Information and Computation 243 (2015) 191–204

Contents lists available at ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

Rational subsets and submonoids of wreath products ☆

Markus Lohrey [a,*], Benjamin Steinberg [b,1], Georg Zetzsche [c]

[a] Universität Siegen, Department für Elektrotechnik und Informatik, Germany
[b] City College of New York, Department of Mathematics, United States
[c] Technische Universität Kaiserslautern, Fachbereich Informatik, Germany

ARTICLE INFO

Article history:
Received 31 August 2013
Available online 12 December 2014

ABSTRACT

It is shown that membership in rational subsets of wreath products $H \wr V$ with H a finite group and V a virtually free group is decidable. On the other hand, it is shown that there exists a fixed finitely generated submonoid in the wreath product $\mathbb{Z} \wr \mathbb{Z}$ with an undecidable membership problem.

1. Introduction

The study of algorithmic problems in group theory has a long tradition. Dehn, in his seminal paper from 1911 [8], introduced the word problem (Does a given word over the generators represent the identity?), the conjugacy problem (Are two given group elements conjugate?) and the isomorphism problem (Are two given finitely presented groups isomorphic?), see [28] for general references in combinatorial group theory. Starting with the work of Novikov and Boone from the 1950's, all three problems were shown to be undecidable for finitely presented groups in general. A generalization of the word problem is the *subgroup membership problem* (also known as the *generalized word problem*) for finitely generated groups: Given group elements $g, g_1, \ldots, g_n$, does g belong to the subgroup generated by $g_1, \ldots, g_n$? Explicitly, this problem was introduced by Mihailova in 1958, although Nielsen had already presented an algorithm for the subgroup membership problem for free groups in his paper from 1921 [31].

Motivated partly by automata theory, the subgroup membership problem was further generalized to the *rational subset membership problem*. Assume that the group G is finitely generated by the set X (where $a \in X$ if and only if $a^{-1} \in X$). A finite automaton A with transitions labeled by elements of X defines a subset $L(A) \subseteq G$ in the natural way; such subsets are the rational subsets of G. The rational subset membership problem asks whether a given group element belongs to $L(A)$ for a given finite automaton (in fact, this problem makes sense for any finitely generated monoid). The notion of a rational subset of a monoid can be traced back to the work of Eilenberg and Schützenberger from 1969 [11]. Other early references are [1,14]. Rational subsets of groups also found applications for the solution of word equations (here, quite often the term rational constraint is used) [9,23]. In automata theory, rational subsets are tightly related to valence automata: For any group G, the emptiness problem for valence automata over G (which are also known as G-automata) is decidable if and only if G has a decidable rational subset membership problem. See [12,19,20] for details on valence automata and G-automata.

For free groups, Benois [2] proved that the rational subset membership problem is decidable using a classical automaton saturation procedure (which yields a polynomial time algorithm). For commutative groups, the rational subset membership

☆ This work was supported by the DAAD research project RatGroup.
* Corresponding author.
E-mail address: lohrey@eti.uni-siegen.de (M. Lohrey).
1 This author was partially supported by a grant from the Simons Foundation (#245268 to Benjamin Steinberg).

http://dx.doi.org/10.1016/j.ic.2014.12.014

can be solved using integer programming. Further (un)decidability results on the rational subset membership problem can be found in [24] for right-angled Artin groups, in [32] for nilpotent groups, and in [26] for metabelian groups. In general, groups with a decidable rational subset membership problem seem to be rare. In [25] it was shown that if the group G has at least two ends, then the rational subset membership problem for G is decidable if and only if the submonoid membership problem for G (Does a given element of G belong to a given finitely generated submonoid of G?) is decidable.

In this paper, we investigate the rational subset membership problem for wreath products. The wreath product is a fundamental operation in group theory. To define the wreath product $H \wr G$ of two groups G and H, one first takes the direct sum $K = \bigoplus_{g \in G} H$ of copies of H, one for each element of G. An element $g \in G$ acts on K by permuting the copies of H according to the left action of g on G. The corresponding semidirect product $K \rtimes G$ is the wreath product $H \wr G$.

In contrast to the word problem, decidability of the rational subset membership problem is not preserved under wreath products. For instance, in [26] it was shown that for every non-trivial group H, the rational subset membership problem for $H \wr (\mathbb{Z} \times \mathbb{Z})$ is undecidable. The proof uses an encoding of a tiling problem, which uses the grid structure of the Cayley graph of $\mathbb{Z} \times \mathbb{Z}$.

In this paper, we prove the following two new results concerning the rational subset membership problem and the submonoid membership problem for wreath products:

(i) The submonoid membership problem is undecidable for $\mathbb{Z} \wr \mathbb{Z}$. The wreath product $\mathbb{Z} \wr \mathbb{Z}$ is one of the simplest examples of a finitely generated group that is not finitely presented, see [6,7] for further results showing the importance of $\mathbb{Z} \wr \mathbb{Z}$.
(ii) For every finite group H and every virtually free group[2] V, the group $H \wr V$ has a decidable rational subset membership problem; this includes for instance the famous lamplighter group $\mathbb{Z}_2 \wr \mathbb{Z}$.

For the proof of (i) we encode the acceptance problem for a 2-counter machine (Minsky machine [29]) into the submonoid membership problem for $\mathbb{Z} \wr \mathbb{Z}$. One should remark that $\mathbb{Z} \wr \mathbb{Z}$ is a finitely generated metabelian group and hence has a decidable subgroup membership problem [33,34]. For the proof of (ii), an automaton saturation procedure is used. The termination of the process is guaranteed by a well-quasi-order (wqo) that refines the classical subsequence wqo considered by Higman [17].

Wqo theory has also been applied successfully for the verification of infinite state systems. This research led to the notion of well-structured transition systems [13]. Applications in formal language theory are the decidability of the membership problem for leftist grammars [30] and Kunc's proof of the regularity of the solutions of certain language equations [21]. A disadvantage of using wqo theory is that the algorithms it yields are not accompanied by complexity bounds. The membership problem for leftist grammars [18] and, in the context of well-structured transition systems, several natural reachability problems [5,36] (e.g. for lossy channel systems) have even been shown not to be primitive recursive. The complexity status for the rational subset membership problem for wreath products $H \wr V$ (H finite, V virtually free) thus remains open. Actually, we do not even know whether the rational subset membership problem for the lamplighter group $\mathbb{Z}_2 \wr \mathbb{Z}$ is primitive recursive.

As mentioned earlier, the rational subset membership problem is undecidable for every wreath product $H \wr (\mathbb{Z} \times \mathbb{Z})$, where H is a non-trivial group. We conjecture that this can be generalized to the following result: For every non-trivial group H and every non-virtually free group G, the rational subset membership problem for $H \wr G$ is undecidable. The reason is that the undecidability proof for $H \wr (\mathbb{Z} \times \mathbb{Z})$ [26] only uses the grid-like structure of the Cayley graph of $\mathbb{Z} \times \mathbb{Z}$. In [22] it was shown that the Cayley graph of a group G has bounded tree width if and only if the group is virtually free. Hence, if G is not virtually free, then the Cayley-graph of G has unbounded tree width, which means that finite grids of arbitrary size appear as minors in the Cayley-graph of G. One might therefore hope to again reduce a tiling problem to the rational subset membership problem for $H \wr G$ (for H non-trivial and G not virtually free).

Our decidability result for the rational subset membership problem for wreath products $H \wr V$ with H finite and V virtually free can be also interpreted in terms of tree automata with additional data values. Consider a tree walking automaton operating on infinite rooted trees. Every tree node contains an additional data value from a finite group such that all but finitely many nodes contain the group identity. Besides navigating in the tree, the tree automaton can multiply (on the right) the group element from the current tree node with another group element (specified by the transition). The automaton cannot read the group element from the current node. Our decidability result basically says that reachability for this automaton model is decidable.

2. Rational subsets of groups

Let G be a finitely generated group and X a finite symmetric generating set for G (symmetric means that X is closed under taking inverses). For a subset $B \subseteq G$ we denote with B^* the *submonoid* of G generated by B. The subgroup generated by B is $\langle B \rangle$. The set of *rational subsets* of G is the smallest set that (i) contains all finite subsets of G and (ii) that is closed under union, product, and *. Alternatively, rational subsets can be represented by finite automata. Let $A = (Q, G, E, q_0, Q_F)$ be a finite automaton, where transitions are labeled with elements of G: Q is the finite set of states, $q_0 \in Q$ is the

[2] Recall that a group is virtually free if it has a free subgroup of finite index.