To Infinity and Beyond

Ines Klimann

To Infinity and Beyond*

Ines Klimann
Univ Paris Diderot, Sorbonne Paris Cité, IRIF,
UMR 8243 CNRS, F-75013 Paris, France,
klimann@irif.fr

September 4, 2017

Abstract

We prove that if a group generated by a bireversible Mealy automaton contains an element of infinite order, its growth blows up and is necessarily exponential. As a direct consequence, no infinite virtually nilpotent group can be generated by a bireversible Mealy automaton.

The study on how (semi)groups grow has been highlighted since Milnor's question on the existence of groups of intermediate growth (faster than any polynomial and slower than any exponential) in 1968 [12], and the very first example of such a group given by Grigorchuk [5]. Uncountably many examples have followed this first one, see for instance [6]. Bartholdi and Erschler have even obtained results on precise computations of growth, in particular they proved that if a function satisfies some frame property, then there exists a finitely generated group with growth equivalent to it [1]. Besides, for now, intermediate growth and automaton groups, that is groups generated by Mealy automata, seem to have a very strong link, since the only known examples of intermediate growth groups are either automaton groups, or based on such groups.

There exists no criterium to test if a Mealy automaton generates a group of intermediate growth and it is not even known if this property is decidable. However, there is no known example in the litterature of a bireversible Mealy automaton generating an intermediate growth group and it is legitimate to wonder if it is possible. This article enter in this scope. We prove that if there exists at least one element of infinite order in a group generated by a bireversible Mealy automaton, then its growth is necessarily exponential. It has been conjuctered, and proved in some cases [4], that an infinite group generated by a bireversible Mealy automaton always has an element of infinite order, which suggests that, indeed, a group generated by a bireversible Mealy automaton either is finite, or has exponential growth.

Finally, let us mention the work by Brough and Cain to obtain some criteria to decide if a semigroup is an automaton semigroup [2]. Our work can be seen as partially answering a similar question: can a given group be generated by a bireversible Mealy automaton? A consequence of our result is that no infinite virtually nilpotent group can be.

This article is organized as follows. In Section 1, we define the automaton groups and the growth of a group, and give some properties on the connected components of the powers of a Mealy automaton. In Section 2, we study the behaviour of some equivalence classes of words on the state set of a Mealy automaton. Finally, the main result takes place in Section 3.

1 Basic notions

In all the article, if E is a finite set, its cardinality is denoted by $|E|$. A *finite word* of *length* n on E is a finite sequence of n elements of E and is denoted classically as the concatenation of its elements. The set of finite words over E is denoted by E^*, the set of non-empty finite words by E^+, and the set of words of length n by E^n. In general the elements of E are written in plain letters, *e.g.* q, while the words on E are written in bold letters, *e.g.* $\mathbf{u}$. The length of $\mathbf{u}$ is denoted by $|\mathbf{u}|$, its letters are numbered from 0

*This work was partially supported by the French *Agence Nationale pour la Recherche*, through the Project **MealyM** ANR-JS02-012-01.

to $\mathbf{u} - 1$ and if i is an integer, its ($i \mod |\mathbf{u}|$)-th letter is denoted by $\mathbf{u}\{i\}$; for example its first letter is $\mathbf{u}\{0\}$, while its last letter is $\mathbf{u}\{-1\}$. If L is a set of words on E, $L\{i\}$ denotes the set $\{\mathbf{u}\{i\} \mid \mathbf{u} \in L\}$.

1.1 Semigroups and groups generated by Mealy automata

We first recall the formal definition of an automaton. A *(finite, deterministic, and complete) automaton* is a triple $\big(Q, \Sigma, \delta = (\delta_i \colon Q \to Q)_{i\in\Sigma}\big)$, where the *state set* Q and the *alphabet* Σ are non-empty finite sets, and the δ_i are functions.

A *Mealy automaton* is a quadruple $\mathcal{A} = (Q, \Sigma, \delta, \rho)$, such that (Q, Σ, δ) and (Σ, Q, ρ) are both automata. In other terms, a Mealy automaton is a complete, deterministic, letter-to-letter transducer with the same input and output alphabet. Its *size* is the cardinality of its state set and is denoted by $\#\mathcal{A}$.

The graphical representation of a Mealy automaton is standard, see Figure 1. But, for practical reasons, we use sometimes other graphical representations for the transitions. For example the transition from x to z with input letter 0 and output letter 1 in the automaton of Figure 1 can be represented

$$\text{either by} \quad x \xrightarrow{0|1} z\,, \qquad \text{or by} \quad x \quad \underset{\displaystyle\downarrow\atop 1}{\overset{0}{\longrightarrow}} \quad z \ .$$

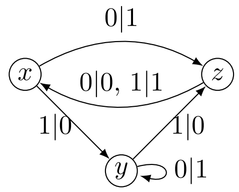

Figure 1: The Aleshin automaton.

Let $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ be a Mealy automaton. Each state $q \in Q$ defines a mapping from Σ^* into itself, recursively by:

$$\forall i \in \Sigma,\ \forall \mathbf{s} \in \Sigma^*, \qquad \rho_q(i\mathbf{s}) = \rho_q(i)\rho_{\delta_i(q)}(\mathbf{s})\ .$$

The image of the empty word is itself. For each $q \in Q$, the mapping ρ_q is length-preserving and prefix-preserving. We say that ρ_q is the function *induced* by q. For $\mathbf{u} = q_1 \cdots q_n \in Q^n$ with $n > 0$, set $\rho_{\mathbf{u}} \colon \Sigma^* \to \Sigma^*, \rho_{\mathbf{u}} = \rho_{q_n} \circ \cdots \circ \rho_{q_1}$.

The semigroup of mappings from Σ^* to Σ^* generated by $\{\rho_q, q \in Q\}$ is called the *semigroup generated by* $\mathcal{A}$ and is denoted by $\langle \mathcal{A} \rangle_+$.

A Mealy automaton $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ is *invertible* if the functions ρ_q are permutations of the alphabet Σ. In this case, the functions induced by the states are permutations on words of the same length and thus we may consider the group of mappings from Σ^* to Σ^* generated by $\{\rho_q, q \in Q\}$: it is called the *group generated by* $\mathcal{A}$ and is denoted by $\langle \mathcal{A} \rangle$.

When $\mathcal{A}$ is invertible, define its *inverse* $\mathcal{A}^{-1}$ as the Mealy automaton with state set Q^{-1}, a disjoint copy of Q, and alphabet Σ, where the transition $p^{-1} \xrightarrow{j|i} q^{-1}$ belongs to $\mathcal{A}^{-1}$ if and only if the transition $p \xrightarrow{i|j} q$ belongs to $\mathcal{A}$. Clearly the action induced by the state p^{-1} of $\mathcal{A}^{-1}$ is the reciprocal of the action induced by the corresponding state p in $\mathcal{A}$.

A Mealy automaton $(Q, \Sigma, \delta, \rho)$ is *reversible* if the functions δ_i induced on Q by the input letters of the transitions are permutations. The connected components of a reversible automaton are strongly connected. In a reversible automaton of state set Q and alphabet Σ, for any word $\mathbf{s} \in \Sigma^*$ and any state q, there exists exactly one path in the automaton with label $\mathbf{s}$ and final state q, hence we can consider the *backtrack application* induced by q: it associates to $\mathbf{s}$ the output label $\mathbf{t} \in \Sigma^{|\mathbf{s}|}$ of this single path.

A Mealy automaton is *coreversible* if the functions induced on Q by the letters as output letters of the transitions are permutations.

A Mealy automaton is *bireversible* if it is both reversible and coreversible. It is quite simple to see that the applications and the backtrack applications induced by the states of a bireversible automaton are permutations.

Two Mealy automata are said to be *isomorphic* if they are identical up to the labels of their states.

We extend to δ the former notations on ρ, in a natural way. Hence $\delta_i\colon Q^* \to Q^*, i \in \Sigma$, are the functions extended to Q^*, and for $\mathbf{s} = i_1 \cdots i_n \in \Sigma^n$ with $n > 0$, we set $\delta_{\mathbf{s}}\colon Q^* \to Q^*,\ \delta_{\mathbf{s}} = \delta_{i_n} \circ \cdots \circ \delta_{i_1}$.

1.2 Growth of a semigroup or of a group

Let H be a semigroup generated by a finite set S. The *length* of an element g of the semigroup, denoted by $|g|$, is the length of its shortest decomposition as a product of generators:

$$|g| = \min\{n \mid \exists s_1, \ldots, s_n \in S,\ g = s_1 \cdots s_n\}\ .$$

The *growth function* γ_H^S of the semigroup H with respect to the generating set S enumerates the elements of H with respect to their length:

$$\gamma_H^S(n) = |\{g \in H\ ;\ |g| \leq n\}|\ .$$

The *growth functions* of a group are defined similarly by taking symmetrical generating sets.

The growth functions corresponding to two generating sets are equivalent [11], so we may define the *growth* of a group or a semigroup as the equivalence class of its growth functions. Hence, for example, a finite (semi)group has a bounded growth, while an infinite abelian (semi)group has a polynomial growth, and a non-abelian free (semi)group has an exponential growth.

It is quite easy to obtain groups of polynomial or exponential growth. Answering a question of Milnor [12], Grigorchuk gave an example of an automaton group of intermediate growth [5]: faster than any polynomial, slower than any exponential, opening thus a new classification criterium for groups, that has been deeply studied since this seminal article (see [7] and references therein). Besides, intermediate growth and automaton groups seem to have a very strong link, since the only known examples of intermediate growth groups in the literature are based on automaton groups.

Note an important point for our purpose: let G be a group finitely generated by S, and $(I_n)_{n>0}$ a sequence of subsets of G, compatible with the length of the elements, *i.e.* the sets I_n are pairwise distinct and the elements of I_n have all length less than or equal to n. The growth function of $(I_n)_{n>0}$ is given by $(\sum_{k\leq n} |I_n|)_{n>0}$; if it grows exponentially, then so does G. In the same spirit, a group which admits a subgroup of exponential growth grows exponentially.

1.3 The powers of a Mealy automaton and their connected components

The powers of a Mealy automaton have been shown to play an important role in the finiteness and the order problem for an automaton (semi)groups, as highlighted in [8, 10, 4]. The *n-th power* of the automaton $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ is the Mealy automaton

$$\mathcal{A}^n = \big(\ Q^n, \Sigma, (\delta_i\colon Q^n \to Q^n)_{i\in\Sigma}, (\rho_{\mathbf{u}}\colon \Sigma \to \Sigma)_{\mathbf{u}\in Q^n}\ \big)\ .$$

Note that the powers of a reversible (*resp.* bireversible) Mealy automaton are reversible (*resp.* bireversible).

The (semi)group generated by a connected component of some power of $\mathcal{A}$ is a sub(semi)group of the (semi)group generated by $\mathcal{A}$.

Let $\mathbf{u}$ and $\mathbf{v}$ be elements of Q^+ and $\mathcal{C}$ be a connected component of some power of $\mathcal{A}$: $\mathbf{v}$ *can follow* $\mathbf{u}$ *in* $\mathcal{C}$ if $\mathbf{uv}$ is the prefix of some state of $\mathcal{C}$. We denote by $\{\mathbf{u}? \looparrowright \mathcal{C}\}$ the set of the states which can follow $\mathbf{u}$ in $\mathcal{C}$:

$$\{\mathbf{u}? \looparrowright \mathcal{C}\} = \{q \in Q \mid \mathbf{u}q \text{ is the prefix of some state of } \mathcal{C}\}\ .$$

We define similarly the fact that $\mathbf{v}$ *can precede* $\mathbf{u}$ in $\mathcal{C}$ if $\mathbf{vu}$ is the suffix of some state of $\mathcal{C}$, and we introduce the set

$$\{?\mathbf{u} \looparrowright \mathcal{C}\} = \{q \in Q \mid q\mathbf{u} \text{ is the suffix of some state of } \mathcal{C}\}\ .$$

The aim of this section is to give some intuition on the links between the connected components of consecutive powers of $\mathcal{A}$. Since a word can be extended with a prefix or a suffix, most of the results exposed here are expressed in both cases, but only the first result is proved in both cases, to show how bireversibility allow to consider similarly the actions and the backtrack actions.

Lemma 1. *Let $\mathcal{A}$ be a bireversible Mealy automaton with state set Q and $\mathcal{C}$ a connected component of one of its powers. If $\mathbf{u} \in Q^+$ is a proper prefix of some state of $\mathcal{C}$, then the cardinality of the set $\{\mathbf{u}? \looparrowright \mathcal{C}\}$ depends only on the length of $\mathbf{u}$.*

Proof. Suppose that $\mathbf{u}'$ is such that $\mathbf{u}\mathbf{u}'$ is a state of $\mathcal{C}$, and let $\mathbf{v}$ be a prefix of some state $\mathbf{v}\mathbf{v}'$ of $\mathcal{C}$ with the same length as $\mathbf{u}$. Since $\mathcal{C}$ is a connected component in a reversible Mealy automaton, it is strongly connected, so there exists a word $\mathbf{s} \in \Sigma^*$ such that $\delta_{\mathbf{s}}(\mathbf{u}\mathbf{u}') = \mathbf{v}\mathbf{v}'$. Now, consider the action induced by $\mathbf{s}$ on $\mathbf{u}p$, for $p \in \{\mathbf{u}? \looparrowright \mathcal{C}\}$:

$$\begin{array}{ccc} & \mathbf{s} & \\ \mathbf{u} & \longrightarrow & \mathbf{v} \\ & \mathbf{s}' & \\ p & \longrightarrow & p' \end{array}$$

Since the automaton $\mathcal{A}$ is reversible, the action induced by $\mathbf{s}'$ is a permutation of Q, and we have

$$|\{\mathbf{u}? \looparrowright \mathcal{C}\}| \leq |\{\mathbf{v}? \looparrowright \mathcal{C}\}| \,.$$

The reciprocal inequality is obtained symmetrically. ☐

Lemma 2. *Let $\mathcal{A}$ be a bireversible Mealy automaton with state set Q and $\mathcal{C}$ a connected component of one of its powers. If $\mathbf{u} \in Q^+$ is a proper suffix of some state of $\mathcal{C}$, then the cardinality of the set $\{?\mathbf{u} \looparrowright \mathcal{C}\}$ depends only on the length of $\mathbf{u}$.*

Proof. Suppose that $\mathbf{u}'$ is such that $\mathbf{u}'\mathbf{u}$ is a state of $\mathcal{C}$, and let $\mathbf{v}$ be a suffix of some state $\mathbf{v}'\mathbf{v}$ of $\mathcal{C}$ with the same length as $\mathbf{u}$. Since $\mathcal{C}$ is a connected component in a reversible Mealy automaton, it is strongly connected, so there exist words $\mathbf{s}, \mathbf{t} \in \Sigma^*$ such that $\delta_{\mathbf{s}}(\mathbf{u}'\mathbf{u}) = \mathbf{v}'\mathbf{v}$ and $\rho_{\mathbf{u}'\mathbf{u}}(\mathbf{s}) = \mathbf{t}$:

$$\begin{array}{ccc} & \mathbf{s} & \\ \mathbf{u}' & \longrightarrow & \mathbf{v}' \\ & \mathbf{s}' & \\ \mathbf{u} & \longrightarrow & \mathbf{v} \\ & \mathbf{t} & \end{array}$$

Now, consider the backtrack action induced by $\mathbf{t}$ on $p\mathbf{u}$, for $p \in \{?\mathbf{u} \looparrowright \mathcal{C}\}$:

$$\begin{array}{ccc} p & \longrightarrow & p' \\ & \mathbf{s}' & \\ \mathbf{u} & \longrightarrow & \mathbf{v} \\ & \mathbf{t} & \end{array}$$

Since the automaton $\mathcal{A}$ is bireversible, the backtrack action induced by $\mathbf{s}'$ is a permutation of Q, and we have

$$|\{?\mathbf{u} \looparrowright \mathcal{C}\}| \leq |\{?\mathbf{v} \looparrowright \mathcal{C}\}| \,.$$

The reciprocal inequality is obtained symmetrically. ☐

Consider a state q of $\mathcal{A}$. For any integer $n > 0$, we denote by $\mathrm{cc}(q^n)$ the connected component of q^n in $\mathcal{A}^n$. The sequence of such components has some properties which we give here. These properties can be seen as properties of the branch represented by q^ω in the Schreier trie of $\mathcal{A}$ (also known as the orbit tree of the dual of $\mathcal{A}$) which has been introduced in [10, 4] (to keep this article self-contained, we give here only the properties of this branch, but for a more global intuition on the constructions, the reader can consult these references).

The first point is given by Lemma 1: for any $n > 0$, the component $\mathrm{cc}(q^{n+1})$ can be seen as several full copies of the component $\mathrm{cc}(q^n)$; indeed, if $\mathbf{u}$ and $\mathbf{v}$ are states of $\mathrm{cc}(q^n)$, then in $\mathrm{cc}(q^{n+1})$ there are as many states with prefix $\mathbf{u}$ as states with prefix $\mathbf{v}$, *i.e.*

$$\forall \mathbf{u} \in \mathrm{cc}(q^n), \forall \mathbf{v} \in \mathrm{cc}(q^n),\ |\{\mathbf{u}? \looparrowright \mathrm{cc}(q^{n+1})\}| = |\{\mathbf{v}? \looparrowright \mathrm{cc}(q^{n+1})\}| \,.$$

Hence the ratio between the size of $\mathrm{cc}(q^{n+1})$ and the size of $\mathrm{cc}(q^n)$ is necessarily an integer: it is the cardinality of the set $\{\mathbf{u}? \looparrowright \mathrm{cc}(q^{n+1})\}$ for any state $\mathbf{u}$ of $\mathrm{cc}(q^n)$, and in particular for $\mathbf{u} = q^n$.

We define by

$$\left(\frac{\#\,\mathrm{cc}(q^{n+1})}{\#\,\mathrm{cc}(q^{n})}\right)_{n>0} = \left(|\{q^n ? \looparrowright \mathrm{cc}(q^{n+1})\}|\right)_{n>0}$$

the *sequence of ratios* associated to the state q.

Lemma 3. *Let $\mathcal{A}$ be a bireversible Mealy automaton with state set Q, $q \in Q$ a state of $\mathcal{A}$, and $\mathbf{u}$ and $\mathbf{v}$ be two elements of Q^+. If $\mathbf{uv}$ is a state of $\mathrm{cc}(q^{|\mathbf{uv}|})$, then $\mathbf{v}$ is a state of $\mathrm{cc}(q^{|\mathbf{v}|})$ and*

$$\{\mathbf{uv}? \looparrowright \mathrm{cc}(q^{|\mathbf{uv}|+1})\} \subseteq \{\mathbf{v}? \looparrowright \mathrm{cc}(q^{|\mathbf{v}|+1})\}\ .$$

Proof. Take $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ and let $p \in \{\mathbf{uv}? \looparrowright \mathrm{cc}(q^{|\mathbf{uv}|+1})\}$.

Since $\mathcal{A}$ is reversible, there exist a word $\mathbf{s} \in \Sigma^*$ such that $\delta_{\mathbf{s}}(\mathbf{uv}p) = q^{|\mathbf{uv}|+1}$:

$$\begin{array}{ccc} & \mathbf{s} & \\ \mathbf{u} & \longrightarrow & q^{|\mathbf{u}|} \\ & \mathbf{s}' & \\ \mathbf{v} & \longrightarrow & q^{|\mathbf{v}|} \\ & \mathbf{s}'' & \\ p & \longrightarrow & q \\ & \downarrow & \end{array}$$

Hence $\delta_{\mathbf{s}'}(\mathbf{v}) = q^{\mathbf{v}}$ and so $\mathbf{v} \in \mathrm{cc}(q^{|\mathbf{v}|})$, and $\delta_{\mathbf{s}'}(\mathbf{v}p) = q^{|\mathbf{v}|+1}$, which means that $p \in \{\mathbf{v}? \looparrowright \mathrm{cc}(q^{|\mathbf{v}|+1})\}$. ☐

Lemma 4. *Let $\mathcal{A}$ be a bireversible Mealy automaton with state set Q, $q \in Q$ a state of $\mathcal{A}$, and $\mathbf{u}$ and $\mathbf{v}$ be two elements of Q^+. If $\mathbf{uv}$ is a state of $\mathrm{cc}(q^{|\mathbf{uv}|})$, then $\mathbf{u}$ is a state of $\mathrm{cc}(q^{|\mathbf{u}|})$ and*

$$\{?\mathbf{uv} \looparrowright \mathrm{cc}(q^{|\mathbf{uv}|+1})\} \subseteq \{?\mathbf{u} \looparrowright \mathrm{cc}(q^{|\mathbf{u}|+1})\}\ .$$

As $\{q^n? \looparrowright \mathrm{cc}(q^{n+1})\} \subseteq \{q^{n+1}? \looparrowright \mathrm{cc}(q^{n+2})\}$ by Lemma 3, it is straightforward to see that the sequence of ratios associated to q decreases:

$$\forall n > 0,\ \frac{\#\,\mathrm{cc}(q^{n+2})}{\#\,\mathrm{cc}(q^{n+1})} \leq \frac{\#\,\mathrm{cc}(q^{n+1})}{\#\,\mathrm{cc}(q^{n})}\ ,$$

and hence is ultimately constant. We say that q *has a constant ratio* if this sequence is in fact constant, and then the unique value of the sequence of ratios associated to q is called the *ratio of* q.

It has been proven in [10] that q induces an action of infinite order if and only if the sizes of the components $(\mathrm{cc}(q^n))_{n>0}$ are unbounded, *i.e.* the limit of the sequence of ratios associated to q is greater than 1.

We study now some properties on followers and predecessors in the components $\mathrm{cc}(q^n)$, when q has a constant ratio.

The next lemma is an improvement of Lemma 3.

Lemma 5. *Let $\mathcal{A}$ be a bireversible Mealy automaton, and q be a state of $\mathcal{A}$ of constant ratio. Let $\mathbf{u}$ and $\mathbf{v}$ be two elements of Q^+ such that $\mathbf{uv}$ is a state of $\mathrm{cc}(q^{|\mathbf{uv}|})$. We have:*

$$\{\mathbf{uv}? \looparrowright \mathrm{cc}(q^{|\mathbf{uv}|+1})\} = \{\mathbf{v}? \looparrowright \mathrm{cc}(q^{|\mathbf{v}|+1})\}\ .$$

Proof. The left part is a subset of the right one by Lemma 3 and both sets have the same cardinality, which is the ratio of q, by hypothesis. ☐

In particular, by taking the word $\mathbf{v}$ of length 1 in the previous lemma, we can see that the set of followers of a word $\mathbf{w}$ in $\mathrm{cc}(q^n)$ only depends on its last letter $\mathbf{w}\{-1\}$.

Lemma 6. *Let $\mathcal{A}$ be a bireversible Mealy automaton of state set Q, q be a state of $\mathcal{A}$ of constant ratio, and $n > 1$ be an integer. If $\mathbf{u} \in Q^+$ is a suffix of some state of $\mathrm{cc}(q^n)$, then the set $\{?\mathbf{u} \looparrowright \mathrm{cc}(q^n)\}$ only depends on $\mathbf{u}\{0\}$, the first letter of $\mathbf{u}$.*

The next lemma links up the sets of followers and of predecessors in $\mathrm{cc}(q^n)$ when q has a constant ratio.

Lemma 7. *Let $\mathcal{A}$ be a bireversible Mealy automaton of state set Q, q be a state of $\mathcal{A}$ of constant ratio, and $n > 1$ be an integer. The sets of followers and of predecessors in $\mathrm{cc}(q^n)$ have the same cardinality which is the ratio of q.*

Proof. By Lemmas 5 and 6, we only have to prove that

$$|\{q? \looparrowright \mathrm{cc}(q^n)\}| = |\{?q \looparrowright \mathrm{cc}(q^n)\}| \, .$$

Even simpler: notice that if $\mathbf{u}$ is a prefix of some state of $\mathrm{cc}(q^n)$, then it is also a prefix of some state in $\mathrm{cc}(q^{n+k})$ for any $k > 0$, and it has the same followers in both. Of course, an equivalent property holds for the sets of predecessors.

So it is sufficient to prove that

$$|\{q? \looparrowright \mathrm{cc}(q^2)\}| = |\{?q \looparrowright \mathrm{cc}(q^2)\}| \, ,$$

which is true because

$$|\,\mathrm{cc}(q^2)| = |\,\mathrm{cc}(q)| \times |\{q? \looparrowright \mathrm{cc}(q^2)\}| = |\{?q \looparrowright \mathrm{cc}(q^2)\}| \times |\,\mathrm{cc}(q)| \, .$$

□

2 Several equivalences on words

2.1 Minimization and Nerode classes

Let $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ be a Mealy automaton.

The *Nerode equivalence* $\equiv$ *on* Q is the limit of the sequence of increasingly finer equivalences $(\equiv_k)$ recursively defined by:

$$\begin{aligned} \forall p, q \in Q, \qquad\qquad p \equiv_0 q &\iff \rho_p = \rho_q \, , \\ \forall k \geqslant 0,\ p \equiv_{k+1} q &\iff \big(p \equiv_k q \quad \wedge \quad \forall i \in \Sigma,\ \delta_i(p) \equiv_k \delta_i(q)\big) \, . \end{aligned}$$

Since the set Q is finite, this sequence is ultimately constant. For every element q in Q, we denote by $[q]$ the class of q w.r.t. the Nerode equivalence, called the *Nerode class* of q. Extending to the n-th power of $\mathcal{A}$, we denote by $[\mathbf{u}]$ the Nerode class in Q^n of $\mathbf{u} \in Q^n$.

Two states of a Mealy automaton belong to the same Nerode class if and only if they represent the same element in the generated (semi)group, *i.e.* if and only if they induce the same action on Σ^*. Two words on Q of the same length n are *equivalent* if they belong to the same Nerode class in Q^n. By extension, any two words on Q are *equivalent* if they induce the same action.

The *minimization* of $\mathcal{A}$ is the Mealy automaton $\mathfrak{m}(\mathcal{A}) = (Q/{\equiv}, \Sigma, \tilde{\delta}, \tilde{\rho})$, where for every (q, i) in $Q \times \Sigma$, $\tilde{\delta}_i([q]) = [\delta_i(q)]$ and $\tilde{\rho}_{[q]} = \rho_q$. This definition is consistent with the standard minimization of "deterministic finite automata" where instead of considering the mappings $(\rho_q \colon \Sigma \to \Sigma)_q$, the computation is initiated by the separation between terminal and non-terminal states.

A Mealy automaton is *minimal* if it has the same size as its minimization.

Two states of two different connected reversible minimal Mealy automata with the same alphabet induce the same action if and only if the automata are isomorphic and both states are in correspondance by this isomorphism. As a direct consequence, if two connected reversible minimal Mealy automata have different sizes, then any two states of each of them cannot be equivalent.

As we have seen in Section 1.3, a state q of an invertible-reversible Mealy automaton induces an action of infinite order if and only if the sizes of the $(\mathrm{cc}(q^n))_{n>0}$ are unbounded. The proof of [10] can be easily adapted to see that q induces an action of infinite order if and only if the sizes of the $(\mathfrak{m}(\mathrm{cc}(q^n)))_{n>0}$ are unbounded, but you can see it by a direct argument: if the sizes are bounded, there is an infinite set $I \subseteq \mathbb{N}$ such that all the element $(\mathfrak{m}(\mathrm{cc}(q^n)))_{n\in I}$ are isomorphic, and in this sequence there exist at least two different integer $i \neq j$ such that q^i and q^j are represented by the same state in the minimal automata, and so they induce the same action; if the sizes are unbounded, the sequence $(\#\,\mathfrak{m}(\mathrm{cc}(q^n)))_{n>0}$ has infinitely many values, and each value corresponds to a different action for the corresponding power of q.

Note that the Nerode classes of a connected reversible Mealy automaton have the same cardinality. The size of the minimization automaton in this case is the ratio between its size and the cardinality of the Nerode classes.

Lemma 8. *Let $\mathcal{A}$ be a connected bireversible Mealy automaton, N a Nerode class of a connected component of one of its powers, and p and q two elements of $N\{-1\}$. There are as many elements of N with last letter p as with last letter q.*

Proof. The proof of this lemma is quite similar to the proof of Lemma 6 considering not words of length 1 as predecessors, but words on length $n-1$, where n is the length of the states in N. □

2.2 Restricted Nerode classes

When the considered automaton is not connected, it can be interesting to consider the restriction of the Nerode class of an element to its connected component: we denote it by $\llbracket q \rrbracket$ et call it the *restricted Nerode class* of q.

Lemma 9. *The restricted Nerode classes of two elements in the same connected component of a reversible Mealy automaton have the same cardinality.*

Let $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ be a bireversible automaton and q a state of $\mathcal{A}$ of constant ratio. As it will be discussed in Section 3, the result of this article is somehow a generalization of a much simpler result proved in [9], in the case where all the powers of $\mathcal{A}$ are connected. The strategy used then is based on the fact that $\llbracket q^n \rrbracket q \subseteq \llbracket q^{n+1} \rrbracket$ when all the powers of $\mathcal{A}$ are connected. However in the more general case we study here, this fact is false: a priori there is no inclusion link between $\llbracket q^n \rrbracket$ and $\llbracket q^{n+1} \rrbracket$, because if $\mathbf{u}$ is a state of $\llbracket q^n \rrbracket$, then nothing ensures that $\mathbf{u}q$ belongs to $\mathrm{cc}(q^{n+1})$; hence we have to find a different strategy. For this purpose, we introduce the *q-restricted Nerode class* of q^n, *i.e.* the set of states of $\llbracket q^n \rrbracket$ which admit q as a suffix: $\llbracket q^n \rrbracket\!\!\bullet = \llbracket q^n \rrbracket \cap Q^* q$.

The aim of this section is to study the sequence $(\llbracket q^n \rrbracket\!\!\bullet)_{n>0}$.

Lemma 10. *There is an inclusion link in the sequence of q-restricted Nerode classes:*

$$\forall n > 0,\ \llbracket q^n \rrbracket\!\!\bullet\, q \subseteq \llbracket q^{n+1} \rrbracket\!\!\bullet\ .$$

Proof. Let $\mathbf{u}$ be an element of $\llbracket q^n \rrbracket\!\!\bullet$: $\mathbf{u}$ is a state of $\mathrm{cc}(q^n)$ and $\{\mathbf{u}? \looparrowright \mathrm{cc}(q^{n+1})\}$ depends only on $\mathbf{u}\{-1\} = q$ from Lemma 5, so in particular q can follow $\mathbf{u}$ since $q \in \{q? \looparrowright \mathrm{cc}(q^{n+1})\}$. Since $\mathbf{u}$ and q^n induce the same action, so do $\mathbf{u}q$ and q^{n+1}. □

The next results give more information on the growth of the q-restricted Nerode classes of q^n with respect to n.

Proposition 11. *Let $\mathcal{A}$ be a bireversible Mealy automaton, and q be a state of $\mathcal{A}$ of constant ratio k. The ratio between the sizes of $\llbracket q^{n+1} \rrbracket\!\!\bullet$ and $\llbracket q^n \rrbracket\!\!\bullet$ is an integer and:*

$$\forall n > 0,\ \frac{|\llbracket q^{n+1} \rrbracket\!\!\bullet|}{|\llbracket q^n \rrbracket\!\!\bullet|} = |\llbracket q^{n+1} \rrbracket\!\!\bullet\{-2\}|\ .$$

In particular this ratio cannot be greater than k.

Proof. If $p \in \llbracket q^{n+1} \rrbracket\!\!\bullet\{-2\}$, then the sets $\llbracket q^{n+1} \rrbracket\!\!\bullet \cap Q^* pq$ and $\llbracket q^{n+1} \rrbracket\!\!\bullet \cap Q^* qq$ have the same cardinality; indeed, an element $\mathbf{u} \in Q^* p$ satisfies $\mathbf{u}q \in \llbracket q^{n+1} \rrbracket\!\!\bullet$ if and only if $\mathbf{u} \in \llbracket q^n \rrbracket$ by Lemmas 10 and 5 (since by hypothesis p can precede q in $\llbracket q^{n+1} \rrbracket$). So by Lemma 8, $|\llbracket q^n \rrbracket \cap Q^* p| = |\llbracket q^n \rrbracket\!\!\bullet|$ and the result follows.

Since $p \in \llbracket q^{n+1} \rrbracket\!\!\bullet\{-2\}$ can precede q in $\mathrm{cc}(q^{n+1})$, we obtain the bound $k = \{?q \looparrowright \mathrm{cc}(q^2)\}$ from Lemmas 6 and 7. □

Proposition 12. *Let $\mathcal{A}$ be a bireversible Mealy automaton, and q be a state of $\mathcal{A}$ of constant ratio k. The sequence*

$$\left(\frac{|\llbracket q^{n+1} \rrbracket\!\!\bullet|}{|\llbracket q^n \rrbracket\!\!\bullet|} \right)_{n>0}$$

is ultimately increasing to a limit less than or equal to k.

Proof. Consider the sequence $(\llbracket q^n \rrbracket\!\!\bullet)_{n>0}$ and particularly the sequence $(\llbracket q^n \rrbracket\!\!\bullet\{0\})_{n>0}$: from Lemma 10, this sequence increases. Denote by Q_1 its limit: $Q_1 = \llbracket q^n \rrbracket\!\!\bullet\{0\}$ for n large enough, say $n \geq N$; in particular this set contains q.

Now, suppose $n > N$ and take $p \in \llbracket q^{n+1} \rrbracket\!\!\bullet\{-2\}$: clearly $(\llbracket q^{n+1} \rrbracket\!\!\bullet \cap Q^* pq)\{0\}$ is a subset of $Q_1 = \llbracket q^{n+1} \rrbracket\!\!\bullet\{0\} = \llbracket q^n \rrbracket\!\!\bullet\{0\}$; since it has the same cardinality as the set $(\llbracket q^{n+1} \rrbracket\!\!\bullet \cap Q^* qq)\{0\} = \llbracket q^n \rrbracket\!\!\bullet\{0\}$ by

Lemma 8, it is in fact equal to Q_1. But q belongs to Q_1, so it means that the set $\llbracket\, q^{n+1} \,\rrbracket\!\!\bullet \cap qQ^*pq$ is not empty, take $\mathbf{u}$ one of its elements. By Lemma 6, q can precede $\mathbf{u}$ in $\mathrm{cc}(q^{n+2})$ and $q\mathbf{u} \in \llbracket\, q^{n+2} \,\rrbracket\!\!\bullet$. Hence any penultimate letter in $\llbracket\, q^{n+1} \,\rrbracket\!\!\bullet$ is also a penultimate letter in $\llbracket\, q^{n+2} \,\rrbracket\!\!\bullet$:

$$\llbracket\, q^{n+1} \,\rrbracket\!\!\bullet\{-2\} \subseteq \llbracket\, q^{n+2} \,\rrbracket\!\!\bullet\{-2\}\,.$$

The result is now a direct consequence of Proposition 11 □

3 Main result

The following theorem is proved in [9]:

Theorem 13. *A semigroup generated by an invertible-reversible Mealy automaton whose all powers are connected has exponential growth.*

The main result of this article, Theorem 14, is somehow a generalization of this result because all the elements of a semigroup generated by an invertible-reversible Mealy automaton whose all powers are connected have infinite order [10]. To prove this generalization, we need to reinforce the hypothesis on the structure of the automaton which is supposed here to be bireversible and not only invertible-reversible, but we do not use anymore the really strong hypothesis on the connected powers. Since it is (easily) decidable if a Mealy automaton is bireversible, while the condition on the powers is not known to be decidable or undecidable, except in very restricted cases, the result here is way more interesting and powerful, but it is also more tricky to establish. The question of the existence of elements of infinite order in a semigroup generated by a bireversible automaton is under study for several years now and has been solved in quite a few cases [8, 10, 4].

Here is the generalized version of the former theorem we prove in this section:

Theorem 14. *A group generated by a bireversible Mealy automaton which contains an element of infinite order has exponential growth.*

Note that the result still holds for the generated semigroup and the proof is easily adaptable.

Proof. Let $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ be a bireversible Mealy automaton and $\mathbf{u} \in (Q \sqcup Q^{-1})^*$ which induces an action of infinite order. The Mealy automaton $(\mathcal{A} \cup \mathcal{A}^{-1})^{|\mathbf{u}|}$ is bireversible, $\mathbf{u}$ is one if its state, and it generates a subgroup of $\mathcal{A}$. So without lost of generality, we can suppose that $\mathbf{u}$ is in fact a state of $\mathcal{A}$. To be consistent with the rest of the article, let us call it q.

For any integer $i > 0$, note $r_i = \frac{\#\,\mathrm{cc}(q^{i+1})}{\#\,\mathrm{cc}(q^i)}$. The sequence of ratios associated to q is of the form $(r_1, r_2, \ldots, r_j, r_{j+1} = r_j, \ldots)$, where $r_i \geq r_{i+1}$ for any $i \geq 1$ and $r_i = r_j$ for any $i \geq j$. Now, consider the component $\mathrm{cc}(q^j)$ as a Mealy automaton and $\mathbf{q} = q^j$ as its state: the state $\mathbf{q}$ induces an action of infinite order and the sequence of ratios associated to $\mathbf{q}$ is of the form $(r_j^j, r_j^j, \ldots)$: $\mathbf{q}$ has constant ratio. Moreover, $\mathrm{cc}(\mathbf{q})$ generates a subgroup of the group $\langle \mathcal{A} \rangle$, so if we prove that $\langle \mathrm{cc}(\mathbf{q}) \rangle$ has exponential growth, so has $\langle \mathcal{A} \rangle$. So, without loss of generality we can suppose that q has a constant ratio, say k.

It is quite immediate to obtain the following inequalities:

$$\forall n > 0,\ \frac{|\,\mathrm{cc}(q^n)|}{|Q| \times |\,\llbracket\, q^n \,\rrbracket\!\!\bullet\,|} \leq \frac{|\,\mathrm{cc}(q^n)|}{|\llbracket q^n \rrbracket|} \leq \frac{|\,\mathrm{cc}(q^n)|}{|\,\llbracket\, q^n \,\rrbracket\!\!\bullet\,|}\,. \tag{1}$$

Indeed, the right part is a consequence of the fact that $\llbracket\, q^n \,\rrbracket\!\!\bullet \subseteq \llbracket q^n \rrbracket$, and the left part of Lemma 8 and the fact that $\llbracket q^n \rrbracket = \cup_{p \in Q}(\llbracket q^n \rrbracket \cap Q^*p)$.

The central part in (1) is in fact the size of the minimization of $\mathrm{cc}(q^n)$, and the cardinality of $\mathrm{cc}(q^n)$ is equal to $|Q| \times k^{n-1}$ since q has constant ratio k, so (1) can be re-written as:

$$\forall n > 0,\ \frac{k^{n-1}}{|\,\llbracket\, q^n \,\rrbracket\!\!\bullet\,|} \leq \#\,\mathfrak{m}(\mathrm{cc}(q^n)) \leq \frac{|Q| \times k^{n-1}}{|\,\llbracket\, q^n \,\rrbracket\!\!\bullet\,|}\,. \tag{2}$$

Let us prove that for n large enough, $|\,\llbracket\, q^{n+1} \,\rrbracket\!\!\bullet\,| < k \times |\,\llbracket\, q^n \,\rrbracket\!\!\bullet\,|$. From Proposition 11 we know that the corresponding non strict inequality is satisfied. Now, from Propositions 11 and 12 we know that for N large enough, if the equality holds at rank N, it also holds at any rank greater than N: for any $n \geq N$, $|\,\llbracket\, q^{n+1} \,\rrbracket\!\!\bullet\,| = k \times |\,\llbracket\, q^n \,\rrbracket\!\!\bullet\,|$. This means that for n large enough, the value of the n-th term of the sequence $(|\,\llbracket\, q^n \,\rrbracket\!\!\bullet\,|)_{n>0}$ is ck^{n-1}, where c does not depend on n. Hence by the right part of Equation (2), the minimizations of the connected powers of q have bounded size, which implies that q has finite order as seen in Section 2.1, and this is in contradiction with the hypotheses.

Denote by ℓ the limit of the sequence

$$\left(\frac{|[\![q^{n+1}]\!]|}{|[\![q^{n}]\!]|} \right)_{n>0}$$

(it exists from Proposition 12): $\ell > 1$ because q has infinite order and $\ell < k$ from the above paragraph. For n large enough, there exists a constant c such that $|[\![q^{n}]\!]| = \frac{\ell^n}{kc}$.

So Equation (2) becomes:

$$\forall n > N,\ c\left(\frac{k}{\ell}\right)^{n} \leq \#\,\mathfrak{m}(\mathrm{cc}(q^n)) \leq c|Q|\left(\frac{k}{\ell}\right)^{n}. \tag{3}$$

Since $\ell < k$, there exists α such that $\left(\frac{k}{l}\right)^{\alpha} > |Q|$. Let us denote $\mathbf{u} = q^{\alpha}$ and $K = \left(\frac{k}{\ell}\right)^{\alpha}$, we have that for n large enough:

$$c \cdot K^n \leq \#\,\mathfrak{m}(\mathrm{cc}(\mathbf{u}^n)) \leq c \cdot |Q| \cdot K^n < c \cdot K^{n+1} \leq \#\,\mathfrak{m}(\mathrm{cc}(\mathbf{u}^{n+1})) \leq c \cdot |Q| \cdot K^{n+1}. \tag{4}$$

Consequently, the minimizations of the components $\mathrm{cc}(\mathbf{u}^n)$ are pairwise not isomorphic, for n large enough, because they do not have the same size. So their states induce different elements of the group $\mathcal{A}$. Hence the sets

$$I_n = \{\rho_{\mathbf{v}} \mid \mathbf{v} \text{ is a state of } \mathfrak{m}(\mathrm{cc}(\mathbf{u}^n))\}$$

are pairwise disjoint. By Equation (4), the growth of the sequence $(I_n)_{n>0}$ is exponential, and so is the growth of $\mathcal{A}$. □

By combining Theorem 14 with the fact that connected bireversible Mealy automata of prime size cannot generate infinite Burnside groups [4], we have:

Corollary 15. *Any infinite group generated by a bireversible connected Mealy automaton of prime size has exponential growth.*

Another consequence of Theorem 14 concerns virtually nilpotent groups. This class is important in the classification of groups and contains in particular all the abelian groups. It is known that any infinite virtually nilpotent group contains an element of infinite order [3, Proposition 10.48] and has polynomial growth [13]. This leads to

Corollary 16. *No infinite virtually nilpotent group can be generated by a bireversible Mealy automaton.*

Acknowledgement

The author is very grateful to Dmytro Savchuk for suggesting Corollary 16.

References

[1] L. Bartholdi and A. Erschler. Groups of given intermediate word growth. *Ann. Inst. Fourier*, 64(5):2003–2036, 2014.

[2] T. Brough and A.J. Cain. Automaton semigroups: New constructions results and examples of non-automaton semigroups. *Theoretical Computer Science*, 674:1 – 15, 2017.

[3] C. Drutu and M. Kapovich. Lectures on geometric group theory. URL: `https://www.math.ucdavis.edu/~kapovich/EPR/ggt.pdf`.

[4] Th. Godin and I. Klimann. On bireversible Mealy automata and the Burnside problem. *Theor. Comput. Sci.*, 2017. extended version of MFCS'16, to appear.

[5] R. Grigorchuk. Degrees of growth of finitely generated groups and the theory of invariant means. *Izv. Akad. Nauk SSSR Ser. Mat.*, 48-5:939–985, 1984.

[6] R. Grigorchuk. Degrees of growth of finitely generated groups, and the theory of invariant means. *Mathematics of the USSR-Izvestiya*, 25(2):259, 1985.

[7] R. Grigorchuk and I. Pak. Groups of intermediate growth: an introduction for beginners, 2006. arXiv:math/0607384.

[8] I. Klimann. Automaton semigroups: The two-state case. *Theor. Comput. Syst. (special issue STACS'13)*, pages 1–17, 2014.

[9] I. Klimann. On level-transitivity and exponential growth. *Semigroup Forum*, Sep 2016.

[10] I. Klimann, M. Picantin, and D. Savchuk. A connected 3-state reversible Mealy automaton cannot generate an infinite Burnside group. In *DLT' 15*, volume 9168 of *LNCS*, pages 313–325, 2015.

[11] A. Mann. *How groups grow*, volume 395 of *Lecture Note Series*. The London Mathematical Society, 2012.

[12] J. Milnor. Advanced problem 5603. *MAA Monthly*, 75:685–686, 1968.

[13] J.A. Wolf. Growth of finitely generated solvable groups and curvature of riemanniann manifolds. *J. Differential Geom.*, 2(4):421–446, 1968.