Rational subsets and submonoids of wreath products*

Markus Lohrey[1], Benjamin Steinberg[2], and Georg Zetzsche[3]

[1] Universität Leipzig, Institut für Informatik
[2] City College of New York, Department of Mathematics
[3] Technische Universität Kaiserslautern, Fachbereich Informatik

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, 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 [25] 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 in 1921 an algorithm for the subgroup membership problem for free groups.

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 [8]. Other early references are [1, 11]. Rational subsets of groups also found applications for the solution of word equations (here, quite often the term rational constraint is used) [6, 20]. In automata theory, rational subsets are tightly related to valence automata (see [9, 16, 17] for details): 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.

* This work was supported by the DAAD research project RatGroup. The second author was partially supported by a grant from the Simons Foundation (#245268 to Benjamin Steinberg). Omitted proofs can be found in the long version [24] of this paper.

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 can be solved using integer programming. Further (un)decidability results on the rational subset membership problem can be found in [21] for right-angled Artin groups, in [28] for nilpotent groups, and in [23] for metabelian groups. In general, groups with a decidable rational subset membership problem seem to be rare. In [22] 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 [23] 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 [4, 5] for further results showing the importance of $\mathbb{Z} \wr \mathbb{Z}$.

(ii) For every finite group H and every virtually free group[4] 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 [26]) 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 [29, 30]. 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 [14].

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 [10]. Applications in formal language theory are the decidability of the membership problem for leftist grammars [27] and Kunc's proof of the regularity of the solutions of certain language equations [18]. A disadvantage of using wqo theory is that the algorithms it yields are not accompanied by complexity bounds. The membership problem for leftist grammars [15] and, in the context of well-structured transition systems, several natural reachability problems [3, 32] (e.g. for lossy channel systems) have even been shown

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

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.

2 Rational subsets of groups

Let G be a finitely generated group and X a finite symmetric generating set for G (symmetric means that $x \in X \Leftrightarrow x^{-1} \in X$). For a subset $B \subseteq G$ we denote with B^* (resp. $\langle B \rangle$) the *submonoid* (resp. subgroup) of G generated by B. The set of *rational subsets* of G is the smallest set that contains all finite subsets of G and 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 initial state, $Q_F \subseteq Q$ is the set of final states, and $E \subseteq Q \times G \times Q$ is a finite set of transitions. Every transition label $g \in G$ can be represented by a finite word over the generating set X. The subset $L(A) \subseteq G$ accepted by A consists of all group elements $g_1 g_2 g_3 \cdots g_n$ such that there exists a sequence of transitions $(q_0, g_1, q_1), (q_1, g_2, q_2), (q_2, g_3, q_3), \ldots, (q_{n-1}, g_n, q_n) \in E$ with $q_n \in Q_F$. The *rational subset membership problem* for G is the following decision problem: Given a finite automaton A as above and an element $g \in G$, does $g \in L(A)$ hold? Since $g \in L(A)$ if and only if $1_G \in L(A)g^{-1}$, and $L(A)g^{-1}$ is rational, too, the rational subset membership problem for G is equivalent to the question whether a given automaton accepts the group identity.

The *submonoid membership problem* for G is the following decision problem: Given elements $g, g_1, \ldots, g_n \in G$, does $g \in \{g_1, \ldots, g_n\}^*$ hold? Clearly, decidability of the rational subset membership problem for G implies decidability of the submonoid membership problem for G. Moreover, the latter generalizes the classical subgroup membership problem for G (also known as the generalized word problem), where the input is the same as for the submonoid membership problem for G but it is asked whether $g \in \langle g_1, \ldots, g_n \rangle$ holds.

In our undecidability results in Sec. 5, we will actually consider the non-uniform variant of the submonoid membership problem, where the submonoid is fixed, i.e., not part of the input.

3 Wreath products

Let G and H be groups. Consider the direct sum $K = \bigoplus_{g \in G} H_g$, where H_g is a copy of H. We view K as the set $H^{(G)} = \{f \in H^G \mid f^{-1}(H \setminus \{1_H\}) \text{ is finite}\}$ of all mappings from G to H with finite support together with pointwise multiplication as the group operation. The group G has a natural left action on $H^{(G)}$ given by $gf(a) = f(g^{-1}a)$, where $f \in H^{(G)}$ and $g, a \in G$. The corresponding semidirect product $H^{(G)} \rtimes G$ is the wreath product $H \wr G$. In other words:

- Elements of $H \wr G$ are pairs (f, g), where $f \in H^{(G)}$ and $g \in G$.

– The multiplication in $H \wr G$ is defined as follows: Let $(f_1, g_1), (f_2, g_2) \in H \wr G$. Then $(f_1, g_1)(f_2, g_2) = (f, g_1 g_2)$, where $f(a) = f_1(a) f_2(g_1^{-1} a)$.

The following intuition might be helpful: An element $(f, g) \in H \wr G$ can be thought of as a finite multiset of elements of $H \setminus \{1_H\}$ that are sitting at certain elements of G (the mapping f) together with the distinguished element $g \in G$, which can be thought of as a cursor moving in G. If we want to compute the product $(f_1, g_1)(f_2, g_2)$, we do this as follows: First, we shift the finite collection of H-elements that corresponds to the mapping f_2 by g_1: If the element $h \in H \setminus \{1_H\}$ is sitting at $a \in G$ (i.e., $f_2(a) = h$), then we remove h from a and put it to the new location $g_1 a \in H$. This new collection corresponds to the mapping $f_2' \colon a \mapsto f_2(g_1^{-1} a)$. After this shift, we multiply the two collections of H-elements pointwise: If in $a \in G$ the elements h_1 and h_2 are sitting (i.e., $f_1(a) = h_1$ and $f_2'(a) = h_2$), then we put the product $h_1 h_2$ into the location a. Finally, the new distinguished G-element (the new cursor position) becomes $g_1 g_2$.

If H (resp. G) is generated by the set A (resp. B) with $A \cap B = \emptyset$, then $H \wr G$ is generated by $A \cup B$.

Proposition 1. *Let K be a subgroup of G of finite index m and let H be a group. Then $H^m \wr K$ is isomorphic to a subgroup of index m in $H \wr G$.*

4 Decidability

We show that the rational subset membership problem is decidable for groups $G = H \wr V$, where H is finite and V is virtually free. First, we will show that the rational subset membership problem for $G = H \wr F_2$, where F_2 is the free group generated by a and b, is decidable. For this we make use of a particular well-quasi-order.

A well-quasi-order Recall that a *well-quasi-order (wqo)* on a set A is a reflexive and transitive relation $\preceq$ such that for every infinite sequence $a_1, a_2, a_3, \ldots$ with $a_i \in A$ there exist $i < j$ such that $a_i \preceq a_j$. In this paper, $\preceq$ will always be antisymmetric as well; so $\preceq$ will be a well partial order.

For a finite alphabet X and two words $u, v \in X^*$, we write $u \preceq v$ if there exist $v_0, \ldots, v_n \in X^*$, $u_1, \ldots, u_n \in X$ such that $v = v_0 u_1 v_1 \cdots u_n v_n$ and $u = u_1 \cdots u_n$. The following theorem was shown by Higman [14] (and independently Haines [13]).

Theorem 1 (Higman's Lemma). *The order $\preceq$ on X^* is a wqo.*

Let H be a group. For a monoid morphism $\alpha \colon X^* \to H$ and $u, v \in X^*$ let $u \preceq_\alpha v$ if there is a factorization $v = v_0 u_1 v_1 \cdots u_n v_n$ with $v_0, \ldots, v_n \in X^*$, $u_1, \ldots, u_n \in X$, $u = u_1 \cdots u_n$, and $\alpha(v_i) = 1$ for $0 \leq i \leq n$. It is easy to see that $\preceq_\alpha$ is indeed a partial order on X^*. Furthermore, let $\preceq_H$ be the partial order on X^* with $u \preceq_H v$ if $v = v_0 u_1 v_1 \cdots u_n v_n$ for some $v_0, \ldots, v_n \in X^*$, $u_1, \ldots, u_n \in X$, and $u = u_1 \cdots u_n$ such that $\alpha(v_i) = 1$ for every morphism $\alpha \colon X^* \to H$ and $0 \leq i \leq n$. Note that if H is finite, there are only finitely many morphisms $\alpha \colon X^* \to H$. The upward closure $U \subseteq X^*$ of $\{\varepsilon\}$ with respect to $\preceq_H$ is the intersection of all preimages $\alpha^{-1}(1)$ for all morphisms $\alpha \colon X^* \to H$, which is therefore regular if H is finite (and a finite automaton for this upward closure can be constructed from X and H). Since for $w =$

$w_1 \cdots w_n, w_1, \ldots, w_n \in X$, the upward closure of $\{w\}$ equals $Uw_1 \cdots Uw_nU$, we can also construct a finite automaton for the upward closure of any given singleton provided that H is finite. In the latter case, we can also show that $\preceq_H$ is a wqo:

Lemma 1. *For every finite group H and finite alphabet X, $(X^*, \preceq_H)$ is a wqo.*[5]

Proof. There are only finitely many morphisms $\alpha\colon X^* \to H$, say $\alpha_1, \ldots, \alpha_\ell$. If $\beta : X^* \to H^\ell$ is the morphism with $\beta(w) = (\alpha_1(w), \ldots, \alpha_\ell(w))$, then for all words $w \in X^*$: $\beta(x) = 1$ if and only if $\alpha(x) = 1$ for all morphisms $\alpha : X^* \to H$. Thus, $\preceq_H$ coincides with $\preceq_\beta$, and it suffices to show that $\preceq_\beta$ is a wqo.

Let $w_1, w_2, \ldots \in X^*$ be an infinite sequence of words. Since H^ℓ is finite, we can assume that all the w_i have the same image under β; otherwise, choose an infinite subsequence on which β is constant. Consider the alphabet $Y = X \times H^\ell$. For every $w \in X^*$, $w = a_1 \cdots a_r$, let $\bar{w} \in Y^*$ be the word

$$\bar{w} = (a_1, \beta(a_1))(a_2, \beta(a_1a_2)) \cdots (a_r, \beta(a_1 \cdots a_r)). \tag{1}$$

Applying Thm. 1 to the sequence $\bar{w}_1, \bar{w}_2, \ldots$ yields $i < j$ with $\bar{w}_i \preceq \bar{w}_j$. This means $\bar{w}_i = u'_1 \cdots u'_r$, $\bar{w}_j = v'_0u'_1v'_1 \cdots u'_rv'_r$ for some $u'_1, \ldots, u'_r \in Y$, $v'_0, \ldots, v'_r \in Y^*$. By definition of $\bar{w}_i$ we have $u'_s = (u_s, h_s)$ for $1 \le s \le r$, where $h_s = \beta(u_1 \cdots u_s)$ and $w_i = u_1 \cdots u_r$. Let $\pi_1\colon Y^* \to X^*$ be the morphism extending the projection onto the first component, and let $v_s = \pi_1(v'_s)$ for $0 \le s \le r$. Then clearly $w_j = v_0u_1v_1 \cdots u_rv_r$. We claim that $\beta(v_s) = 1$ for $0 \le s \le r$, from which $w_i \preceq_\beta w_j$ and hence the lemma follows. Since $\bar{w}_j$ is also obtained according to (1), we have $\beta(u_1 \cdots u_{s+1}) = h_{s+1} = \beta(v_0u_1v_1 \cdots u_sv_su_{s+1})$ for $0 \le s \le r-1$. By induction on s, this implies $\beta(v_s) = 1$ for $0 \le s \le r-1$. Finally, $\beta(v_r) = 1$ follows from $\beta(u_1 \cdots u_r) = \beta(w_i) = \beta(w_j) = \beta(v_0u_1v_1 \cdots u_rv_r) = \beta(u_1 \cdots u_rv_r)$. □

Loops Let $G = H \wr F_2$ and fix free generators $a, b \in F_2$. Recall that every element of F_2 can be represented by a unique word over $\{a, a^{-1}, b, b^{-1}\}$ that does not contain a factor of the form aa^{-1}, $a^{-1}a$, bb^{-1}, or $b^{-1}b$; such words are called *reduced*. For $f \in F_2$, let $|f|$ be the length of the reduced word representing f. Also recall that elements of G are pairs (k, f), where $k \in K = \bigoplus_{g \in F_2} H$ and $f \in F_2$. In the following, we simply write kf for the pair (k, f). Fix an automaton $A = (Q, G, E, q_0, Q_F)$ with labels from G for the rest of Sec. 4. We want to check whether $1 \in L(A)$. Since G is generated as a monoid by $H \cup \{a, a^{-1}, b, b^{-1}\}$, we can assume that $E \subseteq Q \times (H \cup \{a, a^{-1}, b, b^{-1}\}) \times Q$.

A *configuration* is an element of $Q \times G$. For configurations (p, g_1), (q, g_2), we write $(p, g_1) \to_A (q, g_2)$ if there is a $(p, g, q) \in E$ such that $g_2 = g_1g$. For elements $f, g \in F_2$, we write $f \le g$ ($f < g$) if the reduced word representing f is a (proper) prefix of the reduced word representing g. We say that an element $f \in F_2 \setminus \{1\}$ is *of type* $x \in \{a, a^{-1}, b, b^{-1}\}$ if the reduced word representing f ends with x. Furthermore, $1 \in F_2$ is *of type* 1. Hence, the set of *types* is $T = \{1, a, a^{-1}, b, b^{-1}\}$. When regarding the Cayley graph of F_2 as a tree with root 1, the children of a node of type t are of

[5] One can actually show for any group H: $(X^*, \preceq_H)$ is a wqo if and only if for every $n \in \mathbb{N}$, there is $k \in \mathbb{N}$ with $|\langle g_1, \ldots, g_n\rangle| \le k$ for all $g_1, \ldots, g_n \in H$. See the full version [24].

the types $C(t) = \{a, a^{-1}, b, b^{-1}\} \setminus \{t^{-1}\}$. Clearly, two nodes have the same type if and only if their induced subtrees of the Cayley graph are isomorphic. The elements of $D = \{a, a^{-1}, b, b^{-1}\}$ will also be called *directions*.

Let $p, q \in Q$ and $t \in T$. A sequence of configurations

$$(q_1, k_1 f_1) \to_A (q_2, k_2 f_2) \to_A \cdots \to_A (q_n, k_n f_n) \tag{2}$$

(recall that $k_i f_i$ denotes the pair $(k_i, f_i) \in G$) is called a *well-nested* (p, q)*-computation for* t if (i) $q_1 = p$ and $q_n = q$, (ii) $f_1 = f_n$ is of type t, and (iii) $f_i \geq f_1$ for $1 < i < n$ (this last condition is satisfied automatically if $f_1 = f_n = 1$). We define the *effect* of the computation to be $f_1^{-1} k_1^{-1} k_n f_n \in K$. Hence, the effect describes the change imposed by applying the corresponding sequence of transitions, independently of the configuration in which it starts. The *depth* of the computation (2) is the maximum value of $|f_1^{-1} f_i|$ for $1 \leq i \leq n$. We have $1 \in L(A)$ if and only if for some $q \in Q_F$, there is a well-nested (q_0, q)-computation for 1 with effect 1.

For $d \in C(t)$, a well-nested (p, q)-computation (2) for t is called a (p, d, q)*-loop for* t if in addition $f_1 d \leq f_i$ for $1 < i < n$. Note that there is a (p, d, q)-loop for t that starts in (p, kf) (where f is of type t) with effect e and depth m if and only if there exists a (p, d, q)-loop for t with effect e and depth m that starts in (p, t).

Given $p, q \in Q$, $t \in T$, $d \in C(t)$, it is decidable whether there is a (p, d, q)-loop for t: This amounts to checking whether a given automaton with input alphabet $\{a, a^{-1}, b, b^{-1}\}$ accepts a word representing the identity of F_2 such that no proper prefix represents the identity of F_2. Since this can be accomplished using pushdown automata, we can compute the set

$$X_t = \{(p, d, q) \in Q \times C(t) \times Q \mid \text{there is a } (p, d, q)\text{-loop for } t\}.$$

Loop patterns Given a word $w = (p_1, d_1, q_1) \cdots (p_n, d_n, q_n) \in X_t^*$, a *loop assignment for* w is a choice of a (p_i, d_i, q_i)-loop for t for each position i, $1 \leq i \leq n$. The *effect* of a loop assignment is $e_1 \cdots e_n \in K$, where $e_i \in K$ is the effect of the loop assigned to position i. The *depth* of a loop assignment is the maximum depth of an appearing loop. A *loop pattern for* t is a word $w \in X_t^*$ that has a loop assignment with effect 1. The *depth* of the loop pattern is the minimum depth of a loop assignment with effect 1. Note that applying the loops for the symbols in a loop pattern $(p_1, d_1, q_1) \cdots (p_n, d_n, q_n)$ does not have to be a computation: We do not require $q_i = p_{i+1}$. Instead, the loop patterns describe the possible ways in which a well-nested computation can enter (and leave) subtrees of the Cayley graph of F_2 in order to have effect 1. The sets

$$P_t = \{w \in X_t^* \mid w \text{ is a loop pattern for } t\}$$

for $t \in T$ will therefore play a central role in the decision procedure.

Recall the definition of the partial order $\preceq_H$ from Sec. 4. We have shown that $\preceq_H$ is a wqo (Lemma 1). The second important result on $\preceq_H$ is:

Lemma 2. *For each $t \in T$, P_t is an upward closed subset of X_t^* with respect to $\preceq_H$.*

Lemma 1 and 2 already imply that each P_t is a regular language, since the upward closure of each singleton is regular. This can also be deduced by observing that $\preceq_H$ is a monotone order in the sense of [7]. Therein, Ehrenfeucht et al. show that languages that are upward closed with respect to monotone well-quasi-orders are regular. Our next step is a characterization of the P_t that allows us to compute finite automata for them. In order to state this characterization, we need the following definitions.

Let X, Y be alphabets. A *regular substitution* is a map $\sigma\colon X \to 2^{Y^*}$ such that $\sigma(x) \subseteq Y^*$ is regular for every $x \in X$. For $w \in X^*$, $w = w_1 \cdots w_n$, $w_i \in X$, let $\sigma(w) = R_1 \cdots R_n$, where $\sigma(w_i) = R_i$ for $1 \leq i \leq n$. Given $R \subseteq Y^*$ and a regular substitution $\sigma\colon X \to 2^{Y^*}$, let $\sigma^{-1}(R) = \{w \in X^* \mid \sigma(w) \cap R \neq \emptyset\}$. If R is regular, then $\sigma^{-1}(R)$ is regular as well [31, Prop. 2.16], and an automaton for $\sigma^{-1}(R)$ can be obtained effectively from automata for R and the $\sigma(x)$. The alphabet Y_t is given by

$$Y_t = X_t \cup ((Q \times H \times Q) \cap E).$$

We will interpret a word in Y_t^* as that part of a computation that happens in a node of type t: A symbol in $Y_t \setminus X_t$ stands for a transition that stays in the current node and only changes the local H-value and the state. A symbol $(p, d, q) \in X_t$ represents the execution of a (p, d, q)-loop in a subtree of the current node. The morphism $\pi_t\colon Y_t^* \to X_t^*$ is the projection onto X_t^*, meaning $\pi_t(y) = y$ for $y \in X_t$ and $\pi_t(y) = \varepsilon$ for $y \in Y_t \setminus X_t$. The morphism $\nu_t\colon Y_t^* \to H$ is defined by

$$\begin{aligned}\nu_t((p, d, q)) &= 1 \text{ for } (p, d, q) \in X_t\\ \nu_t((p, h, q)) &= h \text{ for } (p, h, q) \in Y_t \setminus X_t.\end{aligned}$$

Hence, when $w \in Y_t^*$ describes part of a computation, $\nu_t(w)$ is the change it imposes on the current node. For $p, q \in Q$ and $t \in T$, define the regular set

$$R^t_{p,q} = \{(p_0, g_1, p_1)(p_1, g_2, p_2) \cdots (p_{n-1}, g_n, p_n) \in Y_t^* \mid p_0 = p, p_n = q\}.$$

Then $\pi_t^{-1}(P_t) \cap \nu_t^{-1}(1) \cap R^t_{p,q}$ consists of those words over Y_t that admit an assignment of loops to occurrences of symbols in X_t so as to obtain a well-nested (p, q)-computation for t with effect 1. Given $d \in C(t)$, $t \in T$, the regular substitution $\sigma_{t,d}\colon X_t \to 2^{Y_d^*}$ is defined by

$$\begin{aligned}\sigma_{t,d}((p, d, q)) &= \bigcup \{R^d_{p',q'} \mid (p, d, p'), (q', d^{-1}, q) \in E\}\\ \sigma_{t,d}((p, u, q)) &= \{\varepsilon\} \text{ for } u \in C(t) \setminus \{d\}.\end{aligned}$$

For tuples $(U_t)_{t\in T}$ and $(V_t)_{t\in T}$ with $U_t, V_t \subseteq X_t^*$, we write $(U_t)_{t\in T} \leq (V_t)_{t\in T}$ if $U_t \subseteq V_t$ for each $t \in T$. We can now state the following fixpoint characterization:

Lemma 3. *$(P_t)_{t\in T}$ is the smallest tuple such that for every $t \in T$ we have $\varepsilon \in P_t$ and*

$$\bigcap_{d\in C(t)} \sigma_{t,d}^{-1}\left(\pi_d^{-1}(P_d) \cap \nu_d^{-1}(1)\right) \subseteq P_t.$$

Given a language $L \subseteq X_t^*$, let $L{\uparrow_t} = \{v \in X_t^* \mid u \preceq_H v \text{ for some } u \in L\}$.

Theorem 2. *The rational subset membership problem is decidable for every group $G = H \wr F$, where H is finite and F is a finitely generated free group.*

Proof. Since $H \wr F$ is a subgroup of $H \wr F_2$ (since F is a subgroup of F_2), it suffices to show decidability for $G = H \wr F_2$. First, we compute finite automata for the languages P_t. We do this by initializing $U_t^{(0)} := \{\varepsilon\}\uparrow_t$ for each $t \in T$ and then successively extending the sets $U_t^{(i)}$, which are represented by finite automata, until they equal P_t: If there is a $t \in T$ and a word

$$w \in \bigcap_{d \in C(t)} \sigma_{t,d}^{-1}\left(\pi_d^{-1}(U_d^{(i)}) \cap \nu_d^{-1}(1)\right) \setminus U_t^{(i)},$$

we set $U_t^{(i+1)} := U_t^{(i)} \cup \{w\}\uparrow_t$ and $U_u^{(i+1)} := U_u^{(i)}$ for $u \in T \setminus \{t\}$. Otherwise we stop. By induction on i, it follows from Lemma 2 and Lemma 3 that $U_t^{(i)} \subseteq P_t$.

In each step, we obtain $U_t^{(i+1)}$ by adding new words to $U_t^{(i)}$. Since the sets $U_t^{(i)}$ are upward closed by construction and there is no infinite (strictly) ascending chain of upward closed sets in a wqo, the algorithm above has to terminate with some tuple $(U_t^{(k)})_{t \in T}$. This, however, means that for every $t \in T$

$$\bigcap_{d \in C(t)} \sigma_{t,d}^{-1}\left(\pi_d^{-1}(U_d^{(k)}) \cap \nu_d^{-1}(1)\right) \subseteq U_t^{(k)}.$$

Since on the other hand $\varepsilon \in U_t^{(k)}$ and $U_t^{(k)} \subseteq P_t$, Lemma 3 yields $U_t^{(k)} = P_t$.

Now we have $1 \in L(A)$ if and only if $\pi_1^{-1}(P_1) \cap \nu_1^{-1}(1) \cap R^1_{q_0,q} \neq \emptyset$ for some $q \in Q_F$, which can be reduced to non-emptiness for finite automata. □

Theorem 3. *The rational subset membership problem is decidable for every group $H \wr V$ with H finite and V virtually free.*

Proof. This is immediate from Thm. 2 and Prop. 1: If F is a free subgroup of index m in V, then $H^m \wr F$ is isomorphic to a subgroup of index m in $H \wr V$ and decidability of rational subset membership is preserved by finite extensions [12, 17]. □

5 Undecidability

In this section, we will prove the second main result of this paper: The wreath product $\mathbb{Z} \wr \mathbb{Z}$ contains a fixed submonoid with an undecidable membership problem. Our proof is based on the undecidability of the halting problem for 2-counter machines.

2-counter machines A *2-counter machine* (also known as Minsky machine) is a tuple $C = (Q, q_0, q_f, \delta)$, where Q is a finite set of *states*, $q_0 \in Q$ is the *initial state*, $q_f \in Q$ is the *final state*, and $\delta \subseteq (Q \setminus \{q_f\}) \times \{c_0, c_1\} \times \{+1, -1, = 0\} \times Q$ is the set of *transitions*. The set of *configurations* is $Q \times \mathbb{N} \times \mathbb{N}$, on which we define a binary relation $\to_C$ as follows: $(p, m_0, m_1) \to_C (q, n_0, n_1)$ if and only if one of the following holds:

- There is $(p, c_i, b, q) \in \delta$ such that $b \in \{-1, 1\}$, $n_i = m_i + b$, and $n_{1-i} = m_{1-i}$.

– There is $(p, c_i, = 0, q) \in \delta$ such that $n_i = m_i = 0$ and $n_{1-i} = m_{1-i}$.

It is well known that every Turing-machine can be simulated by a 2-counter machine (see e.g. [26]). In particular, we have:

Theorem 4. *There is a fixed 2-counter machine $C = (Q, q_0, q_f, \delta)$ such that the following problem is undecidable: Given $m, n \in \mathbb{N}$, does $(q_0, m, n) \to_C^* (q_f, 0, 0)$ hold?*

Submonoids of $\mathbb{Z} \wr \mathbb{Z}$ In this section, we only consider wreath products of the form $H \wr \mathbb{Z}$. An element $(f, m) \in H \wr \mathbb{Z}$ such that the support of f is contained in the interval $[a, b]$ (with $a, b \in \mathbb{Z}$) and $0, m \in [a, b]$ will also be written as a list $[f(a), \ldots, f(b)]$, where in addition the element $f(0)$ is labeled by an incoming (downward) arrow and the element $f(m)$ is labeled by an outgoing (upward) arrow.

We will construct a fixed finitely generated submonoid of the wreath product $\mathbb{Z} \wr \mathbb{Z}$ with an undecidable membership problem. For this, let $C = (Q, q_0, q_f, \delta)$ be the 2-counter machine from Thm. 4. W.l.o.g. we can assume that there exists a partition $Q = Q_0 \cup Q_1$ such that $q_0 \in Q_0$ and

$$\delta \subseteq (Q_0 \times \{c_0\} \times \{+1, -1, = 0\} \times Q_1) \cup (Q_1 \times \{c_1\} \times \{+1, -1, = 0\} \times Q_0).$$

In other words, C alternates between the two counters. Hence, a transition (q, c_i, x, p) can be just written as (q, x, p).

Let $\Sigma = Q \uplus \{c, \#\}$ and let $\mathbb{Z}^\Sigma$ be the free abelian group generated by Σ. First, we prove that there is a fixed finitely generated submonoid M of $\mathbb{Z}^\Sigma \wr \mathbb{Z}$ with an undecidable membership problem. Let $a \notin \Sigma$ be a generator for the right $\mathbb{Z}$-factor; hence $\mathbb{Z}^\Sigma \wr \mathbb{Z}$ is generated by $\Sigma \cup \{a\}$. Let $K = \bigoplus_{m \in \mathbb{Z}} \mathbb{Z}^\Sigma$. In the following, we will freely switch between the description of elements of $\mathbb{Z}^\Sigma \wr \mathbb{Z}$ by words over $(\Sigma \cup \{a\})^{\pm 1}$ and by pairs from $K \rtimes \mathbb{Z}$.

Our finitely generated submonoid M of $\mathbb{Z}^\Sigma \wr \mathbb{Z}$ is generated by the following elements. The right column shows the generators in list notation (elements of $\mathbb{Z}^\Sigma$ are written additively, i.e., as $\mathbb{Z}$-linear combinations of elements of Σ):

$p^{-1}a\#a^2\#aq$ for $(p, = 0, q) \in \delta$	$[\overset{\downarrow}{-p}, \#, 0, \#, \overset{\uparrow}{q}]$	(3)
$p^{-1}a\#aca^2qa^{-2}$ for $(p, +1, q) \in \delta$	$[\overset{\downarrow}{-p}, \#, \overset{\uparrow}{c}, 0, q]$	(4)
$p^{-1}a\#a^3qa^6c^{-1}a^{-8}$ for $(p, -1, q) \in \delta$	$[\overset{\downarrow}{-p}, \#, \overset{\uparrow}{0}, 0, q, 0, 0, 0, 0, 0, -c]$	(5)
$c^{-1}a^8ca^{-8}$	$[\overset{\downarrow\uparrow}{-c}, 0, 0, 0, 0, 0, 0, 0, 0, c]$	(6)
$c^{-1}a\#a^7ca^{-6}$	$[\overset{\downarrow}{-c}, \#, \overset{\uparrow}{0}, 0, 0, 0, 0, 0, 0, c]$	(7)
$q_f^{-1}a^{-1}$	$[\overset{\uparrow}{0}, \overset{\downarrow}{-q_f}]$	(8)
$\#^{-1}a^{-2}$	$[\overset{\uparrow}{0}, 0, \overset{\downarrow}{-\#}]$	(9)

For initial counter values $m, n \in \mathbb{N}$ let $I(m, n) = aq_0a^2c^ma^4c^na^{-6}$; its list notation is

$$[\overset{\downarrow}{0}, \overset{\uparrow}{q_0}, 0, m \cdot c, 0, 0, 0, n \cdot c]. \tag{10}$$

Here is some intuition: The group element $I(m,n)$ represents the initial configuration (q_0,m,n) of the 2-counter machine C. Lemma 4 below states that $(q_0,m,n) \to_C^* (q_f,0,0)$ is equivalent to the existence of $Y \in M$ with $I(m,n)Y = 1$, i.e., $I(m,n)^{-1} \in M$. Generators of type (3)–(7) simulate the 2-counter machine C. States of C will be stored at cursor positions $4k+1$. The values of the first (resp., second) counter will be stored at cursor positions $8k+3$ (resp., $8k+7$). Note that $I(m,n)$ puts a single copy of the symbol $q_0 \in \Sigma$ at position 1, m copies of symbol c (which represents counter values) at position 3, and n copies of symbol c at position 7. Hence, indeed, $I(m,n)$ sets up the initial configuration (q_0,m,n) for C. Even cursor positions will carry the special symbol $\#$. Note that generator (8) is the only generator which changes the cursor position from even to odd or vice versa. It will turn out that if $I(m,n)Y = 1$ ($Y \in M$), then generator (8) has to occur exactly once in Y; it terminates the simulation of the 2-counter machine C. Hence, Y can be written as $Y = U(q_f^{-1}a^{-1})V$ with $U,V \in M$. Moreover, it turns out that $U \in M$ is a product of generators (3)–(7), which simulate C. Thereby, even cursor positions will be marked with a single occurrence of the special symbol $\#$. In a second phase, which corresponds to $V \in M$, these special symbols $\#$ will be removed again and the cursor will be moved left to position 0. This is accomplished with generator (9). In fact, our construction enforces that V is a power of (9).

During the simulation phase (corresponding to $U \in M$), generators of type (3) implement zero tests, whereas generators of type (4) (resp., (5)) increment (resp., decrement) a counter. Finally, (6) and (7) copy the counter value to the next cursor position that is reserved for the counter (that is copied). During such a copy phase, (6) is first applied ≥ 0 many times. Finally, (7) is applied exactly once.

Lemma 4. *For all $m,n \in \mathbb{N}$ we have: $(q_0,m,n) \to_C^* (q_f,0,0)$ if and only if there exists $Y \in M$ such that $I(m,n)Y = 1$.*

The following result is an immediate consequence of Thm. 4 and Lemma 4.

Theorem 5. *There is a fixed finitely generated submonoid M of the wreath product $\mathbb{Z}^\Sigma \wr \mathbb{Z}$ with an undecidable membership problem.*

Finally, we can establish the main result of this section.

Theorem 6. *There is a fixed finitely generated submonoid M of the wreath product $\mathbb{Z} \wr \mathbb{Z}$ with an undecidable membership problem.*

Proof. By Thm. 5 it suffices to reduce the submonoid membership problem of $\mathbb{Z}^\Sigma \wr \mathbb{Z}$ to the submonoid membership problem of $\mathbb{Z} \wr \mathbb{Z}$. If $m = |\Sigma|$, then Prop. 1 shows that $\mathbb{Z}^\Sigma \wr \mathbb{Z} \cong \mathbb{Z}^m \wr m\mathbb{Z}$ is isomorphic to a subgroup of index m in $\mathbb{Z} \wr \mathbb{Z}$. So if $\mathbb{Z} \wr \mathbb{Z}$ had a decidable submonoid membership problem for each finitely generated submonoid, then the same would be true of $\mathbb{Z}^\Sigma \wr \mathbb{Z}$. □

Theorem 6 together with the undecidability of the rational subset membership problem for groups $H \wr (\mathbb{Z} \times \mathbb{Z})$ for non-trivial H [23] implies the following: For finitely generated

non-trivial abelian groups G and H, $H \wr G$ has a decidable rational subset membership problem if and only if (i) G is finite[6] or (ii) G has rank 1 and H is finite.

By [4], $\mathbb{Z} \wr \mathbb{Z}$ is a subgroup of Thompson's group F as well as of Baumslag's finitely presented metabelian group $\langle a, s, t \mid [s,t] = [a^t, a] = 1, a^s = aa^t \rangle$. Hence, we get:

Corollary 1. *Thompson's group F and Baumslag's finitely presented metabelian group both contain finitely generated submonoids with an undecidable membership problem.*

6 Open problems

As mentioned in the introduction, 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 [23]. We conjecture that 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 $H \wr (\mathbb{Z} \times \mathbb{Z})$ [23] only uses the grid-like structure of the Cayley graph of $\mathbb{Z} \times \mathbb{Z}$. In [19] 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).

Another interesting case, which is not resolved by our results, concerns the rational subset membership problem for wreath products $G \wr V$ with V virtually free and G a finitely generated infinite torsion group. Finally, all these questions can also be asked for the submonoid membership problem. We do not know any example of a group with decidable submonoid membership problem but undecidable rational subset membership problem. If such a group exists, it must be one-ended [22].

References

1. A. V. Anisimov. Group languages. *Kibernetika*, 4:18–24, 1971. In Russian; English translation in *Cybernetics 4*, 594–601, 1973.
2. M. Benois. Parties rationnelles du groupe libre. *C. R. Acad. Sci. Paris*, Sér. A, 269:1188–1190, 1969.
3. P. Chambart and P. Schnoebelen. Post embedding problem is not primitive recursive, with applications to channel systems. In *Proc. FSTTCS 2007*, LNCS 4855, 265–276. Springer, 2007.
4. S. Cleary. Distortion of wreath products in some finitely-presented groups. *Pacific Journal of Mathematics*, 228(1):53–61, 2006.
5. T. C. Davis and A. Y. Olshanskii. Subgroup distortion in wreath products of cyclic groups. *Journal of Pure and Applied Algebra*, 215(12):2987–3004, 2011.
6. V. Diekert and A. Muscholl. Solvability of equations in free partially commutative groups is decidable. *International Journal of Algebra and Computation*, 16(6):1047–1069, 2006.

[6] If G has size m, then by Prop. 1, $H^m \cong H^m \wr 1$ is isomorphic to a subgroup of index m in $H \wr G$. Since H^m is finitely generated abelian and decidability of the rational subset membership is preserved by finite extensions [12, 17], decidability for $H \wr G$ follows.

7. A. Ehrenfeucht, D. Haussler, and G. Rozenberg. On regularity of context-free languages. *Theor. Comput. Sci.*, 27:311–332, 1983.
8. S. Eilenberg and M. P. Schützenberger. Rational sets in commutative monoids. *Journal of Algebra*, 13:173–191, 1969.
9. H. Fernau and R. Stiebe. Sequential grammars and automata with valences. *Theor. Comput. Sci.*, 276(1-2):377–405, 2002.
10. A. Finkel and P. Schnoebelen. Well-structured transition systems everywhere! *Theor. Comput. Sci.*, 256(1-2):63–92, 2001.
11. R. H. Gilman. Formal languages and infinite groups. In *Geometric and computational perspectives on infinite groups, 1994*, volume 25 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, 27–51. AMS, 1996.
12. Z. Grunschlag. *Algorithms in Geometric Group Theory*. PhD thesis, University of California at Berkley, 1999.
13. L. H. Haines. On free monoids partially ordered by embedding. *Journal of Combinatorial Theory*, 6:94–98, 1969.
14. G. Higman. Ordering by divisibility in abstract algebras. *Proceedings of the London Mathematical Society. Third Series*, 2:326–336, 1952.
15. T. Jurdzinski. Leftist grammars are non-primitive recursive. In *Proc. ICALP 2008*, LNCS 5126, 51–62. Springer, 2008.
16. M. Kambites. Formal languages and groups as memory. *Communications in Algebra*, 37(1):193–208, 2009.
17. M. Kambites, P. V. Silva, and B. Steinberg. On the rational subset problem for groups. *Journal of Algebra*, 309(2):622–639, 2007.
18. M. Kunc. Regular solutions of language inequalities and well quasi-orders. *Theor. Comput. Sci.* 348(2–3): 277–293, 2005.
19. D. Kuske and M. Lohrey. Logical aspects of Cayley-graphs: the group case. *Annals of Pure and Applied Logic*, 131(1–3):263–286, 2005.
20. M. Lohrey and G. Sénizergues. Theories of HNN-extensions and amalgamated products. In *Proc. ICALP 2006*, LNCS 4052, 681–692. Springer, 2006.
21. M. Lohrey and B. Steinberg. The submonoid and rational subset membership problems for graph groups. *Journal of Algebra*, 320(2):728–755, 2008.
22. M. Lohrey and B. Steinberg. Submonoids and rational subsets of groups with infinitely many ends. *Journal of Algebra*, 324(4):970–983, 2010.
23. M. Lohrey and B. Steinberg. Tilings and submonoids of metabelian groups. *Theory Comput. Syst.*, 48(2):411–427, 2011.
24. M. Lohrey, B. Steinberg and G. Zetzsche. Rational subsets and submonoids of wreath products. http://arxiv.org/abs/1302.2455, arXiv.org, 2013.
25. R. C. Lyndon and P. E. Schupp. *Combinatorial Group Theory*. Springer, 1977.
26. M. L. Minsky. *Computation: Finite and Infinite Machines*. Prentice-Hall International, 1967.
27. R. Motwani, R. Panigrahy, V. A. Saraswat, and S. Venkatasubramanian. On the decidability of accessibility problems (extended abstract). In *Proc. STOC 2000*, 306–315. ACM, 2000.
28. V. Roman'kov. On the occurence problem for rational subsets of a group. In *International Conference on Combinatorial and Computational Methods in Mathematics*, 76–81, 1999.
29. N. S. Romanovskiĭ. Some algorithmic problems for solvable groups. *Algebra i Logika*, 13(1):26–34, 1974.
30. N. S. Romanovskiĭ. The occurrence problem for extensions of abelian groups by nilpotent groups. *Sibirsk. Mat. Zh.*, 21:170–174, 1980.
31. J. Sakarovitch. *Elements of Automata Theory*. Cambridge University Press, 2009.
32. P. Schnoebelen. Verifying lossy channel systems has nonprimitive recursive complexity. *Inf. Process. Lett.*, 83(5):251–261, 2002.