Interactions between Group Theory, Cyber Security, Artificial Intelligence, and Quantum Computation

Delaram Kahrobaei
Department of Computer Science
University of York
Deramore Lane York YO10 5GH
delaram.kahrobaei@york.ac.uk

In this talk, I explore how group theory playing a crucial role in data science and artificial intelligence as well as cyber security and quantum computation. At the same time, how computer science for example machine learning algorithms and computational complexity could help group theorists so tackle their open problems.

Symmetry is present in all forms in the natural and biological structures as well as man-made environments. Computational symmetry applies group-theory to create algorithms that model and analyze symmetry in real data set. The use of symmetry groups in optimizing the formulation of signal processing and machine learning algorithms can greatly enhance the impact of these algorithms in many fields of science and engineering where highly complex symmetries exist.

At the same time, Machine Learning techniques could help with solving long standing group theoretic problems. For example, in the paper [J. Gryak (University of Michigan, Data Science Institute), R. Haralick (The City University of New York, the prize recipient of International Association for Pattern Recognition), D. Kahrobaei, Solving the Conjugacy Decision Problem via Machine Learning, Experimental Mathematics, Taylor & Francis (2019)] the authors use machine learning techniques to solve the conjugacy decision problem in a variety of groups. Beyond their utilitarian worth, the developed methods provide the computational group theorist a new digital "sketchpad" with which one can explore the structure of groups and other algebraic objects, and perhaps yielding heretofore unknown mathematical relationships.

Graph theoretic problems have been of interest of theoretical computer scientists for many years, especially the computational complexity problems for such algorithmic problems. Such studies have been fruitful for one of the millennium problems (P vs NP) of the Clay Math Institute. Since graph groups are uniquely defined by a finite simplicial graph and vice versa, it is clear that there is a natural connection between algorithmic graph theoretic problems and group theoretic problems for graph groups. Since the graph theoretic problems have been of central importance in complexity theory, it is natural to consider some of these graph theoretic problems via their equivalent formulation as group

theoretic problems about graph groups. The theme of the paper [Algorithmic problems in right-angled Artin groups: Complexity and applications, R. Flores, D. Kahrobaei, T. Koberda, J. of Algebra, Elsevier 2019.] is to convert graph theoretic problems for finite graphs into group theoretic ones for graph groups (a.k.a. right-angled Artin) groups, and to investigate the graph theory algebraically. In doing so, new approaches to resolving problems in complexity theory become apparent. The authors are primarily motivated by the fact that some of these group theoretic problems can be used for cryptographic purposes, such as authentication schemes, secret sharing schemes, and key exchange problems.

In the past couple of decades many groups have been proposed for cryptography, for instance: polycyclic groups for public-key exchanges, digital signatures, secret sharing schemes (Eick, Kahrobaei), hyperbolic groups for private key encryption (Chatterji-Kahrobaei), p-groups for multilinear maps (Kahrobaei, Tortora, Tota) among others. [J. Gryak, D. Kahrobaei, The Status of the Polycyclic Group-Based Cryptography: A Survey and Open Problems, Groups Complexity Cryptology, De Gruyter (2016).]

Most of the current cryptosystems are based on number theoretic problems such discrete logarithm problem (DLP) for example Diffie-Hellman key-exchange. Recently there has been some natural connections between algorithmic number theoretic and algorithmic group theoretic problems. For example, it has been shown that for a different subfamily of metabelian groups the conjugacy search problem reduces to the DLP. [J. Gryak, D. Kahrobaei, C. Martinez-Perez, On the conjugacy problem in certain metabelian groups, Glasgow Math. J., Cambridge Univ. Press (2019).]

In August 2015 the National Security Agency (NSA) announced plans to upgrade security standards; the goal is to replace all deployed cryptographic protocols with quantum secure protocols. This transition requires a new security standard to be accepted by the National Institute of Standards and Technology (NIST).

One goal of cryptography, as it relates to complexity theory, is to analyze the complexity assumptions used as the basis for various cryptographic protocols and schemes. A central question is determining how to generate intractable instances of these problems upon which to implement an actual cryptographic scheme. The candidates for these instances must be platforms in which the hardness assumption is still reasonable. Determining if the group-based cryptographic schemes are quantum-safe begins with determining the groups in which these hardness assumptions are invalid in the quantum setting. In what follows we address the quantum complexity of the Hidden Subgroup Problem (HSP) to determine the groups in which the hardness assumption still stands. The Hidden Subgroup Problem (HSP) asks the following: given a description of a group G and a function f from G to X for some finite set X is guaranteed to be strictly H-periodic, i.e. constant and distinct on left (resp. right) cosets of a subgroup H ¡ G, find a generating set for H. Group-based cryptography could be shown to be post-quantum if the underlying security problem is NP-complete or unsolvable; firstly, we need to analyze the problem's equivalence to HSP, then analyze the applicability of Grover's search problem. [K. Horan, D. Kahrobaei, Hidden Subgroup Problem and Post-quantum Group-based Cryptography, Springer Lecture Notes in Computer Science 10931, 2018].