ON THE RATIONAL SUBSET PROBLEM FOR GROUPS

MARK KAMBITES, PEDRO V. SILVA, AND BENJAMIN STEINBERG

ABSTRACT. We use language theory to study the rational subset problem for groups and monoids. We show that the decidability of this problem is preserved under graph of groups constructions with finite edge groups. In particular, it passes through free products amalgamated over finite subgroups and HNN extensions with finite associated subgroups. We provide a simple proof of a result of Grunschlag showing that the decidability of this problem is a virtual property. We prove further that the problem is decidable for a direct product of a group G with a monoid M if and only if membership is uniformly decidable for G-automata subsets of M. It follows that a direct product of a free group with any abelian group or commutative monoid has decidable rational subset membership.

1. INTRODUCTION

A key aspect of combinatorial group theory is the study of algorithmic *decision problems* in finitely generated groups. This trend, which was initiated by Dehn [10], has always remained central to the subject, and has recently been given new impetus by interest in the potential use of group theory as a basis for the development of secure cryptographic systems (see, for example, [37, 39]). The best known example of a group-theoretic decision problem is the *word problem* for a given finitely generated group G: given two words over the generators, decide if they represent the same element, or equivalently, given a word over the generators, decide if it represents the identity.

A natural generalization is the *subgroup membership problem* or *generalized word problem*: given elements $u_1, \ldots, u_n$ and g of G (specified as words over the generators), decide if g lies in the subgroup generated by $u_1, \ldots, u_n$ [30]. More generally still, one can consider the corresponding problem for finitely generated *submonoids* and *subsemigroups* of groups; Margolis, Meakin and Šunić [33] have recently solved the submonoid membership problem for a large class of groups by studying *distortion functions.* Decidability of the subsemigroup problem is of particular interest since it also implies solvability of the *order problem.*

From the point of view of computer science and formal language theory, finitely generated subgroups, submonoids and subsemigroups are examples of *rational subsets* and it is natural also to consider the harder *rational subset problem* for G: given a rational subset of G (specified using a finite automaton over the generators) and a word representing an element of G, decide if the latter belongs to the former.

It is well-known that the subgroup membership problem, and more generally the rational subset problem, is decidable for free groups and for free abelian groups [3, 19, 30]. Many important groups can be built up from these groups using constructions such as *direct products*, *free products* (with and without amalgamation), *HNN extensions* and *graphs of groups* [30, 38]. Hence, a natural next step is to consider the extent to which decidability of these algorithmic problems is preserved under such operations.

Kapovich, Weidmann and Myasnikov [27] have recently studied the subgroup membership problem in fundamental groups of graphs of groups. It is natural to ask whether their results can be extended to the more general rational subset problem. Their approach generalizes the well-known *folding* technique of Stallings [40], which starts with a graph easily constructed from the subgroup generators, and incrementally computes the important part of the Schreier graph associated to a finitely generated subgroup of the free group. This method is essentially automata-theoretic, since the graphs can be viewed as automata recognising progressively larger parts of the membership language of the subgroup [6, 32, 41]. However, the folding technique relies upon a degree of symmetry in the automata (the *dual automaton* property, in the language of [41]) which is particular to the subgroup case, and so does not easily generalize.

The main aim of the present paper is to make a start upon the study of the relationship between the rational subset problem and the constructions described above. Our approach is largely language-theoretic; in Section 3, we introduce an abstract property of languages which corresponds naturally to decidability of rational subset membership. This simple observation establishes a surprisingly deep connection between algorithmic group theory and formal language theory. It immediately yields simple language-theoretic proofs of several non-trivial known results, including the fact that decidability of the rational subset problem is a virtual property, which was first proved by Grunschlag [19]; recall that a virtual property of a group is a property inherited from finite index subgroups and overgroups. Conversely, we are also able to use undecidability of a group-theoretic problem to establish a new undecidability result in language theory: there exists a context-free language for which it is undecidable which regular languages it contains.

In Section 4 we proceed to show that our abstract property is preserved when taking the ancestor set of a language under certain infinite rewriting systems. In Section 5, we apply these results to show that decidability of rational subset membership is preserved under graph of groups constructions [38] with finite edge groups. It follows in particular that it passes through amalgamated free products over finite subgroups, and HNN extensions with finite associated subgroups.

Section 6 introduces a connection between decidability of rational subsets and the theory of G-automata (see for example [17, 25]), that is, rational transductions of group word problems. Specifically, we show that a direct product of the form $G \times M$ has decidable rational subset membership exactly if membership is (uniformly) decidable for G-automata subsets of M. This combines with a group-theoretic interpretation [25] of a theorem of Chomsky and Schützenberger [9] and some classical results on commutative monoids [14, 36] to show that any direct product of a free group with an abelian group (or commutative monoid) has decidable rational subset membership.

Finally, in Section 7 we consider the subgroup membership problem and rational subset problem in the important class of *graph groups* (which are also known as *right-angled Artin groups*, *trace groups* or *free partially commutative groups*). We note some consequences for certain of these groups of our results from Sections 5 and 6, and pose a number of questions regarding other graph groups.

While the primary focus of this paper is on groups, the rational subset problem and associated decision problems are also of interest in more general monoids and semigroups. For example, recent research of Ivanov, Margolis and Meakin [23] has reduced the word problem for a large class of one-relator inverse monoids to the submonoid problem in one-relator groups. Since decidability of rational subset membership is inherited by finitely generated subsemigroups, many of our results about groups have additional implications for monoids and semigroups. We also prove directly some new results for monoids, including the fact that the rational subset problem is decidable for direct products of free groups with free monoids.

2. Preliminaries

In this section, we provide a brief introduction to rational subsets and associated decision problems.

2.1. **Rational Subsets, Languages and Transductions.** Let M be a finitely generated monoid. Recall that a *finite automaton* P over M is a finite directed graph with edges labelled by elements of M, with a distinguished *initial vertex* and a set of distinguished *terminal vertices*. The labelling of edges extends naturally, via the multiplication in M, to a labelling of paths by elements of M. The *subset recognised* by the automaton is the set of all elements of M which label paths between the initial vertex and some terminal vertex. A subset of M recognised by some finite automaton is called a *rational subset* of M. An alternative description of the rational subsets of M is as the smallest collection of subsets of M containing the finite subsets and closed under union, concatenation and generation of submonoids.

A particularly important case arises when $M = \Sigma^*$ is the free monoid on an alphabet Σ, so that the automaton P accepts a language over Σ, which we denote $L(P)$. A rational subset of a free monoid is called a *rational language* or *regular language*. By [5, Proposition III.2.2], the rational subsets of a monoid M are exactly the homomorphic images of regular languages. For a detailed introduction to the theory of regular languages, including a number of alternative definitions, see [13] or [22].

Another significant case is when $M = \Sigma^* \times \Omega^*$ is a direct product of free monoids. A finite automaton over $\Sigma^* \times \Omega^*$ is called a *finite transducer* from Σ^* to Ω^*. A subset recognised by a finite transducer, that is, a rational subset of $\Sigma^* \times \Omega^*$, is called a *rational transduction*. If $\rho \subseteq \Sigma^* \times \Omega^*$ and $L \subseteq \Sigma^*$ then the *image* of L under ρ is the language

$$L\rho = \{v \in \Omega^* \mid (u, v) \in \rho \text{ for some } u \in L\} \ \subseteq\ \Omega^*.$$

If ρ is a rational transduction then we say that the language $L\rho$ is a *rational transduction of* the language L. Rational transductions are a powerful tool for studying relationships between formal languages, and many elementary operations on languages are instances of rational transductions. For example, given a word $w \in \Sigma^*$ it is straightforward to show that there is an effectively constructible rational transduction taking each language $L \subseteq \Sigma^*$ to its *left translation* by w, that is, the language $wL = \{wx \mid x \in L\}$; an analogous result holds for *right translation*. More general information about rational transductions can be found in [5].

2.2. **Encodings and Decision Problems.** We shall work with algorithmic problems in which abstract objects such as monoid elements, automata and languages are regarded as data. Formally, it is necessary to have an agreed system of (not necessarily unique) finite encodings for such objects, but for brevity and clarity it is unhelpful to refer repeatedly to encodings. Typically we shall introduce an encoding along with the definition of a class of objects, but thereafter leave the encoding implicit.

All groups and monoids in this paper will be finitely generated, and we assume that elements are encoded as words over some (except where otherwise stated, fixed) finite monoid generating set. Our algorithms are not *uniform* across groups and monoids, and so we do not need to consider an encoding system for groups and monoids themselves.

Finite automata are presumed to have some suitable encoding, from which we can extract the vertex set and for any pairs of vertices p and q, the (encodings of) labels of all edges from p to q. Languages and subsets are typically of a type recognised by some kind of algorithm or automaton or generated by some kind of grammar, and we assume they are encoded as an automaton, algorithm or grammar.

Now let $\mathcal{C}$ be a set of subsets of a finitely generated monoid M, and suppose we have a fixed system of (not necessarily unique) encodings for elements of $\mathcal{C}$. For example, $\mathcal{C}$ might be the set of rational subsets of M, encoded as finite automata. We say that *membership is uniformly decidable for* $\mathcal{C}$ if there is an algorithm which, given an (encoded) set $S \in \mathcal{C}$, and an (encoded) element $m \in M$, decides if m lies in S. The following elementary proposition says that this property is independent of the choice of finite generating set for M.

Proposition 2.1. *Let X and Y be finite generating sets for a monoid M, and let $\mathcal{C}$ be a set of subsets of M with a system of encoding for its elements. Suppose there exists an algorithm which, given an (encoded) set $S \in \mathcal{C}$ and a word $u \in X^*$, decides if the word u represents an element of the set S. Then there exists an algorithm which, given an (encoded) set $S \in \mathcal{C}$ and a word $v \in Y^*$, decides if the word v represents an element of the set S.*

Proof. For each letter $y \in Y$, let $w_y \in X^*$ be a word representing the same element of M as y. Define a morphism $\rho : Y^* \to X^*$ by $y \mapsto w_y$ for all $y \in Y$. Now a word $v \in Y^*$ represents the same element of M as $v\rho \in X^*$. Hence, it suffices to take the algorithm which, given as input an encoded set $S \in \mathcal{C}$ and a word $v \in Y^*$, computes the word $v\rho \in X^*$ by replacing each letter y of v with w_y, and then uses the algorithm given to check whether $v\rho$ represents an element of S. $\square$

One instance of this problem forms the main focus of this paper. A monoid or group M has *decidable rational subset problem* if membership is uniformly decidable for the rational subsets of M (encoded as finite automata over the generating set). Proposition 2.1 says that this property is invariant under changing the generating set used to specify the element; much the same argument shows that it is also invariant under change of the generator set used for the edge labels in the automaton. Similarly, if a finitely generated monoid M has decidable rational subset problem, then it is clear that if N is a finitely generated submonoid of M then the rational subset problem is also decidable for N. Moreover, given an algorithm for the rational subset problem in M and a finite set of generators for the submonoid N, we can effectively compute an algorithm for the rational subset problem in N.

Decidability of the rational subset problem for a group G implies decidability of the word problem and the subgroup, subsemigroup and submonoid membership problems. Since an element $g \in G$ has finite order exactly if the subsemigroup generated by g contains the identity, an algorithm for the rational subset problem also allows one to decide if a given element has finite order. Moreover, if g does have finite order then, since the word problem is solvable, it is a simple matter to compute the order by enumerating words representing powers and checking if they represent the identity.

2.3. **Groups and Word Problems.** If G is a finitely generated group generated by a subset A then the *word problem* $W_A(G)$ for G with respect to A is the set of all words in A^* which represent the identity in G. More generally, given a monoid M generated by a subset A and an element $m \in M$, we denote by $W_A(M, m)$ the set of all words in A^* representing the element $m \in M$.

3. Regular Intersection Decidability

In this section we observe that decidability of the rational subset problem in a group is equivalent to a natural language-theoretic property of the word problem. By studying the abstract class of languages with this property, we show that many existing results about the rational subset problem for groups can be easily deduced from standard results in language theory. In Section 4, we shall see that this property of languages is preserved when taking ancestor sets under certain infinite rewriting systems. In Section 5, we shall apply these results to the rational subset problem for fundamental groups of graphs of groups, and hence for amalgamated free products and HNN extensions.

We begin by introducing an algorithmic problem that can be associated to any formal language. Let $L \subseteq \Sigma^*$ be a language. The *regular intersection decision problem* or *RID problem* for L is the problem of deciding, given a finite automaton over Σ, whether the language recognised intersects (that is, has non-empty intersection) with L. An algorithm which solves this problem is called an *RID algorithm* for L, and if there exists such an algorithm then L is called *regular intersection decidable* or *RID*. It is easily seen that an RID algorithm solves the RID problem for a unique language; hence, RID languages can be encoded (although not uniquely) as algorithms which solve their RID problem.

The following provides the connection with the rational subset problem for groups, and is our motivation for studying RID languages.

Theorem 3.1. *Let G be a group generated by a finite subset A. Then the following are (effectively) equivalent:*

(i) *rational subset membership is decidable for G;*
(ii) *the word problem for G with respect to A is RID;*
(iii) *the RID problem for $W_A(G, g)$ is decidable uniformly in $g \in G$ (where elements of G are encoded as words in A^*).*

Proof. Let R be a rational subset of G encoded as a regular language L of A^*. Then given an element $g \in G$, one has $g \in R$ if and only if L intersects with $W_A(G, g)$. This establishes the equivalence of (i) and (iii).

That (iii) implies (ii) is immediate. For the converse, let $w \in A^*$ represent $g \in G$ and let $L \subseteq A^*$ be a regular language. Then, since (ii) clearly allows us to solve the word problem, we can effectively compute a word $u \in A^*$ representing g^{-1}. Moreover, we can effectively compute the regular language uL. Now L intersects with $W_A(G, g)$ if and only if $W_A(G)$ intersects with uL; by assumption, we can test the latter. □

Despite the simplicity of the proof, we shall see that Theorem 3.1 establishes a surprisingly deep connection between algorithmic group theory and formal language theory. We observe that the equivalence of (i) and (iii) holds also for monoids. The following proposition summarises some elementary properties of the class of RID languages.

Proposition 3.2. *The class of RID languages is effectively closed under union and rational transduction (and hence also under morphism, inverse morphism, intersection with regular languages and right and left translation). The class of RID languages is strictly contained within the class of recursive languages, and contains the class of indexed languages (and hence also the context-free and regular languages).*

Proof. If L and K are RID languages and R is a regular language then R intersects with $L \cup K$ exactly if it intersects with L or K, so closure under union is clear.

For closure under rational transduction, suppose $L \subseteq A^*$ is RID and $\sigma \subseteq A^* \times B^*$ is a rational transduction; we must show that the language

$$K = L\sigma = \{b \in B^* \mid (a, b) \in \sigma \text{ for some } a \in L\}$$

is RID. To this end, suppose we are given a regular language $Q \subseteq B^*$. Let

$$P = Q\sigma^{-1} = \{a \in A^* \mid (a, b) \in \sigma \text{ for some } b \in Q\}.$$

Then P is a regular language, and moreover can be effectively computed from Q [5, Corollary III.4.2]. Now it is easily verified that K intersects with Q if and only if L intersects with P; by assumption, the latter can be checked.

The class of indexed languages (encoded as indexed grammars) is effectively closed under intersection with regular languages [1, Corollary 3], and has decidable emptiness problem [1, Theorem 4.1]. Thus, one can test if a regular language R intersects with an indexed language L by computing the intersection $L \cap R$, and testing it for emptiness. Hence, indexed languages are RID. Since regular and context-free languages are indexed [1], it follows also that these languages are RID.

Since singleton sets are (effectively computable as) regular sets, the membership problem for a language is reducible to the RID problem, so RID languages are recursive. On the other hand, the group $F_2 \times F_2$ has solvable word problem but undecidable rational subset problem [30, 34]. Hence, by Theorem 3.1, its word problem is recursive but not RID. $\square$

We now discuss a number of consequences of Theorem 3.1 and Proposition 3.2. The following lemma will combine with these results to show that the decidability of the rational subset problem is inherited by finite index overgroups, and hence is a *virtual property*. The idea, which has been used by several authors [15, 17, 20], is essentially a recoding of the Kaloujnine-Krasner embedding [24]. For completeness, we state and prove the lemma explicitly.

Lemma 3.3. *Let G be a finitely generated group and H a finite index subgroup. Let X be a finite generating set for G and Y be a finite generating set for H. Then there is a rational transduction $\sigma \subseteq Y^* \times X^*$ such that $W_X(G) = W_Y(H)\sigma$.*

Proof. Let $g_1, \ldots, g_n$ be a complete set of right coset representatives of H in G, assuming without loss of generality that g_1 is the identity. For each $x \in X$ and $i \in \{1, \ldots, n\}$, choose a word $w_{i,x} \in Y^*$ representing the unique element $h_{i,x} \in H$ such that $g_i x = h_{i,x} g_j$, where $Hg_i x = Hg_j$. Our transducer has vertex set G/H. The labelled edges are of the form $Hg_i \stackrel{(w_{i,x},x)}{\longrightarrow} Hg_i x$ with $x \in X$, $i \in \{1, \ldots, n\}$. The initial vertex and terminal vertex are both the coset H. If $\sigma \subseteq Y^* \times X^*$ is the associated rational transduction, then it is easy to see that $\sigma^{-1} : X^* \to Y^*$ is a partial function such that, for $w \in X^*$, $w\sigma^{-1}$ is defined if and only if w represents an element of H, in which case $w\sigma^{-1}$ is an element of Y^* representing the same element of H as w; in particular $w \in W_X(G)$ if and only if $w\sigma^{-1} \in W_Y(H)$. It follows that $W_Y(H)\sigma = W_X(G)$. $\square$

Theorem 3.1, Proposition 3.2 and Lemma 3.3 immediately yield the following result of Grunschlag [19].

Corollary 3.4. *Let G and H be finitely generated groups such that H is a finite index subgroup of G and suppose that H has decidable rational subset membership. Then G has decidable rational subset membership.*

The easier part of a celebrated theorem of Muller and Schupp [35] states that every finitely generated virtually free group has context-free word problem. Combining this with Theorem 3.1 and Proposition 3.2, we immediately obtain the following result which subsumes a result of Benois [3]. A proof of this nature was first suggested by Margolis and Meakin [31].

Corollary 3.5. *Finitely generated virtually free groups have decidable rational subset problem.*

A significant open question is that of which finitely generated groups have word problems which are *indexed languages* [1, 2, 18, 29]; an answer is likely to be of significant interest in both group theory and language theory. Theorem 3.1 and Proposition 3.2 give an alternative proof of the following result of Lisovik [29], which gives a necessary condition for a group to have indexed word problem.

Corollary 3.6. *Let G be a finitely generated group with indexed word problem. Then G has decidable rational subset membership (and hence decidable subgroup membership problem and order problem).*

We can also use Theorem 3.1 to obtain some purely language theoretic results. We have already observed that the group $F_2 \times F_2$ has undecidable subgroup membership problem [30, 34] and hence, by Theorem 3.1, non-RID word problem. In [20], it is shown that the word problem of this group is the complement of a context-free language. Combining these two we obtain the following.

Corollary 3.7. *The class of complements of context-free languages is not contained in the class of RID languages.*

Since a regular language intersects with a language L exactly if it is not contained in the complement of L, Corollary 3.7 is equivalent to the following statement.

Corollary 3.8. *There exists a context-free language L such that there is no algorithm which decides, given a regular language R, whether R is contained in L.*

We note that the related problems in which the regular language is fixed and the context-free language varies are also undecidable in general, as a consequence of undecidability of completeness for context-free languages; a detailed study of these problems can be found in [21].

4. RID Languages and Monadic Rewriting Systems

In this section, we show that the class of RID languages is closed under the operation of taking ancestor sets with respect to certain infinite rewriting systems. In Section 5 we shall use this result to show that decidability of the rational subset problem passes through graph of groups constructions with finite edge groups.

A *monadic rewriting system* Γ over a finite alphabet Σ is a subset of $\Sigma^* \times (\Sigma \cup \{\varepsilon\})$. An element $(w, x) \in \Gamma$ is normally written $w \to x$. If $\mathcal{C}$ is a class of languages, then Γ is called a *$\mathcal{C}$-monadic rewriting system* if for each $x \in \Sigma \cup \{\varepsilon\}$, the set

$$\Gamma_x = \{w \in \Sigma^* \mid (w \to x) \in \Gamma\}$$

belongs to $\mathcal{C}$. A finite encoding system for the class $\mathcal{C}$ naturally gives rise to a finite encoding system for $\mathcal{C}$-monadic rewriting systems which stores for each $x \in \Sigma \cup \{\epsilon\}$ an encoding of Γ_x. We shall be particularly interested in the case where $\mathcal{C}$ is the class of RID languages, encoded via RID algorithms.

If Γ is a monadic rewriting system, then we write $u \Rightarrow v$ if $u = rws \in \Sigma^*$ and $v = rxs \in \Sigma^*$ with $w \to x \in \Gamma$. We denote by $\Rightarrow^*$ the reflexive, transitive closure of the relation $\Rightarrow$. If $u \Rightarrow^* v$, then v is said to be a *descendant* of u (under Γ) and u is said be an *ancestor* of v (under Γ). If $L \subseteq \Sigma^*$ is a language, then $L\Gamma$ denotes the set of all descendants of L under Γ and $L\Gamma^{-1}$ denotes the set of all ancestors of L under Γ.

It is well-known to computer scientists that the set of descendants of a regular language under a monadic rewriting system is again a regular language. Moreover, if the rewriting system is finite [4, 8] or context-free [7] then one can algorithmically construct an automaton for the language of descendants. The following theorem gives a more general condition under which this is possible.

Theorem 4.1. *Let $\Gamma \subseteq \Sigma^* \times (\Sigma \cup \{\varepsilon\})$ be a monadic rewriting system and let $L \subseteq \Sigma^*$ be a regular language. Then $L\Gamma$ is regular. Moreover, there is an algorithm which, given an RID monadic rewriting system (encoded via the RID algorithms for the Γ_x, $x \in \Sigma \cup \{\varepsilon\}$) and a finite automaton recognising a language $L \subseteq \Sigma^*$, produces an automaton recognising $L\Gamma$.*

Proof. Let M_0 be a finite automaton recognising a language $L \subseteq \Sigma^*$. Clearly, by subdividing edges and adding extra vertices as necessary, we may assume without loss of generality that the edges of M_0 are labelled by elements of $\Sigma \cup \{\varepsilon\}$. Now starting from M_0, we construct a sequence of automata as follows.

The automaton M_{i+1} has the same vertex set as M_i, and all the edges of M_i (which we call *inherited edges* in M_{i+1}), plus some additional edges (called *new edges*) constructed as follows. For each pair of vertices p and q in M_i denote by L^i_{pq} the set of all words labelling paths from p to q in M_i. For each element $x \in \Sigma \cup \{\varepsilon\}$ such that $\Gamma_x \cap L^i_{pq} \neq \emptyset$, M_{i+1} is given a new edge from p to q labelled x (unless M_i already had one).

Moreover, L^i_{pq} is easily seen to be (effectively computable as) a regular language. Hence, if we are given Γ encoded using RID algorithms, we can test whether each Γ_x intersects with L^i_{pq} and so M_{i+1} can be effectively constructed from M_i.

Since every automaton in the sequence has the same vertex set, and at each stage we only add edges labelled by the (finitely many) letters in $\Sigma \cup \{\varepsilon\}$ in places where they do not already exist, the sequence must terminate. That is, there exists j such that $M_k = M_j$ for all $k \geq j$. We claim that $L\Gamma = L(M_k)$.

Clearly $L(M_i) \subseteq L(M_{i+1})$ for each i since we have been adding new edges. We claim that if $v \in L(M_i)$ and $v \Rightarrow w$, then $w \in L(M_{i+1})$. Indeed, suppose $v = rus$ and $w = rxs$ with $u \to x \in \Gamma$. Then v labels a successful path π in M_i and there is a factorisation $\pi = \rho\Upsilon\sigma$ such that the paths ρ, Υ, σ are respectively labelled by r, u, s. Let e, f be the respective initial and terminal vertices of the path Υ. Then either an edge ξ from e to f labelled by x already exists in M_i, or a new edge ξ from e to f with label x is added in the construction of M_{i+1}. Hence $\rho\xi\sigma$ is a successful path labelled by $w = rxs$ in M_{i+1}. It follows immediately that if $u \in L$ and $u \Rightarrow^* w$, then $w \in L(M_r)$ where r is the number of steps needed to derive w from u. Hence $L\Gamma \subseteq L(M_k)$.

To show the converse, it suffices to show that $L(M_{i+1}) \subseteq L(M_i)\Gamma$. Suppose $w \in L(M_{i+1})$. Then M_{i+1} has a path π from the initial vertex to some terminal vertex labelled w; consider a factorisation $w = w_0x_1w_1x_2w_2 \dots x_nw_n$ where, in the path π, each $w_j \in \Sigma^*$ is read along inherited edges and each $x_j \in \Sigma \cup \{\varepsilon\}$ is read along a new edge from e_j to f_j. Now by the construction of M_i, for each x_j there exists $y_j \in \Sigma^*$ such that $y_j \to x_j \in \Gamma$

and y_j labels a path from e_j to f_j in M_i. If follows that the word $v = w_0 y_1 w_1 \dots y_n w_n \in L(M_i)$. Since $v \Rightarrow^* w$, we see that $L(M_{i+1}) \subseteq L(M_i)\Gamma$. Thus $L(M_k) \subseteq L(M_0)\Gamma = L\Gamma$, as required. □

In [7], it is shown that the set of ancestors of a context-free language under a context-free monadic rewriting system is always context-free. We obtain an analogous effective result for RID rewriting systems.

Corollary 4.2. *Let $L \subseteq \Sigma^*$ be an RID language and let Γ be an RID monadic rewriting system over Σ. Then $L\Gamma^{-1}$ is RID. Moreover, there is an algorithm which, given an RID language (encoded as an RID algorithm) and an RID monadic rewriting system Γ (encoded as above), outputs an RID algorithm for $L\Gamma^{-1}$.*

Proof. Let $R \subseteq \Sigma^*$. Then it is straightforward to verify that R intersects with $L\Gamma^{-1}$ if and only if $R\Gamma$ intersects with L.

The corollary is now immediate from Theorem 4.1 since a finite automaton recognising $R\Gamma$ can be effectively constructed and we can use the RID algorithm for L to check whether $R\Gamma$ intersects with L. □

This corollary allows a new interpretation of the rational subset problem.

Corollary 4.3. *Let G be a group with finite generating set A. Then the following are equivalent:*

(i) *G has a decidable rational subset problem;*
(ii) *$W_A(G)$ is RID;*
(iii) *$W_A(G) = \{\varepsilon\}\Gamma^{-1}$ for some RID monadic rewriting system Γ.*

Proof. Theorem 3.1 gives the equivalence of (i) and (ii). To show that (ii) implies (iii) simply take the RID monadic rewriting system consisting of all rules $w \to \varepsilon$ where w belongs to the word problem. The implication (iii) implies (ii) is an immediate consequence of Corollary 4.2 and the fact that singletons are RID languages. □

5. Graphs of Groups, Amalgamated Products and HNN Extensions

In this section, we apply the language-theoretic results of Section 3 to some problems in group theory. We show that decidability of rational subset membership is preserved under graph of groups constructions [38] with finite edge groups. A particular consequence is that this property passes through free products amalgamated over finite subgroups, and under HNN extensions with finite associated subgroups.

We briefly recall the definitions of a graph of groups and its fundamental group; a detailed introduction can be found in [38]. Let Y be a finite, directed graph with (possibly) loops and multiple edges. We denote by $V(Y)$ and $E(Y)$ the vertex and edge sets respectively of Y. Let $\alpha, \omega : E(Y) \to V(Y)$ be the functions which take each edge to its start and end respectively. Suppose we have a fixed-point-free involution $y \mapsto \overline{y}$ on the edge set $E(Y)$ which is orientation-reversing, that is, such that $y\alpha = \overline{y}\omega$ for all $y \in E(Y)$.

A *graph of groups* (G, Y) with underlying graph Y consists of

(i) for each vertex $v \in V(Y)$, a group G_v;
(ii) for each edge $y \in E(Y)$, a group G_y such that $G_y = G_{\overline{y}}$; and
(iii) for each edge $y \in E(Y)$, injective morphisms $\alpha_y : G_y \to G_{y\alpha}$ and $\omega_y : G_y \to G_{y\omega}$ such that $\alpha_y = \omega_{\overline{y}}$ for all $y \in E(Y)$.

We assume that the groups G_v intersect only in the identity, and that they are disjoint from the edge set $E(Y)$. For each $v \in V(Y)$, let $\langle X_v \mid R_v \rangle$ be a monoid presentation for the vertex group G_v, with the different generating sets X_v disjoint. Let B denote the (disjoint) union of $E(Y)$ with all the sets X_v. We define a group $F(G, Y)$ by the monoid presentation

$$\begin{aligned} F(G,Y) \ = \ \langle \ B \ \mid & R_v \ \ (v \in V(Y))\,, \\ & y\overline{y} = 1 \ \ (y \in E(Y))\,, \\ & y(g\omega_y)\overline{y} = g\alpha_y \ \ (y \in E(Y), g \in G_y) \ \rangle. \end{aligned}$$

Fix a vertex $v_0 \in V(Y)$. We say that a word $w \in B^*$ is of *cycle type at* v_0 if it is of the form $w = w_0 y_1 w_1 y_2 w_2 \dots y_n w_n$ where:

(i) each $y_i \in E(Y)$;
(ii) $y_1 \cdots y_n$ is a path in Y starting and ending at v_0;
(iii) $w_0 \in X_{v_0}^*$;
(iv) for $1 \leq i \leq n$, $w_i \in X_{y_i\omega}^*$.

The images in $F(G, Y)$ of the words of cycle type at v_0 form a subgroup $\pi_1(G, Y, v_0)$ of $F(G, Y)$, called the *fundamental group of* (G, Y) *at* v_0. If the graph Y is connected then the fundamental group is (up to isomorphism) independent of the choice of vertex v_0. The groups $F(G, Y)$ and $\pi_1(G, Y, v_0)$ are also easily seen to be independent of the presentations chosen for the vertex groups.

Theorem 5.1. *Let (G, Y) be a finite, connected, non-empty graph of finitely generated groups with finite edge groups. Then the fundamental group of (G, Y) has decidable rational subset problem if and only if every vertex group has decidable rational subset problem. Moreover, the equivalence is effective.*

Proof. Since each vertex group embeds into the fundamental group [38], one implication is immediate.

For the converse, we use the notation defined above. Since the vertex groups are assumed to be finitely generated, we may assume that the generating sets X_v are finite. Moreover, since the edge groups are finite and there are finitely many edges, we may assume without loss of generality that for every edge y, the sets $X_{y\alpha}$ and $X_{y\omega}$ contain a letter representing each non-identity element of $G_{y\alpha}\alpha_y$ and $G_{y\omega}\omega_y$, respectively. Let B be the (disjoint) union of all the sets X_v and the edges of Y. Then B is a finite generating set for the group $F(G, Y)$.

Fix a vertex $v_0 \in V(Y)$, and let $P \subseteq B^*$ denote the set of words of cycle type at v_0. We claim first that the intersection of P with the word problem W of $F(G, Y)$ is RID. To show this we define an RID monadic rewriting system Γ over B with the following three types of rules:

- If v is a vertex and $w \in X_v$ represents the identity of G_v, then there is a rule $w \to \varepsilon$;

- If y is an edge, then there is a rule $y\overline{y} \to \varepsilon$;
- If y is an edge and $h \in X_{y\alpha}$ is a letter representing $g \in G_y\alpha_y$ and $w \in X_{y\omega}^*$ represents $g\omega_y$, then there is a rule $yw\overline{y} \to h$.

Since all the vertex groups G_v are assumed to be RID, it follows easily from Theorem 3.1 and Proposition 3.2 that Γ is an RID monadic rewriting system. Let $L = \{\varepsilon\}\Gamma^{-1}$. Since a singleton language is RID, we deduce by Corollary 4.2 that L is RID (as singletons are clearly RID languages). We claim that L is the intersection of the language P of words of cycle type at v_0 with the word problem W of $F(G, Y)$.

Clearly, the rewriting rules in Γ are relations satisfied in $F(G, Y)$, from which it follows that $L \subseteq W$. It is also easy to see that the rewriting rules in Γ and their inverses preserve paths of cycle type at v_0, so that $L \subseteq P$. Thus, $L \subseteq W \cap P$.

Conversely, suppose that $w \in W \cap P$. Then we can write

$$w = w_0y_1w_1y_2w_2 \ldots y_nw_n$$

as per (i)-(iv) above. We proceed by induction on the parameter n (which we shall term the length of w) to show that $w \in L$. If $n = 0$, then w represents 1 in G_{v_0} and so $w \to \varepsilon \in \Gamma$, whence $w \Rightarrow \varepsilon$, establishing $w \in L$.

Assume that all elements of $W \cap P$ of length at most $k < n$ belong to L. Since $w \in W \cap P$, it follows by [38, Theorem I.11] that there exists i such that $y_{i+1} = \overline{y_i}$ and w_i represents an element $g\omega_{y_i}$ for some $g \in G_{y_i}$. There are two cases: either $g = 1$ or $g \neq 1$. If $g = 1$, then we may apply the rule $w_i \to \varepsilon$ followed by the rule $y_i\overline{y_i} \to \varepsilon$ to show that if $w' = w_0y_1 \ldots w_{i-1}w_{i+1}y_{i+2} \cdots w_n$, then $w \Rightarrow^* w'$. As $w' \in W \cap P$ and has smaller length, it follows by induction that $w' \in L$, from which we obtain $w \in L$. If $g \neq 1$, let $h \in X_{y_i\alpha}$ be a letter representing $g\alpha_{y_i}$. Then by definition $y_iw_i\overline{y_i} \to h$ lies in Γ. Since $y_{i+1} = \overline{y_i}$, if we set $w' = w_0y_1 \ldots w_{i-1}hw_{i+1}y_{i+2} \cdots w_n$, then $w \Rightarrow w'$. Since $w' \in W \cap P$ represents the identity in $F(G, Y)$ and its expression is shorter, we obtain by induction that $w' \Rightarrow^* \varepsilon$ and so $w \Rightarrow^* \varepsilon$. Thus, we conclude that $W \cap P = L$ and so is RID, as claimed.

Now let X be a finite monoid generating set for the fundamental group $\pi_1(G, Y, v_0)$; this group is indeed finitely generated, namely by a set in correspondence with the disjoint union of the generating sets X_v and the set of edges not belonging to some spanning tree for Y [38]. Choose a morphism $\rho : X^* \to B^*$ which takes each element $x \in X$ to some word $w_x \in P$ which represents the same element of $\pi_1(G, Y, v_0)$ as x. Since P is a submonoid of B^*, the image of ρ lies in P. Hence, for any word $w \in X^*$, w lies in the word problem of $\pi_1(G, Y, v_0)$ with respect to X if and only if $w\rho$ lies in W, that is, if and only if $w\rho$ lies in $W \cap P = L$. So the word problem for $\pi_1(G, Y, v_0)$ is an inverse morphic image of an RID language, and so by Proposition 3.2 is RID. The theorem now follows from Theorem 3.1. □

An *HNN extension* is the fundamental group of a graph of groups with a single vertex v and a matched pair $y, \overline{y}$ of loops at v. The vertex group G_v is the base group of the HNN construction, while the edge group $G_y = G_{\overline{y}}$ is isomorphic to the associated subgroups [38]. Hence, we obtain the following corollary.

Corollary 5.2. *Let H be an HNN extension of a group G with finite associated subgroups. Then H has decidable rational subset problem if and only if G has decidable rational subset problem. Moreover, the equivalence is effective.*

Similarly, an *amalgamated free product* corresponds to the fundamental group of a graph of groups with two vertices connected by a matched pair of edges [38], yielding the following result.

Corollary 5.3. *Let H be a free product of groups G_1 and G_2 amalgamated over a finite subgroup. Then H has decidable rational subset problem if and only if G_1 and G_2 have decidable rational subset problem. Moreover, the equivalence is effective.*

We remark that the proof of Theorem 5.1 establishes a more general fact. Recall that if $\mathcal{C}$ is a class of languages closed under inverse morphisms then the property of a finitely generated group having word problem in $\mathcal{C}$ is independent of the finite generating set chosen [20, Lemma 1].

Theorem 5.4. *Let $\mathcal{C}$ be a class of languages closed under inverse morphism, left and right translation and closed under taking the ancestors of $\{\varepsilon\}$ for any $\mathcal{C}$-monadic rewriting system. Then the fundamental group of a finite graph of finitely generated groups with finite edge groups has word problem in $\mathcal{C}$ if all the vertex groups have word problems in $\mathcal{C}$. The converse is true if $\mathcal{C}$ is closed under intersection with regular languages.*

The assumptions of Theorem 5.4 are satisfied by, for example, the class of context-free languages [5, 7]. A well-known theorem of Muller and Schupp [35] augmented by a subsequent result of Dunwoody [12] says that a group has context-free word problem if and only if it is virtually free. Our method therefore gives the following result, which can also be proved in many other ways, for instance from work of Karrass, Pietrowski and Solitar [28].

Corollary 5.5. *Let (G, Y) be a finite, connected graph of groups with finite edge groups. Then the fundamental group of (G, Y) is virtually free if and only if every vertex group is virtually free.*

6. G-automata and Rational Subsets

In this section, we consider the rational subset problem in direct products. We show that if G is a finitely generated group and M a finitely generated monoid, then the rational subset problem for $G \times M$ is decidable exactly if the subsets of M defined by *G-automata* have uniformly decidable membership problem. This combines with a group-theoretic interpretation [25] of a well-known theorem of Chomsky and Schützenberger [9] to give a characterisation of rational subset membership in direct products of the form $F \times M$ with F a free group, in terms of the uniform decidability of membership for context-free subsets of M.

Let G be a finitely generated group. Recall that a *G-automaton over the alphabet* Σ is a finite automaton P over $G \times \Sigma^*$. The *G-automaton language accepted by* P is the set of all words $w \in \Sigma^*$ such that $(1, w)$ belongs to the rational subset recognised by P [17, 25]. The G-automaton languages are exactly the rational transductions of the word problem of

G [25, Proposition 2]. More generally, we say that a *G-automaton over a monoid M* is a finite automaton P over $G \times M$. The *G-automaton subset* recognised by P is the set of all elements $m \in M$ such that $(1, m)$ belongs to the rational subset recognised by P. It is easily seen that the G-automaton subsets are exactly the homomorphic images of G-automaton languages.

Having fixed G and M and some finite generating sets A and B respectively, the G-automata subsets of M have a natural encoding as finite automata over $G \times M$. Thus, we may ask whether membership is uniformly decidable for G-automaton subsets of M; an argument similar to the proof of Proposition 2.1 shows that this property is independent of the choice of generating sets. The following result relates decidability properties of G-automaton subsets to the rational subset membership problem.

Theorem 6.1. *Let G be a finitely generated group, and M a finitely generated monoid. Then the following are equivalent:*

(i) *the rational subset problem for $G \times M$ is decidable;*
(ii) *membership is uniformly decidable for G-automaton subsets of M.*

Proof. Let A and B be finite generating sets for G and M respectively, so that $A \cup B$ is a generating set for $G \times M$. In view of our comments above, we may assume that all words and automata are encoded using these generating sets.

Suppose first that (i) holds, that is, that the rational subset problem is decidable, and that we are given a finite automaton P over $G \times M$ and an element $m \in M$. In view of our choice of generators, the word over B encoding $m \in M$ also encodes the element $(1, m) \in G \times M$. Now m lies in the G-automaton language defined by P if and only if $(1, m)$ lies in the rational subset defined by P. By assumption, this can be tested, so that (ii) holds

Conversely, suppose (ii) holds, and that we are given a finite automaton P defining a rational subset of $R \subseteq G \times M$ and an element $(g, m) \in G \times M$. Since (g, m) is encoded as a word over $A \cup B$, we can easily compute a word representing $(g, 1)$ and from that, a word representing $(g^{-1}, 1)$. It follows that we can construct from P a finite automaton Q recognising the rational subset $(g^{-1}, 1)R$. Now (g, m) lies in R if and only if $(1, m)$ lies in $(g^{-1}, 1)R$, that is, if and only if $(1, m)$ is accepted by Q as a G-automaton. Once again, this can be tested, which shows that (i) holds and completes the proof. □

We note that, since property (i) in the statement of Theorem 6.1 is symmetric in G and M, we obtain the following corollary for G-automaton subsets of groups.

Corollary 6.2. *Let G and H be finitely generated groups. Then the following are equivalent:*

(i) *membership is uniformly decidable for G-automata subsets of H;*
(ii) *membership is uniformly decidable for H-automata subsets of G.*

We now turn our attention to the implications of Theorem 6.1 in the case that the group G is a finitely generated free group F of rank 2 or more. By [25, Theorem 7], which is essentially a group-theoretic restatement of the Chomsky-Schutzenberger theorem [5, 9], the languages accepted by F-automaton are exactly the context-free languages, Combining with Theorem 6.1, we immediately obtain the following corollary, where F_n denotes a free group of rank n.

Corollary 6.3. *Let M be a finitely generated monoid. Then the following are equivalent:*

(i) *the rational subset problem is decidable for the direct product $F_2 \times M$;*
(ii) *the rational subset problem is decidable for the direct product $F_n \times M$ for all $n \geq 0$;*
(iii) *membership is uniformly decidable for context-free subsets of M (encoded as context-free grammars over a finite generating set).*

This leads to a new proof of the following result of Frougny, Sakarovitch and Schupp [16].

Corollary 6.4. *The membership problem for context-free subsets of a free non-abelian group on at least 2 generators is undecidable.*

Proof. If F is a free non-abelian group then $F \times F$ has undecidable subgroup membership problem [30, 34] and hence undecidable rational subset problem. The result now follows from Corollary 6.3. □

Applying known results from language theory, we obtain the following.

Theorem 6.5. *Let F be a free group. The rational subset problem is decidable for:*

(i) *direct products $F \times A$ with A a finitely generated abelian group;*
(ii) *direct products $F \times M$ with M a finitely generated commutative monoid; and*
(iii) *direct products $F \times X^*$ with X a finite set.*

Proof. In each case, by Corollary 6.3, it suffices to show that membership is uniformly decidable for context-free subsets of the monoid in question (encoded as context-free grammars over a finite generating set). This is well-known for the case of a free monoid X^* [22, Section 6.3], so (iii) holds.

Since abelian groups are examples of commutative monoids, it suffices now to prove case (ii). Let M be a commutative monoid generated by a finite subset X; then there is a surjective morphism $\rho : X^* \to M$. Let $\sigma : X^* \to \mathbb{N}^X$ be the canonical morphism from the free monoid X^* to the free commutative monoid $\mathbb{N}^X$ on X; clearly ρ factors through σ via a morphism $\tau : \mathbb{N}^X \to M$.

Now suppose we are given a context-free subset of M (encoded as a context-free grammar over X) and an element $m \in M$ encoded as a word $w \in X^*$. Let L be the language over X generated by the grammar. Then by Parikh's Theorem [36], we can effectively compute a regular language L' such that $L'\sigma = L\sigma$. Hence $L\rho = L'\rho$ is a rational subset of M. But a result of Eilenberg and Schützenberger [14] shows that the preimage of any rational subset of M under τ is a rational subset of $\mathbb{N}^X$. Moreover, the proof is effective: one can effectively find a regular language $L'' \subseteq X^*$ such that $L''\sigma = L'\rho\tau^{-1}$. So $m \in L$ if and only if $w\sigma \in L''\sigma$. Hence we have reduced our problem to the rational subset membership problem for $\mathbb{N}^X$. Now $\mathbb{N}^X$ is a finitely generated submonoid of $\mathbb{Z}^X$. It was observed by Grunschlag [19] that the description of rational subsets in commutative monoids as semilinear sets, due to Eilenberg and Schützenberger [14], leads to an immediate solution of the rational subset membership problem for $\mathbb{Z}^X$ (and hence $\mathbb{N}^X$) via integer programming. This completes the proof. □

7. Graph Groups

In this section, we briefly discuss the subgroup membership problem and rational subset problem for the class of graph groups (which are also known as right-angled Artin groups, trace groups or free partially commutative groups).

Let Γ be a finite undirected graph; we denote by $V(\Gamma)$ the vertex set of Γ, and by $E(\Gamma)$ the edge set of Γ, which we view as a symmetric, reflexive subset of $V(\Gamma) \times V(\Gamma)$. Recall that the graph group $G(\Gamma)$ is the group with presentation

$$\langle\ V(\Gamma)\ \mid\ ef = fe \text{ for all } (e,f) \in E(\Gamma)\ \rangle.$$

The extreme examples of graph groups, obtained when Γ has no edges or is complete, are free groups and free abelian groups respectively. In general, there are many properties of groups which are easily seen to hold for free groups and free abelian groups, but for radically different reasons. Establishing the extent to which such properties hold in general graph groups is often much more difficult, but can be very enlightening. Decidability of the subgroup membership problem and decidability of the rational subset problem are two such properties.

A recent result of Kapovich, Weidmann and Myasnikov [27] shows that the subgroup membership problem is decidable for graph groups on finite graphs without chord-free cycles of length four or more. On the other hand, the graph group on a four-cycle is a direct product of non-abelian free groups; it follows from the results of Mikhailova [30, 34] discussed above that the subgroup membership problem is undecidable for $G(\Gamma)$ whenever Γ contains a chord-free four-cycle. Decidability of the subgroup membership problem seems to be open for graph groups $G(\Gamma)$ where Γ contains chord-free cycles but not of length four; these groups do not contain a direct product of non-abelian groups as a subgroup [26], and so Mikhailova's result does not assist. The following question is an obvious starting point for research in this direction.

Question 7.1. *Is the subgroup membership problem decidable for the graph group on an n-cycle with $n \geq 5$?*

Similarly, we have seen that the rational subset problem is decidable for free groups and free abelian groups. Combining Corollary 5.3 and Theorem 6.5 we immediately obtain decidability for a somewhat larger class.

Corollary 7.2. *The rational subset membership problem is decidable for free products of direct products of a free group with a free abelian group.*

In graph-theoretic terms, Corollary 7.2 applies to $G(\Gamma)$ where every connected component of Γ is the join (see [11]) of a complete graph and a graph with no edges. On the other hand, we saw above that the subgroup membership problem is undecidable for $G(\Gamma)$ where Γ contains a four-cycle without chords, so the rational subset problem is also undecidable in these cases. Many cases remain open; these are summarised in the following question.

Question 7.3. *Is the rational subset membership problem decidable for $G(\Gamma)$ when*

(i) Γ *is a three-edge line?*
(ii) Γ *has no chord-free cycles of length four or more?*
(iii) Γ *is an n-cycle with $n \geq 5$?*
(iv) Γ *contains no chord-free four-cycles?*

Acknowledgements

The authors would like to thank Stuart Margolis and Friedrich Otto for some helpful conversations. The research of the first author was supported by a Marie Curie Intra-European Fellowship within the 6th European Community Framework Programme; he would also like to thank Kirsty for all her support and encouragement. The second author acknowledges support from C.M.U.P., financed by F.C.T. (Portugal) through the programmes POCTI and POSI, with national and European Community structural funds, as well as the European Science Foundation programme AutoMathA. The work of the third author was supported by an NSERC discovery grant.

References

[1] A. V. Aho. Indexed grammars—an extension of context-free grammars. *J. Assoc. Comput. Mach.*, 15:647–671, 1968.
[2] A. V. Aho. Nested stack automata. *J. Assoc. Comput. Mach.*, 16:383–406, 1969.
[3] M. Benois. Parties rationnelles du groupe libre. *C. R. Acad. Sci. Paris Sér. A-B*, 269:A1188–A1190, 1969.
[4] M. Benois. Descendants of regular language in a class of rewriting systems: algorithm and complexity of an automata construction. In *Rewriting techniques and applications (Bordeaux, 1987)*, volume 256 of *Lecture Notes in Comput. Sci.*, pages 121–132. Springer, Berlin, 1987.
[5] J. Berstel. *Transductions and Context-Free Languages.* Informatik. Teubner, 1979.
[6] J.-C. Birget, S. W. Margolis, J. Meakin, and P. Weil. PSPACE-complete problems for subgroups of free groups and inverse finite automata. *Theor. Comp. Sci.*, 242:247–281, 2000.
[7] R. V. Book, M. Jantzen, and C. Wrathall. Monadic Thue systems. *Theoret. Comput. Sci.*, 19(3):231–251, 1982.
[8] R. V. Book and F. Otto. *String-rewriting Systems.* Springer-Verlag, 1993.
[9] N. Chomsky and M. P. Schützenberger. The algebraic theory of context-free languages. In *Computer programming and formal systems*, pages 118–161. North-Holland, Amsterdam, 1963.
[10] M. Dehn. Über unendliche diskontinuierliche Gruppen. *Math. Ann.*, 71(1):116–144, 1911.
[11] C. Droms, B. Servatius, and H. Servatius. Groups assembled from free and direct products. *Discrete Math.*, 109(1-3):69–75, 1992.
[12] M. J. Dunwoody. The accessibility of finitely presented groups. *Invent. Math.*, 81(3):449–457, 1985.
[13] S. Eilenberg. *Automata, languages, and machines. Vol. A.* Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], New York, 1974. Pure and Applied Mathematics, Vol. 58.

[14] S. Eilenberg and M. P. Schützenberger. Rational sets in commutative monoids. *J. Algebra*, 13:173–191, 1969.
[15] G. Z. Elston and G. Ostheimer. On groups whose word problem is solved by a counter automaton. *Theoret. Comput. Sci.*, 320(2-3):175–185, 2004.
[16] C. Frougny, J. Sakarovitch, and P. Schupp. Finiteness conditions on subgroups and formal language theory. *Proc. London Math. Soc. (3)*, 58(1):74–88, 1989.
[17] R. H. Gilman. Formal languages and infinite groups. In *Geometric and computational perspectives on infinite groups (Minneapolis, MN and New Brunswick, NJ, 1994)*, volume 25 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 27–51. Amer. Math. Soc., Providence, RI, 1996.
[18] R. H. Gilman and M. Shapiro. On groups whose word problem is solved by a nested stack automaton. `arXiv:math.GR/9812028`, 1998.
[19] Z. Grunschlag. *Algorithms in Geometric Group Theory.* PhD thesis, University of California at Berkeley, 1999.
[20] D. F. Holt, S. Rees, C. E. Röver, and R. M. Thomas. Groups with context-free co-word problem. *J. London Math. Soc. (2)*, 71(3):643–657, 2005.
[21] J. E. Hopcroft. On the equivalence and containment problems for context-free languages. *Math. Systems Theory*, 3:119–124, 1969.
[22] J. E. Hopcroft and J. D. Ullman. *Formal languages and their relation to automata.* Addison-Wesley, 1969.
[23] S. V. Ivanov, S. W. Margolis, and Meakin. J. C. On one-relator inverse monoids and one-relator groups. *J. Pure Appl. Algebra*, 159:83–111, 2001.
[24] L. Kaloujnine and M. Krasner. Le produit complet des groupes de permutations et le problème d'extension des groupes. *C. R. Acad. Sci. Paris*, 227:806–808, 1948.
[25] M. E. Kambites. Formal languages and groups as memory. `arXiv:math.RA/0601061`, 2006.
[26] M. E. Kambites. On commuting elements and embeddings of graph groups and monoids. `arXiv:math.RA/0601042`, 2006.
[27] I. Kapovich, R. Weidmann, and A. Myasnikov. Foldings, graphs of groups and the membership problem. *Internat. J. Algebra Comput.*, 15(1):95–128, 2005.
[28] A. Karrass, A. Pietrowski, and D. Solitar. Finite and infinite cyclic extensions of free groups. *J. Austral. Math. Soc.*, 16:458–466, 1973. Collection of articles dedicated to the memory of Hanna Neumann, IV.
[29] L. P. Lisovik. Groups defined by nested stack automata. *Questions of algebra*, 13:12–21, 1998. Univ. of Gomel, Belarus.
[30] R. C. Lyndon and P. E. Schupp. *Combinatorial Group Theory.* Springer-Verlag, 1977.
[31] S. W. Margolis and J. Meakin. private communication.
[32] S. W. Margolis and J. Meakin. Free inverse monoids and graph immersions. *Internat. J. Algebra Comput.*, 3:79–99, 1992.
[33] S. W. Margolis, J. Meakin, and Šunik Z. Distortion functions and the membership problem for submonoids of groups and monoids. *Geometric methods in group theory, Contemp. Math*, 372:109–129, 2005.
[34] K. A. Mikhailova. The occurence problem for direct products of groups. *Dokl. Akad. Nauk SSSR*, 119:1103–1105, 1958. English translation in *Soviet Math. Dokl.* 70:201–204, 1966.
[35] D. E. Muller and P. E. Schupp. Groups, the theory of ends, and context-free languages. *J. Comput. System Sci.*, 26(3):295–310, 1983.
[36] R. J. Parikh. On context-free languages. *J. Assoc. Comput. Mach.*, 13:570–581, 1966.
[37] R. L. Rivest. On the notion of pseudo-free groups. In *Theory of cryptography*, volume 2951 of *Lecture Notes in Comput. Sci.*, pages 505–521. Springer, Berlin, 2004.
[38] J.-P. Serre. *Trees.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. Translated from the French original by J. Stillwell, Corrected 2nd printing of the 1980 English translation.
[39] V. Shpilrain. Assessing security of some group based cryptosystems. In *Group theory, statistics, and cryptography*, volume 360 of *Contemp. Math.*, pages 167–177. Amer. Math. Soc., Providence, RI, 2004.
[40] J. Stallings. Topology of a finite graph. *Inv. Math.*, 71:551–565, 1983.

[41] B. Steinberg. Inverse automata and profinite topologies on a free group. *J. Pure Appl. Algebra*, 167(2-3):341–359, 2002.

Fachbereich Mathematik / Informatik, Universität Kassel, 34109 Kassel, Germany
E-mail address: `kambites@theory.informatik.uni-kassel.de`

Departamento de Matemática Pura, Faculdade de Ciências da Universidade do Porto, Rua do Campo Alegre 687 4169-007 Porto, Portugal
E-mail address: `pvsilva@fc.up.pt`

School of Mathematics and Statistics, Carleton University, Ottawa, Ontario, K1S 5B6, Canada
E-mail address: `bsteinbg@math.carleton.ca`