HAL
open science

On the existence of free subsemigroups in reversible automata semigroups

Dominik Francoeur, Ivan Mitrofanov

▶ **To cite this version:**

Dominik Francoeur, Ivan Mitrofanov. On the existence of free subsemigroups in reversible automata semigroups. Groups, Geometry, and Dynamics, 2021, 15 (3), pp.1103-1132. 10.4171/GGD/626 . hal-03964303

HAL Id: hal-03964303

https://hal.science/hal-03964303v1

Submitted on 31 Jan 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Groups Geom. Dyn. 15 (2021), 1103–1132
DOI 10.4171/GGD/626
© 2021 European Mathematical Society
Published by EMS Press
This work is licensed under a CC BY 4.0 license.

On the existence of free subsemigroups in reversible automata semigroups

Dominik Francoeur[1] and Ivan Mitrofanov[2]

Abstract. We prove that the semigroup generated by a reversible Mealy automaton contains a free subsemigroup of rank two if and only if it contains an element of infinite order.

Mathematics Subject Classification (2020). 20M35.

Keywords. automata groups, automata semigroups, free semigroups, word growth.

1. Introduction

Groups and semigroups defined by Mealy automata have attracted considerable attention since their introduction. One of the reasons for this interest is that the apparent simplicity of their definition belies the complex behaviours that they can exhibit. Indeed, among them, one can find infinite finitely generated torsion groups [7], groups and semigroups of intermediate growth and amenable but not elementary amenable groups [8].

It is natural to ask how the properties of a Mealy automaton can influence the algebraic behaviour of the group or semigroup that it generates. In this paper, we investigate the existence of free subsemigroups of rank two in semigroups generated by a reversible Mealy automaton. More precisely, we prove the following theorem.

Theorem 1.1. *Let $\mathcal{M}$ be a reversible Mealy automaton and let $P_{\mathcal{M}}$ be the semigroup generated by $\mathcal{M}$. Then, $P_{\mathcal{M}}$ contains a nonabelian free subsemigroup if and only if $P_{\mathcal{M}}$ contains an element of infinite order.*

As a corollary of Theorem 1.1, we obtain a generalization of a result of Klimann [10], who proved that a group generated by a bireversible automaton is of exponential growth as soon as it contains an element of infinite order.

[1] Dominik Francoeur was supported by a Doc.Mobility grant from the Swiss National Science Foundation.

[2] Ivan Mitrofanov was supported by the "@raction" grant ANR-14-ACHN-0018-01.

Corollary 1.2. *If G is a group generated by an invertible and reversible Mealy automaton, then G is of exponential growth as soon as it contains an element of infinite order. In particular, no infinite virtually nilpotent group can be generated by an invertible and reversible Mealy automaton.*

Organisation of the paper. In Section 2, we define Mealy automata and their duals, as well as several semigroups associated with them. We use the notion of Zappa–Szép product of semigroups to help us describe these different semigroups in a uniform fashion.

The proof of Theorem 1.1 relies on the interplay between the semigroup generated by a reversible automaton and the group generated by its dual automaton. We investigate this connection in Section 3. More precisely, given a reversible Mealy automaton $\mathcal{M}$ and a word u in the set of states of $\mathcal{M}$, we show in Lemma 3.4 that the orbits of the powers of u under the action of the group generated by the dual of $\mathcal{M}$ form a regular language. Furthermore, in Lemma 3.6, we show that u represents an element of infinite order in the semigroup generated by $\mathcal{M}$ if and only if this language is not uniformly bounded.

In Section 4, we use this regular language in the case where it is not uniformly bounded to find a free subsemigroup of rank two in the semigroup generated by a reversible automaton, thus proving Theorem 1.1.

In Section 5, we investigate in more details the orbits of automata groups and semigroups. We first study potential generalizations of Lemma 3.4. We show that if we consider a preperiodic sequence instead of periodic one, a non-reversible Mealy automaton instead of a reversible one, or a subgroup instead the whole group, then the language thus obtained might not be regular. However, for bi-reversible automata, we prove that Lemma 3.4 hold even if we consider preperiodic sequences instead of periodic ones.

We also study the existence of infinite orbits of periodic sequences. We show that there exists an automaton group containing an infinite subgroup such that the orbit of every periodic sequence under the action of this subgroup is finite. However, at the moment, we do not know whether there exists an infinite automaton group such that every periodic sequence has a finite orbit. We discuss what is known about this question in Section 6.

Acknowledgements. The authors would like thank Laurent Bartholdi for suggesting this problem and for many useful discussions.

2. Preliminaries

In this section, we will review some facts about Mealy automata and the semigroups or groups that they generate.

2.1. Alphabets, words and sequences. Let A be a finite set. We will denote by A^* the free monoid on A. In other words, A^* is the set of words in the alphabet A, including the empty word ϵ, equipped with the operation of concatenation. In what follows, we will make no distinction in our notation between the free monoid A^* and its underlying set of words.

We will denote by A^ω the set of right-infinite words in the alphabet A. Thus, elements of A^ω are functions from $\mathbb{N}$ to A. We will call such element *sequences*. There is a well-defined operation of concatenation on the left between an element $u \in A^*$ and an element $\xi \in A^\omega$, whose result is an element of A^ω that we will denote simply by $u\xi \in A^\omega$.

Given some $u = u_0u_1 \dots u_n \in A^*$, we will denote by $u^\omega \in A^\omega$ the sequence

$$u^\omega = u_0u_1 \dots u_nu_0u_1 \dots u_n \dots .$$

For $u = u_0u_1 \dots u_n \in A^*$, we call a *prefix* of u any word of the form $v = u_0u_1 \dots u_m$ with $m \leq n$ and a *subword* of u any word of the form $w = u_iu_{i+1} \dots u_{i+j}$ with $1 \leq i \leq i + j \leq n$. In a similar fashion, we define the notions of prefix, subword and subsequences of elements of A^ω.

2.2. Mealy automata

Definition 2.1. A *Mealy automaton* is a tuple $\mathcal{M} = (Q, A, \tau)$, where Q and A are finite sets called respectively the *set of states* and the *alphabet*, and $\tau\colon Q \times A \to A \times Q$ is a map called the *transition map*.

Please note that we will sometimes omit the word "Mealy", but unless otherwise specified, in the rest of this text, by "automaton" we will mean "Mealy automaton."

Notation. Let $\mathcal{M} = (Q, A, \tau)$ be a Mealy automaton. For $q \in Q$ and $a \in A$, we will write $\tau(q, a) = (q \cdot a, q@a)$.

A Mealy automaton $\mathcal{M} = (Q, A, \tau)$ can be represented by a labelled directed graph called its *Moore diagram* (see Figure 1 for an example). The set of vertices of this graph is Q, and there is an edge from $p \in Q$ to $q \in Q$ labelled by $a|b$ if and only if there exists $a, b \in A$ such that $\tau(p, a) = (b, q)$.

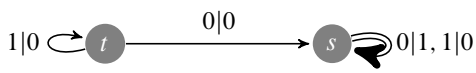

Figure 1. The Moore diagram of a Mealy automaton.

Given an automaton $\mathcal{M}$ and a state $q \in Q$, we can define a map $q\cdot\colon A \to A$ by $(q\cdot)(a) = q \cdot a$ for all $a \in A$. Likewise, for each letter $a \in A$, we can define a map $@a\colon Q \to Q$.

Definition 2.2. A Mealy automaton $\mathcal{M} = (Q, A, \tau)$ is said to be *invertible* if for all $q \in Q$, the map $q\cdot\colon A \to A$ is a bijection. It is said to be *reversible* if for all $a \in A$, the map $@a\colon Q \to Q$ is a bijection. Finally, it is said to be *bi-reversible* if it is invertible, reversible and the map τ is a bijection.

Example 2.3. The automaton given by

$$\mathcal{M} = (\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \tau(q, a) = (q + a, q + a))$$

is invertible, reversible, but not bi-reversible.

The definition of a Mealy automaton is symmetric with respects to the set Q and A. Thus, we can interchange them to obtain a new automaton called the *dual automaton*.

Definition 2.4. Let $\mathcal{M} = (Q, A, \tau)$ be a Mealy automaton. The *dual* of $\mathcal{M}$ is the automaton $\partial\mathcal{M} = (A, Q, \tau')$, where $\tau'\colon A \times Q \to Q \times A$ is given by $\tau'(a, q) = (q@a, q \cdot a)$.

Remark 2.5. Let $\mathcal{M}$ be a Mealy automaton. Then, $\partial(\partial\mathcal{M}) = \mathcal{M}$. Furthermore, $\mathcal{M}$ is reversible if and only if $\partial\mathcal{M}$ is invertible.

2.3. Zappa–Szép product of monoids

Definition 2.6. Let S be a monoid and let X and Y be submonoids of S such that any $s \in S$ can be written in a unique way as $s = xy$ with $x \in X$ and $y \in Y$. Then, S is said to be an *internal Zappa–Szép product* of X and Y, and we write $S = X \bowtie Y$.

If $S = X \bowtie Y$, then for any $x \in X$, $y = Y$ we must have unique elements $x' \in X$, $y' \in Y$ so that $yx = x'y'$. So, we have two functions $Y \times X \to X$, $(y, x) \mapsto y \cdot x$ and $Y \times X \to Y$, $(y, x) \mapsto y@x$.

In $X \bowtie Y$ it is easy to prove properties of $\cdot$ and $@$:

(1) $y_1y_2 \cdot x = y_1 \cdot (y_2 \cdot x)$ for any $y_1, y_2 \in Y$ and $x \in X$;

(2) $y@x_1x_2 = (y@x_1)@x_2$ for any $y \in Y$ and $x_1, x_2 \in X$;

(3) $y \cdot x_1x_2 = (y \cdot x_1)(y@x_1) \cdot x_2$ for any $y \in Y$ and $x_1, x_2 \in X$;

(4) $y_1y_2@x = y_1@(y_2 \cdot x)y_2@x$ for any $y_1, y_2 \in Y$ and $x \in X$.

On the other hand, given two semigroups X and Y with maps $Y \times X \to X$ and $Y \times X \to Y$ which satisfy properties (1)–(4), we can construct their Zappa–Szép product [14].

The property (1) means that $\cdot$ is a left action of Y on X, the property (2) means that $@$ is a right action of X on Y.

The actions of X on Y and of Y on X are not necessarily faithful. We define equivalence relations $\overset{@}{\sim}$ on X and $\dot{\sim}$ on Y as follows:

$$\text{for } x_1, x_2 \in X, \quad x_1 \overset{@}{\sim} x_2 \text{ if and only if } y@x_1 = y@x_2 \text{ for all } y \in Y;$$
$$\text{for } y_1, y_2 \in Y, \quad y_1 \dot{\sim} y_2 \text{ if and only if } y_1 \cdot x = y_2 \cdot x \text{ for all } x \in X.$$

It's clear that $\dot{\sim}$ and $\overset{@}{\sim}$ are congruence relations. Therefore, we can construct new monoids $X/\overset{@}{\sim}$ and $Y/\dot{\sim}$. We denote the actions of $X/\overset{@}{\sim}$ on Y and of $Y/\dot{\sim}$ on X by the same symbols @ and $\cdot$. For $x \in X$, we denote its congruence class by $[x]_{\overset{@}{\sim}} \in X/\overset{@}{\sim}$ and similarly, for $y \in Y$, we denote its congruence class by $[y]_{\dot{\sim}} \in Y/\dot{\sim}$.

In general the action of X on Y does not preserve congruence classes (see Example 2.20), but we can prove something for semigroups with cancellation properties.

Lemma 2.7. *Consider $S = X \bowtie Y$ and let Y have the right cancellation property. Suppose that $x_1, x_2 \in X$ and $x_1 \overset{@}{\sim} x_2$. Then, for any $y \in Y$ we have $y \cdot x_1 \overset{@}{\sim} y \cdot x_2$.*

Proof. We want to show that $s@(y \cdot x_1) = s@(y \cdot x_2)$ for any $s \in Y$. We know that $sy@x_1 = sy@x_2$. Hence,

$$s@(y \cdot x_1)y@x_1 = sy@x_1 = sy@x_2 = s@(y \cdot x_2)y@x_2;$$

Since $y@x_1 = y@x_2$ and Y has the right cancellation property, we conclude that $s@(y \cdot x_1) = s@(y \cdot x_2)$. □

The proof of the next lemma is similar:

Lemma 2.8. *Consider $S = X \bowtie Y$ and let Y have the left cancellation property. Suppose that $y_1, y_2 \in Y$ and $y_1 \dot{\sim} y_2$. Then, for any $x \in X$ we have $y_1@x \dot{\sim} y_2@x$.*

If the action @ preserves congruence classes of Y, we denote the action of X on $Y/\dot{\sim}$ by the same symbol @.

Proposition 2.9. *Consider $S = X \bowtie Y$ and let the right action of X preserve $\dot{\sim}$-congruence classes on Y. Let $\overset{Y}{\sim}$ be the relation on S defined by $s_1 \overset{Y}{\sim} s_2$ if $s_1 = xy_1$, $s_2 = xy_2$, and $y_1 \dot{\sim} y_2$, where $x \in X$ and $y_i \in Y$. Then $\overset{Y}{\sim}$ is a congruence relation and $S/\overset{Y}{\sim} \cong X \bowtie (Y/\dot{\sim})$.*

Proof. It is clear from the fact that $\dot{\sim}$ is an equivalence relations that $\overset{Y}{\sim}$ is an equivalence relation. It remains to show that for all $s_1, s_2, s_3 \in S$, if $s_1 \overset{Y}{\sim} s_2$, then $s_3 s_1 \overset{Y}{\sim} s_3 s_2$ and $s_1 s_3 \overset{Y}{\sim} s_2 s_3$. Let $x, x_3 \in X$ and $y_1, y_2, y_3 \in Y$ be such that $s_1 = xy_1$, $s_2 = xy_2$, and $s_3 = x_3 y_3$, and let us suppose that $y_1 \dot{\sim} y_2$. We have

$$s_3 s_1 = x_3 y_3 x y_1 = x_3 (y_3 \cdot x)(y_3 @ x) y_1;$$
$$s_3 s_2 = x_3 y_3 x y_2 = x_3 (y_3 \cdot x)(y_3 @ x) y_2;$$

and $(y_3 @ x) y_1 \dot{\sim} (y_3 @ x) y_2$.

We also have

$$s_1 s_3 = x y_1 x_3 y_3 = x (y_1 \cdot x_3)(y_1 @ x_3) y_3;$$
$$s_2 s_3 = x y_2 x_3 y_3 = x (y_2 \cdot x_3)(y_2 @ x_3) y_3;$$

$y_1 \cdot x_3 = y_2 \cdot x_3$ and (since the action @ preserves congruence classes) $y_1 @ x_3 \dot{\sim} y_2 @ x_3$.

Any element $s \in S/\overset{Y}{\sim}$ can be represented as $s = xy$ in a unique way, where $x \in X$, $y \in Y/\dot{\sim}$. □

Similarly, we have:

Proposition 2.10. *Consider $S = X \bowtie Y$ and let the left action of Y preserve $\overset{@}{\sim}$-congruence classes on X. Let $\overset{X}{\sim}$ be the relation on S defined by $s_1 \overset{X}{\sim} s_2$ if $s_1 = x_1 y$, $s_2 = x_2 y$ and $x_1 \overset{@}{\sim} x_2$, where $x_i \in X$ and $y \in Y$. Then, $\overset{X}{\sim}$ is a congruence relation, and $S/\overset{X}{\sim} \cong (X/\overset{@}{\sim}) \bowtie Y$.*

2.4. Monoids associated with Mealy automata

Definition 2.11. Let $\mathcal{M} = (Q, A, \tau)$ be a Mealy automaton. We will denote by $\Delta_{\mathcal{M}}$ the semigroup defined by the following presentation:

$$\Delta_{\mathcal{M}} = \langle Q, A \mid qa = (q \cdot a)(q @ a) \rangle.$$

Remark 2.12. As is readily seen from the presentation, the map $\alpha \colon \Delta_{\mathcal{M}} \to \Delta_{\partial\mathcal{M}}$ defined by $\alpha(x_1 x_2 \ldots x_n) = x_n \ldots x_2 x_1$ for $x_1, x_2, \ldots, x_n \in Q \cup A$ is a well-defined anti-isomorphism. Thus, $\Delta_{\mathcal{M}}$ and $\Delta_{\partial\mathcal{M}}$ might not be isomorphic in general, but they are anti-isomorphic.

Proposition 2.13. *Let $\mathcal{M} = (Q, A, \tau)$ be a Mealy automaton. Then $\Delta_{\mathcal{M}}$ is an internal Zappa–Szép product of the free monoids A^* and Q^*, i.e. for any $x \in \Delta_{\mathcal{M}}$, there exists a unique choice of elements $a_1, a_2, \ldots, a_k \in A$ and $q_1, q_2, \ldots, q_l \in Q$ such that $x = (a_1 a_2 \ldots a_k)(q_1 q_2 \ldots q_l)$.*

Proof. Let $(Q \cup A)^*$ be the free monoid on $Q \cup A$ and let $\iota\colon (Q \cup A)^* \to \mathbb{N}_0$ be the map defined by

$$\iota(x_1 x_2 \dots x_n) = |\{(i, j) \mid x_i \in Q, x_j \in A, 1 \le i < j \le n\}|,$$

where $x_1, x_2, \dots, x_n \in Q \cup A$. It is clear that $\iota(x_1 x_2 \dots x_n) = 0$ if and only if there exists $k \in \mathbb{N}$ such that $x_i \in A$ if $1 \le i \le k$ and $x_i \in Q$ if $k < i \le n$.

We define a binary relation $\to$ on $(Q \cup A)^*$ by

$$x_1 \dots x_{i-1} q a x_{i+2} \dots x_n \longrightarrow x_1 \dots x_{i-1}(q \cdot a)(q @ a) x_{i+2} \dots x_n,$$

where $x_1, \dots, x_n \in Q \cup A$, $q \in Q$ and $a \in A$.

One can easily see that if $x \to y$, then $\iota(y) = \iota(x) - 1$. Therefore, as $\iota(x) \ge 0$ for all $x \in (Q \cup A)^*$, there can exist no infinite chain $x_1 \to x_2 \to x_3 \to \cdots$. Furthermore, if $x, y, z \in (Q \cup A)^*$ are such that $x \to y$ and $x \to z$, then there exists $w \in (Q \cup A)^*$ such that $y \to w$ and $z \to w$. Indeed, let us write $x = x_1 x_2 \dots x_n$, $y = y_1 y_2 \dots y_n$ and $z = z_1 z_2 \dots z_n$ (notice that it follows from the definition that y and z must have the same length as x). Then, there exist $i, j \in \mathbb{N}$ such that $y_k = x_k$ for all $k \ne i, i+1$ and $z_k = x_k$ for all $k \ne j, j+1$. If $i = j$, then $y = z$ and there is nothing to prove. If $i \ne j$, then $i \ne j+1$ and $j \ne i+1$, since $x_i, x_j \in Q$ and $x_{i+1}, x_{j+1} \in A$. Thus, we can define $w = w_1 w_2 \dots w_n$, where

$$w_k = \begin{cases} y_k & \text{if } k = i, i+1, \\ z_k & \text{otherwise,} \end{cases}$$

and we get that $y \to w$ and $z \to w$.

Consequently, we can apply the Diamond lemma to conclude that if two words $x, y \in (Q \cup A)^*$ represent the same element in $\Delta_{\mathcal{M}}$, then there exists a unique word $z \in (Q \cup A)^*$ representing the same element and satisfying $\iota(z) = 0$. The result follows. □

Corollary 2.14. *The homomorphisms $i_Q\colon Q^* \to \Delta_{\mathcal{M}}$ and $i_A\colon A^* \to \Delta_{\mathcal{M}}$ are injective.*

This monoid $\Delta_{\mathcal{M}} = A^* \bowtie Q^*$ gives us a left action $\cdot$ of Q^* on A^* and a right action @ of A^* on Q^*.

Remark. We denote by $\cdot$ and @ both functions in Zappa–Szép product and operations of a Mealy automaton, but since these functions give the same results, there should be no risk of confusion.

Note that the actions $\cdot\colon Q^* \times A^* \to A^*$ and $@\colon Q^* \times A^*$ preserve lengths of words. The action of Q can be described by the Moore diagram of $\mathcal{M}$. The action

of $q \in Q$ on A^* is determined as follows: given $a_1 a_2 \dots a_n \in A^*$ and $q \in Q$, find in the Moore diagram the unique path starting at q and whose first label letters read $a_1 \dots a_2$, let $b_1 \dots b_n$ be the second label letters; then $q \cdot a_1 \dots a_n = b_1 \dots b_n$.

For a Mealy automaton $\mathcal{M} = (Q, A, \tau)$ we denote the relation $\dot{\sim}$ on Q^* by $\overset{Q}{\sim}$, the relation $\overset{@}{\sim}$ on A^* by $\overset{A}{\sim}$, the monoid $Q^*\dot{\sim}$ by $P_{\mathcal{M}}$ and the monoid $A^*/\overset{@}{\sim}$ by $D_{\mathcal{M}}$.

Definition 2.15. The semigroup $P_{\mathcal{M}}$ is called the *automaton semigroup* of $\mathcal{M}$. The semigroup $D_{\mathcal{M}}$ is called the *dual automaton semigroup* of $\mathcal{M}$.

The monoid $P_{\mathcal{M}} = Q^*/\overset{Q}{\sim}$ is generated by $[Q]_{\underset{\sim}{Q}}$ and the semigroup $D_{\mathcal{M}}$ is generated by $[A]_{\underset{\sim}{A}}$, where $[\cdot]_{\underset{\sim}{Q}}\colon Q^* \to P_{\mathcal{M}}$ and $[\cdot]_{\underset{\sim}{A}}\colon A^* \to D_{\mathcal{M}}$ are the canonical maps.

Remark 2.16. Under our definitions, the dual automaton semigroup $D_{\mathcal{M}}$ of $\mathcal{M}$ is in general not isomorphic to the automaton semigroup $P_{\partial\mathcal{M}}$ of the dual automaton $\partial\mathcal{M}$. However, it follows from Remark 2.12 that they are canonically anti-isomorphic. Thus, any property preserved by anti-isomorphisms (such as finiteness or the existence of a free subsemigroup) will be true in $P_{\partial\mathcal{M}}$ if and only if it is true in $D_{\mathcal{M}}$. Therefore, to prove Theorem 1.1, it is sufficient to prove the following dual version:

Theorem 2.17. *Let $\mathcal{M} = (Q, A, \tau)$ be an invertible Mealy automaton. Then, there exist elements $y, z \in D_{\mathcal{M}}$ that freely generate a non-commutative free subsemigroup if and only if there exists $x \in D_{\mathcal{M}}$ with infinite order.*

In fact, we will prove a stronger version of Theorem 2.17. To state it, however, we first need a lemma.

Lemma 2.18. *Let $\mathcal{M} = (Q, A, \tau)$ be a Mealy automaton.*

(1) *Let $v, w \in A^*$ be such that $v \overset{A}{\sim} w$ and let $t \in Q^*$. Then $t \cdot v \overset{A}{\sim} t \cdot w$.*

(2) *let $v, w \in Q^*$ be such that $v \overset{Q}{\sim} w$ and let $t \in A^*$. Then $v@t \overset{Q}{\sim} w@t$.*

Proof. Since the monoids Q^* and A^* are cancellative semigroups, it follows from Lemmas 2.8 and 2.7 that the actions of Q^* on $D_{\mathcal{M}}$ and of A^* on $P_{\mathcal{M}}$ are well defined. □

Therefore, we can consider monoids $A^* \bowtie P_{\mathcal{M}}$, $D_{\mathcal{M}} \bowtie Q^*$ and $D_{\mathcal{M}} \bowtie P_{\mathcal{M}}$.

For $S = A^* \bowtie P_{\mathcal{M}}$ we consider the relation $\overset{@}{\sim}$ on A^*, which we will denote by $\overset{D}{\sim}$, and the monoid $D'_{\mathcal{M}} := A^*/\overset{D}{\sim}$.

In other words, the relation $\overset{D}{\sim}$ on A^* is defined by $u_1 \overset{D}{\sim} u_2$ if $x@u_1 \overset{Q}{\sim} x@u_2$ for any $x \in Q^*$.

Here is a stronger version of Theorem 2.17:

Theorem 2.19. *Let $\mathcal{M} = (Q, A, \tau)$ be an invertible Mealy automaton. Then, there exist elements $y, z \in D'_{\mathcal{M}}$ that freely generate a non-commutative free subsemigroup if and only if there exists $x \in D_{\mathcal{M}}$ of infinite order.*

In Section 4, we will prove this theorem and thus prove Theorem 1.1.

Remark. In summary, for a Mealy automaton $\mathcal{M} = (Q, A, \tau)$, we denote by @:

(1) the right part of the operation τ;
(2) the action of A^* on Q^*;
(3) the action of A^* on $P_{\mathcal{M}}$;
(4) the action of $D_{\mathcal{M}}$ on Q^*;
(5) the action of $D_{\mathcal{M}}$ on $P_{\mathcal{M}}$;
(6) the action of $D'_{\mathcal{M}}$ on $P_{\mathcal{M}}$.

Similarly, we denote by $\cdot$:

(1) the left part of the operation τ;
(2) the action of Q^* on A^*;
(3) the action of Q^* on $D_{\mathcal{M}}$;
(4) the action of $P_{\mathcal{M}}$ on A^*;
(5) the action of $P_{\mathcal{M}}$ on $D_{\mathcal{M}}$.

These operations commute with the corresponding projections: for example, if $s@u = s'$ where $s, s' \in Q^*$ and $u \in A^*$, then $[s]_{\underset{\sim}{Q}}@[u]_{\underset{\sim}{A}} = [s']_{\underset{\sim}{Q}}$.

Example 2.20. Consider a Mealy automaton $\mathcal{M} = (Q, A, \tau)$ where $Q = \{a, b, c\}$ and alphabet

$$A := \{x_1, y_1, x_2, y_2, z_1, z_2\}.$$

Its map $\tau\colon Q \times A \to A \times Q$ is defined by the following table. Note that all words in Q^* that contain at least one a act on A^* in the same way (replacing all lower indices by 2).

Table 1

		$q \in Q$		
		a	b	c
$a \in A$	x_1	(x_2, a)	(x_2, a)	(x_2, a)
	y_1	(y_2, a)	(y_2, a)	(y_2, a)
	x_2	(x_2, a)	(x_2, b)	(x_2, c)
	y_2	(y_2, a)	(y_2, c)	(y_2, b)
	z_1	(z_2, a)	(z_1, b)	(z_2, c)
	z_2	(z_2, a)	(z_2, b)	(z_2, c)

Then, $x_1 \overset{D}{\sim} y_1$, because both of x_1 and y_1 map all non-empty words of Q^* to elements $\overset{Q}{\sim}$-equivalent to a.

$b \cdot z_1 \neq c \cdot z_1 \implies b \overset{Q}{\not\sim} c$. Since $b@x_2 = b \overset{Q}{\not\sim} c = b@y_2$, then $x_2 \overset{D}{\not\sim} y_2$. Since $x_1 \overset{D}{\sim} y_1$ but $a \cdot x_1 \overset{D}{\not\sim} a \cdot y_1$, we conclude that the action of $P_{\mathcal{M}}$ on $D'_{\mathcal{M}}$ is not well defined.

2.5. Groups generated by invertible automata. In the case where the automaton $\mathcal{M} = (Q, A, \tau)$ is invertible, it is natural to consider not only the automaton semigroup $P_{\mathcal{M}}$, but an automaton group, which we will define below.

Definition 2.21. Let $\mathcal{M} = (Q, A, \tau)$ be a invertible Mealy automaton and let $Q^{-1} = \{q^{-1} \mid q \in Q\}$ be the set of formal inverses of Q. The *enriched automaton* of $\mathcal{M}$ is the automaton $\widetilde{\mathcal{M}} = (Q \sqcup Q^{-1}, A, \tilde{\tau})$, where $\tilde{\tau}(q, a) = \tau(q, a)$ and $\tilde{\tau}(q^{-1}, q \cdot a) = (a, (q@a)^{-1})$ for all $q \in Q$ and $a \in A$.

Proposition 2.22. *Let $\mathcal{M} = (Q, A, \tau)$ be an invertible Mealy automaton. Then $P_{\widetilde{\mathcal{M}}}$ is a group and for all $q \in Q$ the elements q and q^{-1} are inverse elements.*

Proof. We will prove that $q^{-1}q \cdot u = u$ for any $q \in Q$ and $u \in A^*$ by induction on $|u|$. For $|u| = 0$ this is obvious. Suppose that $u = au'$. Then,

$$q^{-1}qau' = q^{-1}(q \cdot a)(q@a)u' = a(q@a)^{-1}(q@a)u'.$$

By the induction hypothesis, $(q@a)^{-1}(q@a) \cdot u' = u'$. Thus, $q^{-1}q \cdot u = u$. Similarly we show that $qq^{-1} \cdot u = u$ for all $u \in A^*$. □

Corollary 2.23. *Let $\mathcal{M} = (Q, A, \tau)$ be an invertible Mealy automaton such that $P_{\mathcal{M}}$ is a group. Then, $P_{\mathcal{M}} = P_{\widetilde{\mathcal{M}}}$.*

Proof. It is clear from the definition of $\widetilde{\mathcal{M}}$ that $P_{\mathcal{M}} \leq P_{\widetilde{\mathcal{M}}}$. On the other hand, it follows from Proposition 2.22 that if $P_{\mathcal{M}}$ is a group, then the generators of $P_{\widetilde{\mathcal{M}}}$ are contained in $P_{\mathcal{M}}$. We conclude that $P_{\mathcal{M}} = P_{\widetilde{\mathcal{M}}}$. □

Definition 2.24. Let $\mathcal{M} = (Q, A, \tau)$ be an invertible Mealy automaton. The *automaton group* of $\mathcal{M}$ is the group $P_{\widetilde{\mathcal{M}}}$.

In what follows, we will be interested in the existence of elements of infinite order in the semigroup $P_{\mathcal{M}}$ of a Mealy automaton $\mathcal{M}$. If this automaton is invertible, then it is equivalent to look for elements of infinite order in the automaton group $P_{\widetilde{\mathcal{M}}}$, as we will see in the next proposition.

Proposition 2.25. *Let $\mathcal{M} = (Q, A, \tau)$ be an invertible automaton, let $P_{\mathcal{M}}$ be the automaton semigroup of $\mathcal{M}$ and let $P_{\widetilde{\mathcal{M}}}$ be the automaton group of $\mathcal{M}$. Then, $P_{\mathcal{M}}$ contains an element of infinite order if and only if $P_{\widetilde{\mathcal{M}}}$ does.*

Proof. It is clear that if $P_{\mathcal{M}}$ contains an element of infinite order, then so does $P_{\widetilde{\mathcal{M}}}$. To show the converse, let us suppose that every element of $P_{\mathcal{M}}$ is of finite order. Then, the inverse of any element of $P_{\mathcal{M}}$ is also an element of $P_{\mathcal{M}}$, which means that $P_{\mathcal{M}}$ is a group. Therefore, by Corollary 2.23, we get that $P_{\mathcal{M}} = P_{\widetilde{\mathcal{M}}}$, which means that $P_{\widetilde{\mathcal{M}}}$ is a torsion group. □

As we will see below, the dual semigroup is unaffected by the passage to the enriched automaton.

Lemma 2.26. *Let $\mathcal{M} = (Q, A, \tau)$ be an invertible Mealy automaton and $\widetilde{\mathcal{M}}$ be its enriched automaton. Then, for any $q \in Q$ and $v \in A^*$, we have $q^{-1}@v = (q@(q^{-1} \cdot v))^{-1}$.*

Proof. By Proposition 2.22, it suffices to prove that $q^{-1}@(q \cdot v) = (q@v)^{-1}$. If v is of length 1 (i.e. if $v \in A$), then we get by definition that $q^{-1}@(q \cdot v) = (q@v)^{-1}$.

Now, for $v \in A^*$ of length n, let us write $v = v_1 v_2 \dots v_n$, with $v_1, v_2, \dots, v_n \in A$. On the one hand, we have $(q^{-1}q)@v = (q^{-1}@(q \cdot v))(q@v)$. On the other hand,

$$\begin{aligned}(q^{-1}q)@(v_1 \dots v_n) &= ((q^{-1}q)@v_1)@(v_2 \dots v_n)\\ &= ((q@v_1)^{-1}(q@v_1))@(v_2 \dots v_n).\end{aligned}$$

Thus, by induction, $(q^{-1}q)@v = (q@v)^{-1}(q@v)$. It follows that $q^{-1}@(q \cdot v) = (q@v)^{-1}$. □

Lemma 2.27. *Let $\mathcal{M} = (Q, A, \tau)$ be an invertible Mealy automaton and $V \subset A^*$ be a finite set. Then, for any $s \in (Q \sqcup Q^{-1})^*$, there exists $t \in Q^*$ such that $s \cdot v = t \cdot v$ for all $v \in V$.*

Proof. It suffices to show that for all $q^{-1} \in Q^{-1}$, there exists $t \in Q^*$ such that $q^{-1} \cdot v = t \cdot v$ for all $v \in V$. Since the action of Q^* on A^* preserves lengths and the set V is finite, the size of the orbits under the action of Q^* of elements of V is uniformly bounded. This, coupled with the invertibility of $\mathcal{M}$, implies that there exists some $k \in \mathbb{N}$ such that $q^{k+1} \cdot v = v$ for all $v \in V$. Therefore, $q^k \cdot v = q^{-1} \cdot v$ for all $v \in V$, which concludes the proof. □

Proposition 2.28. *Let $\mathcal{M} = (Q, A, \tau)$ be an invertible automaton and $\widetilde{\mathcal{M}}$ be its enriched automaton. Then, $D_{\mathcal{M}} = D_{\widetilde{\mathcal{M}}}$.*

Proof. By definition, $D_{\mathcal{M}} = A^*/\overset{A}{\sim}$ and $D_{\widetilde{\mathcal{M}}} = A^*/\overset{A'}{\sim}$, where $\overset{A}{\sim}$ and $\overset{A'}{\sim}$ are two congruence relations on A^*. We need to show that $\overset{A}{\sim} = \overset{A'}{\sim}$.

Consider $\Delta_{\mathcal{M}}$ as a subsemigroup of $\Delta_{\widetilde{\mathcal{M}}}$. Thus, if $v, w \in A^*$ are such that $s@v = s@w$ for all $s \in (Q \sqcup Q^{-1})^*$, then in particular, $s@v = s@w$ for all $s \in Q^*$. Therefore, if $v \overset{A'}{\sim} w$, then $v \overset{A}{\sim} w$.

On the other hand, suppose that $v \overset{A}{\sim} w$. Then, by definition, we must have $q@v = q@w$ for all $q \in Q$. Let us now consider $q^{-1} \in Q^{-1}$. By Lemma 2.26, we have $q^{-1}@v = (q@(q^{-1} \cdot v))^{-1}$ and $q^{-1}@w = (q@(q^{-1} \cdot w))^{-1}$. Now, by Lemma 2.27, there exists $t \in Q^*$ such that $q^{-1} \cdot v = t \cdot v$ and $q^{-1} \cdot w = t \cdot w$. It follows from Proposition 2.18 that if $v \overset{A}{\sim} w$, then $t \cdot v \overset{A}{\sim} t \cdot w$, which means that $q^{-1} \cdot v \overset{A}{\sim} q^{-1} \cdot w$. Therefore, $q@(q^{-1} \cdot v) = q@(q^{-1} \cdot w)$, which implies that $q^{-1}@v = q^{-1}@w$.

Now, for $s = s_n \dots s_2 s_1 \in (Q \sqcup Q^{-1})^*$, we have $(s_n \dots s_2 s_1)@v = ((s_n \dots s_2)@(s_1 \cdot v))(s_1@v)$ and $(s_n \dots s_2 s_1)@w = ((s_n \dots s_2)@(s_1 \cdot w))(s_1@w)$. From the argument above, we have $s_1 \cdot v \overset{A}{\sim} s_1 \cdot w$ and $s_1@v = s_1@w$. Thus, the result follows by induction. □

It follows from Proposition 2.28 that if we are interested in the dual semigroup of an invertible automaton $\mathcal{M}$, we can assume without loss of generality that $P_{\mathcal{M}}$ is in fact a group.

Definition 2.29. A Mealy automaton $\mathcal{M} = (Q, A, \tau)$ is called *self-invertible* if $P_{\mathcal{M}}$ is a group.

Lemma 2.30. *Let $\mathcal{M} = (Q, A, \tau)$ be an invertible Mealy automaton and let $v, w \in D_{\mathcal{M}}$ be such that $v \overset{D}{\sim} w$. Then, for all $t \in P_{\mathcal{M}}$, we have $t \cdot v \overset{D}{\sim} t \cdot w$.*

Proof. Since $P_{\mathcal{M}}$ can be embedded into a group $P_{\widetilde{\mathcal{M}}}$, the monoid $P_{\mathcal{M}}$ is cancellative. The result follows from Lemma 2.8. □

This means that for an invertible automaton $\mathcal{M}$, the action of $P_{\mathcal{M}}$ on $D'_{\mathcal{M}}$ is well-defined and we can also consider $D'_{\mathcal{M}} \bowtie P_{\mathcal{M}}$.

2.6. Transformation wreath products

Definition 2.31. Let Γ be a monoid acting from the left on a finite set X. Let S be a semigroup, then the *transformation wreath product* $W = S \wr_X \Gamma$ is defined as the semidirect product $\Gamma \ltimes S^X$.

The elements of S^X are functions $f : X \to S$ with coordinatewise multiplication, the monoid Γ acts on S^X from the right as $f^{\pi}(x) = f(\pi(x))$. Elements in $W = S \wr_X \Gamma$ are recorded as pairs (π, f), where π is a function $X \to X$ from Γ and $f \in S^X$. Multiplication in W is given by

$$(\pi_1, f_1)(\pi_2, f_2) = (\pi_1 \pi_2, f_1^{\pi_2} f_2).$$

If S and Γ are groups, then $S \wr_X \Gamma$ is also a group.

Proposition 2.32. *Let $S = B \bowtie A$ and let X be a finite subset of B such that $A \cdot X \subseteq X$. The action of A on X gives us a homomorphism $p_n\colon A \to \mathrm{End}(X)$, where $\mathrm{End}(X)$ is the monoid of maps from X to itself. We also have a map $s\colon A \to A^X$ given by $s(a)(x) = a@x$ for $a \in A$ and $x \in X$. Consider the map*

$$\begin{aligned} \varphi\colon A &\longrightarrow A \wr_X \mathrm{End}(X), \\ a &\longmapsto (p(a), s(a)). \end{aligned}$$

Then φ is a homomorphism.

Proof. We have

$$\varphi(a_1)\varphi(a_2) = (p(a_1), s(a_1))(p(a_2), s(a_2)) = (p(a_1)p(a_2), s_n(a_1)^{p_n(a_2)}s(a_2)).$$

As p is a homomorphism, $p(a_1)p(a_2) = p(a_1a_2)$. Furthermore, for any $x \in X$, we have

$$\begin{aligned} (s(a_1)^{p(a_2)}s(a_2))(x) &= (s(a_1)^{p(a_2)})(x)s(a_2)(x) \\ &= (a_1@(p(a_2)(x)))(a_2@x) \\ &= (a_1@(a_2 \cdot x))(a_2@x) \\ &= a_1a_2@x = s(a_1a_2)(x). \end{aligned}$$

Therefore,

$$s_n(a_1)^{p_n(a_2)}s(a_2) = s(a_1a_2).$$

We conclude that $\varphi(a_1)\varphi(a_2) = \varphi(a_1a_2)$. □

The following lemma is useful in applications to automata semigroups.

Lemma 2.33. *Let $S = B \bowtie A$, where the monoid A has a finite generating set E such that $E@B \subseteq E$. Let $X_1, X_2, \ldots$ be a sequence of finite subsets of B such that $A \cdot X_i \subseteq X_i$ for any X_i, and let $|X_i| < M$ for some constant M independent on i. Then $|\bigcup_i [X_i]_{\underset{\sim}{@}}| < \infty$.*

Proof. For each X_i construct a homomorphism as in Proposition 2.32:

$$\begin{aligned} \varphi_i\colon A &\longrightarrow A \wr_{X_i} \mathrm{End}(X_i) \\ a &\longmapsto (p_i(a), s_i(a)). \end{aligned}$$

Choosing an arbitrary bijection between X_i and the set $Y_i := \{1, 2, \ldots, |X_i|\}$ yields a homomorphism

$$\widetilde{\varphi_i}\colon A \wr_{Y_i} \mathrm{End}(Y_i).$$

Since $\widetilde{\varphi_i}$ is a homomorphism, it is uniquely determined by the image of the generating set E. Since $e@b \in E$ for any $e \in E$ and $b \in B$, we have that $s_i(E) \subseteq E^{X_i}$. It follows that

$$\widetilde{\varphi_i}(E) \subseteq \mathrm{End}(Y_i) \times E^{Y_i},$$

which is a finite set. Hence, for a given value of $|X_i|$, there are only finitely many different homomorphisms $\widetilde{\varphi_i}$.

Therefore, if $|X_i| \leq M$ for all $i \in \mathbb{N}$, there must exist a finite set $\{i_1, i_2, \ldots, i_m\}$ such that for any $i \in \mathbb{N}$, there exists $k \in \mathbb{N}$ such that $\widetilde{\varphi_i} = \widetilde{\varphi_{i_k}}$. In particular, for any $x \in X_i$, there exists a $x' \in X_{i_k}$ such that $a@x = a@x'$ for all $a \in A$, which means that $x \overset{@}{\sim} x'$ by definition. Therefore,

$$\Big|\bigcup_{n=0}^{\infty}[X_i]_{\overset{@}{\sim}}\Big| \leq \sum_{k=1}^{m}|X_{i_k}| < \infty. \qquad \square$$

The following result is well known (see for example [12]), but we include a proof here for completeness.

Theorem 2.34. *Let $\mathcal{M} = (Q, A, \tau)$ be a Mealy automaton. Then $P_{\mathcal{M}}$ is finite if and only if $D_{\mathcal{M}}$ is finite.*

Proof. Suppose $|P_{\mathcal{M}}| = M$. Then, for any $u \in A^*$, the cardinality of the set $Q^* \cdot u$ is not larger than M.

We enumerate all finite words of A^*: $A^* = u_1, u_2, \ldots$. Apply Lemma 2.33 for $S = A^* \bowtie Q^*$, $E = Q$, $X_i = Q^* \cdot u_i$. Then $|D_{\mathcal{M}}| = |[A^*]_{\overset{@}{\sim}}| = |\bigcup_i [X_i]_{\overset{@}{\sim}}| < \infty$.

If $|D_{\mathcal{M}}| < \infty$, we can apply Lemma 2.33 to the dual automaton $\partial\mathcal{M}$ and prove that $P_{\mathcal{M}}$ is finite. $\square$

2.7. Automorphisms of rooted trees. The free monoid A^* can be identified with the $|A|$-regular rooted tree T_A as follows: the set of vertices is A^* and two vertices $v, w \in A^*$ are joined by an edge if and only if there exists $a \in A$ such that $w = va$ or $v = wa$. The *root* of T_A is the empty word ε. The words of A^* of length n form the *n-th level* of T_A.

Consider the group $\mathrm{Aut}(T_A)$ acting on T_A from the left by automorphisms fixing the root. At each level $\mathrm{Aut}(T_A)$ acts by permutations.

A map $f\colon A^* \to A^*$ belongs to $\mathrm{Aut}(T_A)$ if f preserves lengths of words and lengths of longest common prefixes.

Definition 2.35. Let A be a finite alphabet, and let $S = A^* \bowtie X$. If X is a group, the action of X on A^* is faithful and $X \cdot A = A$, this action of X is called *self-similar* and X is called a *self-similar group*.

Self-similar actions on A^* are rooted automorphisms of the tree T_A.

For example, for any self-invertible Mealy automata $\mathcal{M} = (Q, A, \tau)$ the action of $P_{\mathcal{M}}$ on A^* is self-similar.

Remark 2.36. Since the action of Q^* on A^* preserves the tree structure of A^*, we can define the action of Q^* on the set of all right-infinite sequences A^ω: for any $s \in Q^*$ and $a_1a_2\ldots \in A^\omega$ the sequence $\{s \cdot a_1 \ldots a_n\}$ has a limit $b_1b_2\ldots \in A^\omega$, and we write $s \cdot a_1a_2\ldots = b_1b_2\ldots$

3. Orbits of periodic sequences

Let $G \leqslant \mathrm{Aut}(T_A)$ be a group acting on A^* from the left and let x be an element of A^* or an element of A^ω. The orbit of x will be denoted by $G \cdot x$.

3.1. Self-similar groups and regular languages

Notation. Let $a \in A$ and $G \leqslant \mathrm{Aut}(T_A)$ be a subgroup of $\mathrm{Aut}(T_A)$. We denote by a^ω the infinite sequence $aaa\ldots$ and by $\mathrm{Lan}_G(a)$ the language that consists of all prefixes of sequences in $G \cdot a^\omega$.

In other words, $\mathrm{Lan}_G(a) = \bigsqcup_k G \cdot a^k$.

Lemma 3.1. *Let G act self-similarly on A^*, let $a \in A$ and let $v \in \mathrm{Lan}_G(a)$. Then, $\mathrm{Lan}_G(a)$ contains all the subwords of v.*

Proof. It suffices to show that if $v_1 v_2 \in \mathrm{Lan}_G(a)$, then $v_1, v_2 \in \mathrm{Lan}_G(a)$. Let us write $v = v_1 v_2$ and let $g \in G$ be such that $v = g \cdot a^{|v_1|} a^{|v_2|}$. Then, $v_1 = g \cdot a^{|v_1|} \in \mathrm{Lan}_G(a)$ and $v_2 = (g@a^{|v_1|}) \cdot a^{|v_2|} \in \mathrm{Lan}_G(a)$. □

For a given word $v \in \mathrm{Lan}_G(a)$ we say that the cardinality

$$\#\{a \in A : va \in \mathrm{Lan}_G(a)\}$$

is the *degree* of v in $\mathrm{Lan}_G(a)$ and denote this number by $\mathrm{Degree}_{\mathrm{Lan}_G(a)}(v)$ (or by $\mathrm{Degree}(v)$ in case it is clear what language is considered.)

Lemma 3.2. *Let G be a group acting self-similarly on A^*, $a \in A$ and $v_1, v_2 \in \mathrm{Lan}_G(a)$ with $|v_1| = |v_2|$. Then* $\mathrm{Degree}(v_1) = \mathrm{Degree}(v_2)$.

Proof. Let $\mathrm{Degree}(v_1) = d$. Without loss of generality. we consider that

$$v_1 a_1, v_1 a_2, \ldots, v_1 a_d \in \mathrm{Lan}_G(a).$$

There exists $g \in G$ such that $g \cdot v_1 = v_2$. It follows that

$$g \cdot v_1 a_1 = v_2((g@v_2) \cdot a_1), v_2((g@v_2) \cdot a_2), \ldots, v_2((g@v_2) \cdot a_d) \in \mathrm{Lan}_G(a),$$

i.e. $\mathrm{Degree}(v_2) \geq d$. Similarly, $\mathrm{Degree}(v_1) \geq \mathrm{Degree}(v_2)$. □

Lemma 3.3. *Let G be a group with a self-similar action on A^*, $a \in A$ and $k_1 < k_2 \in \mathbb{N}$. Then* $\mathrm{Degree}_{\mathrm{Lan}_G(a)}(a^{k_1}) \geq \mathrm{Degree}_{\mathrm{Lan}_G(a)}(a^{k_2})$.

Proof. If $a^{k_2} a_i \in \mathrm{Lan}_G(a)$, then $a^{k_1} a_i \in \mathrm{Lan}_G(a)$ by Lemma 3.1, since $a^{k_1} a_i$ is a subword of $a^{k_2} a_i$. □

Lemma 3.4. *Let G be a group acting self-similarly on A^* and $a \in A$. Then, there exist $T, d \in \mathbb{N}$ such that* $\mathrm{Degree}_{\mathrm{Lan}_G}(v) = d$ *for all $v \in L_G(a)$ with $|v| \geqslant T$. Furthermore, for any word $v \in A^*$, the following statements are equivalent*:

(1) $v \in \mathrm{Lan}_G(a)$;

(2) *all subwords of v of length at most $T + 1$ belong to* $\mathrm{Lan}_G(a)$.

Proof. Since the sequence of integers $\mathrm{Degree}(a), \mathrm{Degree}(a^2), \mathrm{Degree}(a^3), \ldots$ is non-increasing then there exist $T, d \in \mathbb{N}$ such that $\mathrm{Degree}(a^k) = d$ for $k \geq T$. It follows from Lemma 3.2 that if $|v| \geq T$ then $\mathrm{Degree}(v) = d$. This proves the first claim.

We have (1) $\implies$ (2) by Lemma 3.1. To prove (2) $\implies$ (1), let us first notice that if there are m words of length T in $\mathrm{Lan}_G(a)$, then the previous part implies that there are md^k words of length $T + k$ in $\mathrm{Lan}_G(a)$.

Consider the language

$$\widetilde{\mathrm{Lan}} := \{w \in A^* \mid u \in \mathrm{Lan}_G(a) \text{ for all subwords } u \text{ of } w \text{ of length at most } T + 1.\}$$

It follows from Lemma 3.1 that $\mathrm{Lan}_G(a) \subseteq \widetilde{\mathrm{Lan}}$. On the other hand, we can estimate the number of words of each length in $\widetilde{\mathrm{Lan}}$. It is clear that a word of length at most $T + 1$ belongs to $\widetilde{\mathrm{Lan}}$ if and only if it belongs to $\mathrm{Lan}_G(a)$. Thus, $\widetilde{\mathrm{Lan}}$ and $\mathrm{Lan}_G(a)$ contain the same number of elements of length at most $T + 1$.

We will now show by induction that for all $k \in \mathbb{N}$, $\widetilde{\mathrm{Lan}}$ contains no more than md^k words of length $T + k$. For $k = 1$, this is obvious. Let us now suppose that for some $k \in \mathbb{N}$, there are K words of length $T+k$ in $\widetilde{\mathrm{Lan}}$, where $K \leq md^k$. Then, as the language $\widetilde{\mathrm{Lan}}$ is clearly closed under the operation of taking prefixes, any word $w \in \widetilde{\mathrm{Lan}}$ of length $T + k + 1$ must start with one of these K words. If there are more than dK words of length $T+k+1$, then by the pigeonhole principle, one of these K words can be continued to the right in more than d ways. Thus, if v is the word formed by the last T letters of this word, we have that $\mathrm{Degree}(v) \geq d+1$, which is absurd. Therefore, we can conclude that $\widetilde{\mathrm{Lan}}$ and $\mathrm{Lan}_G(a)$ contain the same number of elements of length l for all $l \in \mathbb{N}$.

This shows that $\mathrm{Lan}_G(a) = \widetilde{\mathrm{Lan}}$. □

It's clear that if $|G \cdot a^\omega| = \infty$ then $d > 1$.

Remark 3.5. Let $P_{\mathcal{M}}$ be a semigroup generated by invertible Mealy automata and let u^ω be an arbitrary periodic sequence. Lemma 3.4 gives us a way to describe the structure of $P_{\mathcal{M}} \cdot u^\omega$: the prefixes of this set form a regular language. In Section 5 we try to generalize this observation.

3.2. Order of elements and finiteness of orbits. Let $\mathcal{M} = (Q, A, \tau)$ be an invertible automaton. As we will see, for $u \in A^*$, the order of $[u]_{\underset{\sim}{A}} \in D_{\mathcal{M}}$ is related to the size of the orbit of $u^\omega \in A^\omega$ under the action of $P_{\mathcal{M}}$.

Lemma 3.6. *Let $\mathcal{M} = (Q, A, \tau)$ be a self-invertible automaton and let $u \in A^*$. Then the following statements are equivalent*:

(1) $|P_{\mathcal{M}} \cdot u^\omega| < \infty$;

(2) $|[P_{\mathcal{M}} \cdot u^n]_{\underset{\sim}{A}}|$ *is bounded independently of* n;

(3) $|[P_{\mathcal{M}} \cdot u^n]_{\underset{\sim}{D}}|$ *is bounded independently of* n;

(4) $\left|\left[\bigcup_{n=0}^{\infty} P_{\mathcal{M}} \cdot u^n\right]_{\underset{\sim}{A}}\right| < \infty$;

(5) $\left|\left[\bigcup_{n=0}^{\infty} P_{\mathcal{M}} \cdot u^n\right]_{\underset{\sim}{D}}\right| < \infty$;

(6) $[u]_{\underset{\sim}{A}}$ *has finite order in* $D_{\mathcal{M}}$;

(7) $[u]_{\underset{\sim}{D}}$ *has finite order in* $D'_{\mathcal{M}}$.

Proof. We will prove

$$(1) \implies (2) \implies (3) \implies (5) \implies (7) \implies (1)$$

and

$$(2) \implies (4) \implies (6) \implies (7).$$

(1) $\implies$ (2) $\implies$ (3). For all $n \in \mathbb{N}$, we have $|P_{\mathcal{M}} \cdot u^n| \leq |P_{\mathcal{M}} \cdot u^\omega| < \infty$. It's clear that $|[P_{\mathcal{M}} \cdot u^n]_{\underset{\sim}{D}}| \leqslant |[P_{\mathcal{M}} \cdot u^n]_{\underset{\sim}{A}}| \leqslant |P_{\mathcal{M}} \cdot u^n|$.

(2) $\implies$ (4). Consider $S = D_{\mathcal{M}} \bowtie Q^*$ and apply Lemma 2.33 to S with $E = Q$ and $X_i = [P_{\mathcal{M}} \cdot u^i]_{\underset{\sim}{A}}$. We get that $\left|\bigcup_i [X_i]_{\underset{\sim}{@}}\right|$ is finite. As $D_{\mathcal{M}}$ acts faithfully on Q^*, this implies that $\left|\bigcup_i [P_{\mathcal{M}} \cdot u^i]_{\underset{\sim}{A}}\right| < \infty$.

(3) $\implies$ (5). From Lemma 2.30 it follows that we can consider the product $S = D'_{\mathcal{M}} \bowtie P_{\mathcal{M}}$. Apply Lemma 2.33 to S with $E = [Q]_{\underset{\sim}{Q}}$ and $X_i = [P_{\mathcal{M}} \cdot u^i]_{\underset{\sim}{D}}$.

(4) $\implies$ (6) and (5) $\implies$ (7). Since $\{u^n\} \subseteq \bigcup_{n=0}^{\infty} P_{\mathcal{M}} \cdot u^n$, we have

$$\{[u]_{\underset{\sim}{A}}^k\} \subseteq \bigcup_{n=0}^{\infty} [P_{\mathcal{M}} \cdot u^n]_{\underset{\sim}{A}} \quad \text{and} \quad \{[u]_{\underset{\sim}{D}}^k\} \subseteq \bigcup_{n=0}^{\infty} [P_{\mathcal{M}} \cdot u^n]_{\underset{\sim}{D}}.$$

(6) $\implies$ (7). This is clear, since $D'_{\mathcal{M}}$ is a quotient of $D_{\mathcal{M}}$.

(7) $\implies$ (1). If $[u]_{\underset{\sim}{D}}$ generates a finite subsemigroup in $D'_{\mathcal{M}}$, then there must exist $k, l \in \mathbb{N}$ with $k < l$ and $[u^k]_{\underset{\sim}{D}} = [u^l]_{\underset{\sim}{D}}$. Then, we must have $\mathrm{St}_{P_{\mathcal{M}}}(u^l) = \mathrm{St}_{P_{\mathcal{M}}}(u^m)$ for all $m \geq l$. Indeed, suppose that there exist $m > l$ and $g \in \mathrm{St}_{P_{\mathcal{M}}}(u^l)$ such that $g \cdot u^m \neq u^m$. Let us assume that m is minimal for this property, meaning

that $g \cdot u^n = u^n$ for all $n < m$. Therefore, $g \in \mathrm{St}_{P_{\mathcal{M}}}(u^{m-1})$. Since $k < l \leq m-1$, we have $g \in \mathrm{St}_{P_{\mathcal{M}}}(u^k)$ and $g@u^k \in \mathrm{St}_{P_{\mathcal{M}}}(u^{m-1-k})$. By the assumption that $u^k \overset{D}{\sim} u^l$, we have $g@u^k = g@u^l$, which implies that $g \in \mathrm{St}_{P_{\mathcal{M}}}(u^{l+m-1-k})$. Since $l-1-k \geq 0$, this means that $g \in \mathrm{St}_{P_{\mathcal{M}}}(u^m)$, a contradiction. Then $\mathrm{St}_{P_{\mathcal{M}}}(u^\omega) = \mathrm{St}_{P_{\mathcal{M}}}(u^l)$ and

$$|P_{\mathcal{M}} \cdot u^\infty| = [P_{\mathcal{M}} : \mathrm{St}_{P_{\mathcal{M}}}(u^\omega)] = [P_{\mathcal{M}} : \mathrm{St}_{P_{\mathcal{M}}}(u^l)] = |P_{\mathcal{M}} \cdot u^l| < \infty. \qquad \square$$

4. Free subsemigroups

4.1. Changing the alphabet. Let $\mathcal{M} = (Q, A, \tau)$ be an invertible Mealy automaton and let $u \in A^*$, $|u| = k$. We can construct a new Mealy automaton $\mathcal{M}_k = (Q, A^k, \tau_k)$, where the map $\tau_k \colon Q \times A^k \to A^k \times Q$ is defined in a natural way. We have $\Delta_{\mathcal{M}_k} \leqslant \Delta_{\mathcal{M}}$.

Suppose $[u]$ has infinite order in $D_{\mathcal{M}}$, then from Lemma 3.6 it follows that $|P_{\mathcal{M}} \cdot u^\omega| = |P_{\mathcal{M}_k} \cdot u^\omega| = \infty$, and thus (again from 3.6) $[u]$ has infinite order in $D_{\mathcal{M}_k}$.

Suppose there is a free non-commutative subsemigroup in $D'_{\mathcal{M}_k}$, then the corresponding elements of $D'_{\mathcal{M}}$ generate a free subsemigroup in $D'_{\mathcal{M}}$ and a free subsemigroup in $D_{\mathcal{M}}$.

Hence, for theorem 2.19, it is enough to only consider the following case:

Proposition 4.1. *Let $\mathcal{M} = (Q, A, \tau)$ be a self-invertible Mealy automaton and let $|P_{\mathcal{M}} \cdot a^\omega| = \infty$ where $a \in A$. Then there exist $x, y \in A^*$ such that $[x]_{\underset{\sim}{D}}$ and $[y]_{\underset{\sim}{D}}$ freely generate a free subsemigroup in $D'_{\mathcal{M}}$.*

4.2. Proof of Proposition 4.1. Apply to $\mathcal{M}$ and a Lemma 3.4 to find numbers T, d such that all words in $\mathrm{Lan}_{P_{\mathcal{M}}}(a)$ with length T have degrees equal to $d > 1$.

We construct a directed labelled graph Γ. Its vertices are $\{v \in \mathrm{Lan}_{P_{\mathcal{M}}}(a) \mid 0 \leq |v| \leq T\}$. Edges of Γ will be labelled by letters of A. Let $v_2 = v_1 a_i$ for some $a_i \in A$, then we draw an arrow $v_1 \to v_2$ with label a_i. If $|v_1| = |v_2| = T$ then we draw an arrow $v_1 \to v_2$ if and only if there exist $a_i, a_j \in A$, $v' \in A^{T-1}$ such that $v_1 = a_i v'$, $v_2 = v' a_j$ and $a_i v' a_j \in \mathrm{Lan}_{P_{\mathcal{M}}}(a)$. In this case, the edge $v_1 \to v_2$ is labelled by a_j.

Some properties of Γ.

(1) The vertices of Γ are divided into levels. The level 0 consists of one vertex V_ε, where $\varepsilon \in A^*$ is the empty word. For any $0 \leq k \leq T$ the k-th level consists of words of $\mathrm{Lan}_{P_{\mathcal{M}}}(a)$ of length k.

(2) $\mathrm{Lan}_{P_{\mathcal{M}}}(a)$ is the set of words that are written along paths starting from V_ε.

(3) For any path in Γ the word that is written along it belongs to $\mathrm{Lan}_{P_{\mathcal{M}}}(a)$.

(4) Any path in Γ with length $\geq T$ ends at a vertex of level T.

(5) For each vertex V of level T, there exists a path from V_ϵ to V of length T.

(6) All vertices of level T have outgoing degree equal to d.

Denote a path starting from $V \in \Gamma$ by ${}_V u$, where u is the word written along this path.

We review some basic facts about directed graphs. We say that a subgraph of a directed graph is *strongly connected* if for any two vertices, there is a directed path joining the first to the second. A *strongly connected component* of a directed graph is a strongly connected subgraph that is maximal for this property, meaning that no additional edges or vertices can be added to it without breaking its property of being strongly connected. The collection of strongly connected components forms a partition of the set of vertices of the graph. If each strongly connected component is contracted to a single vertex, the resulting graph is a directed acyclic graph called the *condensation* of the graph.

In the condensation of Γ there exists a vertex R without any outgoing edge. In the corresponding strongly connected component R of Γ all the outgoing edges must therefore go to R. In particular, all the vertices of R must belong to level T.

Lemma 4.2. *For any $T' \geqslant T$ and $V \in R$ there exists a word $u \in \mathrm{Lan}_{P_{\mathcal{M}}}(a)$ of length T' such that the path ${}_{V_\varepsilon} u$ ends at V.*

Proof. Since R is strongly connected, for any $V_i \in R$ there exists an incoming edge $V_j \to V_i$ for some $V_j \in R$. Hence we can find in R a path of length $T' - T$, ending at V. We conclude using the fact that for any $V_i \in R$, there is a path of length T from the root to V_i. □

Take an arbitrary vertex $V \in R$. As every outgoing edge of V leads to a vertex of R, we can find d cycles ${}_V c_1, \ldots, {}_V c_d$ starting and ending at V and such that their first edges are all different (the cycles can pass through one edge multiple times). Without loss of generality, we can assume that all ${}_V c_i$ have the same length (replacing each cycle ${}_V c_i$ by some power ${}_V c_i^k$ if necessary).

We will prove Proposition 4.1 by contradiction. Let us assume that every two-generated subsemigroup of $D'_{\mathcal{M}}$ is not free.

Lemma 4.3. *If $D'_{\mathcal{M}}$ contains no free two-generated subsemigroup, there exist cycles ${}_V x, {}_V w_1, \ldots, {}_V w_d$ starting and ending at V such that $|w_1| = |w_2| = \cdots = |w_d|$,*

$$[xw_1]_{\underset{\sim}{D}} = [xw_2]_{\underset{\sim}{D}} = \cdots = [xw_d]_{\underset{\sim}{D}} \text{ in } D'_{\mathcal{M}},$$

and the cycles ${}_V w_1, {}_V w_2, \ldots, {}_V w_d$ begin with d different edges.

Proof. We will prove by induction that for any $1 \leqslant k \leqslant d$ there exist $k+1$ cycles ${}_V x, {}_V w_1, \ldots, {}_V w_k$ such that $[xw_1]_{\underset{\sim}{D}} = \cdots = [xw_k]_{\underset{\sim}{D}}$ and ${}_V c_i$ is a beginning of ${}_V w_i$ for any $1 \leq i \leq k$.

The case $k = 1$ is clear. Let us now assume that it is true for some $k < d$ and let us prove that it then also holds for $k+1$. Suppose that we have cycles ${}_V x, {}_V w_1, \ldots, {}_V w_k$ satisfying the above conditions. Since ${}_V w_k$ starts with c_k, we can write ${}_V w_k = {}_V c_k w'$, where ${}_V w'$ is a cycle in Γ. By our assumption, the semigroup generated by $[xc_k w']$ and $[xc_{k+1} w']$ is not free.

This means that there are two different words $W_1, W_2 \in \{a, b\}^*$, such that when all the letters a are replaced by $xc_k w'$, and all the letters b are replaced by $xc_{k+1} w'$ we obtain the same elements in $D'_{\mathcal{M}}$. We denote by $\sim$ this congruence relation on $\{a, b\}^*$.

Without loss of generality, we can assume that $|W_1| = |W_2|$. Indeed, if $|W_1| < |W_2|$, then consider the words $W_1 a W_2$ and $W_2 a W_1$. We have that $W_1 a W_2 \sim W_2 a W_1$. If these words are different as elements of $\{a, b\}^*$, then everything is fine. Otherwise, the $(|W_1| + 1)$th letter of W_2 is a, and then words $W_1 b W_2 \sim W_2 b W_1$ are different as elements of $\{a, b\}^*$.

Let $W_3 \in \{a, b\}^*$ be the largest common prefix of W_1 and W_2. As $W_1 \neq W_2$ and $|W_1| = |W_2|$, we must have that $|W_3| < |W_1|$. Thus, without loss of generality, there exist (possibly empty) words $W'_1, W'_2 \in \{a, b\}^*$ such that $W_1 = W_3 a W'_1$ and $W_2 = W_3 b W'_2$.

Replacing in $W_1 = W_3 a W'_1$ and $W_2 = W_3 b W'_2$ all the letters a by $xc_k w'$ and all the letters b by $xc_{k+1} w'$, we obtain two words $yxc_k w' t_1$ and $yxc_{k+1} w' t_2$, where $|y| = |W_3||xc_k w'|$, $|t_1| = |t_2|$ and $[yxc_k w' t_1]_{\underset{\sim}{D}} = [yxc_{k+1} w' t_2]_{\underset{\sim}{D}}$ in $D'_{\mathcal{M}}$. Note also that ${}_V y$, ${}_V x$, ${}_V c_k$, ${}_V c_{k+1}$, ${}_V w'$, ${}_V t_1$ and ${}_V t_2$ are cycles in Γ.

It is clear that

$$[yxw_1 t_1]_{\underset{\sim}{D}} = [yxw_2 t_1]_{\underset{\sim}{D}} = \cdots = [yxc_k w' t_1]_{\underset{\sim}{D}} = [yxc_{k+1} w' t_2]_{\underset{\sim}{D}} \text{ in } D'_{\mathcal{M}}.$$

Thus, taking the $k+2$ cycles ${}_V yx$, ${}_V w_1 t_1$, ${}_V w_2 t_1$, $\ldots$, ${}_V w_k t_1$, ${}_V c_{k+1} w' t_2$, we conclude that the result is also true for $k+1$. Therefore, by induction, it is true for $k = d$. □

Recall that all the vertices of the strongly connected component R belong to level T. Suppose that there are n vertices in R and denote these vertices by $V_1, \ldots, V_n$. Using Lemma 4.3 for $V_1 \in R$, we find $d+1$ cycles: ${}_{V_1} x, {}_{V_1} w_1, \ldots {}_{V_1} w_d$.

Denote by C the maximum of length of these cycles.

Lemma 4.4. *Let $N > T + C$, $M > N + C$ and let v_1, v_2 be words of length M from $\mathrm{Lan}_{P_{\mathcal{M}}}(a)$ such that v_1 and v_2 have common prefix of length N. Then there exists $\widetilde{v_2} \in \mathrm{Lan}_{P_{\mathcal{M}}}(a)$ such that $|\widetilde{v_2}| = M$, $\widetilde{v_2} \overset{D}{\sim} v_2$, and the words v_1 and $\widetilde{v_2}$ have common prefix of length $N+1$.*

Proof. Suppose $v_1 = pu_1$, $v_2 = pu_2$, $|p| = N$. Lemma 4.2 gives us a word t such that $|t| = N - |x|$, $t \in \mathrm{Lan}_{P_{\mathcal{M}}}(a)$ and the path ${}_{V_\varepsilon}t$ ends at V_1.

There exists a path ${}_{V_\varepsilon}txw_1$, and this path ends at V_1. We can prolong ${}_{V_\varepsilon}txw_1$ in arbitrary way and get a path ${}_{V_\varepsilon}txw_1s$ of length M.

Since txw_1s and $pu_2 = v_2 \in P_{\mathcal{M}} \cdot a^M$, there exists $g \in P_{\mathcal{M}}$ such that $g \cdot v_2 = txw_1s$.

The words $g \cdot v_2 = txw_1s$ and $g \cdot v_1$ have a common prefix tx of length N, and $\mathrm{Degree}_{\mathrm{Lan}_{P_{\mathcal{M}}}(a)}(tx) = d$. As the words w_i each begin with a different letter, there must exist some $1 \le i \le d$ such that the words txw_is and $g \cdot v_1$ have a common prefix of length $(N+1)$. Since $xw_1 \overset{D}{\sim} xw_i$, then $txw_is \overset{D}{\sim} txw_1s$.

Let $\widetilde{v_2} = g^{-1} \cdot txw_is$. The words $\widetilde{v_2}$ and v_1 have common prefix of length $(N+1)$, and it follows from Lemma 2.30 that $\widetilde{v_2} \overset{D}{\sim} v_2$. □

Lemma 4.5. *For all $k \in \mathbb{N}$, we have $|[P_{\mathcal{M}} \cdot a^k]_{\underset{\sim}{D}}| \le |A|^{T+2C+1}$.*

Proof. For $k \le T + 2C + 1$, the result is clear. Let us now assume that $k > T + 2C + 1$.

Let $P_{\mathcal{M}} \cdot a^{T+C+1} = \{v_1, v_2, \ldots, v_K\}$ and let us choose K words $w_1, w_2, \ldots, w_K \in P_{\mathcal{M}} \cdot a^k$ such that for all i, v_i is a prefix of w_i. Notice that $K \le |A|^{T+C+1}$.

Let $u \in P_{\mathcal{M}} \cdot a^k$ be an arbitrary element. By Lemma 3.1, there exists i such that u and w_i have the same prefix of length $T+C+1$. As $|u| = k > T+2C+1$, we have $k - (T + C + 1) > C$, so we can apply Lemma 4.4 to find an element $u_1 \in P_{\mathcal{M}} \cdot a^k$ such that $u_1 \overset{D}{\sim} u$ and u_1 shares with w_i a prefix of length $T+C+2$. If $k - (T + C + 2) > C$, we can apply Lemma 4.4 again to find an element u_2 sharing a prefix of length $T + C + 3$ with w_i and such that $u_2 \overset{D}{\sim} u_1 \overset{D}{\sim} u$. By repeating this process, we can find an element $u' \in P_{\mathcal{M}} \cdot a^k$ having a common prefix of length $k - C$ with w_i and such that $[u']_{\underset{\sim}{D}} = [u]_{\underset{\sim}{D}}$ in $D'_{\mathcal{M}}$.

Therefore, there are at most $K|A|^C$ different elements in $[P \cdot a^k]_{\underset{\sim}{D}}$. As $K \le |A|^{T+C+1}$, the result follows. □

By Lemmas 4.5 and3.6, we must have $|P_{\mathcal{M}} \cdot a^\omega| < \infty$, which is a contradiction. Thus, we conclude that $D'_{\mathcal{M}}$ must contain a free subsemigroup on two generators. This proves Proposition 4.1.

4.3. Proofs of Theorem 1.1 and Corollary 1.2

Proof of Theorem 1.1. Let $\mathcal{M} = (Q, A, \tau)$ be an invertible Mealy automaton. If every element of $D_{\mathcal{M}}$ is of finite order, then $D_{\mathcal{M}}$ clearly contains no free subsemigroup and so neither does $D'_{\mathcal{M}}$.

On the other hand, if there exists $x \in D_{\mathcal{M}}$ of infinite order, then by Lemma 3.6, $|P_{\mathcal{M}} \cdot x^\omega| = \infty$. Thus, it follows from Proposition 4.1 and the discussion preceding it that there exist $y, z \in D'_{\mathcal{M}}$ that freely generate a free subsemigroup in $D'_{\mathcal{M}}$.

This proves Theorem 2.19 and therefore Theorem 2.17. Hence, by Remark 2.16, Theorem 1.1 is proved.

Proof of Corollary 1.2. Let $\mathcal{M} = (Q, A, \tau)$ be an invertible and reversible Mealy automaton and let $G = P_{\widetilde{\mathcal{M}}}$ be the group generated by $\mathcal{M}$. Let us suppose that G contains an element of infinite order. Then, so does $P_{\mathcal{M}}$, by Proposition 2.25.

By Theorem 1.1, we conclude that $P_{\mathcal{M}}$ contains a subsemigroup of rank two. Therefore, G contains a subsemigroup of rank two and is thus of exponential growth.

To prove that no infinite virtually nilpotent group can be generated by an invertible and reversible automaton, it suffices to remark that a finitely generated torsion virtually nilpotent group is finite (see for example [4], Proposition 13.65). Thus, an infinite virtually nilpotent group must contain an element of infinite order. As such a group is of polynomial growth by a theorem of Wolf [13], the result follows.

5. Appendix. Orbits and languages

5.1. Regularity. It follows from Lemma 3.4 that for any invertible Mealy automaton $\mathcal{M} = (Q, A, \tau)$ and any periodic sequence $u^\omega \in A^\omega$, the set of prefixes of its orbit $P_{\mathcal{M}} \cdot u^\omega$ forms a regular language.

What happens if we consider some subgroup of $P_{\mathcal{M}}$ instead of the whole $P_{\mathcal{M}}$, or a pre-periodic word instead of a periodic one, or a non-invertible Mealy automaton?

Example 5.1. There exists an invertible Mealy automaton $\mathcal{N} = (Q_{\mathcal{N}}, A_{\mathcal{N}}, \tau_{\mathcal{N}})$, $a \in A_{\mathcal{N}}$ and $\psi \in Q_{\mathcal{N}}^*$ such that the set L of all prefixes of words in $\langle \psi \rangle \cdot a^\omega$ is not a regular language.

Indeed, let $Q_{\mathcal{N}} = \{\epsilon, s, t, x, y\}$ and

$$A_{\mathcal{N}} = \{a, b, c, d, e, f, g, h, i, j, k\}.$$

The structure of the automaton is given by its map $\tau\colon Q_{\mathcal{N}} \times A_{\mathcal{N}} \to A_{\mathcal{N}} \times Q_{\mathcal{N}}$. The state ϵ is the identity, and $\tau(\epsilon, a) = (a, \epsilon)$ for all $a \in A_{\mathcal{N}}$.

We claim that

(1) x and y commute in $P_{\mathcal{N}}$;

(2) if $m > 0$, then $y^{2^n} x^{2^m} s$ acts on $A_{\mathcal{N}}$ as $(a, b, e, d)(c, f)$ and $(y^{2^n} x^{2^m} s)^4 @ a = y^{2^{n+1}} x^{2^{m-1}} s$ in $P_{\mathcal{N}}$;

(3) $y^{2^n} xs$ acts on $A_{\mathcal{N}}$ as $(a, c, e, d)(b, f)$ and $(y^{2^n} xs)^4 @ a = y^{2^{n+1}} xt$ in $P_{\mathcal{N}}$;

(4) if $n > 0$, then $y^{2^n} x^{2^m} t$ acts on $A_{\mathcal{N}}$ as $(a, j, h, g)(i, k)$ and $(y^{2^n} x^{2^m} t)^4 @ a = y^{2^{n-1}} x^{2^{m+1}} t$ in $P_{\mathcal{N}}$;

(5) $yx^{2^m} t$ acts on $A_{\mathcal{N}}$ as $(a, k, h, g)(i, j)$ and $(yx^{2^m} t)^4 @ a = yx^{2^{m+1}} s$ in $P_{\mathcal{N}}$.

Table 2

letter	in state s	t	x	y
a	(b,ϵ)	(j,ϵ)	(a,ϵ)	(a,ϵ)
b	(e,s)	(b,ϵ)	(c,ϵ)	(b,ϵ)
c	(f,t)	(c,ϵ)	(b,ϵ)	(c,ϵ)
d	(a,ϵ)	(d,ϵ)	(d,ϵ)	(d,y)
e	(d,ϵ)	(e,ϵ)	(f,ϵ)	(e,y)
f	(c,t)	(f,ϵ)	(e,x)	(f,y)
g	(g,ϵ)	(a,ϵ)	(g,x)	(g,ϵ)
h	(h,ϵ)	(g,ϵ)	(h,x)	(i,ϵ)
i	(i,ϵ)	(k,ϵ)	(i,x)	(h,y)
j	(j,ϵ)	(h,t)	(j,ϵ)	(k,ϵ)
k	(k,ϵ)	(i,s)	(k,ϵ)	(j,ϵ)

To see that, we draw the dual Moore diagram of our transducer (see Figure 2). Several loops with empty outputs are not shown.

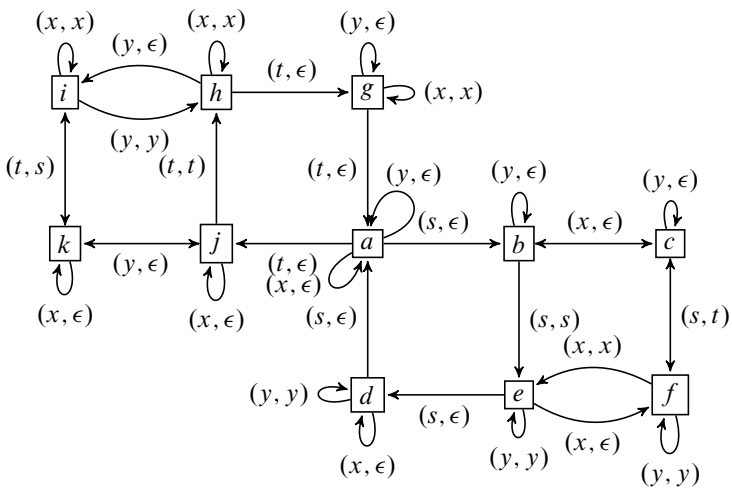

Figure 2. The dual Moore diagram of $\mathcal{N}$.

Consider the element $\psi := yxs \in Q_{\mathcal{N}}^*$. We will show that the set

$$L := \bigcup_{n,m\in\mathbb{N}} \psi^n \cdot a^m$$

is not a regular language. Assume the contrary and consider the following sequence:

$$\begin{array}{lll} \psi_0 := yxs, & \psi_1 := y^2xt, & \psi_2 := yx^2t, \\ \psi_3 := yx^4s, & \psi_4 := y^2x^2s, & \psi_5 := y^4xs, \quad \ldots, \end{array}$$

$$\psi_{i+1} = \begin{cases} y^{2^{n+1}} x^{2^{m-1}} s & \text{if } \psi_i = y^{2^n} x^{2^m} s, m > 0, \\ y^{2^{n+1}} xt & \text{if } \psi_i = y^{2^n} xs, \\ y^{2^{n-1}} x^{2^{m+1}} t & \text{if } \psi_i = y^{2^n} x^{2^m} t, n > 0, \\ yx^{2^{m+1}} s & \text{if } \psi_i = yx^{2^m} t. \end{cases}$$

Remark. This sequence of group elements corresponds to sequence of states (q_i, m_i, n_i) of some Minsky machine. This sequence can be presented as a path along the plane (see Figure 3).

For more about Minsky machines and automata groups, see [1].

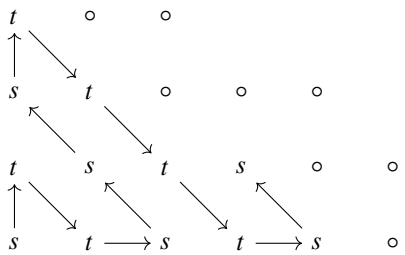

Figure 3. The sequence of elements ψ_i, where only the last letter of each ψ_i is shown.

By induction on n we show that the word a^n is a prefix of $\psi^N \cdot a^\omega$ if and only if $4^n \mid N$. We also show that $\psi^{4^n} @ a^n = \psi_n$. It means that $a^k b \in L$ if and only if ψ_k is of the form $y^{2^n} x^{2^m} s$ (not of the form $y^{2^n} x^{2^m} t$), i.e. $2N^2 + N \leq k \leq 2N^2 + 3N$ for some $N \in \mathbb{N}$.

We recall the following well-known lemma.

Lemma 5.2 (pumping lemma). *Let L be a regular language. Then there exists an integer $p \geq 1$ such that every string $w \in L$ of length at least p can be split into three substrings $w = xyz$, where $|y| \geq 1$, $|xy| < p$ and for any n the word $xy^n z$ is in L.*

Applying this lemma, we get $k_1, k_2 \in \mathbb{N}$ such that $a^{k_1 + nk_2} b \in L$ for any $n \in \mathbb{N}$. But for N big enough we can find k' such that $2N^2 + 3N < k_1 + k'k_2 < 2(N+1)^2 + (N+1)$, so $a^{k_1 + k'k_2} b \notin L$ and we have a contradiction with the regularity of L.

Remark. If we replace $Q_{\mathbb{N}}$ by $Q^3_{\mathbb{N}}$, we will get $\psi \in Q_{\mathbb{N}}$. In the following examples, $Q_{\mathbb{N}}$ will actually mean $Q^3_{\mathbb{N}}$.

Example 5.3. There exist an invertible Mealy automaton $\mathcal{M}_1 = (Q_1, A_1, \tau_1)$ and a pre-periodic sequence $vu^\omega \in A_1^*$ such that the set of prefixes of $Q_1^* \cdot vu^\omega$ does not form a regular language.

Indeed, let $\mathcal{N} = (Q_{\mathcal{N}}, A_{\mathcal{N}}, \tau_{\mathcal{N}})$ and $\psi \in Q_{\mathcal{N}}$ be as in Example 5.1. Then, the set $\bigcup_{n=0}^{\infty} \langle \psi \rangle \cdot a^n$ is not a regular language.

Let $Q_1 := Q_{\mathcal{N}}$, $A_1 := A_{\mathcal{N}} \cup \{a_1\}$, $\tau_1(q, \alpha) = \tau_{\mathcal{N}}(q, \alpha)$ for all $\alpha \in A_{\mathcal{N}}$ and $\tau_1(q, a_1) = (a_1, \psi)$ for any $q \in Q_1$.

Then for any $g \in Q_1^*$ we have $g \cdot a_1 a^n = a_1(\psi^{|g|} \cdot a^n)$, and the set of all prefixes of $Q_1^* \cdot a_1 a^\omega$ is not regular.

Example 5.4. There exist a non-invertible Mealy automaton $M_2 = (Q_2, A_2, \tau_2)$ and a periodic sequence $u^\omega \in A_2^\omega$ such that the set of all prefixes of $Q_2^* \cdot u^\omega$ is not a regular language.

Indeed, let $\mathcal{N} = (Q_{\mathcal{N}}, A_{\mathcal{N}}, \tau_{\mathcal{N}})$, $a \in A_{\mathcal{N}}$ and $\psi \in Q_{\mathcal{N}}$ be as in Example 5.1, so that the set of all prefixes of $\psi^* \cdot a^\omega$ is not a regular language. Let $Q_2 := Q_{\mathcal{N}} \cup \{r_1, r_2, r_3\}$, $A_2 = A_{\mathcal{N}} \cup \{0\}$, $\tau_2(q, \alpha) = \tau_{\mathcal{N}}(q, \alpha)$ for $\alpha \in A_{\mathcal{N}}$, $q \in Q_{\mathcal{N}}$. For any $a_i \in A_{\mathcal{N}}$, let $\tau_2(r_1, a_i) = (0, r_2)$, $\tau_2(r_2, a_i) = (a, r_2)$, $\tau_2(r_3, a_i) = (a, \epsilon)$. Finally, let $\tau_2(q, 0) = (0, \psi)$ for any $q \in Q_2$.

Then $(Q \cup \{r_2, r_3\})^* \cdot a^\omega \subseteq A_{\mathcal{N}}^\omega$ and $r_1 \cdot A_{\mathcal{N}}^\omega = 0a^\omega$. For any $g \in Q_2^*$ we have $g \cdot 0a^\omega = 0(\psi^{|g|} \cdot a^\omega)$. Hence, the prefixes of $Q_2^* \cdot a^\omega$ that start with 0 do not form a regular language. And, obviously, the whole language $\bigcup_{n=0}^{\infty} Q_2^* \cdot a^n$ is not regular.

But not all the results are negative.

Proposition 5.5. *Let $\mathcal{M} = (Q, A, \tau)$ be a bi-reversible Mealy automaton and let $u, v \in A^*$. Then the set of all prefixes of $Q^* \cdot uv^\omega$ forms a regular language.*

Proof. It is enough to consider the case where $u, v \in A$. We may also assume that for any $a \in A^*$, there is a formal inverse $a^{-1} \in A$ such that $(q@a)@a^{-1} = q$ and $(q@a) \cdot a^{-1} = (q \cdot a)^{-1}$ for all $q \in Q$.

Suppose that $g \cdot u = u'$, $g@u = g'$ for some $g \in Q^*$. Then, $g \cdot uv^\omega = u'g' \cdot v^\omega$. We know that $g' \cdot u^{-1} = (g@u) \cdot u^{-1} = (g \cdot u)^{-1} = u'^{-1}$, so $g \cdot uv^\omega = (g' \cdot u^{-1})^{-1} g' \cdot v^\omega$. Since $\mathcal{M}$ is reversible, $Q^* \cdot uv^\omega = \{(g \cdot u^{-1})^{-1} g \cdot v^\omega \mid g \in Q^*\}$.

We know that the set of prefixes of $Q^* \cdot v^\omega$ forms a regular language.

There is a homomorphism $p\colon Q^* \to \mathrm{Sym}(A)$ given by $p(g)(a) = g \cdot a$. We have a sequence of nested finite subgroups

$$\mathrm{Sym}(A) \geq p(\mathrm{St}_{Q^*}(v)) \geq p(\mathrm{St}_{Q^*}(v^2)) \geq p(\mathrm{St}_{Q^*}(v^3)) \geq \dots.$$

There must exist some $n_0 \in \mathbb{N}$ such that $p(\mathrm{St}_{Q^*}(v^n)) = p(\mathrm{St}_{Q^*}(v^{n_0}))$ for all $n \geq n_0$.

Lemma 5.6. *For all $n \geq n_0$, $a \in A$ and $w \in A^n$, the word $aw \in Q^* \cdot uv^n$ if and only if $w \in Q^* \cdot v^n$ and some prefix of aw belongs to $Q^* \cdot uv^{n_0}$.*

Proof. ($\Longrightarrow$) Trivial.

($\Longleftarrow$) Consider two subsets of $\mathrm{Sym}(A)$:

$$S_1 := \{p(g) \mid g \in Q^*, g \cdot v^n = w\} \text{ and } S_2 := \{p(g) \mid g \in Q^*, g \cdot v^{n_0} = w_{1,\ldots,n_0}\}.$$

By assumption, these sets are not empty, and it is obvious that $S_1 \subseteq S_2$. On the other hand, let $g_0 \in Q^*$ be such that $w = g_0 \cdot v^n$. Then,

$$S_1 = p(g_0 \,\mathrm{St}_{Q^*}(v^n)) = p(g_0 \,\mathrm{St}_{Q^*}(v^{n_0})) = S_2.$$

By assumption, there exists $g_1 \in Q^*$ such that $g_1 \cdot uv^{n_0} = aw_{1\ldots n_0}$. Thus, $(g_1@u) \cdot u^{-1} = a^{-1}$ and $(g_1@u) \cdot v^{n_0} = w_{1\ldots n_0}$. Therefore, $p(g_1@u) \in S_2$. As $S_2 = S_1$, there exists $g_2 \in Q^*$ such that $g_2 \cdot v^n = w$ and $p(g_2) = p(g_1@u)$. Let $g_3 = g_2@u^{-1}$. We have

$$g_3 \cdot uv^n = (g_2 \cdot u^{-1})^{-1} g_2 \cdot v^n = aw.$$

Hence, $aw \in Q^* \cdot uv^n$. △

By Lemma 5.6, the set of all prefixes of $Q^* \cdot uv^\omega$ can be expressed as the intersection of two regular languages. It therefore forms a regular language. □

5.2. Action on periodic sequences

Example 5.7. We will show that there exist an invertible Mealy automaton $\mathcal{M} = (Q, A, \tau)$ and an element $\psi \in P_{\mathcal{M}}$ such that

(1) s has infinite order in $P_{\mathcal{M}}$;

(2) for any $u \in A^*$ the orbit $\langle s \rangle \cdot u^\omega$ is finite.

As in Example 5.1, our construction is based on the realisation of Minsky machines as automata groups from [1].

Consider a Minsky machine M with a set of instructions $S = \{a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2\}$. The initial state of M is $(a_1, 0, 0)$, and each next state is determined by the previous one by the following rules:

$$\begin{aligned}
(a_1, m, n) &\longmapsto (b_1, m+1, n+1);\\
(a_2, m, n) &\longmapsto (b_2, m+1, n+1);\\
(b_1, m, n) &\longmapsto (d_1, m-1, n);\\
(b_2, m, n) &\longmapsto (d_2, m, n-1);\\
(c_1, m, n) &\longmapsto (a_1, m-1, n);\\
(c_2, m, n) &\longmapsto (a_2, m, n-1);\\
(d_1, m, n) &\longmapsto (m = 0?a_2 : c_1, m, n);\\
(d_2, m, n) &\longmapsto (n = 0?a_1 : c_2, m, n).
\end{aligned}$$

Here ? : is the ternary operator. There is no final state. In terms of [1], instructions a_1 and a_2 are of type III, b_1 and c_1 are of type IV, b_2 and c_2 are of type V, d_1 has type VII and d_2 has type VIII.

The first states of a working machine are

$$\begin{aligned}(a_1,0,0) &\longmapsto (b_1,1,1) \longmapsto (d_1,0,1) \longmapsto (a_2,0,1) \longmapsto (b_2,1,2)\\ &\longmapsto (d_2,1,1) \longmapsto (c_2,1,1) \longmapsto (a_2,1,0) \longmapsto (b_2,2,1) \longmapsto (d_2,2,0)\\ &\longmapsto (a_1,2,0) \longmapsto (b_1,3,1) \longmapsto (d_1,2,1) \longmapsto (c_1,2,1) \longmapsto (a_1,1,1)\\ &\longmapsto (b_1,2,2) \longmapsto \cdots .\end{aligned}$$

It's easy to see that this machine works in a similar way to the machine from example 5.1, and the sequence of its instruction types III, IV, VII, III, V, ... is not periodic.

We consider the automaton $\mathcal{M}$ with stateset $Q = S^{\pm 1} \sqcup \{\varepsilon, x, x^{-1}, y, y^{-1}\}$ and alphabet

$$A = \{\mathrm{III}_i, \mathrm{IV}_i, \mathrm{V}_i, \mathrm{VII}_j, \mathrm{VIII}_j \mid i = 1, 2, \bar{1}, \bar{2};\ j = 1, \ldots, 4, \bar{1}, \ldots, \bar{4}\}.$$

The state ε is the identity, and $\tau(\varepsilon, a) = (a, \varepsilon)$ for all $a \in A$. All "formal inverses" will be inverse elements in $P_{\mathcal{M}}$.

We define τ in the same way as in section 3.1 of [1]. For example, for elements a_1, a_2 of type III and for all $t \in S \setminus \{a_1, a_2\}$, we define τ as in Table 3. Since M does not stop, the element $\psi := xya_1$ has infinite order in $P_{\mathcal{M}}$.

Table 3

		input letter			
		III_1	III_2	$\mathrm{III}_{\bar{1}}$	$\mathrm{III}_{\bar{2}}$
in state	x	(III_1, x)	(III_2, x)	$(\mathrm{III}_{\bar{1}}, x^{-1})$	$(\mathrm{III}_{\bar{2}}, x^{-1})$
	y	(III_1, y)	(III_2, y)	$(\mathrm{III}_{\bar{1}}, y^{-1})$	$(\mathrm{III}_{\bar{1}}, y^{-1})$
	a_1	(III_2, b_1)	$(\mathrm{III}_1, \epsilon)$	$(\mathrm{III}_{\bar{2}}, \epsilon)$	$(\mathrm{III}_{\bar{1}}, (b_1)^{-1})$
	a_2	(III_2, b_2)	$(\mathrm{III}_1, \epsilon)$	$(\mathrm{III}_{\bar{2}}, \epsilon)$	$(\mathrm{III}_{\bar{1}}, (b_2)^{-1})$
	t	$(\mathrm{III}_{\bar{1}}, \epsilon)$	$(\mathrm{III}_{\bar{2}}, \epsilon)$	$(\mathrm{III}_1, \epsilon)$	$(\mathrm{III}_2, \epsilon)$

We construct a labelled, directed graph Γ, whose vertices are elements of $P_{\mathcal{M}}$. For $g \in P_{\mathcal{M}}$ and $a \in A$, consider the minimal $d(g, a)$ such that $g^{d(g,a)} \cdot a = a$. In our graph we put an edge from g to $g^{d(g,a)} @ a$ with label $(a, d(g, a))$.

For a sequence $w = a_1 a_2 \cdots \in A^{\omega}$ we find a path starting at xya_1 whose edges have first labels $a_1, a_2, \ldots$. The product of second labels of its edges is equal to the size of the orbit of w.

Suppose that in M there is a step $(s, m, n) \mapsto (s', m', n')$. Consider $g = (y^{2^n} x^{2^m} s)^{\pm h}$, where $h \in \langle x, y \rangle$. In [1] it is calculated that all the edges from g go to ε or to elements of form $(y^{2^{n'}} x^{2^{m'}} s')^{\pm h'}$, where $h' \in \langle x, y \rangle$; and all the

edges that do not go to ε have labels that correspond to s. E.g., an edge from $y^{2^n} x^{2^m} d_1$ either has its first label of type VII_j or leads to ε.

Since the sequence of instructions of working M is not periodic, any periodic sequence of labels in Γ leads to ε after a finite number of steps, and the orbit $\langle \psi \rangle \cdot u^\omega$ of any periodic sequence $u^\omega \in A^\omega$ is finite.

6. Outlook

We proved that if $\mathcal{M}$ is a reversible Mealy automaton, the semigroup $P_{\mathcal{M}}$ generated by $\mathcal{M}$ is either periodic or contains a free subsemigroup of rank two. Obviously, if $P_{\mathcal{M}}$ is finite, then it is periodic, but it is natural to ask if the converse holds. More precisely, does there exist a reversible Mealy automaton that generates an infinite periodic semigroup?

To the best of our knowledge, the answer to this question is not known, but there are some partial results in the case of invertible and reversible automata. In this case, by Proposition 2.25, the question reduces to the Burnside problem (i.e. the question of the existence of an infinite finitely generated periodic group) for the class of groups generated by invertible and reversible automata. It was shown in [6] and in [3] that an infinite group generated by an invertible and reversible but not bireversible automaton must contain an element of infinite order. For bireversible automata, it was proved by Klimann in [9] that a group generated by a 2-state bireversible Mealy automaton cannot be infinite and torsion. Klimann, Picantin and Savchuk later proved in [11] that the same result holds for groups generated by a connected 3-state bireversible automaton.

By Lemma 3.6 and Theorem 2.34, we can reformulate our question as follows: does there exist an invertible automaton $\mathcal{M}$ such that the group $P_{\mathcal{M}}$ is infinite, but any periodic sequence u^ω has finite orbit?

There are also some partial results from this point of view. Example 5.7 shows that this is possible if we consider an infinite subgroup of an automaton group. On the other hand, D'Angeli, Francoeur, Rodaro and Wächter showed in [2] that for any finitely generated subgroup of an automaton group, there is a sequence (not necessarily periodic) with an infinite orbit.

6.1. Algorithmic questions. We know that for an invertible automaton $\mathcal{M} = (Q, A, \tau)$ and for some $u \in A^*$, the set of all prefixes of $P_{\mathcal{M}} \cdot u^\omega$ forms a regular language, but we do not know of an effective way to describe it. We do not even know if there exists an algorithm that, for a given invertible automaton $\mathcal{M} = (Q, A, \tau)$ and a given word $u \in A^*$, determines whether or not the orbit $P_{\mathcal{M}} \cdot u^\infty$ is finite.

Note that for a cyclic subgroup of $P_{\mathcal{M}}$ this problem is undecidable [1, 5].

References

[1] L. Bartholdi and I. Mitrofanov, The word and order problems for self-similar and automata groups. *Groups Geom. Dyn.* **14** (2020), no. 2, 705–728. Zbl 07227243 MR 4118634

[2] D. D'angeli, D. Francoeur, E. Rodaro, and J. P. Wächter, Infinite automaton semigroups and groups have infinite orbits. *J. Algebra* **553** (2020), 119–137. Zbl 07181388 MR 4074167

[3] D. D'Angeli and E. Rodaro, Freeness of automaton groups vs boundary dynamics. *J. Algebra* **462** (2016), 115–136. Zbl 1454.20069 MR 3519502

[4] C. Druțu and M. Kapovich, *Geometric group theory.* With an appendix by B. Nica. American Mathematical Society Colloquium Publications, 63. American Mathematical Society, Providence, R.I., 2018. Zbl 1447.20001 MR 3753580

[5] P. Gillibert, An automaton group with undecidable order and Engel problems. *J. Algebra* **497** (2018), 363–392. Zbl 1427.20040 MR 3743185

[6] T. Godin, I. Klimann, and M. Picantin, On torsion-free semigroups generated by invertible reversible Mealy automata. In A.-H. Dediu, E. Formenti, C. Martín-Vide and B. Truthe (eds.), *Language and automata theory and applications.* Proceedings of the 9th International Conference (LATA 2015) held in Nice, March 2–6, 2015. Lecture Notes in Computer Science, 8977. Springer, Cham, 2015, 328–339. Zbl 1405.68197 MR 3344813

[7] R. I. Grigorchuk, On Burnside's problem on periodic groups. *Funktsional. Anal. i Prilozhen.* **14** (1980), no. 1, 53–54. In Russian. Engish translation, *Functional Anal. Appl.* **14** (1980), no. 1, 41–43. Zbl 0595.20029 MR 565099

[8] R. I. Grigorchuk, On Milnor's problem of group growth. *Dokl. Akad. Nauk SSSR* **271** (1983), no. 1, 30–33. In Russian. English translation, *Soviet Math. Dokl.* **28** (1983), no. 1, 23–26. Zbl 0547.20025 MR 712546

[9] I. Klimann, Automaton semigroups: the two-state case. *Theory Comput. Syst.* **58** (2016), no. 4, 664–680. Zbl 1345.20074 MR 3483907

[10] I. Klimann, To infinity and beyond. In J. Chatzigiannakis, Ch. Kaklamanis, D. Marx, and D. Sannella (eds), *45th International Colloquium on Automata, Languages, and Programming.* ICALP 2018, Prague, Czech Republic, July 9–13, 2018. LIPIcs. Leibniz International Proceedings in Informatics, 107 Schloss Dagstuhl. Leibniz-Zentrum für Informatik, Wadern, 2018, Art. No. 131, 12 pp.. Zbl 07376058 MR 3830062

[11] I. Klimann, M. Picantin, and D. Savchuk, A connected 3-state reversible Mealy automaton cannot generate an infinite Burnside group. *Internat. J. Found. Comput. Sci.* **29** (2018), no. 2, 297–314. Zbl 1387.68169 MR 3786472

[12] D. Savchuk and Y. Vorobets, Automata generating free products of groups of order 2. *J. Algebra* **336** (2011), 53–66. Zbl 1239.20032 MR 2802530

[13] J. A. Wolf, Growth of finitely generated solvable groups and curvature of Riemannian manifolds. *J. Differential Geometry* **2** (1968), 421–446. Zbl 0207.51803 MR 0248688

[14] G. Zappa, Sulla costruzione dei gruppi prodotto di due dati sottogruppi permutabili tra loro. In *Atti Secondo Congresso Un. Mat. Ital., Bologna, 1940.* Edizioni Cremonense, Rome, 1942, 119–125. JFM 68.0037.02 Zbl 0026.29104 MR 0019090

Received December 16, 2019

Dominik Francoeur, UMPA, ENS de Lyon site Monod, 46 Allée d'Italie,
69364 Lyon Cedex 7, France

e-mail: dominik.francoeur@ens-lyon.fr

Ivan Mitrofanov, DMA, École Normale Supérieure, 45 rue d'Ulm, 75230 Paris Cedex 05, France

e-mail: phortim@yandex.ru