INFINITE FINITELY GENERATED AUTOMATA SEMIGROUPS
HAVE INFINITE ORBITS

DOMINIK FRANCOEUR

ABSTRACT. We prove that the semigroup generated by a finite state Mealy
automaton \( A = (Q, A, \tau) \) is infinite if and only if there exists some right-
infinite word in the alphabet \( A \) with infinite orbit.

1. INTRODUCTION

A Mealy automaton is a machine that takes as input a letter from an alphabet
\( A \) and, depending on its currently active state, outputs a letter and modifies its
active state (see Figure 1 for an example).

\[
\begin{array}{ccc}
1|0 & \rightarrow & t \\
0|0 & \rightarrow & s \\
v | & \rightarrow & 0|1, 1|0
\end{array}
\]

Figure 1. The Moore diagram of a Mealy automaton.

Such a machine defines a semigroup acting on the Cantor set \( A^\omega \). The generators
correspond to the states of the automaton (\( \{s, t\} \) in the example) and the image of
\( a_0a_1a_2\cdots \in A^\omega \) by the generator \( q \) is the unique right-infinite word
\( b_0b_1b_2\cdots \in A^\omega \) such that \((a_0\mid b_0)(a_1\mid b_1)\cdots \) is a path starting at \( q \).

Despite being produced by very simple rules, semigroups generated by Mealy
automata can be quite rich and have some striking properties. For instance, one
can find among this class finitely generated infinite torsion groups \[3\] as well as
groups \[4\] and semigroups \[1\] of intermediate growth.

One can wonder what sort of restrictions being recursively defined from a finite
amount of data imposes on the algorithmic, structural or dynamical properties
of semigroups generated by finite state Mealy automata. D’Angeli, Rodero and
Wächter recently asked \([2\), Open Problem 3\)] whether such a semigroup could be
infinite while every orbit of its canonical action on the Cantor set is finite. In this
note, we prove that this is not possible (Theorem 8):

**Theorem.** Let \( S \) be the semigroup of endomorphisms of the Cantor set \( A^\omega \) gen-
erated by a finite state Mealy automaton \( A = (Q, A, \tau) \). Then \( S \) is infinite if and
only if there exists \( \xi \in A^\omega \) such that \( |S \cdot \xi| = \infty \).

In fact, our proof yields the slightly stronger following result (Theorem 9):

**Theorem.** Let \( S \) be as above. Then a subsemigroup \( T \leq S \) is infinite if and only
if there exists \( \xi \in A^\omega \) such that \( |T \cdot \xi| = \infty \).

Date: January 31, 2018.
In Section 2 we briefly define the relevant notions and set the notation. The theorem is proved in Section 3. Section 4 contains remarks and examples related to possible generalisations of this result.

Acknowledgement. The author would like to thank Laurent Bartholdi and Ivan Mitrofanov for many useful remarks and discussions. This work was supported by a Doc.Mobility grant from the Swiss National Science Foundation as well as the "@raction" grant ANR-14-ACHN-0018-01 while the author was visiting the École Normale Supérieure in Paris.

2. Preliminaries

2.1. Alphabets and words. Let $A$ be a finite set and $A^*$ be the set of words in the alphabet $A$. The concatenation between two words $u, v \in A^*$ will be denoted by $u \cdot v$. There is a natural prefix order on $A^*$ given by $u \preceq v$ if $u$ is a prefix of $v$, that is, if there exists a (possibly empty) word $w \in A^*$ such that $v = u \cdot w$.

We will denote by $A^\omega$ the set of right-infinite sequences of letters in the alphabet $A$. The concatenation of a finite word $u \in A^*$ on the left and a right-infinite sequence $\xi \in A^\omega$ on the right will be written as $u \cdot \xi$. Given $u \in A^*$ and $\xi \in A^\omega$, we will write $u \preceq \xi$ if $u$ is a prefix of $\xi$ (i.e. if there exists $\zeta \in A^\omega$ such that $\xi = u \cdot \zeta$). Given a strictly increasing sequence $(u_i)_{i \in \mathbb{N}}$ of elements of $A^*$, there exists a unique $\xi \in A^\omega$ such that $u_i \preceq \xi$ for all $i \in \mathbb{N}$.

2.2. Mealy automata. A Mealy automaton is a tuple $A = (Q, A, \tau)$, where $Q$ is a set called the set of states, $A$ is a finite alphabet and $\tau$ is a map

$$\tau: \begin{cases} Q \times A & \rightarrow A \times Q \\ (q, a) & \mapsto (q \cdot a, q \cdot a) \end{cases}.$$

If $Q$ is finite, $A$ is called a finite state Mealy automaton.

A Mealy automaton can be represented by its Moore diagram, which is a directed labelled graph with set of vertices $Q$. For each $q \in Q$ and $a \in A$, there is an edge from $q$ to $q \cdot a$ labelled by $a(q \cdot a)$. See Figure 1 for an example.

2.3. Semigroup generated by a Mealy automaton. Let $A = (Q, A, \tau)$ be a Mealy automaton. For all $q \in Q$, we have a map $q: A \rightarrow A$ that sends $a$ to $q \cdot a$. We can inductively extend this map to a map $q: A^* \rightarrow A^*$ by

$$q \cdot (a \cdot u) = (q \cdot a)^{((q \cdot a) \cdot u)}$$

for $a \in A$ and $u \in A^*$. Thus, $Q$ can be seen as a set of endomorphisms of $A^*$. We will denote by $S = (Q, +, \leq \text{End}(A^*))$ the semigroup generated by $Q$.

For all $u \in A^*$, we can inductively define a map $@u: Q \rightarrow Q$ by the formula

$$q@u = q(a \cdot v) = (q(a)@v)$$

where $a \in A$, $v \in A^*$ are such that $u = a \cdot v$. This map extends to a map $@u: S \rightarrow S$ by the formula

$$(st)@u = (s@(t \cdot u))(t@u).$$

We then see that for all $u, v \in A^*$ and all $s \in S$, we have

$$s \cdot (u \cdot v) = (s \cdot u) \cdot ((s@u) \cdot v).$$
Given $s \in S$ and a strictly increasing sequence $(u_i)_{i \in \mathbb{N}}$ of elements of $A^*$, it follows from the above formula that the sequence $(s \cdot u_i)_{i \in \mathbb{N}}$ is also strictly increasing. Thus, the action of $S$ on $A^*$ extends to an action of $S$ on $A^\omega$. We then have

$$s \cdot (u \cdot \xi) = (s \cdot u) \cdot ((s \cdot u) \cdot \xi)$$

for all $s \in S$, $u \in A^*$ and $\xi \in A^\omega$.

It is easy to construct a Mealy automaton such that the semigroup $S$ it generates is infinite, but for every $\xi \in A^\omega$, the orbit $S \cdot \xi$ of $\xi$ under the action of $S$ is a finite set (see for example Figure 2).

However, as we will prove in the next section, in the case of a finite state Mealy automaton, there must exist an infinite orbit as soon as the semigroup it generates is infinite.

3. Proof of the theorem

As in the previous section, let $A = (Q, A, \tau)$ be a Mealy automaton and $S$ be the semigroup it generates. In what follows, we will assume that $Q$ is finite.

Definition 1. For $v \in A^*$, we define $m_v \in \mathbb{N} \cup \{\infty\}$ by

$$m_v = \sup_{\xi \in A^\omega} |S \cdot (v \cdot \xi)|.$$  

Remark 2. For any $v \in A^*$, we have $m_v = \max_{a \in A} m_{v \cdot a}$. Therefore, if $m_v = \infty$, there exists $a \in A$ such that $m_{v \cdot a} = \infty$.

Lemma 3. If $S$ is infinite, $m_\epsilon = \infty$, where $\epsilon \in A^*$ is the empty word.

Proof. If $m_\epsilon < \infty$, then it follows from Remark 2 that $m_v < \infty$ for all $v \in A^*$. Therefore, there must exist some $M \in \mathbb{N}$ such that $m_v \leq M$ for all $v \in A^*$. Indeed, assume that this is not the case. We can then find a strictly increasing sequence $(m_{v_n})_{n \in \mathbb{N}}$. As Remark 2 implies that $m_\epsilon \geq m_{v_n}$ for all $n \in \mathbb{N}$, we get $m_\epsilon = \infty$, a contradiction.

Hence, if $m_\epsilon < \infty$, then there exists some $M \in \mathbb{N}$ such that $m_v \leq M$ for all $v \in A^*$. This means that the size of the orbits of the action of the semigroup $S$ on $A^\omega$ is bounded by $M$. Since $S$ is finitely generated, there are only finitely many...
different homomorphisms from $S$ to the endomorphisms of a set of size at most $M$. This, combined with the fact that the action of $S$ on $A^*$ is faithful, implies that $S$ is finite (a detailed proof of this fact is given in [2], Proposition 3).

For $v \in A^*$, let $\pi_v : S \to \text{End}(S \cdot v)$ be the homomorphism of semigroups given by $\pi_v(s)(w) = s \cdot w$ for all $w \in S \cdot v$. To shorten the notation, when there is no ambiguity, we will write $s \cdot$ for $\pi_v(s)$.

The set $S^{S \cdot v}$ of maps from $S \cdot v$ to $S$ becomes a semigroup when endowed with the pointwise product. There is a natural right action of $\text{End}(S \cdot v)$ on $S^{S \cdot v}$ given by precomposition. We can thus consider the semigroup $\text{End}(S \cdot v) \ltimes S^{S \cdot v}$.

**Proposition 4.** For all $v \in A^*$, the map 
\[
\psi_v : \begin{cases} 
S & \to \text{End}(S \cdot v) \ltimes S^{S \cdot v} \\
 s & \mapsto (s \cdot, s \@) 
\end{cases}
\]
is a homomorphism (where $s \@ \in S^{S \cdot v}$ is the map that sends $w$ to $s \@ w$).

**Proof.** It is clear that $\psi_v$ maps the identity to the identity. Consider $s_1, s_2 \in S$. We have
\[
\psi_v(s_1)\psi_v(s_2) = (s_1 \@, s_1 \@)(s_2 \@, s_2 \@) = ((s_1 s_2) \@, (s_1 s_2) \@) = \psi_v(s_1 s_2).
\]
Indeed, for any $w \in S \cdot v$, we have
\[
(s_1 s_2)@w = (s_1 @((s_2 \cdot w))(s_2 @w) = (s_1 @((s_2)w))(s_2 @)(w) = ((s_1 @((s_2)w))(s_2 @))(w) .
\]
\[\square\]

**Remark 5.** For every $v \in A^*$, we have $\psi_v(Q) \subseteq \text{End}(S \cdot v) \times Q^{S \cdot v}$, a finite set.

**Remark 6.** For $v \in A^*$, if there exists a bijection $\varphi : S \cdot v \to B$ for some set $B$, then the map
\[
\psi_v^\varphi : S \to \text{End}(B) \ltimes S^B \\
 s \mapsto (\varphi \circ \pi_v(s) \circ \varphi^{-1}, s \@ \varphi^{-1})
\]
is a homomorphism.

**Lemma 7.** Let $v_1, v_2 \in A^*$ be two words in the alphabet $A$. If there exists a bijection $\varphi : S \cdot v_1 \to S \cdot v_2$ such that $\varphi(v_1) = v_2$ and $\psi_{v_1}^\varphi = \psi_{v_2}$, then $m_{v_1 \cdot w} = m_{v_2 \cdot w}$ for all $w \in A^*$.

**Proof.** We will prove that for all $\xi \in A^\omega$, we have $|S \cdot (v_1 \cdot \xi)| = |S \cdot (v_2 \cdot \xi)|$. The result is then immediate.

Notice that if there exist $s_1, s_2 \in S$ such that $s_1 \cdot (v_1 \cdot \xi) = s_2 \cdot (v_1 \cdot \xi)$, then $s_1 \cdot (v_2 \cdot \xi) = s_2 \cdot (v_2 \cdot \xi)$. Indeed,
\[
s_1 \cdot (v_1 \cdot \xi) = (s_1 \cdot v_1)^\sim ((s_1 \@ v_1) \cdot \xi).
\]
Hence, $s_1 \cdot v_1 = s_2 \cdot v_1$ and $(s_1 \@ v_1) \cdot \xi = (s_2 \@ v_1) \cdot \xi$. 


By the hypothesis, we have $\varphi \circ \pi_{v_1} (s_i) \circ \varphi^{-1} = \pi_{v_2} (s_i)$. Hence,

$$s_1 \cdot v_2 = \pi_{v_2} (s_1)(v_2)$$

$$= \varphi \circ \pi_{v_1} (s_1) \circ \varphi^{-1} (v_2)$$

$$= \varphi (\pi_{v_1} (s_2))(v_1)$$

$$= \varphi (\pi_{v_1} (s_2))(v_1)$$

$$= \varphi \circ \pi_{v_1} (s_2) \circ \varphi^{-1}$$

$$= s_2 \cdot v_2.$$

Furthermore, since $s_i \circ \varphi^{-1} (w) = s_i \circ w$ for all $w \in S \cdot v_2$, we get

$$s_i \circ v_2 = s_i \circ \varphi^{-1} (v_1) = s_i \circ v_1.$$

Therefore, $(s_1 \circ v_2) \cdot \xi = (s_2 \circ v_2) \cdot \xi$. It follows that we have $s_1 \cdot (v_2 \cdot \xi) = s_2 \cdot (v_2 \cdot \xi)$.

We can thus define the map

$$\lambda : \begin{cases} S \cdot (v_1 \cdot \xi) & \rightarrow S \cdot (v_2 \cdot \xi) \\ s \cdot (v_1 \cdot \xi) & \rightarrow s \cdot (v_2 \cdot \xi). \end{cases}$$

It is clearly surjective, and by the symmetry of the previous argument, it must also be injective. This concludes the proof. \qed

**Theorem 8.** The semigroup $S$ is infinite if and only if there exists $\xi \in A^\omega$ such that $|S \cdot \xi| = \infty$.

**Proof.** It is clear that if there exists some $\xi \in A^\omega$ such that $|S \cdot \xi| = \infty$, then $S$ must be infinite. Let us prove the converse.

Suppose that $S$ is infinite. For each $u \in A^*$, we define the set

$$T_u = \{ v \in A^* \mid v \geq u \text{ and } m_v = \infty \}.$$

It follows from Remark 2 that $T_u \neq \emptyset$ if and only if $m_u = \infty$, and we know from Lemma 3 that $T_e \neq \emptyset$.

We may assume that there exists some $w \in A^*$ with $m_w = \infty$ and such that for all $v \in T_w$,

$$|S \cdot w| = |S \cdot v|.$$

Indeed, suppose that this is not the case. Then, for every $u \in A^*$ with $m_u = \infty$, there exists some $v \in T_u$ such that $|S \cdot u| < |S \cdot v|$. Thus, starting from $e$, which satisfies $m_e = \infty$, we can construct a strictly increasing sequence $(u_i)_{i \in N}$ of elements of $A^*$ such that $u_{i+1} \in T_{u_i}$ and $|S \cdot u_i| < |S \cdot u_{i+1}|$ for all $i \in N$. Since the sequence $(u_i)_{i \in N}$ is strictly increasing, there exists a unique element $\xi \in A^\omega$ such that $u_i$ is a prefix of $\xi$ for all $i \in N$. It follows from the fact that $|S \cdot u_i| < |S \cdot u_{i+1}|$ that the size of the orbit of $\xi$ is unbounded, which is what we were looking for. Thus, it suffices to consider the case where there exists some $w \in A^*$ as above.

In order to shorten the notation, let us write $B = S \cdot w$. For all $v \in T_w$, the map

$$\varphi_v : \begin{cases} S \cdot v & \rightarrow B \\ s \cdot v & \rightarrow s \cdot w \end{cases}$$

is a well-defined bijection between $S \cdot v$ and $B$ that satisfies $\varphi_v (v) = w$. The fact that it is well-defined and surjective follows immediately from the fact that $v \geq w$, and it then must be a bijection, since $|S \cdot v| = |B|$. 


We know from Lemma 7 that for all $a \in A$ and $v \in T_w$, the value of $m_{v \cdot a}$ depends only on the homomorphism $\psi_{v \cdot} : S \to \text{End}(B) \ltimes S^B$. However, there are only finitely many such homomorphisms. Indeed, a homomorphism from $S$ to $\text{End}(B) \ltimes S^B$ is uniquely determined by the image of the generating set $Q$, and since by Remark 5 we have $\psi_{v \cdot}(Q) \subseteq \text{End}(B) \times Q^B$, we have only finitely many choices, hence finitely many such homomorphisms. Consequently, the set

$$K = \{m_{v \cdot a} \in \mathbb{N} \cup \{\infty\} \mid v \in T_w, a \in A\}$$

is finite. If $K \neq \{\infty\}$, set $M = \max(K \setminus \{\infty\})$. Otherwise, set $M = |B|$. Notice that we always have $M \geq |B|$. Let us consider $x \in w^{-1}A^*$. If $x \in T_w$, we have $|S \cdot x| = |B| \leq M$. If $x \notin T_w$, then it follows from Remark 2 that there exists $v \in T_w$ and $a \in A$ such that $m_x \leq m_{v \cdot a} < \infty$. Then, by the definition of $M$, we get $m_x \leq M$, which implies that $|S \cdot x| \leq M$. Thus, for all $x \in w^{-1}A^*$, we have $|S \cdot x| \leq M$. This implies that $m_w \leq M$, a contradiction.

We conclude that there must exist some $\xi \in A^\omega$ with infinite orbit. □

4. Remarks and examples

It was pointed out to us by Ivan Mitrofanov that the proof of Theorem 8 also works, with minor modifications, if we consider not only $S$ but any finitely generated subsemigroup of $S$. Thus, we get the following result:

**Theorem 9.** Let $S$ be the semigroup generated by a finite state automaton $A = (Q, A, \tau)$ and $T \subseteq S$ be a finitely generated subsemigroup of $S$. Then $T$ is infinite if and only if there exists $\xi \in A^\omega$ such that $|T \cdot \xi| = \infty$.

**Proof.** The proof of Theorem 8 yields the result if one replaces $S$ by $T$ and the maps $\psi_v : S \to \text{End}(S \cdot v) \ltimes S^{S^v}$ by maps $\psi_v : T \to \text{End}(T \cdot v) \ltimes T^{S_{T \cdot v}}$. As $T$ is finitely generated, there are only finitely many of these maps (up to conjugation by bijections), so the argument goes through. □

Notice that in Theorem 9 for the conclusion to hold, the number of states of the automaton has to be finite. If we allow an infinite number of states, then one can obtain finitely generated subgroups where every orbit is finite. For example, for the automaton described in Figure 3, the subsemigroup generated by $x_0$ is infinite, but each of its orbits are finite.

We saw from the example of Figure 2 that if we consider Mealy automata with an infinite number of states, it is possible for every orbit to be finite. However, in that example, the orbits were in fact bounded. Thus, it is natural to ask the following question: given a semigroup generated by a (not necessarily finite state) Mealy automaton, is it true that either there exists an infinite orbit or every orbit is bounded?

As can be seen in the following example, suggested to us by Laurent Bartholdi, it turns out that the answer to this question is negative.
Example 10. Let \( A = \{0, 1, 2\} \) and \( Q = \{e, a_{ij} \mid i \in \mathbb{N}, 1 \leq j \leq i^2\} \) be two sets, and let \( \tau : Q \times A \to A \times Q \) be the map given by \( \tau(e, x) = (x, e) \) for all \( x \in A \) and

\[
\tau(a_{ij}, 0) = \begin{cases} (1, a_{i(j-1)}) & \text{if } j \equiv 1 \mod i \\ (0, e) & \text{otherwise} \end{cases}
\]

\[
\tau(a_{ij}, 1) = \begin{cases} (0, a_{i(j-1)}) & \text{if } j \equiv 1 \mod i \\ (1, e) & \text{otherwise} \end{cases}
\]

\[
\tau(a_{ij}, 2) = \begin{cases} (2, e) & \text{if } j \equiv 1 \mod i \\ (2, a_{i(j-1)}) & \text{otherwise} \end{cases}
\]

(where we set \( a_{00} = e \)). We can then consider the automaton \( A = (Q, A, \tau) \). A part of its Moore diagram is represented in Figure \( \text{Figure 3} \).

The semigroup \( S \) generated by \( A \) is in fact a group, and since it is composed of finitary automorphisms of \( A^\omega \), it is locally finite. We claim that all its orbits are finite but unbounded. To see this, let us first notice that, from the definition, for all \( 1 \leq j \leq i^2 \), all \( n \in \mathbb{N} \) such that \( n \neq i \) and all \( x, y \in \{0, 1\} \), we have \( a_{ij} \circ (x^\omega 2^{n-1} y) = e \). Therefore, for all \( s \in S \), we have

\[
s \circ (x^\omega 2^{n-1} y) \in \langle a_{n1}, a_{n2}, \ldots, a_{nn^2} \rangle,
\]

which is a finite subgroup of \( S \).

Let us consider \( \xi \in A^\omega \). There are two cases: either there exists some finite prefix \( w \) of \( \xi \) such that \( w \) contains exactly two letters in the set \( \{0, 1\} \) or \( \xi \) contains at most one letter in this set. In the second case, it is easy to see that the orbit of \( \xi \) has size at most 2, since elements of \( S \) fix every occurrence of the letter 2 in any word.

Let us now assume that we are in the first case and let \( n \in \mathbb{N}, x, y \in \{0, 1\} \) be such that \( w \) contains the subword \( x^\omega 2^{n-1} y \). Then, it follows from our previous remark that \( s \circ w \in \langle a_{n1}, a_{n2}, \ldots, a_{nn^2} \rangle \) for all \( s \in S \). As \( s \cdot \xi = (s \cdot w)^\omega ((s \circ w) \cdot \xi') \), where \( \xi = w^\omega \xi' \), we conclude that the orbit of \( \xi \) must be finite.

\text{Figure 3. A Mealy automaton generating an infinite semigroup with a finitely generated infinite subsemigroup for which every orbit is finite.}
To see that the orbits of the action of $S$ are unbounded, it suffices to notice that $S$ acts transitively on the sets

$$V_i = \{a_1a_2\ldots a_i \in A^i \mid a_k \in \{0, 1\} \text{ if } k \equiv 1 \mod i, \quad a_k = 2 \text{ otherwise} \}$$

for all $i \in \mathbb{N}$.

References

[1] Bartholdi, Laurent, Illya I. Reznykov, and Vitaliy I. Sushchansky. "The smallest Mealy automaton of intermediate growth." Journal of Algebra 295.2 (2006): 387-414.

[2] D’Angeli, Daniele, Emanuele Rodaro, and Jan Philipp Wächter. "Automaton Semigroups and Groups: on the Undecidability of Problems Related to Freeness and Finiteness." arXiv preprint arXiv:1712.07408 (2017).

[3] Grigorchuk, Rostislav I. "Burnside problem on periodic groups." Funktsional’nyi Analiz i ego Prilozheniya 14.1 (1980): 53-54.

[4] Grigorchuk, Rostislav I. "On the Milnor problem of group growth." Dokl. Akad. Nauk SSSR. Vol. 271. No. 1. 1983.