contain more material than can be reasonably taught at a two-hour class. That allows a lecturer some freedom of choice, and also provides the material for the student's individual work.

No mathematical exposition is possible without mathematical induction, which is unknown to most high school students. The author's experience shows though, that the method of mathematical induction, being properly explained, is well accessible to college freshmen. The very first chapter of the book is devoted to mathematical induction and to a very brief discussion of elementary functions, necessary in the textbook. That sets out the prerequisite level for the whole book. It is supposed that most college freshmen, independently upon their specialization, will benefit from this textbook. However, those lower prerequisites brought an unexpected problem. Certain language, which the college sophomores usually know quite well, can be unfamiliar to some potential readers. Thus, the book explains in more detail than usual, certain parlance, e.g., "necessary and sufficient conditions" or the like. This is especially necessary and useful now due to proliferation of on-line courses, where the student often cannot ask immediately certain "simple" questions. The reader, who is fluent with that material, can skip this material with no harm.

Of course, this is a mathematics textbook, and its reading requires concentration. To develop this culture, the reader is supposed to solve at least some of the included problems, and to analyze the suggested solutions. This is especially important in the times of online education. We remark in passing that it is not unusual, when the students find new solutions of old problems or suggest new problems. The author always welcomes any such input. The book contains more than 600 problems of various levels of difficulty. All of the exercises for the students' individual work are placed in the end of chapters. Many other problems can be found in the cited literature, e.g., in [19].

We thank many people for help. Parts of the book were discussed at the DIMACS Center at Rutgers University during the *Reconnect* conferences. The Reconnect-2019 workshop at the Champlain College in Burlington,

VT, was invaluable in finalizing this project. The present author, as anyone else, has its favorite books; I cannot list all of them, but I want to mention delightful books by M. Schroeder [45] and by L. Lovasz, J. Pelikan and K. Vesztergombi [35]. We want to personally thank the following people: Midge Cozzens, Fred Roberts, David Pallai and the staff of Mercury Learning and Information, who made this project possible.

Alexander I. Kheyfits, PhD.
September 2021