1176-00-91

Delaram Kahrobaei* (dkahrobaei@gc.cuny.edu) and Ramon Flores, , Spain, and Thomas Koberda. NP-Complete Problems in Graph Groups and connection to Post-quantum Cryptography.

Graph groups admit a presentation where the only relations are commutativity relations which are codified in a finite simplicial graph. The fact that these groups are defined by means of a graph imply that there is a tight 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. Motivated by the fact that some of these group theoretic problems can be used for cryptographic purposes, such as authentication schemes, secret sharing schemes, zero-knowledge proofs, hash functions and key exchange protocols. Flores-Kahrobaei-Koberda, in a series of recent papers in [J of Top. Anal, Linear Alg App, Proc. AMS, J of Alg.] have considered these groups as a promising platform for several cryptographic schemes. (Received January 15, 2022)