Contemporary Mathematics

Distortion functions and the membership problem for submonoids of groups and monoids

Stuart W. Margolis, John Meakin, and Zoran Šunić

Abstract. The notion of upper distortion for graded submonoids embedded in groups and monoids is introduced. A finitely generated monoid M is graded if every element of M can be written in only finitely many ways in terms of some fixed system of generators. Examples of such monoids are free monoids, Artin monoids, and monoids satisfying certain small cancellation conditions. Whenever such a monoid is embedded in another monoid or a group G, we define an upper distortion function comparing the intrinsic word metric on M with the extrinsic word metric on M inherited from G. If the word problem in G is solvable, then the membership problem for M in G is solvable if and only if there exists a recursive upper distortion function for M in G.

A particularly good aspect of upper distortion functions, when they exist, is that they lift well under homomorphisms. In order to illustrate this general approach, we solve the membership problem in positively generated submonoids of some one-relator groups, including Baumslag-Solitar groups, surface groups, and some groups given by Adian type relations. To solve these problems we use linear representations (quite often not faithful) in which long products of matrices have large matrix norms, construct upper distortion functions, and lift them back to the original groups.

Introduction

Let G be a monoid and S a set of of elements in G. We denote by $Mon\langle S\rangle$ the submonoid of G generated by S. If G also happens to be a group, we denote by $Gp\langle S\rangle$ the subgroup of G generated by S.

Let G be a monoid generated by X and $M = Mon\langle S\rangle$ be a submonoid of G. The membership problem for M in G is the following: does there exist an algorithm that decides if an arbitrary word over X represents an element in the monoid M?

1991 *Mathematics Subject Classification.* Primary 20F10, 20M05, 20F65.

Key words and phrases. Submonoids, Membership problem, Distortion.

The first named author was supported by the Excellency Center "Group Theoretic Methods in the Study of Algebraic Varieties" of the Israeli Science Foundation and by the Binational Science Foundation of the USA and Israel, grant 1999298/1 and by INTAS through the Network project 99-1224. The first named author also thanks the Department of Mathematics of the University of Nebraska-Lincoln for its hospitality and support during his visits to work on this project during July-August 2002 and July-August 2003.

The second named author was supported by NSF grant DMS-9970471.

One can also consider the membership problem for a monoid $M = Mon\langle S\rangle$ inside a group G generated by X. In this case the membership problem for M in G asks if an arbitrary group word over $X \cup X^{-1}$ represents an element in M. This is a special instance of the more general problem above since in this case $G = Gp\langle X\rangle = Mon\langle X \cup X^{-1}\rangle$. Another special instance is the so called generalized word problem in groups, which asks if a given group word over $X \cup X^{-1}$ represents an element of the subgroup $M = Gp\langle S\rangle = Mon\langle S \cup S^{-1}\rangle$ in the group $G = Gp\langle X\rangle = Mon\langle X \cup X^{-1}\rangle$. The applications we have in mind mainly concern membership in submonoids of groups, but we first discuss a general technique that is useful for the general case as well.

In general, the membership problem for finitely generated submonoids of a monoid or a group is not decidable, even under very strong assumptions on the submonoid and the ambient monoid or group. In particular, it is well known that the generalized word problem for finitely presented groups with decidable word problem is in general undecidable. For example, the generalized word problem is undecidable for finitely generated subgroups of the direct product $F_2 \times F_2$ of two free groups of rank 2 [**19, 20**], or for finitely generated subgroups of small cancellation groups [**22**].

On the other hand, it is known that the membership problem for finitely generated submonoids of finitely generated free groups or free abelian groups is decidable. These facts follow from the much more general results of Benois [**4**] and Grunschlag [**11**] about membership in rational subsets of free groups and free abelian groups respectively. More generally, Grunschlag [**11, 12**] has shown that the decidability of the membership in rational subsets of groups lifts under finite extensions. Thus in particular, the membership problem for all finitely generated submonoids of a virtually free group or a virtually free abelian group is decidable. Membership in quasiconvex subgroups of word hyperbolic groups is decidable [**9**]. More general results along these lines, dealing with the membership problem in groups admitting rational structure with uniqueness, can be found in [**16**]. Sarkisjan [**24**] has shown that membership in the positive submonoid of a finitely presented Adian group (i.e. a group that admits a "cycle-free" presentation [**1, 25**]) is decidable.

Ivanov, Margolis, and Meakin studied in [**14**] the word problem for inverse monoids given by one-relator inverse monoid presentation $M = Inv\langle X|r = 1\rangle$, where r is a cyclically reduced word over $X \cup X^{-1}$. They showed that the word problem for such an inverse monoid M is decidable if the membership problem for the submonoid $P(r)$ generated by the prefixes of the word r inside the corresponding one-relator group G given by the group presentation $G = Gp\langle X|r = 1\rangle$ is decidable. We refer to the submonoid $P(r)$ of G as the *prefix monoid* of G corresponding to r, and to the corresponding membership problem for $P(r)$ as the *prefix membership problem* for G. Note that different words r can define the same group G, while the corresponding prefix monoids are different submonoids of G. Some instances of the prefix membership problem were solved in [**14**]. Some other special cases have been solved by Lindblad [**17**].

In the present paper we develop some general techniques that make use of distortion functions to study the membership problem for submonoids of monoids and groups. These methods, in conjunction with appropriately chosen linear representations, enable us to solve the prefix membership problem for a rather large class

of one-relator groups including Baumslag-Solitar groups, surface groups and some one-relator groups defined by Adian type presentations.

1. General Techniques

Let $M = Mon\langle S\rangle$ be a submonoid of the monoid $G = Mon\langle X\rangle$, with S and X finite. The finiteness assumption is not important in some considerations that follow and is crucial in others. We will avoid any confusion by sticking to the finitely generated case at all times. The membership problem for M in G asks if there exists an algorithm that decides if a word over X can be rewritten as a word over S. Assume that the word problem is decidable in G. Moreover, assume that any S-word can be compared to any X-word in G (for example, the set S is given as a set of X words, or both X and S are given as sets of integer matrices or as sets of finite permutations). Then one can proceed as follows. Following the short-lex order on words over S, compare in G the given X-word w to each S-word. If w represents an element in M this procedure eventually stops by finding an S-word which is equal to w in G. However, the procedure does not stop if w does not represent an element in M. That is the membership problem for a finitely generated submonoid of a monoid with a decidable word problem is recursively enumerable. We want to find conditions that ensure that the membership problem is recursive. Thus we need a way to find out when to stop the comparison and conclude that the element represented by w is not in M.

One way to decide when to stop the above procedure is by using distortion functions. For a monoid $M = Mon\langle S\rangle$ define the *word length* function with respect to S to be the function $|\cdot|_S : M \to \mathbb{N}$ given by

$$|g|_S = \min\{\ k \mid g = s_1 s_2 \dots s_k, \text{ for some } s_i \in S,\ i = 1, \dots, k\ \}.$$

Let $M = Mon\langle S\rangle$ be a submonoid of the monoid $G = Mon\langle X\rangle$. A *distortion function* for M in G with respect to S and X is any non-decreasing function $\delta : \mathbb{N} \to \mathbb{N}$ such that

$$|g|_S \leq \delta(|g|_X),$$

for all $g \in M$.

The above definition of distortion function is rather standard. For example, it appears in [**7**] in the setting of finitely generated subgroups inside finitely presented groups. A related concept, also called a distortion function by Gromov, appears in [**10**].

There is a unique minimum (under pointwise comparison) distortion function for M in G with respect to S and X. It is given by

$$\delta_{S,X}(n) = \max\{\ |g|_S \mid g \in B_G^X(n) \cap M\ \},$$

where $B_G^X(n)$ is the ball of radius n with respect to X in G, consisting of the elements of G whose X-length is at most n. Call this function the *actual distortion* of M in G with respect to S and X.

The following proposition, stated in slightly less general form, also appears in [**7**]. The short proof is given for completeness, since it actually provides an algorithm that solves the membership problem.

PROPOSITION 1.1. *Let $M = Mon\langle S\rangle$ be a submonoid of the monoid $G = Mon\langle X\rangle$, with S and X finite, and let the problem of comparison of X-words and*

S-words in G be decidable. The membership problem for M in G is decidable if and only if there is a recursive distortion function for M in G with respect to S and X.

PROOF. If a recursive distortion function δ for M in G is given, then in order to check if an X-word w represents an element in M one only needs to check if w is equal in G to an S-word of length up to $\delta(n)$, where n is the length of the word w (not necessarily its length in G).

Conversely, if the membership problem is decidable the value of the actual distortion function can be calculated at any n as follows. For each X-word w of length at most n, and there are only finitely many such words, we can check if it represents an element in M. For those w that do represent elements in M the corresponding S-length can be calculated (use the shortlex order on S^* and compare all words in S^* to w until one of them is equal to w in G), and therefore the maximal S-length of an X-word of length n that represents an element in M can also be calculated. □

If M is infinite the distortion function is at least linear and if $|S| \geq 2$ the algorithm from the above proposition is at least exponential.

We provide, without a proof, the following adaptation of a similar observation from [**7**] on the behavior of distortion functions under change of generating sets.

PROPOSITION 1.2. *Let $M = Mon\langle S\rangle = Mon\langle S'\rangle$ be a submonoid of the monoid $G = Mon\langle X\rangle = Mon\langle X'\rangle$, with S, S', X and X' finite. If*

$$C = \max\{\ |x|_{X'} \mid x \in X\ \}, \qquad D = \max\{\ |s'|_S \mid s' \in S'\ \}$$

and δ' is a distortion function for M in G with respect to S' and X' then

$$\delta_{S,X}(n) \leq D\delta'(Cn),$$

for all n.

If $M' = Mon\langle S'\rangle$ is a submonoid of $M = Mon\langle S\rangle$, which in turn is a submonoid of $G = Mon\langle X\rangle$, nothing can be said in general about the distortion for M' in G based on a known distortion function for M in G. Indeed, the distortion for M could be linear (after all M can be taken to be equal to G), while M' could have any possible distortion in G.

Similarly, given a homomorphism $\varphi : G \to G'$ no information on the distortion for M in G can be inferred from a known distortion function for $M' = \varphi(M)$ in G'.

However, the situation is much better for the case of graded monoids and their upper distortion functions, which we now introduce.

DEFINITION 1.3. A monoid M is *graded* if it has a finite system of generators S such that every member of M can be written as a word over S in only finitely many ways.

The use of the term *graded* will be explained in Theorem 1.7. Note that the definition just states that each class of the congruence $\sim$ on S^* that defines M as the factor monoid $M = S^*/\sim$ is finite. Also, the definition implies that a graded monoid cannot have any subgroups different from 1 (in particular, it cannot have any idempotents different from 1) and the only way to write 1 in terms of the generators in S is by using the empty word (in particular, $1 \notin S$).

Here are some natural examples of graded monoids. Let

$$M = Mon\langle S | u_i = v_i, i \in I\rangle$$

be a finitely generated monoid such that the length of u_i is the same as the length of v_i, for all $i \in I$. Since there are a finite number of words of each length over S and the congruence $\sim$ can only identify words of the same length, such a monoid is graded. Important examples of such monoids are Artin monoids and all relatively free monoids in varieties that contain the natural numbers. Of course free monoids are graded. More examples will be discussed after the proof of Theorem 1.7.

DEFINITION 1.4. Let M be a graded monoid with respect to the generating set S. The function $\lambda_S : M \to \mathbb{N}$ defined by

$$\lambda_S(g) = max\{\ k \mid g = s_1 s_2 \dots s_k, \text{ for some } s_i \in S,\ i = 1, \dots, k\ \}$$

is called the *upper word length* function of M with respect to S.

The definition of a graded monoid implies that the upper word length functions are well defined. Moreover, for a finitely generated monoid $M = Mon\langle S\rangle$, the existence of a well defined upper word length function λ_S is equivalent to M being graded with respect to S. We will show that the upper word length function is independent of the system of generators S.

DEFINITION 1.5. A non-identity element of a monoid M is *irreducible* if it cannot be written as a product of non-identity elements of M.

PROPOSITION 1.6. *Let M be a graded monoid with respect to the set S. Let B be the set of irreducible elements of M.*

(1) *S contains B, but does not contain the identity.*
(2) *M is graded with respect to B and the upper word length functions λ_S and λ_B are equal.*
(3) *M is graded with respect to any set S' that contains B but does not contain the identity. Moreover $\lambda_{S'} = \lambda_S = \lambda_B$, for any such set S'.*

PROOF. (1) No monoid can be graded with respect to a set that contains the identity. Thus $1 \notin S$. Every generating set of M must include all irreducible elements. Thus $B \subseteq S$.

(2) Consider $g = s_1 s_2 \dots s_k$, $s_i \in S$, $i = 1, \dots, k$, an arbitrary element of M. If some s_i, $i = 1, \dots, k$, is not irreducible, then g can be represented by a longer word over S, simply by writing s_i first as a product $s_i = g_1 g_2$ of two non-identity elements of M and then by rewriting g_1 and g_2 in terms of S. Thus the longest word over S that represents g must actually be a word over B. This implies that B generates M, M is graded with respect to B and $\lambda_S = \lambda_B$.

(3) Let S' be a set containing B but not the identity. We already know from (2) that B is a generating set for M. Thus S' generates M as well.

Assume that M is not graded with respect to S'. Then there exists an element g in M that can be written in infinitely many ways as a product of the elements in S'. However, no element in S' is the identity, so each of them can be rewritten as a nontrivial product of elements in B. Thus M is not graded with respect to B and this contradicts (2).

Therefore M is graded with respect to S'. The equality $\lambda_{S'} = \lambda_S = \lambda_B$ now follows from (2). □

Thus the upper word length functions, when they exist, are independent of the generating set (under the mild requirement that the identity should not be included

in a generating set). From now on, we will often skip the reference to the generating set when we talk about graded monoids.

We introduce here some related notions that will explain the use of the term *graded* for this class of monoids. Note that, for a graded monoid $M = Mon\langle S\rangle$, the upper length function $\lambda_S : M \to \mathbb{N}$ satisfies:

$$\lambda_S(gh) \geq \lambda_S(g) + \lambda_S(h)$$

for all $g, h \in M$. That is, λ_S is a superadditive function.

Recall that a semigroup N is *nilpotent* if N has a 0 and there is a positive integer k such that every product of k elements of N is 0. It is well known that a finite semigroup is nilpotent if and only if $n^k = 0$ for any element $n \in N$. A semigroup T is *residually finite nilpotent* if for every pair $s \neq t \in T$ there is a morphism $f_{s,t} : T \to N$ from T to a finite nilpotent semigroup N such that $f_{s,t}(s) \neq f_{s,t}(t)$.

Now note that if M is a graded monoid, then $M \setminus \{1\}$ is a subsemigroup of M. For if $1 = xy$ for some $x, y \in M \setminus \{1\}$, then $1 = (xy)^n$ for all $n > 0$ and this contradicts the definition of a graded monoid. Furthermore, the upper length function maps all elements of $M \setminus \{1\}$ into the positive integers.

If T is a semigroup, let $T^n = \{t_1 \dots t_n | t_i \in T, 1 \leq i \leq n\}$. Then T^n is an ideal of T for all $n > 0$ and $T^{n+1} \subseteq T^n$ for all $n > 0$. Let $T = M \setminus \{1\}$ where $M = Mon\langle S\rangle$ is a graded monoid. Clearly, $t \in T^n$ if and only if $\lambda_S(t) \geq n$, so that $T \setminus T^n$ is a finite set for all $n > 0$. We now give several characterizations of graded monoids. A related result was proved in [**15**], Proposition 3.1.

THEOREM 1.7. *Let M be a finitely generated monoid such that $T = M \setminus \{1\}$ is a subsemigroup of M. Then the following conditions are equivalent.*

(1) *M is graded.*
(2) *There exists a superadditive function from $T \to P$, where P is the set of positive integers.*
(3) *The intersection $\cap_{n>0} T^n$ is empty.*
(4) *For every element t in T, there exists $n > 0$ such that $t \in T \setminus T^n$.*
(5) *For every element t in T, there exists $n > 0$ such that $t \in T \setminus T^n$, the set $T \setminus T^2$ of irreducible elements generates T, and the set $T \setminus T^n$ is finite, for all $n > 0$.*
(6) *T is a residually finite nilpotent semigroup without a zero.*

PROOF. First note that, since M is a finitely generated monoid, $T = M \setminus \{1\}$ is a finitely generated semigroup.

(1) $\Rightarrow$ (2) Assume that M is graded. The upper length function $\lambda_S : M \to \mathbb{N}$ restricted to T is a superadditive function from T to the positive integers.

(2) $\Rightarrow$ (3) Assume there exists a superadditive function $f : T \to P$. Then if $t \in T^n$ we have $f(t) \geq n$. Therefore, if $s \in T$ has $f(s) = k$, it follows that $s \notin T^{k+1}$ and thus $\cap_{n>0} T^n$ is empty.

(3) $\Leftrightarrow$ (4) Clear.

(4) $\Leftrightarrow$ (5) It is clear that (5) implies (4).

For the other direction, let $t \in T$ and let n be the smallest positive integer such that $t \in T \setminus T^n$. Therefore t can be written as $t = t_1 \dots t_{n-1}$, for some $t_i \in T$, but cannot be written as any longer product. If $t_i \in T^2$, for some i, we can rewrite t as a product of n elements, a contradiction. This implies that $t_i \in T \setminus T^2$, $i = 1, \dots, n-1$ and therefore $T \setminus T^2$ generates T. Since $T \setminus T^2$ is actually the set of irreducible elements of the semigroup T, it must be included in any generating

set of T. Therefore $T \setminus T^2$ is finite. It follows that $T \setminus T^n$ is finite for all $n > 0$. For if $t \in T \setminus T^n$, then t can be be written as a product of at most $n-1$ elements of the finite set $T \setminus T^2$.

(5) $\Rightarrow$ (1) Assume the condition (5). An element $t \in T \setminus T^n$ can be written in only finitely many ways as a product of at most $n-1$ elements of the finite generating set $T \setminus T^2$. Thus M is graded with respect to $T \setminus T^2$.

(5) $\Rightarrow$ (6) Assume the condition (5).

Then T does not have a zero (or any idempotent for that matter). For if $t \in T$ were an idempotent in T, then $t \in T^n$, for all $n > 0$, a contradiction.

Further, for any two elements $s, t \in T$ there exists $n > 0$ such that $s, t \in T \setminus T^n$. But then $s \neq t$ in the Rees quotient T/T^n.

For all $n > 0$, the Rees quotient T/T^n is a finite semigroup in which T^n is the zero element. Furthermore, T/T^n is nilpotent, since the product of any n elements in T/T^n is equal to the 0 element T^n.

Thus T is a residually finite semigroup without a zero.

(6) $\Rightarrow$ (4) Now assume that T is a residually finite nilpotent semigroup without 0.

We claim that there is no element $t \in T$ that maps to 0 under every morphism from T to a finite nilpotent semigroup. For suppose there was such a t. Then for each $s \in T$, st and ts map to 0 under every morphism of T into a finite nilpotent semigroup. Since T is residually a finite nilpotent semigroup, it follows that $st = ts = t$ for each $s \in T$. Thus t is the 0 element of T, a contradiction.

Therefore, for each $t \in T$, there is a finite nilpotent semigroup and a morphism $f_t : T \to N$ such that $f_t(t) \neq 0$. Choose an integer $n > 0$ such that $N^n = 0$. It follows that $t \in T \setminus T^n$, for some $n > 0$. □

As mentioned above, all Artin monoids are graded. Another class of examples comes from small cancellation theory in semigroups. See [**21**] and [**13**] for an introduction to this theory. Remmers [**21**] proved that a finite presentation of a semigroup that satisfies the small cancellation condition C(3) is graded and Cummings and Goldstein [**6**] proved that any semigroup satisfying the small cancellation conditions C(2) and T(4) is graded. D.A. Jackson[**15**] proved that all Baumslag-Solitar monoids, $BS(k,l) = Mon < a, b | a^k b = ba^l >$, where k and l are positive integers are graded.

Graded (even free) monoids occur frequently as submonoids of finitely presented groups. The following result of Arzhantseva [**3**] provides some quantitative support to this claim. Let X be an alphabet on m letters. A set of cyclically reduced group words over X is called admissible if it generates a subgroup of infinite index in the free group $F(X)$ (and one can easily argue that randomly chosen words tend to generate subgroups of infinite index). Let $N = N(m, n, t)$ be the number of group presentations on m generators with n cyclically reduced relators none of which is longer than t and, for a given admissible set of words S, let $N_S(m, n, t)$ be the number of such presentations that define groups in which S generates a free subgroup. There exists a positive constant c such that

$$N_S/N \geq 1 - e^{ct}.$$

Thus the ratio N_S/N approaches 1 exponentially fast as t grows, i.e, the class of finitely presented groups in which S generates a free group is exponentially generic (in the terminology from [**2**]).

We also note that the class of graded monoids has a remarkably good algorithmic and finite separability theory. A monoid M is *finitely separable* (see [**8**]) if for every proper subset X of M and every $s \notin X$, there is a morphism $f : M \to N$ to a finite monoid N such that $f(s) \notin f(X)$. It is easy to prove that a graded monoid is finitely separable. From this, it is easy to prove that the membership problem for any recursively generated submonoid of such an M is decidable.

We now turn to the "dual" problem of deciding the membership problem for a graded monoid inside a containing monoid or group.

DEFINITION 1.8. Let $M = Mon\langle S\rangle$ be a graded submonoid of $G = Mon\langle X\rangle$, with S and X finite. An *upper distortion function* for M in G with respect to S and X is any non-decreasing function $\lambda : \mathbb{N} \to \mathbb{N}$ such that

$$\lambda_S(g) \leq \lambda(|g|_X),$$

for all $g \in M$.

The minimal (under pointwise comparison) upper distortion function is of independent interest.

DEFINITION 1.9. Let $M = Mon\langle S\rangle$ be a graded submonoid of $G = Mon\langle X\rangle$, with S and X finite. The *actual upper distortion function* $\lambda_{S,X} : \mathbb{N} \to \mathbb{N}$ is defined by

$$\lambda_{S,X}(n) = \max\{\ \lambda_S(g) \mid g \in B_G^X(n) \cap M\ \}.$$

For finite X, the set $B_G^X(n) \cap M$ is finite and therefore the actual upper distortion function $\lambda_{S,X}$ is well defined. Also, since

$$|g|_S \leq \lambda_S(g) \leq \lambda_{S,X}(|g|_X),$$

for $g \in M$, any upper distortion function is a distortion function for M in G. Note that it is possible for a submonoid to be graded without having a recursive upper distortion function, i.e., the membership problem is undecidable in general even for graded submonoids embedded in groups with decidable word problem. For instance, McCool [**18**] provided an example of a finitely presented torsion-free group G with decidable word problem in which the power problem (determining if one element is a power of another) is undecidable. Therefore all cyclic submonoids of G are graded (even free), but the membership problem is undecidable. This means that the corresponding upper distortion functions cannot be recursive.

DEFINITION 1.10. A graded submonoid $M = Mon\langle S\rangle$ of $G = Mon\langle X\rangle$, with S and X finite, is *recursively embedded* if the upper distortion function $\lambda_{S,X}$ is recursive.

Thus graded monoids have well defined upper distortion functions, while recursively embedded graded monoids have recursive upper distortion functions and decidable membership problem.

Let us note a simple geometric aspect of upper distortion functions, which is crucial in the solution of the membership problem for a graded monoid $M = Mon\langle S\rangle$ recursively embedded in $G = Mon\langle X\rangle$. Simply put, long words in S represent elements that are far from the origin 1 in the Cayley graph of G with respect to X. Indeed, if u is a word over S of length $k \geq \lambda(n)$, for some upper distortion function λ, then the element u lies outside of the ball $B_G^X(n)$ of radius

n. Therefore an element represented by such a long S-word u cannot be equal to any element represented by an X-word w of length n.

The following two propositions enable us to deduce that certain graded monoids have recursive embeddings by looking at homomorphic images.

PROPOSITION 1.11. *Let $M = Mon\langle S\rangle$ and $M' = Mon\langle S'\rangle$ be monoids, with S and S' finite, and $\varphi : M \to M'$ a homomorphism with $\varphi(S) \subseteq S'$. If M' is graded with respect to S' then M is graded with respect to S and, for $g \in M$,*

$$\lambda_S(g) \leq \lambda_{S'}(g'),$$

where $g' = \varphi(g)$.

PROOF. Let $g = s_1 s_2 \cdots s_k$, $s_i \in S$, $i = 1, \ldots, k$, be a representation of an element g in M as an S-word of length k. Then $g' = s'_1 s'_2 \cdots s'_k$, $s'_i = \varphi(s_i) \in S'$, $i = 1, \ldots, k$ is a representation of the element $g' = \varphi(g)$ in M' as an S'-word of length k. Thus $k \leq \lambda_{S'}(g')$, i.e., the length of any S-word that represents g is bounded above by $\lambda_{S'}(g')$. This immediately implies that there are only finitely many S-words representing g in M and the longest such word is no longer than $\lambda_{S'}(g')$. Therefore M is graded and $\lambda_S(g) \leq \lambda_{S'}(g')$. □

PROPOSITION 1.12. *Let $M = Mon\langle S\rangle$ be a submonoid of $G = Mon\langle X\rangle$ and $M' = Mon\langle S'\rangle$ a submonoid of $G' = Mon\langle X'\rangle$, with S, S', X and X' finite. Let M' be graded with respect to S' and $\varphi : G \to G'$ be a homomorphism with $\varphi(S) \subseteq S'$. Then M is graded with respect to S and if $\lambda' : \mathbb{N} \to \mathbb{N}$ is an upper distortion function for M' in G', then*

$$\lambda_{S,X}(n) \leq \lambda'(Cn),$$

where $C = \max\{\ |\varphi(x)|_{X'} \mid x \in X\ \}$, holds for the actual upper distortion function for M in G.

PROOF. It is clear from Proposition 1.11 that M is graded with respect to S. For $g \in M$ with $|g|_X \leq n$,

$$\lambda_S(g) \leq \lambda_{S'}(g') \leq \lambda'(|g'|_{X'}) \leq \lambda'(C|g|_X) \leq \lambda'(Cn),$$

where $g' = \varphi(g)$. □

Note that the above proposition, in the special case $\varphi = 1$ and $S = S'$, is an analog of Proposition 1.2 describing the behavior of upper distortion functions under change of generating sets.

Another good property of upper distortion functions that can be extracted from the above proposition is that they are inherited by finitely generated submonoids (set $\varphi = 1$ and $X = X'$).

The following corollaries, which will be used in the applications in the next section, are easy implementations of the above ideas. They provide rather general conditions under which recursive upper distortion functions can be lifted from homomorphic images and used to solve membership problems in the original monoid.

COROLLARY 1.13. *In the setting of Proposition 1.12, if M' is recursively embedded in G', then M is recursively embedded in G and $\lambda : \mathbb{N} \to \mathbb{N}$ given by*

$$\lambda(n) = \lambda'(Cn)$$

is a recursive upper distortion function for M in G, as well as for any finitely generated submonoid of M. The membership problem is then decidable for all such submonoids in G.

COROLLARY 1.14. *Let $M = Mon\langle S\rangle$ be a submonoid of the group $G = Gp\langle X\rangle$. Let $\varphi : G \to \mathbb{Z}$ be a homomorphism such that all generators in S map to positive integers the smallest of which is D and the generators in X map to integers of absolute value at most C. Then $\lambda(n) = \lfloor Cn/D \rfloor$ is an upper distortion function for M in G and the membership problem is decidable for every finitely generated submonoid of M in G.*

PROOF. An upper distortion function for $M' = Mon\langle\varphi(S)\rangle$ in $\mathbb{Z} = Mon\langle\pm 1\rangle$ with respect to $S' = \varphi(S)$ and $X' = \{\pm 1\}$ is given by $\lambda(n) = \lfloor n/D \rfloor$. The conclusion then follows from Corollary 1.13. □

Here is another easy way to recognize graded monoids, which we will also use in the applications that follow.

PROPOSITION 1.15. *Let $M = Mon\langle S\rangle$ be a monoid and (S, R) a rewriting system for M, where $R = \{\ u_i \to v_i \mid i = 1, \ldots, k\ \}$ is the set of rules. Let (S, R') be the reversed rewriting system, where $R' = \{\ v_i \to u_i \mid i = 1, \ldots, k\ \}$.*

(a) If (S, R) is terminating and M is graded with respect to S, then (S, R') is terminating.

(b) If (S, R) is finite and complete, then M is graded with respect to S if and only if (S, R') is terminating.

PROOF. (a) Assume that (S, R) is terminating while (S, R') is not. Then there exist an infinite chain

$$w_0 \longrightarrow' w_1 \longrightarrow' w_2 \longrightarrow' \ldots,$$

where $w_i \to' w_{i+1}$ indicates that w_{i+1} is derived from w_i by application of a single rule in the reversed system (S, R'). This is equivalent to the existence of an infinite chain

$$\ldots \longrightarrow w_2 \longrightarrow w_1 \longrightarrow w_0,$$

in the original system. Since (S, R) is terminating the last chain cannot have repeated terms, thus $w_0 \in M$ can be written in infinitely many ways in terms of S, i.e., M is not graded with respect to S.

(b) One direction of the claim is proved in (a). For the other, assume that (S, R) is a finite complete rewriting system and M is not graded with respect to S. Then there exist infinitely many words $w_1, w_2, \ldots$ that reduce to the same irreducible word w in (S, R). Thus the set of vertices (words) Γ'_w accessible from w in the graph Γ' of the reversed system (S, R') is infinite. Since R' is finite, every vertex has a finite out-degree, so by König's Lemma there exists an infinite path starting at w in Γ'. Thus (S, R') is not terminating. □

2. Applications to the membership problem in submonoids of one-relator groups

In this section, we use upper distortion functions in order to solve the membership problem for some submonoids in one-relator groups.

DEFINITION 2.1. Let G be given by a group presentation

$$G = Gp \langle\ X \mid r = 1\ \rangle.$$

The submonoid $P(r)$ of G generated by the set of prefixes of r is called the *prefix monoid* of G.

The *prefix monoid membership problem* for G is the membership problem for $P(r)$.

Note that different words r may define the same group G, while the corresponding prefix monoids are different, i.e., the problem depends on the particular presentation of G.

As we noted before, graded monoids cannot contain any torsion and thus seemingly upper distortion functions cannot be used in one-relator groups with torsion in order to solve membership problems. However, the following proposition illustrates a simple way to handle the torsion in same cases.

PROPOSITION 2.2. *If $\lambda' : \mathbb{N} \to \mathbb{N}$ is an upper distortion function for the prefix monoid $P(r)$ in*

$$G' = Gp \langle\ X \mid r = 1\ \rangle,$$

then, for $e \geq 1$, the function $\delta : \mathbb{N} \to \mathbb{N}$ given by $\delta(n) = e\lambda'(n)+e-1$ is a distortion function for the prefix monoid $P(r^e)$ in

$$G = Gp \langle\ X \mid r^e = 1\ \rangle.$$

Thus, if λ' is recursive the prefix monoid membership problem is decidable in G.

PROOF. Let $' : G \to G'$ be the natural homomorphism extending the identity map on X. The image of g under $'$ is denoted by g'.

Let g be an element of the prefix monoid $P(r^e)$ with $|g|_S = k$ and let w be an S-word of length k representing g. Then g' is an element of the prefix monoid $P(r)$. All proper prefixes of r^e map to proper prefixes of r except for the prefixes of the form r^t, which map to 1. Let S be the set of proper prefixes of r^e and S' be the set of proper prefixes of r. The largest possible number of appearances of the generator r in w is $(k+1)(e-1)/e$ (otherwise there are at least e consecutive appearances of r in w, which contradicts the fact that the S-length of g is k). This means that g' can be represented by an S'-word of length at least $k-(k+1)(e-1)/e = (k+1)/e-1$. Therefore $\lambda_{S'}(g') \geq (|g|_S+1)/e-1$ and

$$|g|_S \leq e\lambda_{S'}(g') + e - 1 \leq e\lambda'(|g'|_X) + e - 1 \leq e\lambda'(|g|_X) + e - 1 = \delta(|g|_X).$$

□

Thus we may concentrate our efforts on trying to find recursive upper distortion functions for $P(r)$, for r a primitive word, and whenever we are successful we may lift such functions to recursive distortion (definitely not upper distortion because of the torsion) functions for $P(r^e)$, for $e \geq 2$.

Corollary 1.13 indicates that it is useful to have an extensive list of examples of recursive embeddings together with corresponding recursive upper distortion functions. In any new situation we may try to utilize such a list by factoring to the simpler cases we already understand and then lift back the obtained result. In order to provide such a class of examples, we analyze the case of two generators more carefully. However, even the case of two generator one-relator groups will be analyzed by further factoring such groups to $\mathbb{Z}$ or to metabelian matrix groups through appropriate (quite often not faithful) linear representations.

PROPOSITION 2.3. *Let G be given by a group presentation*

$$G = Gp\ \langle\ a, b \mid r = 1\ \rangle$$

where

$$r = a^{n_0} b^{m_1} \dots a^{n_{k-1}} b^{m_k} a^{n_k}.$$

The map

$$a \mapsto \begin{bmatrix} \xi & 0 \\ 0 & 1 \end{bmatrix}, \qquad b \mapsto \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

can be extended to a linear representation $\varphi_\xi : G \to \mathsf{GL}_2(\mathbb{C})$ if and only if ξ is a non-zero solution to the following polynomial system of equations in x

$$x^{exp_a(r)} = 1$$

$$m_1 x^{n_0} + m_2 x^{n_0+n_1} + \dots + m_k x^{n_0+\dots+n_{k-1}} = 0.$$

PROOF. Denote

$$A = \begin{bmatrix} \xi & 0 \\ 0 & 1 \end{bmatrix} \qquad \text{and} \qquad B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \tag{2.1}$$

Then

$$A^{n_0} B^{m_1} \dots A^{n_{k-1}} B^{m_k} A^{n_k} = \begin{bmatrix} \xi^{\sum_{i=0}^{k} a_i} & m_1 \xi^{n_0} + \dots + m_k \xi^{n_0+\dots+n_{k-1}} \\ 0 & 1 \end{bmatrix},$$

and the claim easily follows. □

THEOREM 2.4. *Let G be given by a group presentation*

$$G = Gp\ \langle\ a, b \mid r = 1\ \rangle$$

where

$$r = a^{n_0} b^{m_1} \dots a^{n_{k-1}} b^{m_k} a^{n_k}$$

and $\exp_a(r) = 0$. *If the polynomial equation*

$$m_1 x^{n_0} + m_2 x^{n_0+n_1} + \dots + m_k x^{n_0+\dots+n_{k-1}} = 0$$

has a positive real root, then there exists a recursive upper distortion function for every positively and finitely generated submonoid of G and the membership problem is decidable for such submonoids.

PROOF. Let ξ be a positive real root of the polynomial equation

$$m_1 x^{n_0} + m_2 x^{n_0+n_1} + \dots + m_k x^{n_0+\dots+n_{k-1}} = 0.$$

Consider the case $\xi \neq 1$ first. Let

$$A = \begin{bmatrix} \xi & 0 \\ 0 & 1 \end{bmatrix} \qquad \text{and} \qquad B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

By Proposition 2.3 the map $a \mapsto A,\ b \mapsto B$ extends to a homomorphism $\varphi : G \to G'$ where $G' = Gp\langle A, B\rangle \leq \mathsf{GL}_2(\mathbb{C})$. We will show that the monoid $M' = Mon\langle S\rangle$ recursively embeds in $G' = Mon\langle X\rangle \leq \mathsf{GL}_2(\mathbb{C})$, where $S = \{A, B\}$ and $X = \{A, A^{-1}, B, B^{-1}\}$ and construct a recursive upper distortion function with respect to S and X.

For an arbitrary X-word $W = A^{s_0} B^{t_1} \cdots A^{s_{\ell-1}} B^{t_\ell} A^{s_\ell}$, define $\alpha(W) = \xi^{s_0+\dots+s_\ell}$ and $\beta(W) = t_1 \xi^{s_0} + \dots + t_\ell \xi^{s_0+\dots+s_{\ell-1}}$. Note that

$$W = \begin{bmatrix} \alpha(W) & \beta(W) \\ 0 & 1 \end{bmatrix}.$$

Let $\xi > 1$. Let $W = A^{s_0}B^{t_1}\cdots A^{s_{\ell-1}}B^{t_\ell}A^{s_\ell}$ be an arbitrary word of length at most n and $U = A^{s'_0}B^{t'_1}\cdots A^{s'_{q-1}}B^{t'_q}A^{s'_q}$ be an S-word whose length is greater than $n(1+\xi^n)$. Then either $|U|_A > n$ or $|U|_B > n\xi^n$. In the former case

$$\alpha(W) = \xi^{s_0+\cdots+s_\ell} \leq \xi^n < \xi^{|U|_A} = \xi^{s'_0+\cdots+s'_q} = \alpha(U)$$

and in the latter

$$\beta(W) = t_1\xi^{s_0} + \cdots + t_\ell\xi^{s_0+\cdots+s_{\ell-1}} \leq (|t_1| + \cdots + |t_\ell|)\xi^n \leq n\xi^n <$$
$$|U|_B = t'_1 + \cdots + t'_q \leq t'_1\xi^{s'_0} + \cdots + t'_q\xi^{s'_0+\cdots+s'_{q-1}} = \beta(U).$$

In either case, $U \neq W$, which means that U is not in the ball of radius n with respect to X in G' and therefore the function $\lambda : \mathbb{N} \to \mathbb{N}$ given by $\lambda(n) = n\lceil 1+\xi^n\rceil$ is an upper distortion function for M' in G'. This function is recursive since ξ is an algebraic number.

Let $\xi < 1$. Let $W = A^{s_0}B^{t_1}\cdots A^{s_{\ell-1}}B^{t_\ell}A^{s_\ell}$ be an arbitrary word of length at most n and $U = A^{s'_0}B^{t'_1}\cdots A^{s'_{q-1}}B^{t'_q}A^{s'_q}$ be an S-word whose length is strictly greater than $n\left(1+\frac{1}{\xi^{2n}}\right)$. Then either $|U|_A > n$ o r $|U|_B > n\frac{1}{\xi^{2n}}$. In the former case

$$\alpha(W) = \xi^{s_0+\cdots+s_\ell} \geq \xi^n > \xi^{|U|_A} = \xi^{s'_0+\cdots+s'_q} = \alpha(U)$$

Otherwise, the inequalities $\xi^n \leq \xi^{|U|_A}$ and $|U|_B > n\frac{1}{\xi^{2n}}$ imply

$$\beta(W) = t_1\xi^{s_0} + \cdots + t_\ell\xi^{s_0+\cdots+s_{\ell-1}} \leq (|t_1| + \cdots + |t_\ell|)\xi^{-n} \leq n\frac{1}{\xi^n} < |U|_B\xi^n \leq$$
$$|U|_B\xi^{|U|_A} = (t'_1 + \cdots + t'_q)\xi^{s'_0+\cdots+s'_q} \leq t'_1\xi^{s'_0} + \cdots + t'_q\xi^{s'_0+\cdots+s'_{q-1}} = \beta(U).$$

In either case, $U \neq W$, which means that U is not in the ball of radius n with respect to X in G' and therefore the function $\lambda : \mathbb{N} \to \mathbb{N}$ given by $\lambda(n) = n\left\lceil 1+\frac{1}{\xi^{2n}}\right\rceil$ is an upper distortion function for M' in G'. This function is recursive since ξ is an algebraic number.

Finally, if $\xi = 1$ is a root, then $m_0 + \cdots + m_k = 0$, i.e., we have $exp_a(r) = exp_b(r) = 0$. In this case the map $a \mapsto 1,\ b \mapsto 1$ extends to a homomorphism $\varphi : G \to \mathbb{Z}$ and, by Corollary 1.14, $\lambda : \mathbb{N} \to \mathbb{N}$ given by $\lambda(n) = n$ is an upper distortion function for M in G. □

Note that one can effectively decide, by using Sturm's Theorem on roots in a given real interval, if a polynomial equation in a single variable has a positive root. Thus we can first decide algorithmically if the above theorem applies and then construct a recursive upper distortion function if it does. Moreover, one does not need to work with the bounds provided in the proof given in terms of the algebraic number ξ, since this may prove to be cumbersome. Instead, in the case when $1 < \xi$, one can replace the bound $n\lceil 1+\xi^n\rceil$ by $n(1+\Xi^n)$, where Ξ is the ceiling of ξ. Similarly, when $\xi < 1$, one can replace the bound $n\left\lceil 1+\frac{1}{\xi^{2n}}\right\rceil$ by $n(1+\Xi^{2n})$, where Ξ is the ceiling of $1/\xi$.

Corollary 2.5. *Let G be given by a group presentation*

$$G = Gp\ \langle\ a, b \mid u = v\ \rangle$$

where

$$u = b^{n_0}ab^{n_1}a\ldots ab^{n_k} \qquad \text{and} \qquad v = b^{m_0}ab^{m_1}a\ldots ab^{m_k}.$$

If the polynomial

$$p(x) = (m_k - n_k)x^k + (m_{k-1} - n_{k-1})x^{k-1} + \cdots + (m_1 - n_1)x + (m_0 - n_0)$$

has a positive real root, then there exists a recursive upper distortion function for each positively and finitely generated submonoid of G and the membership problem is decidable for such submonoids.

COROLLARY 2.6. *Let G be given by an Adian type group presentation*

$$G = Gp \langle\ a, b \mid u = v\ \rangle,$$

where u and v are positive words, u starts in a, v starts in b and the last letters of u and v also differ. The following table represents (up to symmetry) all possible relations between the numbers of occurrences of a and b in u and v:

case#	*a's*	*b's*	*additional constraint*
1	$\|u\|_a = \|v\|_a$	$\|u\|_b = \|v\|_b$	
2	$\|u\|_a > \|v\|_a$	$\|u\|_b < \|v\|_b$	
3	$\|u\|_a = \|v\|_a$	$\|u\|_b > \|v\|_b$	
$4'$	$\|u\|_a = \|v\|_a$	$\|u\|_b < \|v\|_b$	*u ends in b*
$4''$	$\|u\|_a = \|v\|_a$	$\|u\|_b < \|v\|_b$	*u ends in a*
5	$\|u\|_a > \|v\|_a$	$\|u\|_b > \|v\|_b$	

,

In each case, except possibly $4''$ and 5, there exists a recursive upper distortion function for each positively and finitely generated submonoid of G and the membership problem is decidable for such submonoids.

PROOF. In case 1, the map $a \mapsto 1,\ b \mapsto 1$ can be extended to a homomorphism to $\mathbb{Z}$. By Corollary 1.14, an upper distortion function is given by $\lambda(n) = n$.

In case 2, the map $a \mapsto |v|_b - |u|_b,\ b \mapsto |u|_a - |v|_a$ can be extended to a homomorphism to $\mathbb{Z}$. By Corollary 1.14, an upper distortion function is given by $\lambda(n) = \lceil Cn/D \rceil$, where $C = \max\{|u|_a - |v|_a, |v|_b - |u|_b\}$ and $D = \min\{|u|_a - |v|_a, |v|_b - |u|_b\}$.

In case 3 and case $4'$, let

$$u = b^{n_0}ab^{n_1}a \ldots ab^{n_k} \qquad \text{and} \qquad v = b^{m_0}ab^{m_1}a \ldots ab^{m_k}.$$

Consider the polynomial

$$p(x) = (m_k - n_k)x^k + (m_{k-1} - n_{k-1})x^{k-1} + \cdots + (m_1 - n_1)x + (m_0 - n_0)$$

We have $p(0) = m_0 - n_0 > 0$, since u starts in a and v in b. On the other hand $p(1) = |v|_b - |u|_b$. Thus, in case 3, $p(1) < 0$ and therefore p has a root between 0 and 1, so Corollary 2.5 applies. In case $4'$, $p(1) > 0$ and $m_k - n_k < 0$, since u ends in b and v ends in a. Thus, p has a root greater than 1, so Corollary 2.5 applies in this case as well. □

EXAMPLE 2.7. Consider the Baumslag-Solitar group

$$G = BS(m, k) = Gp \langle\ a, b \mid ab^m = b^k a\ \rangle,$$

for $m, k \geq 1$. The corresponding polynomial equation is $mx = k$, which has a unique positive root $\xi = k/m$. Thus the membership problem is decidable for every positively and finitely generated submonoid of $BS(m, k)$.

Consider the particular case of $G = BS(1, 2) = Mon\langle X \rangle$, where $X = \{a, a^{-1}, b, b^{-1}\}$. The corresponding root is $\xi = 2$ and the upper distortion

function constructed for the positive submonoid $M = Mon\langle S\rangle$, where $S = \{a, b\}$ in the proof of Theorem2.4 is $n \mapsto n(1 + 2^n)$, which is exponential in n. However, it can be shown that $|b^{2^n}|_S = 2^n$ and $|b^{2n}|_X = |a^{n-1}b^2a^{-n+1}|_X = 2n$, for all $n \geq 1$. Therefore the actual distortion function is asymptotically at least exponential, which means that the actual distortion and the actual upper distortion do not differ by much and the estimate on upper distortion given during the course of the proof in Theorem 2.4 cannot be significantly improved in general.

If one applies the algorithm from Proposition 1.1 to a word w of length n, then one has to compare w to all S-words of length up to $n(1 + 2^n)$. Thus the number of comparisons is potentially $2^{n(1+2^n)}$, which makes for a rather large complexity. In practice however the number of comparisons is often smaller. For example, let $w = bab^{-1}ab^{-1}aba^{-1}b^{-1}ab$. Since the length of the word w is $n = 11$, the number of comparisons seems to be potentially 2^{22539}. We can do much better than this simply by observing that (keeping the notation from the proof of Theorem 2.4) if $u = w$ in G then we must have $U = \varphi(u) = \varphi(w) = W$. It is easy to calculate that $\alpha(W) = 3$ and $\beta(W) = 7$. Now if u is a word of length greater than 10 then either $3 < exp_a(u) = \alpha(U)$ or $7 < exp_b(u) \leq \beta(U)$. Thus we only need to check words u of length at most 10 and the number of needed comparisons is no greater than 2^{10}. In fact, we only need at most 6 comparisons. The equalities $3 = \alpha(W) = \alpha(U) = \exp_a(u)$ indicate that u must have the form $u = b^{t_0}ab^{t_1}ab^{t_2}ab^{t_3}$. Then the equality $\beta(U) = \beta(W)$ yields the equation

$$t_0 + t_1 \cdot 2 + t_2 \cdot 2^2 + t_3 \cdot 2^3 = 7,$$

which has only 6 solutions in non-negative integers leading to the six candidates for comparison $bababa$, b^3aaba, bab^3aa, b^3ab^2aa, b^5abaa and b^7aaa. They are all equal to w in G. In some other group for which $\xi = 2$ is also a root of the corresponding polynomial everything up to this point would have proceeded in exactly the same way, except that the 6 comparisons at the end may give a different result (some or even all of them may not represent the same element in the group as our test word). The point of this digression into complexity issues is not to show that the algorithm from Proposition 1.1 is fast, it most definitely is not, but rather that the linear representation from Theorem 2.4 can be used for more than to merely provide an upper distortion function, which may be close enough to the actual distortion but is in fact often too large when applied to individual "average" words w.

Example 2.8. Note that, in the context of Corollary 2.5 and Corollary 2.6, it is easy to construct examples where the polynomial equation $p(x) = 0$ does have a positive real root even in the cases $4''$ and 5. A more interesting fact is that the embedding of the positive monoid M in the group G can be recursive even if $p(x)$ does not have positive roots. This means that our general techniques involving upper distortion functions have larger scope than the table in Corollary 2.6 indicates. For example, let

$$G = Gp\ \langle\ a, b \mid bababa = a^2\ \rangle$$

and set $M = Mon\langle S\rangle$ and $G = Mon\langle X\rangle$ where $S = \{a, b\}$ and $X = \{a, b, a^{-1}, b^{-1}\}$. The corresponding polynomial equation $1+x+x^2 = 0$ does not have any real roots.

The rewriting system (X, R_G), where

$$\begin{aligned} R_G = \{&aa^{-1} \longrightarrow 1,\\ &a^{-1}a \longrightarrow 1,\\ &b^{-1} \longrightarrow a^{-2}baba,\\ &ba^{-1} \longrightarrow a^{-3}ba^2,\\ &babab \longrightarrow a^2,\\ &ba^3 \longrightarrow a^3b\}, \end{aligned}$$

is a finite complete rewriting system for G. Note that the positive words are invariant under this rewriting system, which means that the normal forms for the elements in M must be positive words. Thus a word in X represents an element in M if and only if its normal form is positive. This gives an easy solution to the membership problem for M in G. However, we will show that M recursively embeds in G, which implies that the membership problem is also decidable for any finitely generated submonoid of the positive monoid M. Indeed, since the positive words are invariant under (X, R_G), the rewriting system (S, R_M), where

$$\begin{aligned} R_M = \{&babab \longrightarrow a^2,\\ &ba^3 \longrightarrow a^3b\}, \end{aligned}$$

is a finite complete rewriting system for M. The reversed system (S, R'_M), with

$$\begin{aligned} R'_M = \{&a^2 \longrightarrow babab,\\ &a^3b \longrightarrow ba^3\} \end{aligned}$$

is terminating. Thus M is graded. This knowledge by itself is not sufficient to solve the membership problem, so let us construct an upper distortion function for M in G. The normal form of an arbitrary X-word w of length at most n cannot be longer than $18n$. Indeed, none of the rules in R_G increases the length except for $b^{-1} \longrightarrow a^{-2}baba$ and $ba^{-1} \longrightarrow a^{-3}ba^2$. Since the system is confluent we can choose in what order to perform the rewriting on w. Apply the rule $b^{-1} \longrightarrow a^{-2}baba$ as many times as possible. After at most n applications a word w' of length at most $6n$ is obtained that does not contain occurrences of b^{-1}. Since no rule in R_G produces occurrences of b^{-1} the rule $b^{-1} \longrightarrow a^{-2}baba$ cannot be applied anymore at any stage of the rewriting process applied to w'. Also, the number of b's in w' cannot be increased anymore during the rewriting process. By using the rules $a^{-1}a \longrightarrow 1$ and $aa^{-1} \longrightarrow 1$ rewrite w' in the form $a^*ba^* \cdots ba^*$ (where the stars represent arbitrary positive or negative powers). Now we (over)estimate the increase in length due to the applications of the rule $ba^{-1} \longrightarrow a^{-3}ba^2$. Note that applications of this rule together with $aa^{-1} \longrightarrow 1$ give, for $t \geq 0$,

$$\begin{aligned} ba^{-(3t+1)} &\xrightarrow{*} a^{-(3t+3)}ba^2\\ ba^{-(3t+2)} &\xrightarrow{*} a^{-(3t+3)}ba\\ ba^{-(3t+3)} &\xrightarrow{*} a^{-(3t+3)}b \end{aligned} \tag{2.2}$$

Apply the reductions (2.2) at the rightmost b that is followed by a negative power of a. The length of the word will be increased by at most 4 and the rule $ba^{-1} \longrightarrow a^{-3}ba^2$ can never again involve this particular occurrence of b (or any other occurrence of b to the right). Rewrite the result again in the form $a^*ba^* \cdots ba^*$. Then

apply the reductions (2.2) to the next rightmost b that is followed by a negative power. The length will be increased again by at most 4, etc. Eventually a word w'' of the form $a^{n_0}ba^{n_1}\cdots ba^{n_k}$ is obtained, where $n_1,\dots,n_k \geq 0$ and n_0 may be positive or negative. Since the number of b's followed by a negative power of a in a word of the form $a^*ba^*\cdots ba^*$ of length at most $6n$ cannot be greater than $3n$, the length of w'' is no greater than $6n + 4\cdot 3n = 18n$ (in fact, with more effort one can give a better bound). If w'' is not a normal form already, further applications of the rules in R_G will only make it shorter. Thus the normal form of w has length at most $18n$. Applying the rules in R'_M to a word of length at most $18n$ leads to a word of length at most $45n$ (only the rule $a^2 \longrightarrow babab$ increases the length, but this rule cannot be applied more than $9n$ times to a word of length $18n$). Thus, if an arbitrary X-word w of length at most n represents an element in M, its upper length $\lambda_S(w)$ with respect to S is at most $45n$, i.e., the function $\lambda : \mathbb{N} \to \mathbb{N}$ given by $\lambda(n) = 45n$ is an upper distortion function for M in G with respect to S and X. The same function is also an upper distortion function for any finitely generated submonoid of M in G.

The following example illustrates a *lifting strategy* that can be used to handle more involved examples by reducing them through homomorphisms to known cases and then lifting back the distortion functions (by Corollary 1.13).

Example 2.9. Let us solve the prefix membership for the one-relator group

$$G = Gp\ \langle\ a, b, c \mid ac^3bc^{-1}b^{-1}a^{-1}b^{-1} = 1\ \rangle.$$

If we add the relation $c = 1$ the obtained factor group is

$$H = Gp\ \langle\ a, b \mid b = 1\ \rangle = Gp\ \langle\ a \mid\ \rangle = \mathbb{Z}.$$

This factorization is not helpful since the prefix b maps to the identity and Proposition 1.12 cannot be applied. However, if we add the relation $c = b$ the corresponding factor group is

$$G' = Gp\ \langle\ a, b \mid ab^2a^{-1}b^{-1} = 1\ \rangle,$$

namely the Baumslag-Solitar group $BS(2, 1)$. There is a recursive upper distortion function for all positively and finitely generated submonoids of $BS(1, 2)$ (see Example 2.7) and all nontrivial prefixes of $r = ac^3bc^{-1}b^{-1}a^{-1}b^{-1}$ map to positive words in $BS(2, 1)$. Therefore, by Proposition 1.12, the prefix membership problem is decidable for $P(r)$ in G.

The lifting strategy is obviously very useful. In particular, it seems that the more generators one has, there is more freedom to choose a homomorphic image with the desirable properties so the strategy should be rather successful. However, it is not clear a priori how to choose such good homomorphic images.

We end by illustrating how the methods of this paper may be used to solve the prefix membership problem for the surface groups of genus $g \geq 2$. This problem has already been solved by Ivanov, Margolis and Meakin in [**14**] by using van Kampen Diagrams. We provide below a solution only in the case of the standard relator. Every cyclic conjugate of the standard relator leads to even easier prefix membership problem that can be handled by constructing an appropriate homomorphism to $\mathbb{Z}$ and using Corollary 1.14.

PROPOSITION 2.10. *The prefix monoid membership problem is decidable for every surface group G_g, $g \geq 2$, given by the presentation*

$$G_g = Gp \langle\ a_1, \ldots, a_g, b_1, \ldots, b_g \mid [a_1, b_1] \cdots [a_g, b_g] = 1\ \rangle.$$

Moreover, the function $\lambda : \mathbb{N} \to \mathbb{N}$ given by $\lambda(n) = n + n^2/4$ is an upper distortion function for the prefix monoid in G_g.

PROOF. Let

$$G = G_2 = Gp \langle\ a, b, c, d \mid [a, b][c, d] = 1\ \rangle.$$

and define the homomorphism $\varphi_g : G_g \to G$ by

$$a_1 \mapsto a, \qquad b_1 \mapsto b, \qquad a_g \mapsto c, \qquad b_g \mapsto d$$

and

$$a_i, b_i \mapsto 1, \qquad \text{for } i = 2, \ldots, g-1.$$

Since the nontrivial prefixes of $[a_1, b_1] \cdots [a_g, b_g]$ map to the nontrivial prefixes of $[a, b][c, d]$ under φ_g it is sufficient to show that the prefix monoid M of G embeds recursively in G and construct an upper distortion function for M in G. Extend the map

$$a, d \mapsto A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad b, c \mapsto B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

to a homomorphism $\varphi : G \to H$, where $H = \langle A, B \rangle \leq \mathsf{SL}_3(\mathbb{Z})$ is the Heisenberg group, i.e., the class 2 free nilpotent group of rank 2. This can be done since $[A, B][B, A] = 1$ is satisfied in any group. We will show that the monoid $M' = Mon\langle A, AB, ABA^{-1}, [A, B] \rangle$ embeds recursively in H and construct an upper distortion function with respect to $S' = \{A, AB, ABA^{-1}, ABA^{-1}B^{-1}\}$ and $X' = \{A, A^{-1}, B, B^{-1}\}$. For an arbitrary upper triangular matrix

$$U = \begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix}$$

representing an element in M', the equalities

$$UA = \begin{bmatrix} 1 & x+1 & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix}, \qquad UAB = \begin{bmatrix} 1 & x+1 & z+x+1 \\ 0 & 1 & y+1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$UABA^{-1} = \begin{bmatrix} 1 & x & z+x+1 \\ 0 & 1 & y+1 \\ 0 & 0 & 1 \end{bmatrix}, \qquad UABA^{-1}B^{-1} = \begin{bmatrix} 1 & x & z+1 \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix}$$

show that $\lambda_{S'}(U) \leq x + z$. On the other hand, for $W = A^{n_0} B^{m_1} \cdots A^{n_{k-1}} B^{m_k} A^{n_k}$,

$$W = \begin{bmatrix} 1 & x(W) & z(W) \\ 0 & 1 & y(W) \\ 0 & 0 & 1 \end{bmatrix},$$

where

$$x(W) = \sum_{i=0}^{k} n_i, \quad y(W) = \sum_{j=1}^{k} m_j, \quad z(W) = \sum_{j=1}^{k} (n_0 + n_1 + \cdots + n_{j-1}) m_j.$$

Therefore, if W has length at most n with respect to X', then $x(W) \leq n$, $z(W) \leq n^2/4$, and an upper distortion function for M' in H with respect to S' and X' is given by $\lambda(n) = n + n^2/4$. □

The equalities

$$(ABA^{-1}B^{-1})^{n^2} = [A, B]^{n^2} = [A^n, B^n] = A^n B^n A^{-n} B^{-n}$$

show that the actual upper distortion for M' in the Heisenberg group is at least quadratic in n. Thus the upper distortion $\lambda(n) = n + n^2/4$ given in the above proposition is a relatively good estimate.

Concluding Remarks

Note that the reason that Theorem 2.4 works is essentially that long products involving the matrices A and B used in a linear representation of G have large matrix norm (it does not matter which norm is used). In fact one can prove that

$$\lim_{n\to\infty} \min\{\ ||L||\ |L = S_1 S_2 \dots S_n,\ S_i \in \{A, B\},\ i = 1, \dots, n\ \} = \infty$$

Thus long products have a large norm and eventually become too large to be equal to the element we want to test for membership. Estimates of the rate of growth lead to estimates of the upper distortion functions and effectively solve the problem.

The above limit is related to the notion of upper (or joint) spectral radius introduced by Rota and Strang[**23**] and the dual notion of lower spectral radius of matrices. Indeed, the upper spectral radius for a set of matrices S over $\mathbb{C}$ is defined by

$$\rho_u(S) = \lim_{n\to\infty} (max\{\ ||L||\ |L = S_1 S_2 \dots S_n,\ S_i \in S,\ i = 1, \dots, n\ \})^{\frac{1}{n}},$$

and the lower spectral radius by

$$\rho_\ell(S) = \lim_{n\to\infty} (min\{\ ||L||\ |L = S_1 S_2 \dots S_n,\ S_i \in S,\ i = 1, \dots, n\ \})^{\frac{1}{n}}.$$

Such limits are difficult, when not impossible, to compute even for sets of 2 matrices. There is extensive literature dealing with estimation of $\rho_u(S)$ and $\rho_\ell(S)$ and deciding if $\rho_u(S) < 1$, $\rho_u(S) \leq 1$, $\rho_\ell(S) \geq 1$, $\rho_\ell(S) > 1$, and so on. See [**5**] for a survey and note that most decision problems of this nature are NP-hard or undecidable. However, the condition $\rho_\ell(S) > 1$ is too strong and implies that the norms of long products of matrices in S grow exponentially fast, which is more than it is needed (indeed our examples show that the growth can be linear). We need methods for choosing sets of matrices with

$$\lim_{n\to\infty} \min\{\ ||L||\ |\ L = S_1 S_2 \dots S_n,\ S_i \in S,\ \ i = 1, \dots, n\ \} = \infty, \tag{2.3}$$

and this condition is not well studied.

In addition, our choice of the set of matrices S is limited by the fact that we want it to generate a homomorphic image of the group we are interested in. All complex representations of a finitely presented group form an affine algebraic set. Each representation is a solution to a finite polynomial system of equations involving the entries of the matrices used for images of the generators. The equations of the system follow from the relations in the given presentation. In the proof of Theorem 2.4 we essentially selected a single point in the variety of all representations of G, showed that it satisfies the norm condition (2.3), and estimated the rate of growth, which is needed in order to construct a recursive upper distortion

function. It seems likely that a much larger class of examples can be handled by extending these techniques. Thus methods of selecting points in algebraic varieties leading to finite sets of matrices satisfying the norm condition (2.3) are needed to handle membership problems in graded monoids inside finitely presented groups with solvable word problem.

Acknowledgments

The authors are thankful to the referee for providing very concrete and useful comments.

References

[1] Sergei I. Adian. Defining relations and algorithmic problems for groups and semigroups. *Trudy Mat. Inst. Steklov.*, 85:123, 1966.

[2] G. N. Arzhantseva and A. Yu. Ol′shanskiĭ. Generality of the class of groups in which subgroups with a lesser number of generators are free. *Mat. Zametki*, 59(4):489–496, 638, 1996.

[3] Goulnara N. Arzhantseva. A property of subgroups of infinite index in a free group. *Proc. Amer. Math. Soc.*, 128(11):3205–3210, 2000.

[4] Michèle Benois. Parties rationnelles du groupe libre. *C. R. Acad. Sci. Paris Sér. A-B*, 269:A1188–A1190, 1969.

[5] Vincent D. Blondel and John N. Tsitsiklis. A survey of computational complexity results in systems and control. *Automatica J. IFAC*, 36(9):1249–1274, 2000.

[6] P. A. Cummings and R. Z. Goldstein. Solvable word problems in semigroups. *Semigroup Forum*, 50(2):243–246, 1995.

[7] Benson Farb. The extrinsic geometry of subgroups and the generalized word problem. *Proc. London Math. Soc. (3)*, 68(3):577–593, 1994.

[8] È. A. Golubov. Finite separability in semigroups. *Sibirsk. Mat. Ž.*, 11:1247–1263, 1970.

[9] M. Gromov. Hyperbolic groups. In *Essays in group theory*, volume 8 of *Math. Sci. Res. Inst. Publ.*, pages 75–263. Springer, New York, 1987.

[10] Mikhael Gromov. Asymptotic invariants of infinite groups. In *Geometric group theory, Vol. 2 (Sussex, 1991)*, volume 182 of *London Math. Soc. Lecture Note Ser.*, pages 1–295. Cambridge Univ. Press, Cambridge, 1993.

[11] Zeph Grunschlag. *Algorithms in geometric group theory*. PhD thesis, University of California at Berkeley, 1999.

[12] Zeph Grunschlag. Computing angles in hyperbolic groups. In *Groups, languages and geometry (South Hadley, MA, 1998)*, volume 250 of *Contemp. Math.*, pages 59–88. Amer. Math. Soc., Providence, RI, 1999.

[13] Peter M. Higgins. *Techniques of semigroup theory*. Oxford Science Publications. The Clarendon Press Oxford University Press, New York, 1992. With a foreword by G. B. Preston.

[14] Sergei V. Ivanov, Stuart W. Margolis, and John C. Meakin. On one-relator inverse monoids and one-relator groups. *J. Pure Appl. Algebra*, 159(1):83–111, 2001.

[15] David A. Jackson. Decision and separability problems for Baumslag-Solitar semigroups. *Internat. J. Algebra Comput.*, 12(1-2):33–49, 2002. International Conference on Geometric and Combinatorial Methods in Group Theory and Semigroup Theory (Lincoln, NE, 2000).

[16] Ilya Kapovich. Detecting quasiconvexity: algorithmic aspects. 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 91–99. Amer. Math. Soc., Providence, RI, 1996.

[17] Steven Lindblad. *Inverse monoids presented by a single sparse relator*. PhD thesis, University of Nebraska - Lincoln, 2003.

[18] James McCool. Unsolvable problems in groups with solvable word problem. *Canad. J. Math.*, 22:836–838, 1970.

[19] K. A. Mikhailova. The occurence problem in direct products of groups. *Dokl. Akad. Nauk SSSR*, 119:1103–1105, 1958.

[20] K. A. Mikhailova. The occurence problem in direct products of groups. *Mat. Sb.*, 70:241–251, 1966.

[21] John H. Remmers. On the geometry of semigroup presentations. *Adv. in Math.*, 36(3):283–296, 1980.
[22] E. Rips. Subgroups of small cancellation groups. *Bull. London Math. Soc.*, 14(1):45–47, 1982.
[23] Gian-Carlo Rota and Gilbert Strang. A note on the joint spectral radius. *Nederl. Akad. Wetensch. Proc. Ser. A 63 = Indag. Math.*, 22:379–381, 1960.
[24] O. A. Sarkisjan. Some relations between word problems and divisibility problems in groups and semigroups. *Izv. Akad. Nauk SSSR Ser. Mat.*, 43(4):909–921, 968, 1979.
[25] John R. Stallings. Adian groups and pregroups. In *Essays in group theory*, volume 8 of *Math. Sci. Res. Inst. Publ.*, pages 321–342. Springer, New York, 1987.

Department of Mathematics, Bar-Ilan University, Ramat-Gan, 52900, Israel
E-mail address: stwm@math.huji.ac.il

Department of Mathematics, 810 Oldfather Hall, University of Nebraska, Lincoln, NE 68588-0323, USA
E-mail address: jmeakin@math.unl.edu

Department of Mathematics, Texas A&M University, College Station, TX, 77843-3368 USA
E-mail address: sunik@math.tamu.edu