



ACADÉMIE
DES SCIENCES
INSTITUT DE FRANCE

Comptes Rendus

Mathématique


Carl-Fredrik Nyberg-Brodde

On the Dehn functions of a class of monadic one-relation monoids

Volume 362 (2024), p. 713-730

Online since: 17 September 2024

<https://doi.org/10.5802/crmath.554>

 This article is licensed under the
CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL LICENSE.
<http://creativecommons.org/licenses/by/4.0/>



*The Comptes Rendus. Mathématique are a member of the
Mersenne Center for open scientific publishing*
www.centre-mersenne.org — e-ISSN : 1778-3569



Research article / *Article de recherche*

Algebra, Algorithmic and computer tools / *Algèbre, Algorithmes et outils informatiques*

On the Dehn functions of a class of monadic one-relation monoids

Sur les fonctions de Dehn d'une classe de monoïdes monadiques à une relation

Carl-Fredrik Nyberg-Brodda ^a

^a Laboratoire d'Informatique Gaspard-Monge, Université Gustave Eiffel (Paris)

E-mail: carl-fredrik.nyberg-brodda@univ-eiffel.fr

Abstract. We give an infinite family of monoids Π_N (for $N = 2, 3, \dots$), each with a single defining relation of the form $bUa = a$, such that the Dehn function of Π_N is at least exponential. More precisely, we prove that the Dehn function $\partial_N(n)$ of Π_N satisfies $\partial_N(n) \geq N^{n/4}$. This answers negatively a question posed by Cain & Maltcev in 2013 on whether every monoid defined by a single relation of the form $bUa = a$ has quadratic Dehn function. Finally, by using the decidability of the rational subset membership problem in the metabelian Baumslag–Solitar groups $BS(1, n)$ for all $n \geq 2$, proved recently by Cadilhac, Chistikov & Zetsche, we show that each Π_N has decidable word problem.

Résumé. Nous donnons une famille infinie de monoïdes Π_N (pour $N = 2, 3, \dots$), chacun avec une seule relation de définition de la forme $bUa = a$, telle que la fonction de Dehn de Π_N est au moins exponentielle. Plus précisément, nous démontrons que la fonction de Dehn $\partial_N(n)$ de Π_N satisfait $\partial_N(n) \geq N^{n/4}$. Cela répond négativement à une question posée par Cain & Maltcev en 2013, à savoir si tout monoïde défini par une seule relation de la forme $bUa = a$ possède une fonction de Dehn quadratique. Enfin, en utilisant la décidabilité du problème de l'appartenance à un sous-ensemble rationnel dans les groupes métabéliens de Baumslag–Solitar $BS(1, n)$ pour tout $n \geq 2$, prouvée récemment par Cadilhac, Chistikov & Zetsche, nous montrons que chaque Π_N a un problème de mots décidable.

2020 Mathematics Subject Classification. 20F10, 20F65.

Note. The author is currently working as Attaché Temporaire d'Enseignement et de Recherche at the Laboratoire d'Informatique Gaspard-Monge, Université Gustave Eiffel (Paris, France).

Manuscript received 13 November 2022, revised 12 July 2023, accepted 14 August 2023.

The word problem for one-relation monoids is arguably the most important unsolved problem in semigroup theory, and has been open for over a century. Given two words u, v over an alphabet A (denoted $u, v \in A^*$), the monoid M with the single defining relation $u = v$ is defined as the quotient of the free monoid A^* by the least congruence containing the pair (u, v) . This monoid is denoted $\text{Mon}\langle A \mid u = v \rangle$. The word problem for such a monoid – a *one-relation monoid* – asks for a decision procedure which, given two words $w_1, w_2 \in A^*$, decides whether (w_1, w_2) lies in the above congruence or not. Despite numerous efforts, the word problem for one-relation monoids in general remains open. Thue [29] gave a still inchoate study of this problem when the defining relation is of the form $u = 1$, where 1 is the empty word, and solved it in some particular cases. Adian in the 1960s made the first targetted effort towards solving the problem, and solved the

word problem in two important cases: first, whenever the relation is of the form $u = 1$ (the *special* case), and second, whenever the relation $u = v$ satisfies that the first letters of u and v differ, and the last letters of u and v differ (the *cycle-free* or *cancellative* case). Both results are proved via a reduction to Magnus' classical theorem on the decidability of the word problem in all one-relator groups [23].

More detailed studies were later made by Adian [2] and Adian & Oganesian [3, 4]. These studies were focussed on the case of *left cycle-free* monoids. In the case of one relation, this says that the relation $u = v$ has the first letters of u and v distinct, but the last letters may coincide. Adian [2] introduced a pseudo-algorithm \mathfrak{A} which, for any given left cycle-free monoid M , gives a procedure for studying the *left divisibility problem* in M . Here, the left divisibility problem refers to the problem of deciding whether a word w_1 is left divisible by some other word w_2 , i.e. if there is some word z such that $w_1 = w_2z$. We detail this pseudo-algorithm in § 1. Using \mathfrak{A} , Adian & Oganesian [4] proved that the word problem for a given one-relation monoid $\text{Mon}\langle A \mid u = v \rangle$ can be reduced to the word problem for a one-relation monoid of one of the forms:

$$(1) \text{Mon}\langle a, b \mid bUa = aVa \rangle, \quad \text{or} \quad (2) \text{Mon}\langle a, b \mid bUa = a \rangle,$$

where U, V are some words, i.e. the word problem for all one-relation monoids reduces to the word problem for all 2-generated left cycle-free one-relation monoids. This reduction is very constructive, and easy to find in practice (see [25, § 3, Example 3.14] for details). The word problem remains open for left cycle-free monoids in general, even lifting the simplifying assumption of a single relation (see [25, § 2.2] for the general definition). Let M_ℓ be a left cycle-free monoid. Other than Adian's classical result that M_ℓ is left cancellative, some further results are known. For example, Valitskas proved that if M_ℓ is also right cancellative, then M_ℓ is group-embeddable.¹ Furthermore, Guba [18, Theorem 5.1] proved that the set of principal right ideals of M_ℓ is a semi-lattice under intersection, and that any finitely generated right ideal of M_ℓ can be generated by two elements. These are strong structural properties not satisfied by all semigroups.

A one-relation monoid of the form $\text{Mon}\langle a, b \mid bUa = a \rangle$ will be called *monadic*. These have seen a good deal of study. Oganesian, in particular, used \mathfrak{A} to prove a number of remarkable statements in this setting. For example, Oganesian [27] proved that the isomorphism problem for one-relation monoids can be reduced to the word problem for all monadic one-relation monoids, and further (see [26]) proved that the word problem for all monadic one-relation monoids reduces to the left divisibility problem for all cycle-free monoids.² More specifically, Oganesian proved the remarkable fact that if M is a monadic one-relation monoid with defining relation $bUa = a$, then the monoid $S(M)$ generated by all suffixes of bUa is cycle-free, and furthermore the word problem for M reduces to the left divisibility problem in $S(M)$. Guba [18] extended this latter result to prove that $S(M)$ embeds in a one-relator group $\overline{G}(M)$ as the submonoid generated by all suffixes of the defining relation of $\overline{G}(M)$. As the left divisibility problem in $S(M)$ reduces to the membership problem for $S(M)$ in $\overline{G}(M)$, this shows that the word problem for all monadic one-relation monoids reduces to the submonoid membership problem for all one-relator groups. We will return to this chain of reductions in § 3.

The starting point for the present article, which is focussed on a class of monadic one-relation monoids, comes in the form of two pre-prints from 2013, by Cain & Maltcev [10, 11]. These pre-prints attempt to construct *finite complete rewriting systems* for monadic left cycle-free monoids M in which the defining relation $bUa = a$ satisfies the condition that bUa has a short "relative length", i.e. the shortest way, in terms of number of alternations, to write bUa as an alternating product of b 's and a 's. Specifically, in [10] it is shown that if bUa is of the form $b^\alpha a^\beta b^\gamma a^\delta$ for some

¹This result was never published; Guba [17, Theorem 4] filled in the details in a later paper.

²Sarkisian claimed a solution to the latter problem, but a gap was found in the 1990s, and it remains open. See [25, § 4.4] for further details.

$\alpha, \beta, \gamma, \delta \geq 1$ (i.e. bUa has relative length 4), then M admits a finite complete rewriting system. In [11], the same claim was made for the case of bUa having relative length 6; however, as we shall see, the monoid Π_2 of this article demonstrates the existence of gap in the proof (but not, a priori, a counterexample to the statement), see § 3.

Their approach was in line with answering the (still open) question of whether every one-relation monoid admits a finite complete rewriting system. Of course, a positive answer to this question would resolve the word problem, and so would represent an incredible leap forward from our current understanding; however, a negative answer may be obtained even without involving the word problem. Based on historical results, such a negative answer may be obtained via considering appropriate types of homological finiteness properties, see e.g. [21]. For recent progress on this subject, see the result by Gray & Steinberg [15] that every one-relation monoid satisfies the homological finiteness property FP_∞ , a condition satisfied by all monoids admitting finite complete rewriting systems.

Cain & Maltcev noticed, based on their rewriting systems constructed, that the Dehn function of all monadic one-relation monoids $\text{Mon}\langle a, b \mid bUa = a \rangle$ in which bUa has relative length 4 is at most quadratic. This prompted the authors to ask the following question, see [10, Open Problem 5.1 (1)]:

Question (Cain & Maltcev, 2013). *Does every monoid $\text{Mon}\langle a, b \mid bUa = a \rangle$ have at most quadratic Dehn function?*

Here, the Dehn function is a measure of the complexity of the “naïve” method of attempting to solve the word problem in a given monoid, see § 1 for details. In this article, we provide a negative answer to their question. More specifically, we will show the following main theorem:

Theorem 1. *For every $N \geq 2$, the Dehn function ∂_N of the one-relation monoid*

$$\Pi_N = \text{Mon}\langle a, b \mid aa(ba)^N = a \rangle$$

satisfies $\partial_N(n) \geq N^{n/4}$, i.e. the Dehn function of Π_N is at least exponential.

Hence, Theorem 1 answers negatively Cain & Maltcev’s question. The proof of Theorem 1 is enacted via the proof of a Main Lemma, which shows that for every $k \geq 1$ and every $N \geq 2$ we have

$$ab^{2k}a^{2k}a = b^{2k-1}a^{2k}baa \quad \text{in } \Pi_N,$$

but that the shortest sequence of elementary transformations of Π_N verifying this grows exponentially in k (with base N).

In spite of the above result, in § 3 we will also prove (Theorem 19) that the word problem is decidable in all Π_N , by reducing it to the decidability of the rational subset membership problem in solvable Baumslag–Solitar groups. Finally, we will mention some links with other results, including residual finiteness, positive one-relator groups, finite complete rewriting systems, automaticity, and one-relation inverse monoids.

1. Transformations in cycle-free monoids

We assume the reader is familiar with the basics of combinatorial group and semigroup theory, in particular the theory of presentations. The reader may consult [1, 24, 28] if they are not. We will denote monoid (resp. group) presentations as $\text{Mon}\langle A \mid R \rangle$ (resp. $\text{Gp}\langle A \mid R \rangle$), where A is the generating set, and R is the set of defining relations resp. relators. The free monoid on an alphabet A is denoted A^* . For two words $u, v \in A^*$ with a maximal shared prefix p , i.e. $u = pu'$ and $v = pv'$ (p may be empty) and the first letters of u' and v' differ (or both are empty), we let $(u, v)_{p\text{-red}}$ denote the pair (u', v') , i.e. the pair obtained by removing the maximal shared prefix of u and v .

We say that the pair (u, v) is *(left-)reduced* if $(u, v)_{\text{p-red}} = (u, v)$, i.e. u and v have no shared non-empty prefix. We omit many of the details of Adian’s theory of cycle-free monoids, and refer the reader to [25].

1.1. Dehn functions

For a finitely presented monoid $M = \text{Mon}\langle A \mid R \rangle$, each equivalence class of a word $w \in A^*$ can be regarded as a metric space. Concretely, if $u, v \in A^*$ are such that $u = v$ in M , then we can define a metric $\partial_M(u, v)$ as the shortest sequence of elementary transformations of M transforming u into v , i.e. the shortest sequence of applications of relations connecting u and v . Overloading notation, this metric gives rise to the monotone non-decreasing *Dehn function* $\partial_M: \mathbb{N} \rightarrow \mathbb{N}$ (also called the *least isoperimetric function*) for M defined as:

$$\partial_M(n) = \max \{ \partial_M(u, v) : u, v \in A^*, u =_M v \text{ and } |u| + |v| \leq n \}.$$

Here $|v|$ denotes the length of $v \in A^*$ (as a word over the alphabet A). In other words, $\partial_M(n)$ measures the complexity of the “naïve” approach to solving the word problem in a monoid via enumerating equalities by using the defining relations. It is easy to see that the word problem for M is decidable if and only if $\partial_M(n)$ is a recursive function (with respect to any generating set A). For two functions $\varphi, \psi: \mathbb{N} \rightarrow \mathbb{N}$, we write $\varphi \leq \psi$ if there is a constant $c \in \mathbb{N}$ such that $\varphi(n) \leq c\psi(cn) + cn$ for all $n \in \mathbb{N}$, and we write $\varphi \sim \psi$ if $\varphi \leq \psi$ and $\psi \leq \varphi$. Then \sim is an equivalence relation on the set of all functions $\varphi: \mathbb{N} \rightarrow \mathbb{N}$. The equivalence class – i.e. the asymptotic growth rate – of ∂_M under \sim can easily be shown to not depend on the particular finite generating set A chosen (which justifies our somewhat abusive suppression of any mention of the generating set above). Thus, we may speak of a monoid having a linear, quadratic, polynomial, exponential, etc., Dehn function, where e.g. M having a quadratic Dehn function means that $\partial_M(n) \sim n^2$. This is true, for example, for the free commutative monoid $\mathbb{N} \times \mathbb{N} \cong \text{Mon}\langle a, b \mid ab = ba \rangle$, in which proving that $a^n b^n$ equals $b^n a^n$ requires $\sim n^2$ elementary transformations.

1.2. Algorithm \mathfrak{A}

In 1976, Adian [2] described a pseudo-algorithm for solving the left divisibility problem in a given left cycle-free monoid (and hence also the word problem). This pseudo-algorithm is called \mathfrak{A} , and takes as input the defining relations of a left cycle-free presentation for a monoid M , a word w , and a letter x , and outputs either “yes” or “no”, depending on whether w is left divisible by x in M . It is termed a pseudo-algorithm rather than an algorithm because it does not always terminate, and it has no built-in mechanism for detecting non-termination, even for a fixed set of defining relations and letter. In the sequel, we will be somewhat sloppy and write \mathfrak{A} as taking only a single word as input (with a minor modification below to allow for two words), and let context make the defining relations and the letter clear.

We will only describe \mathfrak{A} for the case of a left cycle-free one-relation monoid $M = \text{Mon}\langle a, b \mid bP = aQ \rangle$. For a full description, we refer the reader to [25, § 4.2]. We will make use of *prefix decompositions* of a word (with respect to the above presentation). Let $A = \{a, b\}$. For a word $w \in A^*$, we find the *prefix decomposition* $\mathfrak{R}(w)$ of w as follows. From left to right, factorise w into a product of maximal prefixes of either bP or aQ (as M is left cycle-free, this is well-defined). If any of these maximal prefixes is the entire defining word bP or aQ , then we stop, and call this the *head* of $\mathfrak{R}(w)$. The remaining suffix of w is called the *tail* of $\mathfrak{R}(w)$. If $\mathfrak{R}(w)$ has no head, then it is called a *headless* decomposition. We write

$$\mathfrak{R}(w) = w_1 \mid w_2 \mid \cdots \mid w_k \boxed{H} w'$$

to denote that the w_i are maximal proper prefixes of bP or aQ , and that $H = bP$ or $H = aQ$ is the head of the prefix decomposition of w ; the word w' is the tail. In the case of a headless decomposition, we write this simply

$$\mathfrak{R}(w) = w_1 | w_2 | \cdots | w_k.$$

Example 2. Let $M_0 = \text{Mon}\langle a, b \mid b^2 a^2 = a \rangle$. We give an example of two prefix decompositions with a head, and one that is headless.

$$\mathfrak{R}(bbbbabbaabbab) = bb | bba \boxed{bbaa} | bbab. \quad (1)$$

$$\mathfrak{R}(bbabbababab) = bba | bba | b \boxed{a} | bab. \quad (2)$$

$$\mathfrak{R}(bbabbabb) = bba | bba | bb. \quad (3)$$

We shall see below that results due to Adian allow us to conclude, from the latter of these three decompositions, that $bbabbabb$ is *not* left divisible by a in M_0 .

We shall make one notational simplification. If the prefix decomposition of a word w begins with $p > 1$ copies of a prefix u , i.e. if $\mathfrak{R}(w)$ is of the form

$$\mathfrak{R}(w) = \underbrace{u | u | \cdots | u}_{p \text{ times}} | v \cdots \quad (4)$$

and none of these occurrences of u are the head (if any) of the decomposition, then we will simply write this as

$$\mathfrak{R}(w) = u^p | v \cdots .$$

This is not very abusive, as we know by the prefix decomposition (4) that u^p is not itself a prefix of any defining relation.

Adian's algorithm \mathfrak{A} , with input a word w and a letter $x \in A$, is now described as follows. First, if w begins with x , the procedure halts, and outputs YES. Otherwise, compute the prefix decomposition $\mathfrak{R}(w)$. If $\mathfrak{R}(w)$ is headless, then halt, and output NO. If $\mathfrak{R}(w)$ has a head, then replace the head by the other side of the defining relation. This results in a word w' . We say $\mathfrak{A}_x^{(1)}(w) = w'$ or simply $\mathfrak{A}^{(1)}(w) = w'$ (leaving the letter x implicit). We then iterate this procedure, finding $\mathfrak{A}^{(2)}(w), \mathfrak{A}^{(3)}(w), \dots$. This process does not always terminate.

Example 3. We continue Example 2. Fixing the letter $x = a$, and suppressing it in writing \mathfrak{A} below, we have, using the decompositions (1) and (2), that

$$\mathfrak{A}^{(1)}(bbbbabbaabbab) = bbbba \cdot a \cdot bbab,$$

$$\mathfrak{A}^{(1)}(bbabbababab) = bbabbab \cdot bbaa \cdot bab,$$

and as $bbabbabb$ has a headless prefix decomposition, \mathfrak{A} terminates immediately on input $bbabbabb$. We leave the reader to verify that

$$\mathfrak{A}^{(2)}(bbbbabbaabbab) = bbabbab,$$

which has a headless prefix decomposition. Furthermore, it is not hard to see that \mathfrak{A} does not terminate on input $bbabbabababab$ as above. Indeed, we even have

$$\mathfrak{A}^{(1)}(ba) = bbbba, \quad \mathfrak{A}^{(2)}(ba) = bbbbaaa, \quad \dots, \quad \mathfrak{A}^{(i)}(ba) = b^{2i+1} a^{i+1}, \dots$$

and so \mathfrak{A} does not even terminate on input ba .

In general, as our alphabet consists of only two letters a and b , when writing $\mathfrak{A}(w)$, we will implicitly assume that the letter x is simply the letter which w does not begin with (as otherwise \mathfrak{A} would terminate immediately).

Theorem (Adian, 1976). *Let $M = \text{Mon}\langle A \mid R \rangle$ be a left cycle-free monoid. Suppose \mathfrak{A} is applied to a word $u \in A^*$. Then u is left divisible by $x \in A$ if and only if \mathfrak{A} terminates, when input u and x , in a word beginning with x . That is, u is left divisible by x if and only if \mathfrak{A} outputs YES on input u and x .*

In view of the remarkable result by Guba [18, Theorem 4.1] that the word problem is equivalent to the left divisibility problem in the case of monadic left cycle-free one-relation monoids, it follows that the halting problem for \mathfrak{A} for the monoid is in these cases equivalent to the word problem for the monoid.

We shall make a notational modification for \mathfrak{A} , and use this to denote another, very closely related, algorithm. This will operate on pairs of words $u, v \in A^*$ with no common non-empty prefix, as follows. First, if either of u or v are empty, then \mathfrak{A} halts. If both u and v are non-empty, then \mathfrak{A} will perform a single step of Adian's (usual) algorithm \mathfrak{A} on u . Suppose $\mathfrak{A}^{(1)}(u) = u'$. Then we set $\mathfrak{A}^{(1)}(u, v) = (u', v)_{\text{p-red}}$. As this results in a pair of words (u'', v') with no common non-empty prefix, we may iterate \mathfrak{A} on (u'', v') , obtaining $\mathfrak{A}^{(2)}(u, v)$, etc. When we write $\mathfrak{A}^{(k)}(u, v) = (\varepsilon, \varepsilon)$, we mean that \mathfrak{A} takes *exactly* k steps to reach $(\varepsilon, \varepsilon)$ when applied to the pair (u, v) .

The following is one of the key properties of \mathfrak{A} , and is a direct and easy reformulation of the proof of [2, Theorem 1].

Proposition 4 (Adian, 1976). *Let $M = \text{Mon}\langle A \mid R \rangle$ be a left cycle-free monoid, and $u, v \in A^*$. Then $u =_M v$ if and only if there is some (necessarily unique) $k \in \mathbb{N}$ such that $\mathfrak{A}^{(k)}(u, v) = (\varepsilon, \varepsilon)$. Furthermore, if such k exists, then $\partial_M(u, v) = k$.*

In other words, stated geometrically (and for the reader familiar with the details of semigroup diagrams, cf. e.g. [18]), for equal words u and v , \mathfrak{A} can be used to produce a (u, v) -diagram with the least number of cells over all (u, v) -diagrams. Furthermore, this is the only (u, v) -diagram with this number of cells.

2. Equalities in Π_N

2.1. Basic lemmas in Π_N

As mentioned in the introduction, the monoids

$$\Pi_N = \text{Mon}\langle a, b \mid baa(ba)^N = a \rangle,$$

where $N \geq 2$, hold center stage. In the sequel, we will so frequently use the abbreviation

$$X = ba$$

that it deserves its own line. Note that this makes the defining relation of Π_N as $XaX^N = a$. We state two lemmas on word transformations via \mathfrak{A} as applied to Π_N . In the sequel, whenever we write “word” we mean “word over $\{a, b\}$ ”; whenever we write \mathfrak{A} , we mean \mathfrak{A} as applied to Π_N ; when we write “ u is left divisible by v ” we mean “ u is left divisible by v in Π_N ”, etc.

Lemma 5. *Let P, Q be arbitrary words. Suppose $\mathfrak{A}^{(k)}(P) = W$ for some word W and $k \in \mathbb{N}$. If either*

- (1) *P begins with a , and is left divisible by b ; or*
- (2) *P begins with b , and is left divisible by a .*

Then we have $\mathfrak{A}^{(k)}(PQ) = WQ$.

The proof is easy by using Adian's Theorem on \mathfrak{A} (as above) to conclude that for all $k_0 < k$ the word $\mathfrak{A}^{(k_0)}(P)$ has a head, so the head of the prefix decomposition of $\mathfrak{A}^{(k_0)}(PQ)$ is inside this distinguished subword P .

Lemma 6. *Let $Y = bY'$ be a word beginning with b . Let $\ell \geq 0$ be such that for all $0 \leq k \leq \ell$, we have that $\mathfrak{A}^{(k)}(Y)$ also begins with b . Then for all $s \geq 1$, we have $\mathfrak{A}^{(s)}(b^s Y) = b^s \mathfrak{A}^{(s)}(Y)$.*

The proof of this lemma is immediate by strong induction on ℓ .

2.2. The Main Lemma

We now turn to the proof of Theorem 1, which will pass via a Main Lemma. For every $k \geq 0$, we define the following pairs of words:

$$U_k = ab^{2k} a^{2k} a, \quad V_k = b^{2k-1} a^{2k} baa.$$

The main equalities we shall prove are the following:

$$U_k = V_k \quad \text{in } \Pi_N \text{ for all } k \geq 1 \text{ and all } N \geq 2. \tag{5}$$

We remark immediately that the words U_k and V_k do *not* depend on N . That is, these words are equal in all Π_N . Indeed, we have

$$|U_k| = |V_k| = 4k + 2.$$

We shall prove that although the equality $U_k = V_k$ holds in Π_N , this can only be proved using sequences of elementary transformations whose length are exponential, with exponent k and base N^2 . More precisely, we prove the following:

Main Lemma. *For every $k \geq 1$ and $N \geq 2$, we have $U_k = V_k$ in Π_N . Furthermore, the shortest chain of elementary transformations of Π_N verifying this equality has length $\sigma_N(k)$, where*

$$\sigma_N(k) := \frac{2N}{N^2 - 1} (N^{2k} - 1) + 4k - 2.$$

In other words, we have $\partial_N(U_k, V_k) = \sigma_N(k)$.

Using the Main Lemma it is easy to see that Theorem 1 follows. Indeed, assuming it holds, we find the following:

Proof of Theorem 1. First, we have $|U_k| + |V_k| = 8k + 4$. Let $n \in \mathbb{N}$ with $n \geq 4$, and let $k \in \mathbb{N}$ be the greatest k such that $n \geq 8k + 4$. In particular, $k = \lfloor \frac{n-4}{8} \rfloor$. Then by the Main Lemma we have

$$\partial_N(n) \geq \partial_N(8k + 4) \geq \partial_N(U_k, V_k) \sim N^{2k} = N^{2 \lfloor \frac{n-4}{8} \rfloor} \sim N^{n/4}.$$

Hence $\partial_N(n) \geq N^{n/4}$, and Π_N has Dehn function $\partial_N(n)$ at least exponential. □

The remainder of the section will be devoted to the proof of the Main Lemma.

2.3. Proof of the Main Lemma

Let us recall the definition of the words U_k and V_k , for $k \geq 1$:

$$U_k = ab^{2k} a^{2k} a, \quad V_k = b^{2k-1} a^{2k} baa.$$

As noted above, we shall also very frequently make use of the abbreviation $X = ba$. Thus, the defining relation of Π_N is $XaX^N = a$. The overall strategy of the proof is to apply \mathfrak{A} to the pair (U_k, V_k) . This process will be divided into two parts. The first will serve to reduce the pair (U_k, V_k) to one of the form (W, a) , where the precise form of W depends both on k and N . The second part will be to reduce the pair (W, a) to a pair $(X^p aX^{pN}, a)$, where $p = p(k, N)$ is a “very large” number. Of course, no matter the value of p , we have that Adian’s algorithm reduces $(X^p aX^{pN}, a)$ to $(\varepsilon, \varepsilon)$ in X^p steps. In total, keeping a precise count, Adian’s algorithm will take $\sigma_N(k)$ steps to reduce (U_k, V_k) to $(\varepsilon, \varepsilon)$, which will complete our proof by Proposition 4.

We begin with a somewhat technical lemma, but which is often very useful. In essence, the lemma says that X 's can be "pushed" to the right of an aa , as long as one applies an appropriate multiplicative factor of N^2 .

Lemma 7. *Let $p, q \geq 0$. Then $\mathfrak{A}^{(pN+p)}(X^p aaX^q) = aaX^{q+pN^2}$.*

Proof. The proof of the claim is now by induction on p . If $p = 0$, then there is nothing to prove. Assume the lemma is proved for all $p < p'$ with $p' > 0$. We prove the claim for $p = p'$. As $p > 0$, the prefix decomposition of $W = X^p aaX^q = X^{p-1} baaaX^q$ is

$$\mathfrak{R}(X^p aaX^q) = X^{p-1} | baa \boxed{a} X^q,$$

so we find that $\mathfrak{A}^{(1)}(W) = X^{p-1} baa \cdot (ba)^1 aX^N \cdot X^q$. Here, the prefix decomposition is easily found to be

$$\mathfrak{R}(X^p abaaX^N X^q) = X^{p-1} | baa(ba)^1 \boxed{a} X^N X^q,$$

and so $\mathfrak{A}^{(2)}(W) = X^{p-1} baa(ba)^2 aX^{2N} X^q$. Continuing iteratively, we thus find that

$$\mathfrak{A}^{(N)}(W) = X^{p-1} \underline{baa(ba)^N} aX^{N^2} X^q,$$

where the head of the prefix decomposition of this word is the underlined segment $baa(ba)^N$. Consequently,

$$\mathfrak{A}^{(N+1)}(W) = X^{p-1} aaX^{q+N^2}$$

and as $\mathfrak{A}^{((p-1)N+p-1)}(X^{p-1} aaX^{q+N^2}) = aaX^{q+N^2+(p-1)N^2}$ by the inductive hypothesis, we find that

$$\mathfrak{A}^{(pN+p)}(W) = \mathfrak{A}^{(N+1+(p-1)N+p-1)}(W) = aaX^{q+pN^2},$$

which is what was to be proved. □

We define three sequences s_N, t_N , and T_N of natural numbers as follows:

$$s_N(n) = \begin{cases} N, & \text{if } n = 0, \\ N^2 s_N(n-1) - N^2 + N, & \text{if } n > 0. \end{cases}$$

$$t_N(n) = \begin{cases} 0, & \text{if } n = 0, \\ (N+1)(s_N(n-1) - 1) + 1, & \text{if } n > 0. \end{cases}$$

$$T_N(n) = \sum_{i=0}^n t_N(i).$$

Note that $t_N(n)$ is defined via a recurrence on s_N , rather than on t_N . For example, for $N = 2$, the sequences begin as follows:

$$s_2(n): 2, 6, 22, 86, 342, 1366, \dots,$$

$$t_2(n): 0, 4, 16, 64, 256, 1024, \dots,$$

$$T_2(n): 0, 4, 20, 84, 340, 1364, \dots$$

The reader may well recognise the sequence $t_2(n)$ above, and that $s_2(n)$ appears very similar to $T_2(n)$; of course, this is no coincidence. Indeed, it is an easy exercise in undergraduate combinatorics to derive a closed form for the three sequences above, as follows:

Lemma 8. *The sequences s_N, t_N , and T_N admit the following closed forms:*

(1) $s_N(n) = \frac{N}{N+1}(N^{2n+1} + 1)$ for all $n \geq 0$.

(2) $t_N(n) = (N^2)^n$ for all $n > 0$.

(3) $T_N(n) = \frac{N^2}{N^2-1}(N^{2n} - 1)$ for all $n \geq 0$.

Having diverged somewhat from considering words, we now return to our words U_k and V_k . We begin with a useful lemma, which will use all three of the above functions.

Lemma 9. *Let $q \geq 0$. Let Q be an arbitrary word. Then*

$$\mathfrak{A}^{(T_N(q))} (X^N (aX^N)^{2q}, a^{2q}Q) = (X^{s_N(q)}, Q).$$

Proof. The proof is by induction on q . If $q = 0$, then $X^N (aX^N)^{2q} = X^N$, and as $T_N(q) = 0$ and $s_N(q) = N$, the claim holds. Assume the claim holds for all $q < q'$ for some $q' > 0$. We prove the claim for $q = q'$.

As $X^N (aX^N)^{2(q-1)}$ is, by the inductive hypothesis, left divisible by a , it follows from Lemma 5, taking $P = X^N (aX^N)^{2(q-1)}$, and the inductive hypothesis that we have

$$\mathfrak{A}^{(T_N(q-1))} (X^N (aX^N)^{2q}, a^{2q}Q) = (X^{s_N(q-1)} (aX^N)^2, a^2Q).$$

We will now rewrite this pair further. First, we find the prefix decomposition of $X^{s_N(q-1)} (aX^N)^2$ as:

$$\begin{aligned} \mathfrak{R} (X^{s_N(q-1)} (aX^N)^2) &= \mathfrak{R} (X^{s_N(q-1)-1} baaX^N (aX^N)), \\ &= X^{s_N(q-1)-1} \boxed{baaX^N} aX^N, \end{aligned}$$

and hence we find, replacing this head by a , that

$$\mathfrak{A}^{(1)} (X^{s_N(q-1)} (aX^N)^2, a^2Q) = (X^{s_N(q-1)-1} aaX^N, a^2Q). \tag{6}$$

By Lemma 7, we have

$$\begin{aligned} \mathfrak{A}^{((s_N(q-1)-1)(N+1))} (X^{s_N(q-1)-1} aaX^N) &= aaX^{N+(s_N(q-1)-1)N^2} \\ &= aaX^{N^2 s_N(q-1) - N^2 + N} \\ &= aaX^{s_N(q)}. \end{aligned} \tag{7}$$

Now, applying Lemma 5 with $P = X^{s_N(q-1)-1} aaX^N$, we can combine (6) and (7), and thus find:

$$\begin{aligned} \mathfrak{A}^{((s_N(q-1)-1)(N+1)+1)} (X^{s_N(q-1)} (aX^N)^2, a^{2q}Q) &= (aaX^{s_N(q)}, aaQ)_{\text{p-red}} \\ &= (X^{s_N(q)}, Q). \end{aligned} \tag{8}$$

Thus we are almost done by induction; it remains to count the steps performed in transforming $(X^N (aX^N)^{2q}, a^{2q}Q)$ to $(X^{s_N(q)}, Q)$. By the inductive hypothesis, we first have $T_N(q-1)$ steps in transforming the pair $(X^N (aX^N)^{2q}, a^{2q}Q)$ to $(X^{s_N(q-1)} (aX^N)^2, a^2Q)$. The above reasoning shows that an additional

$$(s_N(q-1) - 1)(N+1) + 1$$

steps were subsequently performed. Thus the total number of steps performed was

$$T_N(q-1) + \underbrace{(s_N(q-1) - 1)(N+1) + 1}_{t_N(q)} = T_N(q-1) + t_N(q) = T_N(q),$$

which is what was to be shown. □

Lemma 10. *Let W be an arbitrary word. For all $k \geq 1$ and $N \geq 2$, we have*

$$\mathfrak{A}^{(T_N(k-1)+2k-1)} (aW, V_k) = (X^{s_N(k-1)-1} W, a).$$

Proof. Of course, the prefix decomposition of aW has the distinguished letter a as its head. In particular, we find $\mathfrak{A}(aW) = baaX^N W$, and hence, removing the shared prefix b from $baaX^N W$ and V_k , we find:

$$\mathfrak{A}^{(1)} (aW, V_k) = (\underline{b} \cdot aaX^N W, \underline{b} \cdot b^{2k-2} a^{2k} baa)_{\text{p-red}} = (aaX^N W, b^{2k-2} a^{2k} baa).$$

The head of $aaX^N W$ is the first distinguished a . Hence, continuing iteratively, continuously removing the b 's from the beginning of the second entry of the pair, we eventually find:

$$\begin{aligned}\mathfrak{A}^{(2k-1)}(aW, V_k) &= \left(\underline{baa}X^N \cdot (aX^N)^{2k-2} W, \underline{baaa}^{2k-2} baa \right)_{\text{p-red}} \\ &= \left(X^N (aX^N)^{2k-2} W, a^{2k-2} baa \right)_{\text{p-red}}.\end{aligned}$$

If $k = 1$, then $(X^N (aX^N)^{2k-2} W, a^{2k-2} baa) = (X^N W, baa)$, and as, by definition, $X^N = (ba)^N$, we have that $(X^N W, baa)_{\text{p-red}} = (X^{N-1} W, a)$, as required.

Thus, assume that $k > 1$. By Lemma 9, we have

$$\begin{aligned}\mathfrak{A}^{(T_N(k-1))} \left(X^N (aX^N)^{2k-2}, a^{2k-2} baa \right) &= \left(X^{s_N(k-1)}, baa \right)_{\text{p-red}}, \\ &= \left(X^{s_N(k-1)-1}, a \right).\end{aligned}$$

As the proof of Lemma 9 shows that the prefix decomposition of each of the $T_N(k-1)$ intermediary words in this rewriting has a head, we may perform the above rewriting first when applying \mathfrak{A} to the pair $(X^N (aX^N)^{2k-2} W, a^{2k-2} baa)$. Hence, combining this rewriting with the above $2k-1$ steps, we find

$$\mathfrak{A}^{(T_N(k-1)+2k-1)}(aW, V_k) = \left(X^{s_N(k-1)-1} W, a \right).$$

This is precisely what was to be shown. \square

We are now ready to enact the first part of Adian's algorithm on the pair (U_k, V_k) . It is worth keeping in mind that this part will only affect the first letter a in the word U_k , but will transform all of V_k into a .

Lemma 11. *For every $k \geq 1$ and $N \geq 2$, we have*

$$\mathfrak{A}^{(T_N(k-1)+2k-1)}(U_k, V_k) = \left(X^{s_N(k-1)-1} b^{2k} a^{2k} a, a \right).$$

Proof. This is immediate by Lemma 10, taking $aW = U_k = ab^{2k} a^{2k} a$. \square

Thus we have completed the first part of Adian's algorithm when applied to the pair (U_k, V_k) . Already, this is a large number of steps – note that $T_N(k)$ grows as N^{2k} , so if we could prove (by whatever means) that $U_k = V_k$ in Π_N , then we could conclude just on the basis of this first part that Π_N has at least an exponential Dehn function. We continue with our precise count of the steps.

The second part of Adian's algorithm now consists in proving that, for all $k \geq 1$ and $N \geq 2$, we have that $X^{s_N(k-1)-1} b^{2k} a^{2k} a$ is equal to a in Π_N .

Lemma 12. *For every $p \geq 1$ and $q > 1$ and $N \geq 2$, we have*

$$\mathfrak{A}^{(pN+p+1)} \left(b^{2q-1} X^p a^{2q} \right) = b^{2(q-1)-1} X^{pN^2-N} a^{2(q-1)}.$$

Proof. Note that the word $b^{2q-1} X^p a^{2q}$ is of the form $b^{2q-1} X^p aaQ$ for a word Q . By Lemma 7, we have that $\mathfrak{A}^{(pN+p)}(X^p aa) = aaX^{pN^2}$, and as no word in the corresponding sequence of elementary transformations begins with a except the last, i.e. aaX^{pN^2} , it hence follows from Lemma 6 that

$$\mathfrak{A}^{(pN+p)} \left(b^{2q-1} X^p aa \cdot a^{2q-2} \right) = b^{2q-1} aaX^{pN^2} a^{2q-2}.$$

Consequently, as the prefix decomposition of $b^{2q-1} aaX^{pN^2} a^{2q-2}$ is

$$\mathfrak{A} \left(b^{2q-1} aaX^{pN^2} a^{2q-2} \right) = b^{2q-2} \boxed{baaX^N} X^{pN^2-N} a^{2q-2},$$

we find that

$$\begin{aligned} \mathfrak{A}^{(pN+p+1)}(b^{2q-1} X^p a a \cdot a^{2q-2}) &= b^{2q-2} a X^{pN^2-N} a^{2q-2} \\ &= b^{2(q-1)-1} X^{pN^2-N+1} a^{2(q-1)}. \end{aligned}$$

This is precisely what was to be shown. □

For ease of bookkeeping, we define another three sequences $s'_N, t'_N,$ and T'_N of natural numbers as follows:

$$\begin{aligned} s'_N(n) &= \begin{cases} 1, & \text{if } n = 0, \\ N^2 s'_N(n-1) - N + 1, & \text{if } n > 0. \end{cases} \\ t'_N(n) &= \begin{cases} 0, & \text{if } n = 0, \\ (N+1)s'_N(n-1) + 1, & \text{if } n > 0. \end{cases} \\ T'_N(n) &= \sum_{i=0}^n t'_N(i). \end{aligned}$$

Note that $t'_N(n)$ is defined via a recurrence on $s'_N,$ rather than on $t'_N.$ For example, for $N = 2$ these sequences begin:

$$\begin{aligned} s'_2(n) &: 1, 3, 11, 43, 171, 683, \dots, \\ t'_2(n) &: 0, 4, 10, 34, 130, 514, \dots, \\ T'_2(n) &: 0, 4, 14, 48, 178, 692, \dots \end{aligned}$$

Analogously to Lemma 8, we can easily find closed form expressions for these functions.

Lemma 13. *The sequences $s'_N, t'_N,$ and T'_N admit the following closed forms:*

- (1) $s'_N(n) = \frac{N}{N+1} (N^{2n} + \frac{1}{N})$ for all $n \geq 0.$
- (2) $t'_N(n) = N^{2n} + 2$ for all $n \geq 1.$
- (3) $T'_N(n) = \frac{N}{N^2-1} (N^{2n} - 1) + 2n$ for all $n \geq 0.$

We remark that an immediate consequence of Lemma 8 and Lemma 13 is the relationship

$$s'_N(k) - 1 = N(s_N(k-1) - 1). \tag{9}$$

We shall presently use this. First, however, we will use our new functions $s'_N, t'_N,$ and T'_N to count the number of steps performed by \mathfrak{A} to prove that $b^{2k} a^{2k} a$ is left divisible by $a.$

Lemma 14. *For every $k \geq 1$ and $N \geq 2,$ we have*

$$\mathfrak{A}^{(T'_N(k))}(b^{2k} a^{2k} a) = a X^{s'_N(k)}.$$

Proof. Consider the word $b^{2k} a^{2k} a = b^{2k-1} X^1 a^{2k}.$ We may apply Lemma 12 to this word to find that

$$\begin{aligned} \mathfrak{A}^{(N+2)}(b^{2k-1} X^1 a^{2k}) &= b^{2(k-1)-1} X^{N^2-N+1} a^{2(k-1)} \\ \therefore \mathfrak{A}^{(t'_N(1))}(b^{2k-1} X^1 a^{2k}) &= b^{2(k-1)-1} X^{s'_N(1)} a^{2(k-1)} \end{aligned}$$

Of course, the word $b^{2(k-1)-1} X^{s'_N(1)} a^{2(k-1)}$ is also of the correct form for applying Lemma 12, and we find

$$\mathfrak{A}^{((N+1)s'_N(1)+1)}(b^{2(k-1)-1} X^{s'_N(1)} a^{2(k-1)}) = b^{2(k-2)-1} X^{N^2 s'_N(1)-N+1} a^{2(k-2)}.$$

As $t'_N(2) = (N+1)s'_N(1) + 1$ and $s'_N(2) = N^2 s'_N(1) - N + 1,$ we conclude

$$\mathfrak{A}^{(t'_N(1)+t'_N(2))}(b^{2k} a^{2k} a) = b^{2(k-2)-1} X^{s'_N(2)} a^{2(k-2)}.$$

This word is again of the required form to apply Lemma 12, etc. and hence, continuing iteratively for $k - 1$ steps and using $T'_N(k) = \sum_{i=1}^k t'_N(i)$, we find

$$\mathfrak{A}^{(T'_N(k-1))} (b^{2k} a^{2k} a) = bX^{s'_N(k-1)} a^2. \tag{10}$$

Rewriting $bX^{s'_N(k-1)} a^2$ is easy. Indeed, by Lemma 7 we have

$$\mathfrak{A}^{((N+1)s'_N(k-1))} (bX^{s'_N(k-1)} a^2) = baaX^{N^2 s'_N(k-1)}. \tag{11}$$

Note that $(N + 1)s'_N(k - 1) = t'_N(k) - 1$. Furthermore, we obviously have

$$\mathfrak{A}^{(1)} (baaX^{N^2 s'_N(k-1)}) = aX^{N^2 s'_N(k-1) - N}, \tag{12}$$

and $N^2 s'_N(k - 1) - N = s'_N(k)$. We can now assemble all our rewritings (10), (11), and (12), to find that

$$\mathfrak{A}^{(T'_N(k-1)+t'_N(k)-1+1)} (b^{2k} a^{2k} a) = aX^{s'_N(k)-1}$$

which is to say

$$\mathfrak{A}^{(T'_N(k))} (b^{2k} a^{2k} a) = aX^{s'_N(k)-1}.$$

This is precisely what was to be proved. □

Note that no word, except the last, in the rewriting process described in the proof of Lemma 14 begins with a . In particular, any prefix decomposition of $X^q b^{2k} a^{2k}$ is simply a prefix decomposition of $b^{2k} a^{2k}$ preceded by q prefixes of the form $X | X | \dots | X |$. Therefore, just as in the statement of Lemma 6 (replacing b^s with $(ba)^s = X^s$) that Lemma 14 also describes the rewriting process for $X^q b^{2k} a^{2k}$, for any $q \geq 0$. In particular, taking $q = s_N(k - 1) - 1$, we conclude:

Lemma 15. *For every $k \geq 1$, we have*

$$\mathfrak{A}^{(T'_N(k))} (X^{s_N(k-1)-1} b^{2k} a^{2k} a, a) = (X^{s_N(k-1)-1} aX^{s'_N(k)-1}, a).$$

By (9), the pair of words produced in Lemma 15 is of the form $(X^p aX^{pN}, a)$. We are now almost done, as Adian's algorithm applied to any word $X^p aX^{pN}$ will clearly result in a after p steps. We write out the exact statement and a brief proof.

Lemma 16. *For every $k \geq 1$, we have*

$$\mathfrak{A}^{(s_N(k-1)-1)} (X^{s_N(k-1)-1} aX^{s'_N(k)-1}, a) = (\varepsilon, \varepsilon).$$

Proof. First, note that by (9) we have that the word

$$X^{s_N(k-1)-1} aX^{s'_N(k)-1}$$

is of the form $X^p aX^{pN}$ for $p \geq 0$. For any word of this form, it is easy to see that it is equal to a ; indeed, one may with little difficulty write down the sequence of transformations carried out by \mathfrak{A} directly. One may also note that the rewriting system $XaX^N \rightarrow a$ will rewrite any word $X^p aX^{pN}$ to a in p steps, and that the resulting sequence of elementary transformations is right directed – indeed, there are no independent transformations (cf. [2] for this terminology). Hence, by Proposition 4, this sequence must be the one produced by \mathfrak{A} , so $\mathfrak{A}^{(p)}(X^p aX^{pN}, a) = (\varepsilon, \varepsilon)$, as desired. □

This completes the description of the second part of the action of \mathfrak{A} when applied to the pair (U_k, V_k) . For brevity, let

$$\sigma_N(k) = \underbrace{T_N(k-1) + (2k-1)}_{\text{Lemma 11}} + \underbrace{T'_N(k)}_{\text{Lemma 15}} + \underbrace{(s_N(k-1)-1)}_{\text{Lemma 16}}. \tag{13}$$

Then $\sigma_N(k)$ is the total number of steps taken by \mathfrak{A} to rewrite the pair (U_k, V_k) into $(\varepsilon, \varepsilon)$, as it is simply the sum of the number of steps in the indicated lemmas; explicitly, we have the following:

Proposition 17. *For every $N \geq 2$ and $k \geq 1$, we have*

$$\mathfrak{A}^{(\sigma_N(k))}(U_k, V_k) = (\varepsilon, \varepsilon). \tag{14}$$

Hence, the shortest sequence of elementary transformations verifying the identity $U_k = V_k$ in Π_N has length $\sigma_N(k)$.

Proof. First, the equality (14) follows by first performing the rewriting from Lemma 11, followed by the one in Lemma 15, followed finally by the one in Lemma 16. The second part of the proposition now follows from the first by Proposition 4. \square

We give a closed form expression for $\sigma_N(k)$.

Lemma 18. *For every $N \geq 1$ and $k \geq 1$, we have*

$$\sigma_N(k) = \frac{2N}{N^2 - 1} (N^{2k} - 1) + 4k - 2.$$

In particular, we have $\sigma_N(k) \sim N^{2k}$.

Proof. This follows immediately from the definition (13), the closed form expressions for $T_N(k-1)$ and $s_N(k-1)$ from Lemma 8, the closed form expression for $T'_N(k)$ from Lemma 13, and elementary algebraic manipulations. \square

By Lemma 18, notice that for fixed N , we have

$$\sigma_N(k) = 2 \left(2k + 1 + \sum_{i=1}^k N^{2i} \right).$$

For example, for a fixed N we have that $\sigma_N(k)$ for $k = 1, 2, \dots$ begins:

$$\sigma_N(k): 2(N + 1), 2(N^3 + N + 3), 2(N^5 + N^3 + N + 5), \dots$$

This is a particularly simple expression for $\sigma_N(k)$. As an example, when $N = 2$, we have the following values for $k = 1, 2, \dots$:

$$\sigma_2(k): 6, 26, 94, 354, 1382, 5482, 21870, \dots$$

In summary, for example taking $k = 4$ and $N = 2$, \mathfrak{A} will terminate on the pair

$$(U_4, V_4) = (ab^8a^8a, b^7a^8baa),$$

requiring a total of 354 steps to do so. Similarly (and somewhat strikingly), if one instead takes $N = 4$, then \mathfrak{A} will take 34966 steps to prove that $U_4 = V_4$ in Π_4 .

The statement of the Main Lemma is now obtained by combining Proposition 17 and Lemma 18. This completes the proof of the Main Lemma. \square

3. Some remarks on Π_N

We make some general remarks on the monoids Π_N . First, we note that it is very tempting to conjecture that the Dehn function of Π_N is exponential, and not just bounded below by an exponential function. Proving this, however, seems somewhat intricate. Baumslag–Solitar groups $BS(k, \ell)$ with $|k| \neq |\ell|$ are well-known to have exponential Dehn function; this is proved in two steps. First, Gersten [14, Theorem B] gave a series of null-homotopic words whose van Kampen diagrams require a very large number of cells to fill. Thus the Dehn function is at least exponential. Second, one uses the fact that such Baumslag–Solitar groups are asynchronously automatic [5, Corollary E1] and any group with this property has at most exponential Dehn function, see [13]. We have, in essence (using word transformations rather than diagrams), effected the first step for our “Baumslag–Solitar”-esque monoids Π_N . However, the second seems

more elusive, as it is not clear that the Π_N are automatic (see below), nor does this take into account the fact that automaticity is a less powerful property for semigroups than groups. We will, at least, prove that the Dehn function of Π_N is always recursive.

Note, first, that the *group* defined by the same presentation as Π_N is easily recognised as one of the famous characters of combinatorial group theory:

$$\begin{aligned} \text{Gp} \langle a, b \mid baa(ba)^N = a \rangle &= \text{Gp} \langle a, b \mid baa(ba)^{N-1}b = 1 \rangle \\ &\cong \text{Gp} \langle a, b \mid bab^{N-1}ba^{-1} = 1 \rangle \\ &= \text{Gp} \langle a, b \mid a^{-1}ba = b^{-N} \rangle = \text{BS}(1, -N), \end{aligned}$$

a metabelian Baumslag–Solitar group, where the indicated isomorphism comes from applying the free group automorphism induced by $a \mapsto a$ and $b \mapsto ba^{-1}$. All metabelian Baumslag–Solitar groups are residually finite, and hence have decidable word problem, providing an alternative route to using Magnus' theorem in this case. It may therefore be tempting to conjecture that Π_N is also residually finite for every N . This, however, is not at all the case. In general, it is an open problem to classify which one-relation monoids are residually finite; however, in the monadic case $\text{Mon}\langle a, b \mid bUa = a \rangle$, a full classification due to Bouwsma exists, but seems relatively unknown (e.g. it is not included in the reference list of [25]).

Theorem (Bouwsma, 1993). *The monoid defined by $\text{Mon}\langle a, b \mid bUa = a \rangle$ is residually finite if and only if $U = b^k$ for some $k \geq 0$.*

That is, the only residually finite 2-generated monadic one-relation monoids are those of the form $\text{Mon}\langle a, b \mid b^k a = a \rangle$. The result was never published, except in Bouwsma's 1993 Ph.D. thesis [8, Corollary 2.5] (supervised by G. Lallement). From the above, we immediately conclude that Π_N is *not* residually finite for any N . We must therefore turn to an alternative approach to solving the word problem in Π_N . To do this, we turn to a remarkable result by Guba [18] and the decidability of the rational subset membership problem in the metabelian Baumslag–Solitar groups $\text{BS}(1, N)$. We refer the reader to the survey [22] for details and definitions regarding the rational subset membership problem in groups.

Theorem 19. *For every $N \geq 2$, the word problem in Π_N is decidable. In particular, the Dehn function of Π_N is recursive.*

Proof. In proving this, we will defer to an article and method by Guba [18, Theorem 2.1], and refer the reader to this article for an introduction to the notation, which is rather cumbersome to define succinctly here. The core idea of the proof is that the word problem for any monadic one-relation monoid $\text{Mon}\langle a, b \mid bUa = a \rangle$ can be reduced to the membership problem in a fixed submonoid of some one-relator group $G = \text{Gp}\langle B \mid w = 1 \rangle$, where Guba gives a procedure to effectively compute B and w from bUa . We will use this procedure to show that, in the case of Π_N , the group G is a solvable Baumslag–Solitar group, in which the submonoid membership problem is decidable. We now give the details.

The submonoid of Π_N generated by the suffixes of the defining word, i.e. the *monoid of ends*, is denoted $S(\Pi_N)$. It is clear that this is generated by a and ba . It follows immediately from the proof of [18, Corollary 3.1] that

$$S(\Pi_N) \cong \text{Mon} \langle x, y \mid yxy^N = x \rangle$$

with the isomorphism $x \mapsto a$ and $y \mapsto ba$. This is a cycle-free presentation, so $S(\Pi_N)$ embeds in the one-relator group with the same presentation via the identity map, which is obviously $\text{BS}(1, -N)$. In fact, to see this embedding is very simple, as every suffix of $baa(ba)^N$ is left divisible by ba . To see this, it suffices to show that a is left divisible by ba , as every suffix of $baa(ba)^N$

begins either with ba or with a . But $ba \cdot a(ba)^N = a$, so obviously this holds. Hence, the graph of ends of Π_N has only a single component (cf. [18, p. 1145]), and hence $\overline{G}(\Pi_N) = \text{BS}(1, -N)$.

The word problem for Π_N reduces to its left divisibility problem. By Oganessian’s result [26, Theorem 1], the left divisibility problem in Π_N reduces to the left divisibility problem in $S(\Pi_N)$. The left divisibility problem in $S(\Pi_N)$ can be reduced to the submonoid membership problem in $\overline{G}(\Pi_N) = \text{BS}(1, -N)$, see [18, Corollary 2.1] for details. But the submonoid membership problem, indeed the rational subset membership problem, is decidable for any $\text{BS}(1, N)$ with $N \geq 2$ by [9, Theorem 3.3]. It is well-known that $\text{BS}(1, N)$ and $\text{BS}(1, -N)$ are commensurable (see e.g. [12, Lemma 6.1]), and as decidability of the rational subset membership problem is inherited by taking subgroups (obviously) and by taking finite extensions (by Grunschlag [16]), we conclude that the rational subset membership problem, and hence also the submonoid membership problem, is decidable in $\text{BS}(1, -N)$. This solves the word problem in Π_N . \square

Remark 20. The non-Russian-reading reader interested in Oganessian’s remarkable work on the connection between left cycle-free monoids Π and their associated semigroup of ends $S(\Pi)$ may first be inclined to consult the English translation of [26]. Unfortunately, this translation is rather poor, and can make for confusing reading.³ Instead, we advise the reader to first consult Guba’s overview of Oganessian’s work in the case of a single relation, found in [18].

Remark 21. One can prove, using automata-theoretic methods, that \mathfrak{A} in fact always terminates for Π_N whenever $N \geq 1$, see [8, Theorem 4.3]. This provides an alternative proof of Theorem 19, but as the Ph.D. thesis [8] is not easily accessible, we have opted for the above proof. Note that as \mathfrak{A} always terminates, it follows, using an encoding due to Guba (see [25, § 6.4] for details) that the Collatz-like function $f_N: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ defined by:

$$f_N(m, n) = \begin{cases} \left(\lfloor \frac{m}{2} \rfloor, \lfloor \frac{n}{2} \rfloor \right) & \text{if } m \equiv n \pmod{2}, \\ \left(\frac{m}{2}, 2^{2N+1}n + \frac{1}{3}(2^{2N+1} + 1) \right) & \text{if } m \neq n \text{ and } m \equiv 0 \pmod{2}, \\ (n, m) & \text{if } m \neq n \text{ and } m \equiv 1 \pmod{2}. \end{cases}$$

always terminates for any input pair $(m, n) \in \mathbb{N} \times \mathbb{N}$ and any $N \geq 2$, where termination is meant in the sense that the sequence

$$(m, n) \rightarrow f_N(m, n) \rightarrow f_N^2(m, n) \rightarrow \dots$$

eventually results in $f_N^\ell(m, n) = (0, k)$ or $(k, 0)$ for some $k, \ell \in \mathbb{N}$.

3.1. Superexponential Dehn functions

It would be interesting to see how quickly the Dehn function of a one-relator monoid can grow, even if exhibiting a non-recursive growth currently seems somewhat out of reach. A good starting point seems to be the following:

Question 22. *Does there exist a one-relation monoid $\text{Mon}\langle a, b \mid bUa = a \rangle$ whose Dehn function is not bounded above by any finite tower of exponentials?*

The exponential growth found as a lower bound for the Dehn function of Π_N in this article is, of course, connected to the exponential Dehn function of the Baumslag–Solitar group $\text{BS}(1, -N)$. One way of resolving Question 22 would be connected with the following well-known result. Gersten [14] proved that the one-relator group

$$\text{BG} = \text{Gp} \langle a, b \mid [a, bab^{-1}] = a^{-1} \rangle$$

³For two brief examples, on p. 89 (of the translation), the system (2) is said to have “no cycles” instead of the correct “no left cycles”; on p. 92, one reads “it is impossible to find out whether X is divisible by d ”, but it should read “it is possible”. Further examples are not hard to find.

introduced by Baumslag [6], has a Dehn function which is not bounded above by any finite tower of exponentials. This group, however, is not a positive one-relator group, as it is easily observed to not be residually solvable (indeed, it is clear that a lies in every term of the derived series), but every positive one-relator group is residually solvable [7]. We therefore pose the following, purely group-theoretic, question:

Question 23. *Does there exist a positive one-relator group whose Dehn function is not bounded above by any finite tower of exponentials?*

While a positive answer to Question (23) would not have a direct implication for Question 22 (or vice versa), it would seem to have a strong indication towards a positive answer.

3.2. Finite complete rewriting systems and automaticity

In [11], Cain & Maltcev claimed that every one-relation monoid with a presentation of the form

$$\text{Mon} \langle a, b \mid b^\alpha a^\beta b^\gamma a^\delta b^\epsilon a^\rho = a \rangle,$$

i.e. a monadic one-relation monoid with defining relation $bUa = a$ in which bUa has relative length 6, admits a finite complete rewriting system. This claim is repeated (by the author of the present article) in [25, p. 339]. Cain & Maltcev further claim that using these rewriting systems, one may observe that every such monoid has at most quadratic Dehn function. By the results in this present article, this cannot, however, be correct; taking $N = 2$, the monoid Π_2 is defined by

$$\Pi_2 = \text{Mon} \langle a, b \mid baababa = a \rangle,$$

but by Theorem 1 its Dehn function is at least exponential. The source of the error is that their claimed finite complete rewriting system for Π_2 is not complete. This leads us to pose the following question.

Question 24. *Does Π_N admit a finite complete rewriting system for all $N \geq 2$?*

Of course, an affirmative answer to Question 24 would give an alternative proof of decidability of the word problem in Π_N (i.e. Theorem 19). Finally, we note a connection with automaticity and the fellow traveller property, and ask the following natural question (we refer the reader to [19] for definitions and more details):

Question 25. *Are the monoids Π_N (bi)automatic?*

By [30, Theorem 4.1], any left cancellative automatic monoid whose automatic structure satisfies the fellow traveller property has an at most quadratic Dehn function. An affirmative answer to Question 25 would thus, in view of Theorem 1, give a rather simple family of left cancellative automatic monoids without the fellow traveller property.

Remark 26. We wish to make a final remark regarding a well-known result due to Ivanov, Margolis & Meakin [20]. This asserts (as a special case) that the word problem for any monoid $\text{Mon} \langle a, b \mid bUa = a \rangle$ reduces to the word problem for the special one-relation inverse monoid $\text{Inv} \langle a, b \mid a^{-1}bUa = 1 \rangle$. In particular, the word problem for Π_N reduces to the word problem for $I_N = \text{Inv} \langle a, b \mid a^{-1}baa(ba)^N = 1 \rangle$. Based on the results above, we conjecture that the Dehn function for I_N is also (at least) exponential, and indeed that the word problem for I_N is decidable.

Acknowledgments

I wish to express my sincere gratitude to Janet Hughes (Penn. State Univ.) for her reference services, and to Alan Cain (Univ. Nova de Lisboa) for useful discussions pertaining to [10, 11].

Declaration of interests

The authors do not work for, advise, own shares in, or receive funds from any organization that could benefit from this article, and have declared no affiliations other than their research organizations.

References

- [1] S. I. Adian, *Defining relations and algorithmic problems for groups and semigroups*, American Mathematical Society, 1966. Translated from the Russian by M. Greendlinger.
- [2] S. I. Adian, “Word transformations in a semigroup that is given by a system of defining relations”, *Algebra Logic* **15** (1976), pp. 379–386. [*Algebra i Logika* **15**, 6 (1976)].
- [3] S. I. Adian and G. U. Oganessian, “On the word and divisibility problems in semigroups with a single defining relation”, *Math. USSR, Izv.* **12** (1978), pp. 207–212. [*Izv. Akad. Nauk SSSR Ser. Mat.* **42**, 2 (1978)].
- [4] S. I. Adian and G. U. Oganessian, “On the word and divisibility problems for semigroups with one relation”, *Math. Notes* **41** (1987), pp. 235–240. [*Mat. Zametki* **41**, 3 (1987)].
- [5] G. Baumslag, S. M. Gersten, M. Shapiro and H. Short, “Automatic groups and amalgams”, *J. Pure Appl. Algebra* **76** (1991), no. 3, pp. 229–316.
- [6] G. Baumslag, “A non-cyclic one-relator group all of whose finite quotients are cyclic”, *J. Aust. Math. Soc.* **10** (1969), pp. 497–498.
- [7] G. Baumslag, “Positive one-relator groups”, *Trans. Am. Math. Soc.* **156** (1971), pp. 165–183.
- [8] J. B. Bouwsma, *Semigroups presented by a single relation*, PhD thesis, Pennsylvania State University, USA, 1993.
- [9] M. Cadilhac, D. Chistikov and G. Zetsche, “Rational subsets of Baumslag-Solitar groups”, in *47th International Colloquium on Automata, Languages, and Programming*, Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2020.
- [10] A. Cain and V. Maltcev, “Monoids $\text{Mon}\langle a, b : a^\alpha b^\beta a^\gamma b^\delta = b \rangle$ admit finite complete rewriting systems”, 2013. <https://arxiv.org/abs/1302.0982>.
- [11] A. Cain and V. Maltcev, “Monoids $\text{Mon}\langle a, b : a^\alpha b^\beta a^\gamma b^\delta a^\epsilon b^\varphi = b \rangle$ admit finite complete rewriting systems”, 2013. <https://arxiv.org/abs/1302.2819v1>.
- [12] M. Casals-Ruiz, I. Kazachkov and A. Zakharov, “Commensurability of Baumslag-Solitar groups”, *Indiana Univ. Math. J.* **70** (2021), no. 6, pp. 2527–2555.
- [13] D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson and W. P. Thurston, *Word processing in groups*, Jones and Bartlett Publishers, Boston, 1992.
- [14] S. M. Gersten, “Dehn functions and l_1 -norms of finite presentations”, in *Algorithms and classification in combinatorial group theory (Berkeley, CA, 1989)*, Springer, 1992, pp. 195–224.
- [15] R. D. Gray and B. Steinberg, “A Lyndon’s identity theorem for one-relator monoids”, *Sel. Math., New Ser.* **28** (2022), no. 3, article no. 59.
- [16] Z. Grunschlag, *Algorithms in geometric group theory*, PhD thesis, 1999, p. 127. University of California, Berkeley, USA.
- [17] V. S. Guba, “Conditions for the embeddability of semigroups into groups”, *Mat. Zametki* **56** (1994), no. 2, pp. 3–14.
- [18] V. S. Guba, “On a relation between the word problem and the word divisibility problem for semigroups with one defining relation”, *Izv. Math.* **61** (1997), no. 6, pp. 1137–1169. [*Izv. Ross. Akad. Nauk Ser. Mat.* **61**, 6 (1997)].
- [19] M. Hoffmann and R. M. Thomas, “A geometric characterization of automatic semigroups”, *Theor. Comput. Sci.* **369** (2006), no. 1-3, pp. 300–313.

- [20] S. V. Ivanov, S. W. Margolis and J. C. Meakin, “On one-relator inverse monoids and one-relator groups”, *J. Pure Appl. Algebra* **159** (2001), no. 1, pp. 83–111.
- [21] Y. Kobayashi, “Finite homotopy bases of one-relator monoids”, *J. Algebra* **229** (2000), no. 2, pp. 547–569.
- [22] M. Lohrey, “The rational subset membership problem for groups: a survey”, in *Groups St Andrews 2013*, Cambridge University Press, 2015, pp. 368–389.
- [23] W. Magnus, “Das Identitätsproblem für Gruppen mit einer definierenden Relation”, *Math. Ann.* **106** (1932), no. 1, pp. 295–307.
- [24] W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory: Presentations of groups in terms of generators and relations*, Interscience Publishers [John Wiley & Sons], New York-London-Sydney, 1966.
- [25] C.-F. Nyberg-Brodde, “The word problem for one-relation monoids: a survey”, *Semigroup Forum* **103** (2021), no. 2, pp. 297–355.
- [26] G. U. Oganessian, “Semigroups with one relation and semigroups without cycles”, *Math. USSR, Izv.* **20** (1983), pp. 89–95. [*Izv. Akad. Nauk SSSR Ser. Mat.* **46** (1982)].
- [27] G. U. Oganessian, “The isomorphism problem for semigroups with one defining relation”, *Math. Notes* **35** (1984), pp. 360–363. [*Mat. Zametki* **35**, 5 (1984)].
- [28] N. Ruškuc, *Semigroup Presentations*, PhD thesis, University of St Andrews, 1995.
- [29] A. Thue, “Probleme über Veränderungen von Zeichenreihennach gegebenen Regeln”, *Christiana Videnskabs-Selskabs Skrifter* **10** (1914).
- [30] X. Wang, W. Xie and H. Lin, “Finiteness and Dehn functions of automatic monoids having directed fellow traveller property”, *Semigroup Forum* **79** (2009), no. 1, pp. 15–21.