Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

The complexity of the equation solvability problem over nilpotent groups[☆,☆☆]

Attila Földvári

Institute of Mathematics, University of Debrecen, Pf. 400, Debrecen, 4002, Hungary

ARTICLE INFO

Article history:
Received 27 April 2017
Available online xxxx
Communicated by Derek Holt

MSC:
20F10
20F18
13P15

Keywords:
Nilpotent groups
Equation solvability
Equivalence
Computational complexity
Polynomial time algorithm

ABSTRACT

Let $\mathbf{G}$ be a finite, nilpotent group. The computational complexity of the equation solvability problem over $\mathbf{G}$ is known to be in P. The complexity is understood in the length of the equation over $\mathbf{G}$. So far the fastest algorithm to decide whether or not an equation of length n has a solution over $\mathbf{G}$ was running in $O\left(n^{|\mathbf{G}|^{|\mathbf{G}|^{\cdots^{|\mathbf{G}|^{|\mathbf{G}|}}}}}\right)$ time. Here the height of the tower is the nilpotency class of $\mathbf{G}$. We prove that one can decide in $O\left(n^{\frac{1}{2}|\mathbf{G}|^2\log|\mathbf{G}|}\right)$ time whether an equation of length n has a solution over $\mathbf{G}$. The key ingredient of the proof is to represent group expressions using the polycyclic presentation of p-groups.

1. Introduction

One of the earliest problems of algebra is the equation solvability problem. This question asks whether or not an equation over a finite algebraic structure has a solution.

[☆] The research was supported by the National Research, Development and Innovation Fund of Hungary, financed under the K109185 and FK 124814 funding schemes.

[☆☆] EMBERI ERŐFORRÁS TÁMOGATÁSKEZELŐ

E-mail address: foldvari.attila@science.unideb.hu.

https://doi.org/10.1016/j.jalgebra.2017.10.002
0021-8693/© 2017 Elsevier Inc. All rights reserved.

Typical examples are finding a root of a polynomial over a field, or solving a congruence over the residue class ring $\mathbb{Z}_m$. Recently, many such classical problems arose in a new perspective, namely to consider their computational complexity.

The *equation solvability problem over a finite group* $\mathbf{G}$ asks whether or not two group expressions (i.e. products of variables and elements of $\mathbf{G}$) can attain the same value for some substitution from $\mathbf{G}$. In other words, for group expressions S, T one needs to find whether or not the equation $S = T$ has a solution over $\mathbf{G}$. Since $\mathbf{G}$ is finite, this problem is decidable by checking all possible substitutions from $\mathbf{G}$. In this paper we investigate the computational complexity of the equation solvability problem where $\mathbf{G}$ is a finite nilpotent group.

Goldmann and Russel [1,2] proved that if $\mathbf{G}$ is not solvable, then the equation solvability problem is NP-complete, while if $\mathbf{G}$ is nilpotent then the equation solvability problem over $\mathbf{G}$ is in P. Here, the computational complexity is understood in the length of the two input group expressions. In their papers, Goldmann and Russell [1,2] reduce the equation solvability problem over a finite nilpotent group $\mathbf{G}$ to recognizing languages by non-uniform finite automata over $\mathbf{G}$. In their reduction they apply the results of Péladeau and Thérien [10,11] in a fundamental manner. This way, it is easy to get lost in the chain of thoughts if one wants to recover how the algorithm of Goldmann and Russel manipulates the input group expressions S and T in order to determine whether or not the equation $S = T$ has a solution over $\mathbf{G}$. Furthermore, the algorithm is known to be polynomial in the sizes of S and T, but the degree of this polynomial is not explicitly stated. The reduction in [1,2] applies Ramsey's theorem, suggesting that the degree of the polynomial is multiply exponential.

Later Horváth [4] gave a straight proof for nilpotent groups only using group expressions and directly arriving at the Ramsey argument. Horváth proves that for a finite nilpotent group $\mathbf{G}$ the image of any group expression can be computed by substitutions where at most $|\mathbf{G}|^{|\mathbf{G}|^{\cdots|\mathbf{G}|^{|\mathbf{G}|}}}$-many variables differ from the identity element. Here, the height of the tower is the nilpotency class of $\mathbf{G}$. This yields to an $O\left(n^{|\mathbf{G}|^{|\mathbf{G}|^{\cdots|\mathbf{G}|^{|\mathbf{G}|}}}}\right)$ time algorithm for checking equations of length n. Horváth explicitly asks in [4, Problem 3] whether the exponent of the time complexity can be bounded by a polynomial in the size of the group $\mathbf{G}$.

In this paper we answer Horváth's question [4, Problem 3] by decreasing the exponent of the time complexity significantly. With the polycyclic presentation of p-groups we give a completely new approach to representing group expressions. We prove that for a p-group of order p^α, and for a group expression T over $\mathbf{P}$ of length n, the image of T can be computed in $O\left(n^{\frac{1}{2}(2p-2)^\alpha \alpha}\right)$ time (see Lemma 4 for details). Let log denote the base 2 logarithm. An immediate consequence for a nilpotent group $\mathbf{G}$ is that equation solvability over $\mathbf{G}$ can be decided in polynomial time, where the degree of the polynomial is $\frac{1}{2}\left|\mathbf{G}\right|^2 \log\left|\mathbf{G}\right|$: