Journal of Algebra 433 (2015) 208–230

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

The complexity of the equivalence and equation solvability problems over meta-Abelian groups

Gábor Horváth

Institute of Mathematics, University of Debrecen, Pf. 12, Debrecen, 4010, Hungary

ARTICLE INFO

Article history:
Received 25 July 2014
Available online 17 April 2015
Communicated by Derek Holt

MSC:
20F10
13M10
20F70
68Q17

Keywords:
Finite meta-Abelian groups
Equivalence
Equation solvability
Computational complexity
Polynomial time algorithm
Module equivalence
Module equation solvability

ABSTRACT

We provide polynomial time algorithms for deciding equation solvability and identity checking over groups that are semidirect products of two finite Abelian groups. Our main method is to reduce these problems to the sigma equation solvability and sigma equivalence problems over modules for commutative unital rings.

1. Introduction

Investigations into the algorithmic aspects of the equivalence problem for various finite algebraic structures commenced in the early 1990s. The *equivalence problem* for a finite ring $\mathcal{R}$ asks whether or not two polynomials p and q are equivalent over $\mathcal{R}$ (denoted by

E-mail address: ghorvath@science.unideb.hu.

http://dx.doi.org/10.1016/j.jalgebra.2015.03.015

$\mathcal{R} \models p \approx q$), i.e. if p and q determine the same function over $\mathcal{R}$. The *equation solvability problem* is one of the oldest problems of algebra: it asks whether or not two expressions p and q can attain the same value for some substitution over a finite ring $\mathcal{R}$, i.e. if the equation $p = q$ can be solved over $\mathcal{R}$. Note, that these problems usually have a 'term' version, as well, where the input polynomials cannot contain constants from the ring $\mathcal{R}$. In this paper we deal with these problems for which the inputs are polynomials, but the term versions of our theorems follow from the proofs, as well. From now on, we refer to these problems as the equivalence problem and the equation solvability problem.

First Hunt and Stearnes [19] investigated the equivalence problem for finite commutative rings. Later Burris and Lawrence [3] generalized their result to non-commutative rings, and established a dichotomy theorem for rings: for finite nilpotent rings the equivalence problem can be solved in polynomial time in the length of the two input polynomials, and for non-nilpotent rings the equivalence problem is coNP-complete. Similar result can be proved for the equation solvability problem: for non-nilpotent rings the NP-completeness follows from the argument of Burris and Lawrence, for nilpotent rings the equation solvability problem is in P [12].

The proof of Burris and Lawrence reduces the satisfiability (SAT) problem to the equivalence problem by using long products of sums of variables. Nevertheless, a polynomial is usually given as a sum of monomials. Of course, the length of a polynomial may change if expanded into a sum of monomials. For example, the polynomial $\prod_{i=1}^{n} (x_i + y_i)$ has linear length in n written as a product of sums, but has exponential length if expanded into a sum of monomials. Such a change in the length suggests that the complexity of the equivalence problem might be different if the input polynomials are restricted to be written as sums of monomials. Thus, Lawrence and Willard [25] introduced the sigma equivalence and sigma equation solvability problems, i.e. when the input polynomials over the given ring are presented as sums of monomials where each monomial has the form $\alpha_1 \dots \alpha_m$ with each α_i a variable or an element of the ring. They formulated a conjecture about the complexity of the sigma equivalence and sigma equation solvability problems. Namely, if the factor by the Jacobson radical is commutative, then the sigma equivalence and sigma equation solvability problems are solvable in polynomial time, otherwise the sigma equivalence problem is coNP-complete, and the sigma equation solvability problem is NP-complete.

Szabó and Vértesi proved the coNP-complete part of the conjecture in [33]. They prove a stronger result for matrix rings: the equivalence problem is coNP-complete even if the input polynomials are restricted to only one monomial, that is the equivalence problem is coNP-complete for the multiplicative semigroup of matrix rings. To this problem they reduce the equivalence problem over the multiplicative subgroup of matrix rings, which is coNP-complete by [15]. Almeida, Volkov and Goldberg proved an even more general result about semigroups (showing that the equivalence problem is coNP-complete for a semigroup if the equivalence problem is coNP-complete for the direct product of its maximal subgroups) yielding the same result for matrix rings [2]. For most matrix rings,