Introduction

The goal of this book is to showcase new directions in group theory motivated by computer science. The subtitle (GAGTA book) reflects the fact that the book follows the course of the Geometric and Asymptotic Group Theory with Applications (GAGTA) conference series in transitioning from geometric group theory, which dominated group theory in the late twentieth century, to group theory of the twenty-first century, which has strong connections to computer science.

Since its inception in the 1980s, geometric group theory produced a great deal of important results that were not limited to metric properties of groups, but included also results (such as a solution of Tarski's problems, for example) that can be formulated without mentioning any metric. Now that geometric group theory is drifting further and further away from group theory to geometry, it is natural to look for new tools and new directions in group theory, and this is what we are trying to do in the present book.

In his "Millennium problems", Smale points out that he considers the "P versus NP" problem a gift to mathematics from computer science. The same actually goes for the whole theory of computational complexity, and a notable focus of this book is on the (time and/or space) complexity of various algorithmic problems in group theory, including "traditional" problems such as the word, conjugacy, subgroup membership and isomorphism problems, as well as problems recently influenced by theoretical computer science, including the knapsack problem, the Post correspondence problem and others. Along with the worst-case complexity of algorithms we address the *generic-case* complexity, or complexity on random inputs (see Chapter 1), which is more relevant to real-life applications, particularly in information security. The very concept of randomness is very important and nontrivial for infinite groups. We discuss various approaches to defining random elements, random subgroups and even random groups in Chapters 1 and 2. Of particular interest is the concept of a random matrix, since it admits several different approaches due to the versatile nature of matrices (see Chapter 3).

Randomness is closely related to how one defines complexity of a given element of a given set, which is also important for understanding computational complexity of algorithms (operating on a given set), since the latter is defined as a function of complexity of individual elements. For example, for group elements, the idea of using Kolmogorov complexity as an alternative to the more traditional geodesic length leads to spectacular applications of *data compression* techniques from computer science to algorithmic problems in group theory, specifically the word problem. This is described in Chapter 4.

We also address, in Chapter 5, an emerging area named *discrete optimization in groups*, which deals with adaptations of several well-known problems in computer

https://doi.org/10.1515/9783110667028-201

science (e. g., the subset sum problem, the knapsack problem and the Post correspondence problem) in various groups typically studied in combinatorial group theory.

Finally, in the concluding Chapter 6 we describe several algorithmic problems in group theory motivated by (public-key) cryptography. This includes not only a shift of paradigm from decision to search problems, but also "brand new" problems, notably the hidden subgroup problem (HSP). The importance of the latter problem is due to the fact that Shor's polynomial-time quantum algorithm (for the factoring and discrete logarithm problems), as well as several of its extensions, relies on the ability of quantum computers to solve the HSP for finite abelian groups. It is speculated that for some non-abelian groups, the HSP may be resilient to quantum algorithms and therefore those groups might serve as platforms for so-called *post-quantum* cryptographic schemes. We note that the HSP was originally defined for finite groups, but some authors recently offered ways to generalize it to infinite groups.

Acknowledgments
We are grateful to Moses Ganardi, Dima Grigoriev, Daniel König, Philipp Reh, and Paul Schupp for many valuable comments and discussions. The work of Ilya Kapovich was partially supported by the NSF grants DMS-1710868 and DMS-1905641. The work of Markus Lohrey was partially supported by the DFG grant Lo748/12-1. The work of Vladimir Shpilrain was partially supported by the ONR grant N000141512164. The work of Pascal Weil was partially supported by Project DeLTA, ANR-16-CE40-0007.

Frédérique Bassino, Ilya Kapovich, Markus Lohrey,
Alexei Myasnikov, Cyril Nicaud, Andrey Nikolaev,
Igor Rivin, Vladimir Shpilrain, Alexander Ushakov, Pascal Weil