AUTOMATA OVER A BINARY ALPHABET GENERATING FREE GROUPS OF EVEN RANK

BENJAMIN STEINBERG, MARIYA VOROBETS, AND YAROSLAV VOROBETS

Abstract. We construct automata over a binary alphabet with $2n$ states, $n \geq 2$, whose states freely generate a free group of rank $2n$. Combined with previous work, this shows that a free group of every finite rank can be generated by finite automata over a binary alphabet. We also construct free products of cyclic groups of order two via such automata.

1. Introduction

The binary odometer is a finite state automaton over a binary alphabet generating a free group of rank 1. For a long time, it was an open question whether there is a finite state automaton generating a non-abelian free group [7]. The first examples were provided by Glasner and Mozes [6]. The smallest examples they obtained were a 14-state automaton over a 6-letter alphabet generating a free group of rank 7 and a 6-state automaton over a 14-letter alphabet generating a free group of rank 3. Nekrashevych afterwards constructed an automaton with 6 states over a binary alphabet generating a free group of rank two [13]; again the states of the automaton are not free generators and, in fact, it was shown in [7] that no two state automaton over a binary alphabet generates a free group.

Brunner and Sidki conjectured in [4] that the states of a certain 3-state automaton over a binary alphabet, constructed by Aleshin [1] in 1983, freely generate a free group of rank 3. Aleshin constructed this automaton, together with a certain five state automaton, in order to construct a free subgroup of rank 2 in the group of all finite state transformations, but his proof [1] is not complete. In [16] the second and third authors answered positively the conjecture of Brunner and Sidki, showing that the Aleshin automaton freely generates a free group of rank 3. In a sequel paper [17], they considered a series of Aleshin-type automata with $2n+1$ states, $n \geq 1$, over a binary alphabet that freely generate a free group of rank $2n+1$. Moreover, it was shown that the disjoint union of any two distinct automata in

Date: Version of September 29, 2006.

Key words and phrases. Free groups, automaton groups, self-similar groups, bireversible automata.

The first author acknowledges the support of NSERC.

The third author is supported by a Clay Research Scholarship.

this series generates their free product. Thus they established that, for every possible rank $n \geq 3$, except 4 and 6, there is a free group of rank n generated by an n-state automaton over a binary alphabet. In the process, Aleshin's claim [1] was verified. It should be noted, however, that connected automata were constructed only for free groups of odd rank.

In this paper we construct a new family of finite automata over a binary alphabet generating free groups. Our family contains, for any $n \geq 2$, a connected $2n$-state automaton freely generating a free group of rank $2n$. In particular, combined with the results of [16, 17] and [13], this shows that a free group of any rank can be generated by a finite state automaton over a binary alphabet and, moreover, if $n \geq 3$, then an n-state connected automaton does the job.

Nekrashevych's construction [13] was based on a result of Muntyan and Savchuk [13, Theorem 1.4], showing that a certain 3-state automaton over a binary alphabet, related to Aleshin's automaton, generates a free product of three cyclic groups of order two. The second and third authors, in [17], in turn showed that there are connected $2n+1$ state automata over a binary alphabet generating a free product of $2n+1$ cyclic groups of order two for any $n \geq 1$. Again the disjoint union of distinct automata from this family generate their free product and so they were able to construct, for any $n \geq 3$, a finite state automaton generating a free product of n cyclic groups of order two (in this setting they could add a single isolated state to obtain products of 4 and 6 cyclic groups of order two). In this paper we use our family to construct, for any $n \geq 2$, a $2n$-state connected automaton over a binary alphabet generating a free product of $2n$ cyclic groups of order two.

All automata discussed in this paper are bireversible and it is an open problem to construct an automaton that is not bireversible generating a free non-abelian group. By an unpublished result of Abert, such an automaton cannot be contracting in the sense of [13].

The paper is organized as follows. The second section gives the reader the basic background about groups generated by finite state automata, with a special emphasis on dual automata and bireversible automata. In particular, we discuss our conventions for dealing with dual automata. The third section introduces the automata that will play a key role in this paper. The fourth section proves the main results on freeness.

2. Automaton groups

In this section, we collect some of the basic notions from the theory of groups generated by finite state automata, also called automaton groups. This is a special case of the notion of a self-similar group [13], due to Nekrashevych, but is the principal case that has been studied. For more information consult [7, 13].

2.1. **Preliminaries and notation for free monoids.**

First some preliminaries and notation. If A is a finite alphabet (that is a finite set), then A^*

denotes the free monoid on A. If $w = a_1 \cdots a_n \in A^*$, then the *reversal* of w is the word $w^\rho = a_n \cdots a_1$. We set $A^\pm = A \cup A^{-1}$, where A^{-1} is a disjoint set in bijection with a via a map $a \mapsto a^{-1}$. Then $(A^\pm)^*$ is the *free monoid with involution*, where the involution is defined in the usual way. The group of involution-preserving automorphisms of $(A^\pm)^*$ is isomorphic to S_A via the map sending $\sigma \in S_A$ to the map $\sigma^\pm : (A^\pm)^* \to (A^\pm)^*$ defined by

$$\sigma^\pm(a_1^{e_1} \cdots a_n^{e_n}) = \sigma(a_1)^{e_1} \cdots \sigma(a_n)^{e_n}$$

with $a_i \in A$ and $e_i \in \{\pm 1\}$. Sometimes we shall wish to distinguish $\sigma^\pm$ from the permutation of $A^\pm$ obtained by restricting $\sigma^\pm$ to letters. So if $\sigma \in S_A$, then $\overline{\sigma} \in S_{A^\pm}$ denotes the permutation defined by $\overline{\sigma}(a^e) = \sigma(a)^e$ for $a \in A$, $e = \pm 1$. The map $\sigma \mapsto \overline{\sigma}$ is of course a monomorphism $S_A \to A_{A^\pm}$. To each element $\sigma \in S_A$, we can also associate an automorphism $\sigma^* : A^* \to A^*$ by defining $\sigma^*(a) = \sigma(a)$. Note that $\sigma^\pm = \overline{\sigma}^*$.

2.2. **Mealy automata.** A *finite (Mealy) automaton* [5, 11] $\mathcal{A}$ is a 4-tuple (Q, A, δ, λ) where Q is a finite set of states, A is a finite alphabet, $\delta : Q \times A \to Q$ is the transition function and $\lambda : Q \times A \to A$ is the output function. We shall always write, for $q \in Q$ and $a \in A$, $\delta(q, a) = q_a$ and $\lambda(q, a) = q(a)$. Automata are usually represented by so-called *Moore diagrams.* The Moore diagram for $\mathcal{A}$ is a directed graph with vertex set Q. The edges are of the form $q \xrightarrow{a|q(a)} q_a$. For example Aleshin's automaton [1] is given by the Moore diagram in Figure 1.

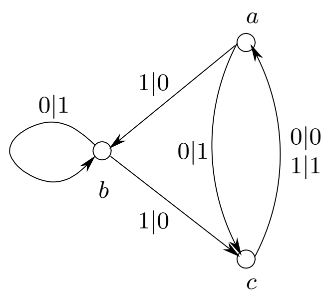

FIGURE 1. Aleshin's automaton A

For instance, in state b with input 1, the automaton outputs 0 and moves to state c. Sometimes we shall just draw the transitions and omit the output from the Moore diagram; the resulting graph is called the *transition diagram.* The transition and output functions of an automaton $\mathcal{A}$ extend inductively to the free monoid A^* via the rules:

$$q_{au} = (q_a)_u \tag{2.1}$$

$$q(au) = q(a)q_a(u) \tag{2.2}$$

where $a \in A$, $u \in A^*$.

We use $\mathcal{A}_q$ to denote the *initial automaton* $\mathcal{A}$ with designated start state q. Sometimes, when no confusion can occur, we use simply the letter q to denote this initial automaton. Abusing notation, there is a function $\mathcal{A}_q : A^* \to A^*$ given by $w \mapsto q(w)$. For instance, with A the automaton above, $\mathsf{A}_b(010) = 100$. In general the function $\mathcal{A}_q$ is length preserving and preserves common prefixes. It extends continuously to the set of right infinite words A^ω via the formula

$$\mathcal{A}_q(a_0 a_1 \cdots) = \lim_{n\to\infty} \mathcal{A}_q(a_0 \cdots a_n) \tag{2.3}$$

where A^ω is given the product topology, making it homeomorphic to a Cantor set [7]. If one defines a metric on A^ω by defining $d(u,v) = |A|^{-|u\wedge v|}$, where $u \wedge v$ is the longest common prefix of u and v, then $\mathcal{A}_q$ is a metric contraction (where we say a map f is a *metric contraction* if $d(f(u), f(v)) \leq d(u,v)$). If, for each q, the function $a \mapsto q(a)$ is a permutation, then each $\mathcal{A}_q$ is invertible and induces an isometry of A^ω [7, 13]. In this case the automaton is called *invertible*. The *inverse automaton* $\mathcal{A}^{-1}$ of $\mathcal{A}$ is the automaton obtained by taking the Moore diagram for $\mathcal{A}$ and swapping the left hand side and right hand side of the edge labels. We usually denote the state of $\mathcal{A}^{-1}$ corresponding to q by q^{-1}. One can check that $\mathcal{A}^{-1}_{q^{-1}} = (\mathcal{A}_q)^{-1}$ [7, 13]. Figure 2 shows the Moore diagram for the inverse of Aleshin's automaton from Figure 1.

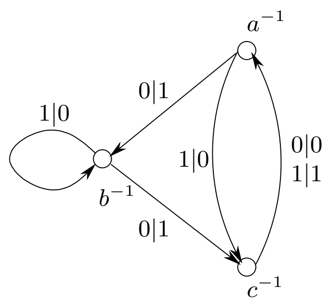

FIGURE 2. The inverse of Aleshin's automaton

It is well known that if $\mathcal{A}_q$ and $\mathcal{B}_s$ are transformations computed by finite state initial automata, then the composition $\mathcal{B}_s\mathcal{A}_q$ can be computed by a finite state initial automaton [5, 7, 13]. If $\mathcal{A}$ is an automaton over an alphabet A, we write $\mathbb{S}(\mathcal{A})$ for the semigroup of transformations of A^* (or equivalently A^ω) generated by the functions $\mathcal{A}_q$ with $q \in Q$. If $\mathcal{A}$ is invertible, we write $\mathbb{G}(\mathcal{A})$ for the group of transformations generated by the initial automata associated to the states of $\mathcal{A}_q$. Groups generated by finite state automata, also called *automaton groups*, are a very important special case of the general notion of a *self-similar* group [13]. A self-similar group is what one gets by allowing infinite state automata in the definition of an automaton group. If $\mathcal{A}$ is an invertible automaton, we write $\mathcal{A}^{\pm}$ for the automaton whose Moore diagram is the disjoint union $\mathcal{A}$ and $\mathcal{A}^{-1}$. It is easy to see that $\mathcal{A}^{\pm}$ is an invertible automaton, which is its own inverse and that $\mathbb{S}(\mathcal{A}^{\pm}) = \mathbb{G}(\mathcal{A})$.

If we denote by T the rooted Cayley tree of A^* with root vertex the empty string, then $\mathbb{G}(\mathcal{A})$ acts on the left of T by tree automorphisms of T [2, 7, 13] via the action (2.2). The induced action on the boundary ∂T (the space of infinite directed paths from the root) is just the action (2.3) of $\mathbb{G}(\mathcal{A})$ on A^ω.

The automorphism group $\mathrm{Aut}(T)$ is the iterated (permutational) wreath product of countably many copies of the left permutation group (S_A, A) [3, 2, 7, 13, 14], where S_A denotes the symmetric group on A. In this paper, our notation will be such that the wreath product of left permutation groups has a natural projection to its leftmost factor; dual notation is used for right permutation groups. For a group $\Gamma = \mathbb{G}(\mathcal{A})$ generated by an automaton over A, one has an embedding

$$(\Gamma, A^\omega) \hookrightarrow (S_{|A|}, A) \wr (\Gamma, A^\omega) \tag{2.4}$$

where the map sends $\mathcal{A}_q$ to the element with wreath product coordinates:

$$\mathcal{A}_q = \lambda_q(\mathcal{A}_{q_{a_1}}, \ldots, \mathcal{A}_{q_{a_n}}) \tag{2.5}$$

where $A = \{a_1, \ldots, a_n\}$ and $\lambda_q(a) = \lambda(q, a)$. See [2, 7, 15, 13] for more details. As an example, if $\mathcal{A}$ is Aleshin's automaton from Figure 1, then $a = (01)(c, b)$, $b = (01)(b, c)$ and $c = (a, a)$; similarly, for the inverse of Aleshin's automaton (Figure 2), $a^{-1} = (01)(b^{-1}, c^{-1})$, $b^{-1} = (01)(c^{-1}, b^{-1})$ and $c^{-1} = (a^{-1}, a^{-1})$. Notice that data (2.5), as q varies over all states, completely encodes the automaton $\mathcal{A}$ and so sometimes we shall give an automaton via the wreath product coordinates.

We also shall need the notion of sections and the minimal automaton. Let $a \in A$. Then there is a homeomorphism $L_a : A^\omega \to A^\omega$ given by $L_a(w) = aw$; metrically this is a contraction by a factor of $1/|A|$. If $f : A^\omega \to A^\omega$ is any metric contraction, then, by definition of the metric, there is a function $A \to A$, which we also denote by f (abusing notation), so that, for any word $w \in A^\omega$, $f(aw) = f(a)w'$, some $w' \in A^\omega$. Define, for $a \in A$, $f_a : A^\omega \to A^\omega$ by $f_a = L_{f(a)}^{-1} f L_a$. Then f_a is also a metric contraction, which is an isometry whenever f is one. The map f_a is called the *section* of f at a. It is straightforward to verify that $f(aw) = f(a)f_a(w)$. Notice that if $\mathcal{A}$ is a finite state automaton, then $(\mathcal{A}_q)_a = \mathcal{A}_{q_a}$ — that is the notation q_a is unambiguous if we identify functions and states. One can also define inductively the section f_w for any word $w \in A^*$; of course $f_\varepsilon = f$, where ε is the empty string. We remark that for any word $w \in A^*$ of length n, there is a unique word of length n, denoted $f(w)$, so that $f(wA^\omega) \subseteq f(w)A^\omega$; this coincides with our previous definition if $n = 1$. With this definition, one has $f(wu) = f(w)f_w(u)$ for any word $u \in A^\omega$.

If $f : A^\omega \to A^\omega$ is a metric contraction, then the minimal automaton of f is the possibly infinite automaton $\mathcal{A}(f)$ with state set $\{f_w \mid w \in A^*\}$ (of course for different $u, w \in A^*$, it may be the case that $f_u = f_w$). The transitions are given by $\delta(f_u, a) = f_{ua}$ and the output by $\lambda(f_u, a) = f_u(a)$. It is easy to see that $\mathcal{A}(f)_{f_u} = f_u$ and in particular $\mathcal{A}(f)_{f_\varepsilon} = f$. One can prove that f is computed by a finite state automaton if and only if $\mathcal{A}(f)$ is finite and that $\mathcal{A}(f)$ is the unique automaton with minimal number of states computing f [5, 7]. Moreover, it is well known that $\mathcal{A}(f)$ is polynomial time computable from any automaton computing f. Notice that if f is invertible, then $\mathcal{A}(f)$ must be invertible and $\mathcal{A}(f)^{-1} = \mathcal{A}(f^{-1})$.

The following formula will be useful later. Let $f_n, \cdots, f_1 : A^\omega \to A^\omega$ be metric contractions. Then one easily checks that, for $w \in A^*$,

$$(f_n \cdots f_1)_w = (f_n)_{f_{n-1}\cdots f_1(w)} \cdots (f_2)_{f_1(w)}(f_1)_w \tag{2.6}$$

Suppose that $\mathcal{A} = (Q, A^\pm, \delta, \lambda)$ is an automaton and $\sigma \in S_A$. Then we need the following straightforward observation on how to construct an automaton computing $\sigma^*\mathcal{A}_q$ for any $q \in Q$. The proof is left to the reader.

Proposition 2.1. *Let $\mathcal{A} = (Q, A, \delta, \lambda)$ be an automaton and $\sigma \in S_A$. Define $\sigma[\mathcal{A}] = (Q, A, \delta, \sigma\lambda)$. Then $\sigma[\mathcal{A}]_q = \sigma^*\mathcal{A}_q$.*

In fact the proposition can be obtained as a special case of the general construction for composing automata [5, 7, 13], using that automorphisms are precisely the functions computed by invertible automata with a single state. If $A = Q^\pm$ and $\sigma \in S_A$, then in particular we can apply the above proposition to understand $\sigma^\pm\mathcal{A}_q$.

Another notion that we shall need is that of the transition monoid of an automaton. If $\mathcal{A} = (Q, A, \delta, \lambda)$ is an automaton, then the *transition monoid* of $\mathcal{A}$, denoted $M(\mathcal{A})$, is the finite monoid of all transformations of Q of the form $q \mapsto q_w$ with $w \in A^*$. It is easy to check that this is indeed a finite monoid. It is well known [5] that the transition monoid $M(\mathcal{A}(f))$ of the minimal automaton $\mathcal{A}(f)$ is a quotient of the transition monoid of any other initial automaton computing f. In other words, it is an algebraic invariant of f. In this paper we shall be particularly interested in the case that $M(\mathcal{A})$ and $M(\mathcal{A}^{-1})$ are groups.

A key fact about transition monoids is that if f and g are two finite state transformations of A^ω, then the transition monoid $M(\mathcal{A}(fg))$ is a quotient of a submonoid of the wreath product of right transformation monoids $M(\mathcal{A}(f)) \wr M(\mathcal{A}(g))$ [5, 11]. Thus if $\mathcal{C}$ is a class of finite monoids closed under taking wreath product, submonoids and quotient monoids — for instance the class of finite groups — then the set of finite state transformations with transition monoid in $\mathcal{C}$ is a semigroup of metric contractions. We shall call the group of units of this semigroup the *group of $\mathcal{C}$-isometries of A^ω*. The case where $\mathcal{C}$ is the collection of finite groups, gives rise to the group of so-called bireversible automata [6, 12, 16, 17], as we shall see below.

2.3. **The dual automaton.** The way we have defined automata, they scan their input from left to right, outputting each time they process a letter. Clearly one can also define a *right-to-left scanning automaton* in a dual manner: so one has a 4-tuple (Q, A, δ, λ) as before, but now $\delta : A \times Q \to Q$

and $\lambda : A \times Q \to A$. One then sets $\delta(a, q) = {}_a q$ and $\lambda(a, q) = aq$ and extends to A^* via:

$$ {}_{ua}q = {}_u({}_a q) \tag{2.7} $$
$$ (ua)q = u_a q(aq) \tag{2.8} $$

If $\mathcal{A}$ is an invertible right-to-left scanning automaton, then $\Gamma = \mathbb{G}(\mathcal{A})$ is a group of permutations of A^* (or isometries of the space of left infinite words ${}^{\omega}A$, or automorphisms of the left Cayley tree of A^*) acting on the right. It preserves length and common suffixes, that is $(uw)\mathcal{A}_q = u\mathcal{A}_{{}_w q} w\mathcal{A}_q$ for $u, w \in A^*$.

There is an embedding of Γ into the wreath product of right permutation groups

$$ (A^{\omega}, \Gamma) \hookrightarrow ({}^{\omega}A, \Gamma) \wr (A, S_{|A|}) \tag{2.9} $$

where the map sends $\mathcal{A}_q$ to the element with wreath product coordinates:

$$ \mathcal{A}_q = (\mathcal{A}_{{}_{a_1}q}, \ldots, \mathcal{A}_{{}_{a_n}q})\lambda_q \tag{2.10} $$

where $A = \{a_1, \ldots, a_n\}$ and $a\lambda_q = \lambda(a, q)$.

Now if $\mathcal{A} = (Q, A, \delta, \lambda)$ is an automaton, then there is an associated right-to-left scanning automaton, called the *dual automaton* of $\mathcal{A}$, which is denoted $\widehat{\mathcal{A}}$ and is given by $\widehat{\mathcal{A}} = (A, Q, \lambda, \delta)$ [7]. So one obtains $\widehat{\mathcal{A}}$ from $\mathcal{A}$ by switching the states and the alphabet, switching the input and the output functions and switching the way we scan words as the automaton operates. So one has for $q \in Q$ and $a \in A$

$$ {}_q a = q(a) $$
$$ qa = q_a $$

One then has, inductively, for $q_n, \ldots, q_1 \in Q$ and $a \in A$,

$$ \begin{aligned} {}_{q_n \cdots q_2 q_1} a &= q_n q_{n-1} \cdots q_1(a) = \mathcal{A}_{q_n} \cdots \mathcal{A}_{q_1}(a) \\ q_n \cdots q_2 q_1 a &= (q_n)_{q_{n-1} \cdots q_1(a)} \cdots (q_2)_{q_1(a)} (q_1)_a \\ &= (q_n)_{\mathcal{A}_{q_{n-1}} \cdots \mathcal{A}_{q_1}(a)} \cdots (q_2)_{\mathcal{A}_{q_1}(a)} (q_1)_a \end{aligned} \tag{2.11} $$

One can interpret the first line of (2.11) as saying that in state a, on input $q_n \cdots q_1$, $\widehat{\mathcal{A}}$ goes to the state which is the output of $\mathcal{A}_{q_n} \cdots \mathcal{A}_{q_1}$ on the letter a. In other words, the transition diagram of $\widehat{\mathcal{A}}$ is the Schreier graph of the action of $\mathbb{S}(\mathcal{A})$ on the first level of the tree. The second/third lines of (2.11), in light of (2.6), says that the output of state a with input $q_n \cdots q_1$ is a word in Q^* representing the section of $\mathcal{A}_{q_n} \cdots \mathcal{A}_{q_1}$ at a. The following result, proved in [16] in a slightly different language, is then immediate by induction.

Theorem 2.2. *Let $\mathcal{A} = (Q, A, \delta, \lambda)$ be a finite state automaton with dual $\widehat{\mathcal{A}}$. Then if $a_1, \ldots, a_m \in A$ and $q_n, \ldots, q_1 \in Q$, then*

$$ {}_{q_n \cdots q_2 q_1} \widehat{\mathcal{A}}_{a_1} \cdots \widehat{\mathcal{A}}_{a_m} = \mathcal{A}_{q_n} \cdots \mathcal{A}_{q_1}(a_1 \cdots a_m) $$

$$(q_n \cdots q_2 q_1)\widehat{\mathcal{A}}_{a_1} \cdots \widehat{\mathcal{A}}_{a_m} = (q_n)_{\mathcal{A}_{q_{n-1}} \cdots \mathcal{A}_{q_1}(a_1 \cdots a_m)} \cdots (q_2)_{\mathcal{A}_{q_1}(a_1 \cdots a_m)} (q_1)_{a_1 \cdots a_m}$$

In particular, by (2.6)*,* $(q_n \cdots q_2 q_1)\widehat{\mathcal{A}}_{a_1} \cdots \widehat{\mathcal{A}}_{a_m}$ *is a word in* Q^* *representing in* $\mathbb{S}(\mathcal{A})$ *the section* $(\mathcal{A}_{q_n} \cdots \mathcal{A}_{q_1})_{a_1 \cdots a_m}$ *of* $q_n \cdots q_1$ *at* $a_1 \cdots a_m$*.*

Corollary 2.3. *Let* $\mathcal{A}$ *be an automaton with state set* Q*. Suppose that* $u, v \in Q^*$ *and* v *is in the orbit of* u *under* $\mathbb{S}(\widehat{\mathcal{A}})$*, that is* $v = us$ *for some* $s \in \mathbb{S}(\widehat{\mathcal{A}})$*. Then* v *represents a section of* u*.*

Let A be the Aleshin automaton from Figure 1. Then the dual automaton for $\mathsf{A}^{\pm}$ is given by Figure 3.

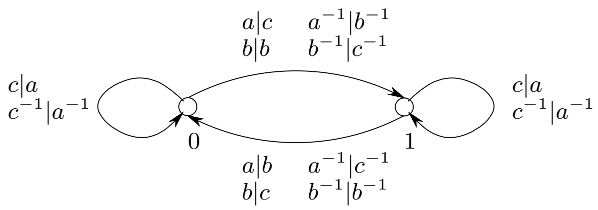

FIGURE 3. The dual of $\mathsf{A}^{\pm}$

2.4. **Reversible and bireversible automata.** The dual automaton is most useful when it is invertible. We discuss this situation here. A finite state automaton $\mathcal{A} = (Q, A, \delta, \lambda)$ is called *reversible* if, for all $a \in A$, $q, q' \in Q$, one has that $q_a = q'_a$ implies $q = q'$. That is the map $q \to q_a$ is a permutation for all $a \in A$. This is equivalent to asking that the transition monoid $M(\mathcal{A})$ be a group. In particular, a function $f : A^\omega \to A^\omega$ can be computed by a reversible automaton if and only if the minimal automaton $\mathcal{A}(f)$ is reversible. We then say that the metric contraction f is *reversible*. An invertible automaton is called *bireversible* if both it and its inverse are reversible. Notice that if $\mathcal{A}$ is bireversible, then $\mathcal{A}^{\pm}$ is also bireversible. An isometry $f : A^\omega \to A^\omega$ is called bireversible if f and f^{-1} are reversible or, equivalently, the minimal automaton $\mathcal{A}(f)$ is bireversible.

As mentioned earlier, since the class of finite groups is closed under wreath product, submonoids and quotients, the collections of all reversible metric contractions of A^ω forms a semigroup, denoted $\mathsf{Rev}(A)$, called the semigroup of reversible automata. The group of units of $\mathsf{Rev}(A)$ is then denoted $\mathsf{BiRev}(A)$ and its elements are precisely the bireversible isometries. One calls $\mathsf{BiRev}(A)$ the group of bireversible automata. See [6, 12] for relations between $\mathsf{BiRev}(A)$ and commensurators.

If $\mathcal{A}$ is a bireversible automaton, then $\mathbb{G}(\mathcal{A})$ is a finitely generated subgroup of $\mathsf{BiRev}(A)$. It turns out that such groups are particularly apt for analysis via their dual automata and they have some remarkable properties. First of all, the reversibility of $\mathcal{A}$ and $\mathcal{A}^{-1}$ is equivalent to asking that, for each $a \in A$, the maps $q \mapsto q_a$ and $q^{-1} \mapsto q_a^{-1}$ are invertible. But this is exactly the same as asking that $\widehat{\mathcal{A}}$ and $\widehat{\mathcal{A}^{-1}}$ be invertible. This proves the following well-known result [13, 16].

Proposition 2.4. *A finite automaton $\mathcal{A}$ is bireversible if and only if $\widehat{\mathcal{A}}$ and $\widehat{\mathcal{A}^{-1}}$ are invertible.*

We also need the following trivial observation: any subsemigroup of a finite group is a subgroup since the inverse of an element is a positive power. In particular, any semigroup of permutations of a finite set is a group. If $\mathcal{A}$ is an invertible automaton acting on A^*, then $\mathbb{S}(\mathcal{A})$ acts by permutations on the finite set A^n and hence acts as a finite group of permutations of A^n. Thus $\mathbb{S}(\mathcal{A})$ and $\mathbb{G}(\mathcal{A})$ have the same orbits on A^n. Summarizing, we obtain the following [16].

Lemma 2.5. *Let $\mathcal{A} = (Q, A, \delta, \lambda)$ be an invertible automaton. Then the orbits of $\mathbb{S}(\mathcal{A})$ and of $\mathbb{G}(\mathcal{A})$ on A^* are the same.*

Corollary 2.6. *Let $\mathcal{A} = (Q, A, \delta, \lambda)$ be a bireverisble automaton. Let $u, v \in Q^*$ and suppose that $ug = v$ for some $g \in \mathbb{G}(\widehat{\mathcal{A}})$. Then v represents a section of u and u represents a section of v.*

Proof. Since $u = vg^{-1}$, it suffices to show that v represents a section of u. But this follows from Lemma 2.5 and Corollary 2.2. □

In particular, we have the following criterion for triviality in a bireversible automaton group:

Corollary 2.7 (Triviality criterion)**.** *Let $\mathcal{A} = (Q, A, \delta, \lambda)$ be a bireversible automaton and let $w \in (Q^{\pm})^*$. Then the following are equivalent:*

(1) *w represents the trivial element of $\mathbb{G}(\mathcal{A})$*
(2) *all sections of w are trivial*
(3) *w has a section that is trivial*
(4) *w is in the orbit under $\mathbb{G}(\widehat{\mathcal{A}^{\pm}})$ of an element $u \in (Q^{\pm})^*$ that is trivial in $\mathbb{G}(\mathcal{A})$*
(5) *the whole orbit of w under $\mathbb{G}(\widehat{\mathcal{A}^{\pm}})$ represents the trivial element of $\mathbb{G}(\mathcal{A})$.*

Proof. Clearly (1) implies (2) since all sections of the identity transformation are trivial. The implication (2) $\Longrightarrow$ (3) is trivial. For (3) $\Longrightarrow$ (4), suppose that the section of w at $a_1 \cdots a_m \in A^*$ is trivial. Then, by Theorem 2.2, $u = w\widehat{\mathcal{A}^{\pm}}_{a_1} \cdots \widehat{\mathcal{A}^{\pm}}_{a_m}$ represents the section of w at $a_1 \cdots a_m$ and hence is trivial in $\mathbb{G}(\mathcal{A})$, so (4) holds. To see that (4) implies (1), we have by Corollary 2.6 that w is a section of the transformation represented by u. But since u represents the identity transformation and every section of the identity is the identity, it follows that w represents the trivial element of $\mathbb{G}(\mathcal{A})$. Clearly (5) implies (4). On the other hand, (2) implies (5) by Corollary 2.6. □

The implication (4) implies (1) was established in [16] and is the key tool to proving freeness. Indeed, there is the following criterion for freeness of a bireversible automaton group that is immediate from Corollary 2.7.

Corollary 2.8 (Freeness criterion)**.** *Let $\mathcal{A} = (Q, A, \delta, \lambda)$ be a bireversible automaton. Then $\mathbb{G}(\mathcal{A})$ is a free group, freely generated by the transformations $\mathcal{A}_q$, $q \in Q$, if and only for each freely irreducible word $w \in (Q^{\pm})^*$, there is a word u in the orbit of w under $\mathbb{G}(\widehat{\mathcal{A}^{\pm}})$ such that u represents a non-trivial element of $\mathbb{G}(\mathcal{A})$.*

This leads to the following basic strategy for proving that the group generated by a bireversible automaton is free.

Definition 2.9 (Pattern)**.** A word in the alphabet $\{*, *^{-1}\}$ is called a *pattern.* A word $w \in (Q^{\pm})^*$ is said to *follow* the pattern u if the image of w under the map sending Q to $*$ and Q^{-1} to $*^{-1}$ is u.

The basic strategy is then to show that all freely irreducible words following any given pattern are in the same orbit of $\mathbb{G}(\widehat{\mathcal{A}^{\pm}})$ and then to show that each pattern is followed by some element that does not act trivially on words of length 1. This strategy was successfully used by the second and third authors to prove that the Aleshin automata and its relatives are free [16, 17]. Glasner and Mozes used a similar criterion in their construction of free groups generated by automata [6].

Let us point out another property of bireversible automata that is implied by Corollary 2.7. We view A^ω as a measure space by taking the product of the uniform measure on A. For a transformation $f : A^\omega \to A^\omega$, we denote by $\mathrm{Fix}(f)$ the set of fixed points of f; it is a closed subspace of A^ω. The reader is referred to [9, 10] for the definition of the Kesten and the Kesten-von Neumann-Serre spectral measures.

Corollary 2.10. *Let $\mathcal{A} = (Q, A, \delta, \lambda)$ be a bireversible automaton and let $1 \neq g \in \mathbb{G}(\mathcal{A})$. The $\mathrm{Fix}(g)$ is nowhere dense and has measure zero. Hence the Kesten and the Kesten-von Neumann-Serre spectral measures with respect to any generating set for $\mathbb{G}(\mathcal{A})$ coincide.*

Proof. Suppose that $\mathrm{Fix}(g)$ is not nowhere dense. Then it contains a cylinder set wA^ω with $w \in A^*$. It follows that the section g_w is trivial. But then Corollary 2.7 shows that g is trivial.

It is shown in [10] that, for any transformation $f : A^\omega \to A^\omega$ computed by a finite state automaton, $\mathrm{Fix}(f)$ is nowhere dense if and only if it has measure zero, proving the second statement.

The condition $\mathrm{Fix}(g)$ has measure zero for all non-trivial elements $g \in \mathbb{G}(\mathcal{A})$ was shown to imply that the Kesten and the Kesten-von Neumann-Serre spectral measures with respect to any generating set for $\mathbb{G}(\mathcal{A})$ coincide. □

This means that for bireversible automata, one can attempt to compute the Kesten spectral measure along the lines of [8, 10]. Having completed the general theory we need for this paper, we now turn to the series of finite state automata in question.

3. The dramatis personæ

In this section we shall introduce the various automata used throughout this paper. We shall try to remind the reader explicitly when an automaton is right-to-left scanning, but it should be kept that we always take this to be the case for dual automata.

3.1. **The Aleshin automaton and its relatives.** We record here several results from [16] about Aleshin's automaton that we shall require in the sequel. Let A be Aleshin's automaton from Figure 1 and let $\mathsf{D} = \widehat{\mathsf{A}^{\pm}}$ be the right-to-left scanning automaton from Figure 3.

Theorem 3.1 ([16]). *If $p \in \{*, *^{-1}\}^*$ is a pattern, then $\mathbb{G}(\mathsf{D})$ acts transitively on the set of freely irreducible words following p. In particular, $\mathbb{G}(\mathsf{D})$ acts transitively on $\{a, b, c\}^*$.*

In the paper [16], the dual automaton is viewed as scanning from left to right, instead of right to left as we do in this paper. But this does not affect the validity of Theorem 3.1 since the notions of pattern and freely irreducible words are left-right dual, as is $\{a, b, c\}^*$. Consider the right-to-left scanning automaton E whose Moore diagram is in Figure 4.

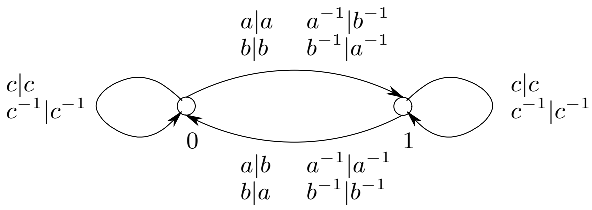

Figure 4. The right-to-left scanning automaton E

Proposition 3.2 ([16]). *$\mathbb{G}(\mathsf{D})$ is generated by E_0 and the automorphisms $(ab)^{\pm}$, $(bc)^{\pm}$.*

We remark that $\mathsf{E}_1 = \mathsf{E}_0(ab)^{\pm}$ [16] and so also belongs to $\mathbb{G}(\mathsf{D})$.

3.2. **A family of bireversible automata with an even number of states.** If $\mathcal{A} = (Q, \{0, 1\}, \delta, \lambda)$ is an invertible automaton over a binary alphabet, we say that a state $q \in Q$ is *active* if $q(0) = 1$, $q(1) = 0$; otherwise we say that q is *inactive*. We consider a family $\mathfrak{F}$ of bireversible automata over a binary alphabet defined as follows. The state set of a member $\mathcal{A} \in \mathfrak{F}$ is $Q_n = \{a, b, c, d_1, d_2, \ldots, d_n\}$, where $n \geq 1$ can be any odd number. In wreath product coordinates (c.f. (2.5)), $\mathcal{A}$ is given by:

$$a = (01)(c, b), \; b = (01)(b, c), \; c = \sigma_0(d_1, d_1)$$

$$d_i = \sigma_i(d_{i+1}, d_{i+1}), 1 \leq i \leq n-1 \text{ and } d_n = \sigma_n(a,a)$$

where the only restrictions on the $\sigma_i \in S_{\{0,1\}}$, $i = 0, \ldots, n$, is that an *odd* number of them are not the identity — that is, an odd number of the states $c, d_1, \ldots, d_n$ are active. In Figures 5 and 6, respectively, we give four-state and six-state examples from the family $\mathfrak{F}$.

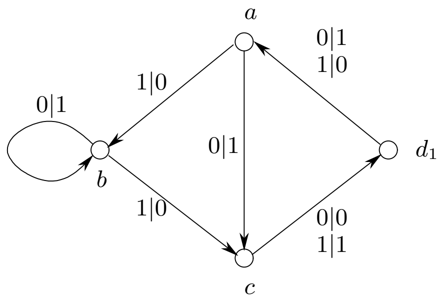

FIGURE 5. A four-state automaton from $\mathfrak{F}$

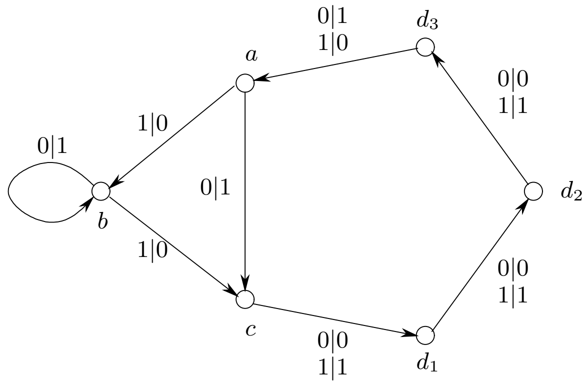

FIGURE 6. A six-state automaton from $\mathfrak{F}$

The inverse of $\mathcal{A}$ is given in wreath product coordinates (2.5) by:

$$a^{-1} = (01)(b^{-1}, c^{-1}),\ b^{-1} = (01)(c^{-1}, b^{-1}),\ c^{-1} = \sigma_0(d_1^{-1}, d_1^{-1})$$
$$d_i^{-1} = \sigma_i(d_{i+1}^{-1}, d_{i+1}^{-1}), 1 \leq i \leq n-1 \text{ and } d_n^{-1} = \sigma_n(a^{-1}, a^{-1})$$

Proposition 3.3. *Any automaton from the family $\mathfrak{F}$ is bireversible.*

Proof. Let $\mathcal{A}$ have state set Q_n. Then the input letter 0 acts on the states of $\mathcal{A}$ as the $(n+2)$-cycle $(acd_1 \cdots d_n)$ while the input letter 1 acts on the states of $\mathcal{A}$ as the $(n+3)$-cycle $(abcd_1 \cdots d_n)$. Thus $\mathcal{A}$ is reversible. Similarly, 0 acts on the states of $\mathcal{A}^{-1}$ as the $(n+3)$-cycle $(a^{-1}b^{-1}c^{-1}d_1^{-1} \cdots d_n^{-1})$ and 1 acts as the $(n+2)$-cycle $(a^{-1}c^{-1}d_1^{-1} \cdots d_n^{-1})$, so $\mathcal{A}^{-1}$ is reversible and hence $\mathcal{A}$ is bireversible. $\square$

We fix for the rest of this section a member $\mathcal{A} = (Q_n, \{0,1\}, \delta, \lambda)$ of the family $\mathfrak{F}$. Let A denote the set of active states of $\mathcal{A}^{\pm}$ and I the set of inactive states. Notice that a state q is active if and only if q^{-1} is active; that is A and I are closed under the involution. Let $\mathcal{D} = \widehat{\mathcal{A}^{\pm}}$ be the dual of the disjoint union of $\mathcal{A}$ and $\mathcal{A}^{-1}$. The state set of $\mathcal{D}$ is $\{0,1\}$. Since active states of $\mathcal{A}$ switch 0 and 1, while inactive states do not, it follows that each input letter from A to $\mathcal{D}$ switches states, while each input letter from I does not. Thus the transition diagram of $\mathcal{D}$ has the form in Figure 7.

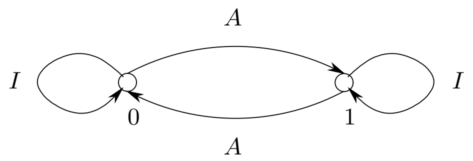

FIGURE 7. The transition diagram for the right-to-left scanning automata $\mathcal{D}$, $\mathcal{E}$ and $\mathcal{F}$

The proof of Proposition 3.3 shows that the output function of $\mathcal{D}_0$ on letters is given by the permutation

$$\delta_0 = (acd_1 \cdots d_n)(a^{-1}b^{-1}c^{-1}d_1^{-1} \cdots d_n^{-1})$$

while the output function of $\mathcal{D}_1$ on letters is given by the permutation

$$\delta_1 = (abcd_1 \cdots d_n)(a^{-1}c^{-1}d_1^{-1} \cdots d_n^{-1})$$

In wreath product coordinates (2.10), and using functional notation for $Q_n^{\pm}$-tuples, we can then write $\mathcal{D}_0 = (D_0, \delta_0)$, $\mathcal{D}_1 = (D_1, \delta_1)$ where $D_0, D_1 : Q_n^{\pm} \to \mathbb{G}(\mathcal{D})$ are given by

$$qD_i = \begin{cases} \mathcal{D}_{\overline{i}} & q \in A \\ \mathcal{D}_i & q \in I \end{cases}$$

with the notation $\overline{0} = 1$, $\overline{1} = 0$; this notation shall reoccur throughout the rest of the paper without comment.

The right-to-left scanning automaton $\mathcal{D}$ has the following useful property, which the reader easily checks: if one reverses all the arrows in the Moore diagram of $\mathcal{D}$, then you get back exactly $\mathcal{D}$, only with the states 0 and 1 reversed. Basically, the arrows with left side labelled by elements of I remain as they were, while the arrows with left side labelled by A from 0 and 1 are switched with the corresponding arrows from 1 to 0. One can then obtain via an easy induction that if u is in the orbit under $\mathbb{S}(\mathcal{D})$ of v, then u^{ρ} is in the orbit under $\mathbb{S}(\mathcal{D})$ of v^{ρ}. But for invertible automata, the orbit of the group and the semigroup are the same by Lemma 2.5, so we have proven:

Lemma 3.4. *Let $u, v \in Q_n^{\pm}$. Then u and v are in the same $\mathbb{G}(\mathcal{D})$-orbit if and only if u^{ρ} and v^{ρ} are in the same $\mathbb{G}(\mathcal{D})$-orbit.*

3.3. **The supporting cast.** We shall also need to define and study several auxiliary right-to-left scanning automata that will play a key role in proving transitivity of $\mathbb{G}(\mathcal{D})$ on patterns. Since we shall deal exclusively for the next few sections with right-to-left scanning automata, we shall use the convention that permutations act on the right of their arguments and compose them appropriately: e.g. $(ab)(abc) = (ac)$. Define a right-to-left scanning automaton $\mathcal{E} = (\{0,1\}, Q_n^{\pm}, \delta_E, \lambda_E)$ using the same transition diagram as $\mathcal{D}$ (see Figure 7) but with a different output function, modelled on E from Figure 4. Let $\varepsilon_0 = (a^{-1}b^{-1})$ and $\varepsilon_1 = (ab)$. Then we have $\mathcal{E}_0$ act on letters by ε_0 and $\mathcal{E}_1$ by ε_1. So in wreath product coordinates (2.10), $\mathcal{E}_0 = (E_0, \varepsilon_0)$, $\mathcal{E}_1 = (E_1, \varepsilon_1)$ where

$$qE_i = \begin{cases} \mathcal{E}_{\bar{i}} & q \in A \\ \mathcal{E}_i & q \in I \end{cases}$$

Recall that if $\sigma \in S_{Q_n}$, then $\overline{\sigma}$ denotes the induced involution-preserving permutation of $S_{Q_n^{\pm}}$. One can verify by direct computation:

$$\begin{aligned}
\varepsilon_0\overline{(acd_1\cdots d_n)} &= (a^{-1}b^{-1})\overline{(acd_1\cdots d_n)} = \delta_0 \\
\varepsilon_1\overline{(acd_1\cdots d_n)} &= (ab)\overline{(acd_1\cdots d_n)} = \delta_1 \\
\varepsilon_0\overline{(abcd_1\cdots d_n)} &= (a^{-1}b^{-1})\overline{(abcd_1\cdots d_n)} = \delta_1 \\
\varepsilon_1\overline{(abcd_1\cdots d_n)} &= (ab)\overline{(abcd_1\cdots d_n)} = \delta_0
\end{aligned}$$

We can then deduce from the right-to-left scanning dual to Proposition 2.1 the following lemma.

Lemma 3.5. *We have the equalities:*

(1) $\mathcal{D}_0 = \mathcal{E}_0(acd_1\cdots d_n)^{\pm}$
(2) $\mathcal{D}_1 = \mathcal{E}_1(acd_1\cdots d_n)^{\pm}$
(3) $\mathcal{D}_0 = \mathcal{E}_1(abcd_1\cdots d_n)^{\pm}$
(4) $\mathcal{D}_1 = \mathcal{E}_0(abcd_1\cdots d_n)^{\pm}$

Lemma 3.5 indicates that we should study $\mathbb{G}(\mathcal{E})$. The analysis is completely analogous to the situation for E from [16].

Lemma 3.6. *The group $\mathbb{G}(\mathcal{E})$ is a Klein 4-group. More precisely:*

(1) $\mathcal{E}_0^2 = \mathcal{E}_1^2 = 1$
(2) $\mathcal{E}_i(ab)^{\pm} = \mathcal{E}_{\bar{i}}$, $i = 0, 1$
(3) $\mathcal{E}_1\mathcal{E}_0 = (ab)^{\pm} = \mathcal{E}_0\mathcal{E}_1$

Proof. First observe that $\mathcal{E} = \mathcal{E}^{-1}$. Indeed the only edges of the Moore diagram for which both sides of the label are not the same are: $0 \xrightarrow{a^{-1}|b^{-1}} 1$, $0 \xrightarrow{b^{-1}|a^{-1}} 1$, $1 \xrightarrow{a|b} 0$ and $1 \xrightarrow{b|a} 0$. But interchanging the left and right sides of the labels just switches the first two arrows and switches the last two arrows thereby having no effect on the automaton. It follows $\mathcal{E}_0 = \mathcal{E}_0^{-1}$ and $\mathcal{E}_1 = \mathcal{E}_1^{-1}$, establishing (1).

For (2) and (3), observe that $(a^{-1}b^{-1})\overline{(ab)} = (ab)$ and $(ab)\overline{(ab)} = (a^{-1}b^{-1})$. Thus Proposition 2.1 shows that $\mathcal{E}_0 = \mathcal{E}_1(ab)^{\pm}$ and $\mathcal{E}_1 = \mathcal{E}_0(ab)^{\pm}$. Thus

$$\mathcal{E}_0\mathcal{E}_1 = \mathcal{E}_0^2(ab)^{\pm} = (ab)^{\pm}$$

Hence

$$\mathcal{E}_1\mathcal{E}_0 = (\mathcal{E}_0\mathcal{E}_1)^{-1} = ((ab)^{\pm})^{-1} = (ab)^{\pm}$$

finishing the proof. □

As a consequence, we obtain:

Lemma 3.7. *One has:*

(1) $\mathcal{D}_0^{-1}\mathcal{D}_1 = (bc)^{\pm}$
(2) $\mathcal{D}_0\mathcal{D}_1^{-1} = (ab)^{\pm}$

Hence, for all $\sigma \in S_{a,b,c}$, one has $\sigma^{\pm} \in \mathbb{G}(\mathcal{D})$.

Proof. We calculate:

$$\mathcal{D}_0^{-1}\mathcal{D}_1 = (d_n \cdots d_1 ca)^{\pm}\mathcal{E}_0\mathcal{E}_0(abcd_1 \cdots d_n)^{\pm} = (bc)^{\pm}$$
$$\mathcal{D}_0\mathcal{D}_1^{-1} = \mathcal{E}_0(acd_1 \cdots d_n)^{\pm}(d_n \cdots d_1 cba)^{\pm}\mathcal{E}_0 = \mathcal{E}_0(ab)^{\pm}\mathcal{E}_0 = (ab)^{\pm}$$

where the last equality follows from Lemma 3.6, which implies that $\mathcal{E}_0$ and $(ab)^{\pm}$ commute. □

Our next auxiliary right-to-left scanning automaton, called $\mathcal{F}$, again has transition diagram from Figure 7. Let $\varphi_0 = (a^{-1}b^{-1})\overline{(cd_1 \cdots d_n)}$ and $\varphi_1 = (ab)\overline{(cd_1 \cdots d_n)}$. Then the output of $\mathcal{F}_0$ on letters is given by the permutation φ_0 and the output of $\mathcal{F}_1$ on letters is given by the permutation φ_1. So in wreath product coordinates (2.10), $\mathcal{F}_0 = (F_0, \varphi_0)$ and $\mathcal{F}_1 = (F_1, \varphi_1)$ where

$$qF_i = \begin{cases} \mathcal{F}_{\bar{i}} & q \in A \\ \mathcal{F}_i & q \in I \end{cases}$$

Proposition 2.1 shows that

$$\mathcal{F}_0 = \mathcal{E}_0(cd_1 \cdots d_n)^{\pm} = \mathcal{D}_0(ac)^{\pm} \text{ and } \mathcal{F}_1 = \mathcal{E}_1(cd_1 \cdots d_n)^{\pm} = \mathcal{D}_1(ac)^{\pm}$$

where the equalities involving $\mathcal{D}$ come from Lemma 3.5. As a consequence of Lemma 3.7, we obtain:

Lemma 3.8. *$\mathcal{F}_0, \mathcal{F}_1 \in \mathbb{G}(\mathcal{D})$. In fact, $\mathbb{G}(\mathcal{D}) = \langle \mathcal{F}_0, \mathcal{F}_1, (ac)^{\pm} \rangle$.*

This leads us to investigate further the structure of $\mathcal{F}$.

Lemma 3.9. *The following facts hold for $\mathcal{F}$:*

(1) $\mathcal{F}_i = \mathcal{F}_{\bar{i}}(ab)^{\pm} = (ab)^{\pm}\mathcal{F}_{\bar{i}}$, $i = 0, 1$
(2) $\mathcal{F}_0\mathcal{F}_1 = \mathcal{F}_1\mathcal{F}_0$
(3) *if $w(x, y) \in \{x, y\}^*$, then*

$$w(\mathcal{F}_0, \mathcal{F}_1) = \begin{cases} \mathcal{F}_0^{|w|} & \text{if } w \text{ has an even number of } ys \\ \mathcal{F}_0^{|w|}(ab)^{\pm} = \mathcal{F}_0^{|w|-1}\mathcal{F}_1 & \text{if } w \text{ has an odd number of } ys \end{cases}$$

Proof. Let $i \in \{0,1\}$. Now, Lemma 3.6 gives us:

$$\mathcal{F}_i = \mathcal{E}_i(cd_1\cdots d_n)^{\pm} = \mathcal{E}_{\bar{i}}(ab)^{\pm}(cd_1\cdots d_n)^{\pm} = \mathcal{F}_{\bar{i}}(ab)^{\pm}$$

But Lemma 3.6 implies that $(ab)^{\pm}$ commutes with $\mathcal{E}_{\bar{i}}$, so we also get:

$$\mathcal{F}_i = \mathcal{E}_{\bar{i}}(ab)^{\pm}(cd_1\cdots d_n)^{\pm} = (ab)^{\pm}\mathcal{E}_{\bar{i}}(cd_1\cdots d_n)^{\pm} = (ab)^{\pm}\mathcal{F}_{\bar{i}}$$

For (2), we now have $\mathcal{F}_0\mathcal{F}_1 = \mathcal{F}_0(ab)^{\pm}\mathcal{F}_0 = \mathcal{F}_1\mathcal{F}_0$. Item (3) follows immediately (1) and (2). $\square$

Now if $m \geq 1$, then the sections of $\mathcal{F}_0^m$ are of the form $w(\mathcal{F}_0,\mathcal{F}_1)$ where $|w| = m$. Thus $\mathcal{F}_0^m$ has at most two sections, itself $\mathcal{F}_0^m$ and $\mathcal{F}_0^m(ab)^{\pm}$.

Let $n \geq 1$ be the odd number associated to our automaton $\mathcal{A}$ with state set Q_n from the family $\mathfrak{F}$. We want to show that $\mathcal{F}_0^{n+1}$ has two sections. More precisely let $\mathcal{G}$ be the right-to-left scanning automaton with Moore diagram in Figure 8, where we take the convention that if the right side of the label of an edge equals the left side then we omit the right side.

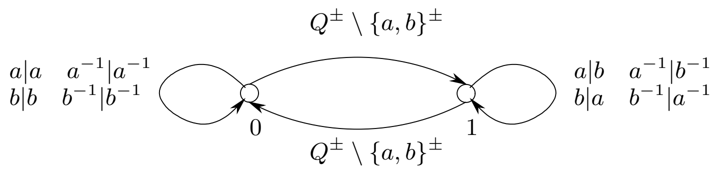

FIGURE 8. The Moore diagram for the right-to-left scanning automaton $\mathcal{G}$

In wreath product coordinates (2.10), we have $\mathcal{G}_0 = (G_0, 1)$, $\mathcal{G}_1 = (G_1, \overline{(ab)})$ where

$$qG_i = \begin{cases} G_i & q \in \{a,b\}^{\pm} \\ G_{\bar{i}} & \text{else} \end{cases}$$

The proof of our next lemma is essentially an exercise is computing powers of elements in wreath products. It is the key place where we use that $\mathcal{A}$ has an odd number of active states.

Lemma 3.10. *$\mathcal{F}_0^{n+1} = \mathcal{G}_0$, $\mathcal{F}_0^{n+1}(ab)^{\pm} = \mathcal{F}_0^n\mathcal{F}_1 = \mathcal{G}_1$. In particular, $\mathcal{G}_0, \mathcal{G}_1 \in \mathbb{G}(\mathcal{D})$.*

Proof. Recall that in wreath product coordinates, we have $\mathcal{F}_0 = (F_0, \varphi_0)$ where F_0 takes active states to $\mathcal{F}_1$ and inactive states to $\mathcal{F}_0$ and $\varphi_0 = (a^{-1}b^{-1})\overline{(cd_1\cdots d_n)}$. Then $\varphi_0^{n+1} = 1$, as $n+1$ is even. So $\mathcal{F}_0^{n+1} = (f, 1)$ where $f = F_0{}^{\varphi_0}F_0{}^{\varphi_0^2}F_0\cdots{}^{\varphi_0^n}F_0$. Notice that $\{a,b\}^{\pm}$ is invariant under φ_0 and that F_0 takes on the constant value $\mathcal{F}_1$ on $\{a,b\}^{\pm}$, since these states are all active. It follows that $qf = \mathcal{F}_1^{n+1} = \mathcal{F}_0^{n+1}$ (this last equality by Lemma 3.9) for $q \in \{a,b\}^{\pm}$. On the other hand, $\{c, d_1, \ldots, d_n\}$ and $\{c^{-1}, d_1^{-1}, \ldots, d_n^{-1}\}$ are cycles of length $n+1$ for φ_0. Thus, for $q \in Q \setminus \{a,b\}$ and $e = \pm 1$, one has that $q^e f = \prod_{r\in Q} r^e F_0$ where the product is taken in cyclic order starting from q. Actually, the order doesn't matter since F_0 only takes on the values $\mathcal{F}_0$ and $\mathcal{F}_1$ and these elements commute. So one has $q^e f = w(\mathcal{F}_0, \mathcal{F}_1)$ where $w(x, y)$ is a word of length $n+1$. The occurrences of the variable x come from inactive states in $Q \setminus \{a, b\}$ while the occurrences of the variable y come from the active states in this set. Since by hypothesis $\mathcal{A}$ has an odd number of active states in this set, we conclude by Lemma 3.9 that $q^e f = \mathcal{F}_0^{n+1}(ab)^{\pm} = \mathcal{F}_0^n \mathcal{F}_1$.

Let us abuse notation and, for $g \in \mathbb{G}(\mathcal{D})$, denote also by g the function $\mathbb{G}(\mathcal{D})^{Q^{\pm}}$ that takes on the constant value g. Then one has that

$$\mathcal{F}_0^n \mathcal{F}_1 = \mathcal{F}_0^{n+1}(ab)^{\pm} = (f, 1)((ab)^{\pm}, \overline{(ab)}) = (f(ab)^{\pm}, \overline{(ab)})$$

In particular, Lemma 3.9 implies that if $qf = \mathcal{F}_i$, then $qf(ab)^{\pm} = \mathcal{F}_{\bar{i}}$. Converting wreath product coordinates to automata, we see that on inputs in $\{a, b\}^{\pm}$, both $\mathcal{F}_0^{n+1}$ and $\mathcal{F}_0^n \mathcal{F}_1$ remain in the same state, while on inputs from $Q^{\pm} \setminus \{a, b\}^{\pm}$ they both switch states. On letters, $\mathcal{F}_0^{n+1}$ acts as the identity, while $\mathcal{F}_0^n \mathcal{F}_1$ acts as the permutation $\overline{(ab)}$. Thus $\mathcal{F}_0 = \mathcal{G}_0$, $\mathcal{F}_1 = \mathcal{G}_1$, as required. □

We remark that $\mathcal{G} = \mathcal{G}^{-1}$, and so the order of $\mathcal{F}_0$ (and hence $\mathcal{F}_1$) is $2(n+1)$. However, we shall not use this fact anywhere.

3.4. **A second family of automata.** Let $\mathfrak{F}'$ be the family of all automata that can be obtained from a member of $\mathfrak{F}$ by switching which states are active and inactive. So, for example, the Moore diagram of the element of $\mathfrak{F}'$ corresponding to the automaton in Figure 5 is given by Figure 9.

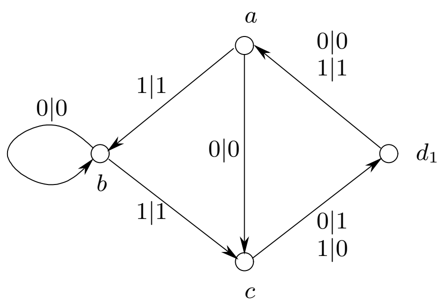

FIGURE 9. A four-state automaton from $\mathfrak{F}'$

If $\mathcal{A} = (Q_n, \{0, 1\}, \delta, \lambda) \in \mathfrak{F}$ and $\mathcal{A}'$ is the corresponding automaton in $\mathfrak{F}'$, then in the terminology of Proposition 2.1, $\mathcal{A}' = (01)[\mathcal{A}]$ and so $\mathbb{G}(\mathcal{A}') = \langle (01)^* \mathcal{A}_q \mid q \in Q_n \rangle$. In wreath product coordinates (2.5), $\mathcal{A}'$ is given by:

$$a = (c, b),\ b = (b, c),\ c = \sigma_0'(d_1, d_1)$$
$$d_i = \sigma_i'(d_{i+1}, d_{i+1}), 1 \le i \le n-1 \text{ and } d_n = \sigma_n'(a, a)$$

where σ_i' is the unique element of $S_2 \setminus \{\sigma_i\}$. Thus $(\mathcal{A}')^{-1}$ is described in wreath product coordinates by:

$$a^{-1} = (c^{-1}, b^{-1}),\ b^{-1} = (b^{-1}, c^{-1}),\ c^{-1} = \sigma_0'(d_1^{-1}, d_1^{-1})$$
$$d_i^{-1} = \sigma_i'(d_{i+1}^{-1}, d_{i+1}^{-1}), 1 \leq i \leq n-1 \text{ and } d_n^{-1} = \sigma_n'(a^{-1}, a^{-1})$$

from which it is immediate that $(\mathcal{A}')^{-1} = \mathcal{A}'$ and so each element $\mathcal{A}_q'$, with $q \in Q_n$, is its own inverse. We summarize this discussion as a lemma.

Lemma 3.11. *Let $\mathcal{A} = (Q, A, \delta, \lambda) \in \mathfrak{F}$ and let $(01)[\mathcal{A}] \in \mathfrak{F}'$ be the corresponding automaton. Then $(01)[\mathcal{A}]_q = (01)^*\mathcal{A}_q$ and $((01)^*\mathcal{A}_q)^2 = 1$.*

4. Freeness results

In this section, we prove, for $\mathcal{A} \in \mathfrak{F}$, that $\mathbb{G}(\mathcal{A})$ is a free group, freely generated by the states, and that $\mathbb{G}((01)[\mathcal{A}])$ is a free product of cyclic groups of order two, again freely generated by the states.

4.1. **Freeness for automata in $\mathfrak{F}$.** Let's fix $\mathcal{A} = (Q_n, \{0,1\}, \delta, \lambda)$ from the family $\mathfrak{F}$ for the remainder of the section. Let $\mathcal{D}, \mathcal{E}, \mathcal{F}, \mathcal{G}$ be as in the previous section.

Lemma 4.1. *The action of $\mathbb{G}(\mathcal{D})$ on $Q_n^{\pm}$ preserves patterns and sends freely irreducible words to freely irreducible words.*

Proof. Clearly $\mathbb{G}(\mathcal{D})$ preserves patterns since δ_0 and δ_1 preserve Q_n and Q_n^{-1}. To see that being freely irreducible is preserved, it suffices to show that words with a factor of the form xx^{-1} with $x \in Q_n^{\pm}$ are preserved by the action of $\mathbb{G}(\mathcal{D})$. Lemma 3.8 shows that $\mathbb{G}(\mathcal{D})$ is generated by $\mathcal{F}_0$, $\mathcal{F}_1$ and $(ac)^{\pm}$. Clearly $(ac)^{\pm}$ preserves factors of the form xx^{-1} $x \in Q_n^{\pm}$. On elements of $((Q_n \setminus \{a,b\})^{\pm})^*$, both $\mathcal{F}_0$ and $\mathcal{F}_1$ acts as $(cd_1 \cdots d_m)^{\pm}$ and so preserve factors of the form xx^{-1} with $x \in (Q_n \setminus \{a,b\})^{\pm})$. On the other hand, $\mathcal{F}_0(xx^{-1}) = xx^{-1}$ for $x \in \{a,b\}$ while $\mathcal{F}_0(a^{-1}a) = b^{-1}b$, $\mathcal{F}_0(b^{-1}b) = a^{-1}a$. A similar computation shows that $\mathcal{F}_1$ preserves such factors. This completes the proof. $\square$

Next we show that each non-empty pattern contains an element that changes the first letter of a word and hence a non-trivial element.

Proposition 4.2. *Let $p \in \{*, *^{-1}\}^*$ be a non-empty pattern. Then there is a freely irreducible word $w \in (Q_n^{\pm})$, following the pattern p, such that w acts non-trivially on $\{0,1\}^*$.*

Proof. We construct such a w acting non-trivially on the first letter of a word. Recall that an element x^e, with $x \in Q_n$, $e = \pm 1$, acts non-trivially on the first letter of a word in $\{0,1\}^*$ if and only if x is an active state of $\mathcal{A}$. First construct a word v by replacing each $*$ in p by a and each $*^{-1}$ by b^{-1}. Evidently, v is freely irreducible and follows p. If v acts non-trivially on the first letter of a word, we are done. Else, since both a and b^{-1} are active, it follows that the total number of as and b^{-1}s is even. Choose any inactive state q from $\{c, d_1, \ldots, d_n\}$; since there are an even number of elements in this set and by hypothesis an odd number are active, we can find such a state q. Now we obtain a new word w by replacing the first letter of v by q or q^{-1} according to whether the first letter of p is $*$ or $*^{-1}$. Then w is still freely irreducible and now the number of letters in w corresponding to actives states is odd. So w acts non-trivially on the first letter of each word. □

We shall prove now that $\mathbb{G}(\mathcal{D})$ acts transitively on the set of freely irreducible words following any given pattern. Then Corollary 2.8, in light of Proposition 4.2, will imply that $\mathbb{G}(\mathcal{A})$ is a free group on $n+3$ generators, the elements $\mathcal{A}_q$, $q \in Q_n$, being a free basis.

A key tool in proving the transitivity on patterns is a standard lemma (c.f. [16]) that plays an important role in the induction argument. For $u \in (Q_n^{\pm})^*$, we denote by $\mathrm{Stab}(u)$ the stabilizer of u in $\mathbb{G}(\mathcal{D})$. Recall that $\mathbb{G}(\mathcal{D})$ acts on the right of words, scanning from right to left.

Lemma 4.3. *Let p be a non-empty pattern and let p_0 be the pattern obtained from p by removing its first letter. Then $\mathbb{G}(\mathcal{D})$ acts transitively on the set of freely irreducible words following p if and only if it acts transitively on the set of freely irreducible words following p_0 and there is a freely reducible word w following p so that $\mathrm{Stab}(w_0)$, where w_0 is obtained by removing the first letter of w, acts transitively on the set of freely irreducible words following p with suffix w_0.*

Proof. Suppose first that $\mathbb{G}(\mathcal{D})$ acts transitively on the set of freely irreducible words following p. Then, by ignoring first letters, it is immediate that it acts transitively on the set of freely irreducible words following p_0. Moreover, if w is any freely irreducible word following p and w_0 is the suffix of w obtained by removing the first letter, then $\mathbb{G}(\mathcal{D})$ acts transitively on the set of freely irreducible words following p with suffix w_0. But if $xw_0g = yw_0$ then $g \in \mathrm{Stab}(w_0)$, so $\mathrm{Stab}(w_0)$ acts transitively on such words.

For the converse, suppose that w is a word following p as in the hypothesis and let w_0 be obtained by removing the first letter of w. Let v be a word following the pattern p. Then by assumption, there exists $g \in \mathbb{G}(\mathcal{D})$ such that $vg = xw_0$ for some x. Moreover, xw_0 is freely irreducible and follows p by Lemma 4.1. Then our assumption on $\mathrm{Stab}(w_0)$ gives us an element $g' \in St_{w_0}$ with $xw_0g' = w$. Thus $vgg' = w$. This establishes the transitivity on the pattern p. □

Now we turn to the "Critical Lemma", whose consequences shall be used over and over again. It allows us to use the powerful results of [16] concerning the dual to Aleshin's automaton.

Lemma 4.4 (Critical Lemma)**.** *Let $H \leq \mathbb{G}(\mathcal{D})$ be the subgroup generated by $\mathcal{G}_0, \mathcal{G}_1$, $(ab)^{\pm}$ and $(bc)^{\pm}$. Let $a_1, \ldots, a_m, b_1, \cdots, b_m \in \{a, b, c\}$, $x_1, x_m \in ((Q_n \setminus \{a, b, c\})^{\pm})^*$, $x_2, \ldots, x_{m-1} \in (Q_n \setminus \{a, b, c\})^{\pm}$ and $e_1, \ldots, e_m \in \{\pm 1\}$.*

Then there exists $g \in H$ such that

$$x_m a_m^{e_m} x_{m-1} \cdots x_2 a_1^{e_1} x_1 g = x_m b_m^{e_m} x_{m-1} \cdots x_2 b_1^{e_1} x_1 \tag{4.1}$$

Proof. Let Γ be the group of transformations of $(\{a,b,c\}^{\pm})^*$ generated by E_0, $(ab)^{\pm}$ and $(bc)^{\pm}$ (see Figure 4). This is the same as the group generated by the dual automaton to Aleshin's automata by Proposition 3.2. By Theorem 3.1, Γ acts transitively on $\{a,b,c\}^*$. We basically simulate the action of Γ using H.

More precisely, we show that if γ is a generator of Γ and $a_m \cdots a_1 \gamma = b_m \cdots b_1$, then there exists $g \in H$ so that (4.1) holds. The result then follows from the transitivity of Γ on $\{a,b,c\}^*$. If $\gamma = (ab)^{\pm}$ or $(bc)^{\pm}$, then we can take $g = \gamma$. This leaves us with $\gamma = \mathsf{E}_0$.

Suppose first that that x_1 has odd length. Then

$$x_m a_m^{e_m} x_{m-1} \cdots x_2 a_1^{e_1} x_1 \mathcal{G}_1 = x_m a_m^{e_m} x_{m-1} \cdots x_2 a_1^{e_1} \mathcal{G}_0 x_1$$

next we observe that $x_{i+1} a_i$ switches states in $\mathcal{G}$ if and only if $a_i \in \{a,b\}$ while a_i switches states in E if and only if $a_i \in \{a,b\}$. Moreover, E_0, E_1 act on letters from $\{a,b,c\}$ as the identity, respectively, as (ab). On the other hand $\mathcal{G}_0$, $\mathcal{G}_1$ act on letters from $\{a,b,c\}^{\pm}$ as the identity, respectively, $\overline{(ab)}$. Thus $x_{i+1} a_i^{e_i} \mathcal{G}_j = x_{i+1} (a_i \mathsf{E}_j)^{e_i}$. Combining these two observations we see that taking $g = \mathcal{G}_1$ gives the equality (4.1). If x_1 has even length, then

$$x_m a_m^{e_m} x_{m-1} \cdots x_2 a_1^{e_1} x_1 \mathcal{G}_0 = x_m a_m^{e_m} x_{m-1} \cdots x_2 a_1^{e_1} \mathcal{G}_0 x_1$$

and the same argument applies to show that $g = \mathcal{G}_0$ does the job. $\square$

Let us state a corollary that we shall use frequently in the sequel.

Corollary 4.5. *Let $w = d_1^{e_m} a_m d_1^{e_{m-1}} \cdots d_1^{e_1} a_1 d_1^k$ with $a_j \in \{a,b\}^{\pm}$, $e_j \in \{\pm 1\}$, all j, and $k \in \mathbb{Z}$ (we admit the possibility $w = d_1^k$, i.e. $m = 0$). Then $a^e w$, $b^e w$ and $c^e w$, where $e \in \{\pm 1\}$ is fixed, are in the same orbit of $\mathcal{G}(\mathcal{D})$. Moreover, if $n > 1$, then, for $1 < i \le n$, $d_i^e w$ is also in this orbit.*

Proof. The Critical Lemma immediately applies to show that $a^e w$, $b^e w$ and $c^e w$ are in the same orbit. Suppose now $n > 1$. First observe, since $(\{a,b\}^{\pm})^*$ is invariant under the action of $\mathcal{F}_0, \mathcal{F}_1$:

$$d_i^e w \mathcal{F}_0^{n-i+1} = c^e d_{n-i+2}^{e_m} b_m d_{n-i+2}^{e_{m-1}} \cdots d_{n-i+2}^{e_2} b_2 d_{n-i+2}^k = c^e u$$

with the $b_j \in \{a,b\}^{\pm}$. Now by the Critical Lemma, there exist $g_1, g_2 \in H$ so that $c^e u g_1 = a^e u$ and $c^e u g_2 = b^e u$. Again using that $(\{a,b\}^{\pm})^*$ is invariant under the action of $\mathcal{F}_0, \mathcal{F}_1$, we see that one of $a^e u \mathcal{F}_0^{-(n-i+1)}$, $b^e u \mathcal{F}_0^{-(n-i+1)}$ is $a^e w$ and the other is $b^e w$. This completes the proof. $\square$

A further property of the subgroup H that we shall need later is contained in the following lemma.

Lemma 4.6. *Let $x \in Q^{\pm}$ and $w \in (Q_n^{\pm})^*$. Suppose that $h \in H$ and $wxh = uy$ where $y \in Q_n$. Then there exists $h' \in H$ such that $wxxh' = uyy$.*

Proof. By an easy induction on the length of g, it suffices to verify this for the generators $(ab)^{\pm}$, $(bc)^{\pm}$, $\mathcal{G}_0$, $\mathcal{G}_1$ of H. Actually, Lemma 3.10 shows that $\mathcal{G}_1 = \mathcal{G}_0(ab)^{\pm}$ so we can omit $\mathcal{G}_1$. If $h = (ab)^{\pm}, (bc)^{\pm}$, we can clearly take $h' = h$. If $h = \mathcal{G}_0$ and $x \in \{a, b\}^{\pm}$, then we can again take $h' = h$ since x labels a loop at each vertex of $\mathcal{G}$. If $x = c^{\pm 1}$, then take $h' = \mathcal{G}_1$. $\square$

Another technical lemma that we shall need is the following variant on Corollary 4.5.

Lemma 4.7. *Let $e \in \{\pm 1\}$ and $u \in (\{a, d_1\}^{\pm})^*$. Then $b^e u$ and $c^e u$ are in the same orbit under $\mathbb{G}(\mathcal{D})$. Moreover, if $n > 1$ and $1 < i \leq n$, then $d_i^e u$ is in the same $\mathbb{G}(\mathcal{D})$-orbit as $b^e u$ and $c^e u$.*

Proof. Clearly $b^e u(bc)^{\pm} = c^e u$ and so they are in the same orbit. Suppose $n > 1$ and $1 < i \leq n$. First observe that $d_i^e u(ac)^{\pm} = d_i^e u'$ where $u' \in (\{c, d_1\}^{\pm})^*$. Then $d_i^e u' \mathcal{F}_0^{n-i+1} = c^e u''$ where $u'' \in (\{d_{n-i+1}, d_{n-i+2}\}^{\pm})^*$. Now $c^e u''(ac)^{\pm} = a^e u''$ and $c^e u''(bc)^{\pm} = b^e u''$. Since $\mathcal{F}_0^{-1}$ preserves $\{a^e, b^e\}$, one of the pair $a^e u'' \mathcal{F}_0^{-(n-i+1)}$, $b^e u'' \mathcal{F}_0^{-(n-i+1)}$ is $a^e u'$ and the other is $b^e u'$. Then $b^e u'(ac)^{\pm} = b^e u$, establishing that $b^e u$ is in the orbit of $d_i^e u$. $\square$

We now turn to the main technical proposition of the paper, where we prove transitivity on the patterns.

Proposition 4.8. *Let $p \in \{*, *^{-1}\}^*$ be a pattern. Then $\mathbb{G}(\mathcal{D})$ acts transitively on the set of freely irreducible words in $(Q_n^{\pm})^*$ following the pattern p.*

Proof. The proof goes by induction on the length of the pattern p. Clearly, the statement is true for the empty pattern. For patterns of length 1, the result holds since the permutation δ_0 acts transitively on Q_n^{-1} while δ_1 acts transitively on Q_n. Suppose that the proposition is true for all patterns of length m and suppose that p has length $m+1$. We shall use without comment throughout that $\sigma^{\pm} \in \mathbb{G}(\mathcal{D})$ whenever $\sigma \in S_{a,b,c}$.

First we handle the case $p = * * \cdots *$ or $*^{-1} *^{-1} \cdots *^{-1}$. Let $e \in \{\pm 1\}$. Consider $w = d_1^{e(m+1)}$. By Lemma 4.3 it suffices to show that $\mathrm{Stab}(d_1^{em})$ acts transitively on $\{x^e d_1^{em} \mid x \in Q_n\}$. By Corollary 4.5, we have that, for $1 < i \leq n$, $d_i^e d_1^{em}$ is in the same orbit as $a^e d_1^{em}$, $b^e d_1^{em}$ and $c^e d_1^{em}$. Thus, all we need to do is show that we can change the first letter of w to some other letter, leaving the rest of w alone. Now

$$d_1^{e(m+1)} \mathcal{F}_0^{-1}(ac)^{\pm} = c^{e(m+1)}(ac)^{\pm} = a^{e(m+1)}$$

Set $i = 0$ if $e = 1$ and $i = 1$ if $e = -1$. Then:

$$a^{e(m+1)} \mathcal{F}_i = \begin{cases} (b^e a^e)^{\frac{m+1}{2}} & m+1 \text{ even} \\ a^e (b^e a^e)^{\frac{m}{2}} & m+1 \text{ odd} \end{cases}$$

We break the proof into two cases, depending on whether $m+1$ is even or odd. Suppose that $m+1$ is even. Then $(b^e a^e)^{\frac{m+1}{2}}(ac)^{\pm} = (b^e c^e)^{\frac{m+1}{2}}$ and

$$(b^e c^e)^{\frac{m+1}{2}} \mathcal{F}_i = \begin{cases} (a^e d_1^e)^{\frac{m+1}{2}} & c \text{ active} \\ (a^e d_1^e b^e d_1^e)^{\frac{m+1}{4}} & c \text{ inactive and } 4 \mid m+1 \\ (b^e d^e)(a^e d_1^e b^e d_1^e)^{\frac{m-1}{4}} & c \text{ inactive and } 4 \nmid m+1 \end{cases}$$

By the Critical Lemma, in all cases we can find an element $g \in H$ the changing the first letter of $(b^e c^e)^{\frac{m+1}{2}} \mathcal{F}_i$ to, say c^e, and leaving the remaining letters alone. Then, by undoing the previous transformations (not including g), we have managed to change the first letter, and only the first letter, of w as required.

Suppose now that $m+1$ is odd. Then $a^e(b^e a^e)^{\frac{m}{2}}(bc)^{\pm} = a^e(c^e a^e)^{\frac{m}{2}}$. Then

$$a^e(c^e a^e)^{\frac{m}{2}} \mathcal{F}_i = \begin{cases} a^e(d_1^e a^e)^{\frac{m}{2}} & c \text{ active} \\ a^e(d_1^e b^e d_1^e a^e)^{\frac{m}{4}} & c \text{ inactive and } m/2 \text{ even} \\ b^e d_1^e a^e(d_1^e b^e d_1^e a^e)^{\frac{m-2}{4}} & \text{inactive and } m/2 \text{ odd} \end{cases}$$

Again, by the Critical Lemma, we can change the first letter of $a^e(c^e a^e)^{\frac{m}{2}} \mathcal{F}_i$ to c^e and then undo the previous transformations with the result that the first letter only of w is changed. This finishes the case at hand.

The next case we handle is when p begins with $*^e *^{-e}$, where $e \in \{\pm 1\}$. Let $w = a^e d_1^{-e} \cdots$ be the word following the pattern p starting with a^e and alternating $a^{\pm 1}$ with $d_1^{\pm 1}$. Let $w_0 = d_1^{-e} \cdots$ be the word obtained from w by removing the first letter a^e. By Lemma 4.3, it suffices to show that $\mathrm{Stab}(w_0)$ acts transitively on the words of the form $x^e w_0$ where $x \in Q_n \setminus \{d_1\}$. But this is immediate from Corollary 4.5.

If the last two letters of the pattern p are $*^e *^{-e}$, then the previous case and Lemma 3.4 show that all freely irreducible words following p are in one orbit. Thus we are left with the case of a pattern of the form $*^{e_2} *^{e_2} \cdots *^{e_1} *^{e_1}$ where $e_1, e_2 \in \{\pm 1\}$. We begin with the case where the length $m+1$ of our pattern p is odd. Consider $w = a^{e_2} d_1^{e_2} \cdots d_1^{e_1} a^{e_1}$, the alternating word of length $m+1$ in $a^{\pm 1}$ and $d_1^{\pm 1}$ following the pattern p and starting with a^{e_2}. Let $w_0 = d_1^{e_2} \cdots d_1^{e_1} a^{e_1}$ be the word obtained by deleting the first a^{e_2} from w. By Corollary 4.5, w is in the same orbit as $b^{e_2} w_0$, $c^{e_2} w_0$ and $d_i^{e_2} w_0$, for $1 < i \leq n$. We thus just need to show that we can find an element of $\mathbb{G}(\mathcal{D})$ that changes the first letter of $d_1^{e_2} w_0$ and leaves the suffix w_0 alone (or failing this, try and prove transitivity by some dirty trick). Let u be the word obtained from w_0 by changing the last letter from a^{e_1} to $d_1^{e_1}$; so $u = d_1^{e_2} \cdots d_1^{e_1} d_1^{e_1}$ where the part in the middle alternates the letters $a^{\pm 1}$ and $d_1^{\pm 1}$. By induction, there exists $g \in \mathbb{G}(\mathcal{D})$ such that $w_0 g = u$. Hence, $d_1^{e_2} w_0 g = x^{e_2} u$ where $x \in Q_n$. Suppose first that $x \in Q_n \setminus \{d_1\}$. Choose $y \in Q_n \setminus \{d_1, x\}$. Then, by Corollary 4.5, we can find $g' \in \mathbb{G}(\mathcal{D})$ so that $x^{e_2} u g' = y^{e_2} u$. Then $d_1^{e_2} w_0 g g' g^{-1} = z^{e_2} w_0$ with $z \in Q_n \setminus \{d_1\}$ and we are done. So suppose instead that $x = d_1$. Then $w_1 = x^{e_2} u = d_1^{e_2} d_1^{e_2} \cdots d_1^{e_1} d^{e_1}$, where the middle part alternates $a^{\pm 1}$ and $d_1^{\pm 1}$. Thus w_1 differs from $d_1^{e_2} w_0$ only in the last letter. Consider the reversals:

$$(d_1^{e_2} w_0)^\rho = a^{e_1} d_1^{e_1} \cdots d_1^{e_2} d_1^{e_2} = a^{e_1} v \text{ and } w_1^\rho = d^{e_1} d_1^{e_1} \cdots d_1^{e_2} d_1^{e_2} = d^{e_1} v$$

Since $d_1^{e_2} w_0$ and w_1 are in the same $\mathbb{G}(\mathcal{D})$-orbit, Lemma 3.4 implies that $(d_1^{e_2} w_0)^\rho = a^{e_1} v$ and $w_1^\rho = d_1^{e_1} v$ are in the same orbit. By Corollary 4.5, $a^{e_1} v$ is in the same orbit as $b^{e_1} v$, $c^{e_1} v$ and $d_i^{e_1} v$, for $1 < i \leq n$. Thus $\mathrm{Stab}(v)$ acts transitively on the set of freely irreducible words of length $m+1$ following the reverse pattern p^ρ with suffix v. Hence, by Lemma 4.3, $\mathbb{G}(\mathcal{D})$ acts transitively on the set of freely irreducible words following the pattern p^ρ. Lemma 3.4 then shows that $\mathbb{G}(\mathcal{D})$ acts transitively on the set of freely irreducible words following the pattern p.

Our final (and most difficult) case arises when the length $m+1$ of p is even. Then consider $w = a^{e_2} d_1^{e_2} \cdots a^{e_1} d_1^{e_1}$ the alternating word of length $m+1$ in $a^{\pm 1}$ and $d_1^{\pm 1}$ following p. Let $w_0 = d_1^{e_2} \cdots a^{e_1} d_1^{e_1}$ be the word obtained by removing the first letter a^{e_2}. By Corollary 4.5, w is in the same orbit as a $b^{e_2} w_0$, $c^{e_2} w_0$ and $d_i^{e_2} w_0$, for $1 < i \leq n$. So again we just need to show that we can find an element of $\mathbb{G}(\mathcal{D})$ that changes the first letter of $w' = d_1^{e_2} w_0$ and leaves the suffix w_0 alone (or find some more dirty tricks). Let u be the word obtained from w_0 by changing the last letter from $d_1^{e_1}$ to a^{e_1}; so $u = d_1^{e_2} \cdots a^{e_1} a^{e_1}$ where the part in the middle alternates $a^{\pm 1}$ and $d_1^{\pm 1}$. By induction, there exists $g \in \mathbb{G}(\mathcal{D})$ such that $w_0 g = u$. So $w_1 = w' g = d_1^{e_2} w_0 g = x^{e_2} u$ with $x \in Q_n$. Suppose first that $x \in \{a, b, c\}$. Let $u = u' a^{e_1} a^{e_1}$. By the Critical Lemma, there exists $h \in H$ such that

$$x^{e_2} u' a^{e_1} h = y^{e_2} u' a^{e_1}$$

where $y \in \{a, b, c\} \setminus \{x\}$. Then, by Lemma 4.6, we can find $h' \in H$ such that

$$x^{e_2} u h' = x^{e_2} u' a^{e_1} a^{e_1} h' = y^{e_2} u' a^{e_1} a^{e_1}$$

Then $w' g h' g^{-1}$ changes the first letter of w' and leaves the suffix w_0 alone, as required. Thus we are left with the case that $x \in \{d_1, \ldots, d_n\}$. Assume first that $x = d_i$ with $1 < i \leq n$. Then Lemma 4.7 shows that there is an element $g_0 \in \mathbb{G}(\mathcal{D})$ with $d_i^{e_2} u g_0 = b^{e_2} u$. Then $w' g g_0 g^{-1}$ is a word ending in w_0 but with a different first letter than w' and we are done.

We turn to the case $x = d_1$, so $w_1 = w' g = d_1^{e_2} u$. Notice that w_1 and w' differ only in the last letter. Therefore,

$$\begin{aligned} w'^\rho &= d_1^{e_1} a^{e_1} \cdots d_1^{e_2} d_1^{e_2} = d_1^{e_1} r \\ w_1^\rho &= a^{e_1} a^{e_1} \cdots d_1^{e_2} d_1^{e_2} = a^{e_1} r \end{aligned}$$

where r is an alternating word in $a^{\pm 1}$ and $d_1^{\pm 1}$ starting with a^{e_1}. By Lemma 3.4, we have that w'^ρ, w_1^ρ are in the same $\mathbb{G}(\mathcal{D})$-orbit, since w' and w_1 are in the same orbit. Lemma 4.7 shows that $b^{e_1} r$, $c^{e_1} r$ and $d_i^e r$, for $1 < i \leq n$, are all in the same $\mathbb{G}(\mathcal{D})$-orbit. The conclusion that we may draw is that $\mathrm{Stab}(r)$ has no singleton orbits on the set $Q_n^{e_1} r$.

Our goal now is to show transitivity on freely irreducible words following the reverse pattern p^ρ. To do this, consider the alternating word $t = a^{e_1}d_1^{e_1}\cdots a^{e_2}d_1^{e_2}$ following the pattern p^ρ. Let $t_0 = d_1^{e_1}\cdots a^{e_2}d_1^{e_2}$ be the word obtained by removing the first letter of t. We show $\mathrm{Stab}(t_0)$ acts transitively on the set of $Q_n^{e_1}t_0$; this will give the desired transitivity by Lemma 4.3. By Corollary 4.5, $\{y^{e_1}t_0 \mid y \in Q_n \setminus \{d_1\}\}$ is in a single orbit. So it suffices to show that $\mathrm{Stab}(t_0)$ has no singleton orbits on $Q_n^{e_1}t_0$. By induction, there exists $g' \in \mathbb{G}(\mathcal{D})$ such that $t_0g' = r$. Hence the action of $\mathrm{Stab}(t_0)$ on $Q_n^{e_1}t_0$ is conjugate to the action of $\mathrm{Stab}(r)$ on $Q_n^{e_1}r$ — but the latter was already shown to have no singleton orbits. This establishes the transitivity for p^ρ and hence, by Lemma 3.4, for p. This completes the proof of the proposition. □

As a consequence of Propositions 4.8 and 4.2 and in light of Corollary 2.8, we have proven our main theorem:

Theorem 4.9. *If $\mathcal{A}$ belongs to the family $\mathfrak{F}$, then the states of $\mathcal{A}$ freely generate a free group. In particular for every even number $n \geq 4$, there is an n-state connected automaton over a binary alphabet, whose states freely generate a free group of rank n.*

4.2. **Free products of cyclic groups.** We obtain the result for the family $\mathfrak{F}'$ from the result for the family $\mathfrak{F}$ using a straightforward fact from combinatorial group theory, a proof of which can be found in [17, Lemma 6.5].

Lemma 4.10. *Suppose that G is a group generated by elements $g_0, g_1, \ldots, g_k$, $k \geq 1$, satisfying $g_i^2 = 1$, $0 \leq i \leq k$. Let H be the subgroup generated by $h_1, \ldots, h_k$, where $h_i = g_0g_i$, $1 \leq i \leq k$. Then G is a free product of $k+1$ cyclic groups of order two, freely generated by $g_0, \ldots, g_k$, if and only if H is a free group of rank k, freely generated by $h_1, \ldots, h_k$.*

Theorem 4.9, in light of Lemmas 3.11 and 4.10, establishes the following result:

Theorem 4.11. *Let $\mathcal{A} = (Q_n, \{0,1\}, \lambda, \delta) \in \mathfrak{F}$, with $n \geq 1$, and let $(01)[\mathcal{A}] \in \mathfrak{F}'$ be the corresponding automaton. Then the group generated by the free monoid automorphism $(01)^*$ and the elements $(01)^*\mathcal{A}_q = (01)[\mathcal{A}]_q$, with $q \in Q_n$, is a free product of $n+4$ cyclic groups of order two, freely generated by $(01)^*$ and the $n+3$ states of $(01)[\mathcal{A}]_q$. In particular, the states of each member of $\mathfrak{F}'$ freely generate a free product of cyclic groups of order two.*

References

1. S. V. Aleshin, *A free group of finite automata*, Mosc. Univ. Math. Bull. **38** (1983), 10–13.
2. L. Bartholdi, R. I. Grigorchuk and Z. Šunić, *Branch groups* in: "Handbook of Algebra", Vol. 3, 989–1112, North-Holland, Amsterdam, 2003.

3. H. Bass, M. V. Otero-Espinar, D. Rockmore and C. Tresser, "Cyclic Renormalization and Automorphism Groups of Rooted Trees", Lecture Notes in Mathematics, **1621**. Springer-Verlag, Berlin, 1996.
4. A. M. Brunner and S. Sidki, *The generation of* $\mathrm{GL}(n, \mathbf{Z})$ *by finite state automata*, Internat. J. Algebra Comput. **8** (1998), 127–139.
5. S. Eilenberg, "Automata, Languages and Machines", Academic Press, New York, Vol. A, 1974; Vol. B, 1976.
6. Y. Glasner and S. Mozes, *Automata and square complexes*, Geom. Dedicata **111** (2005), 43–64.
7. R. I. Grigorchuk, V. V. Nekrashevich and V. I. Sushchanskii, *Automata, dynamical systems, and groups*, Tr. Mat. Inst. Steklova **231** (2000), 134–214. English translation in: R. I. Grigorchuk, (ed.), "Dynamical systems, automata, and infinite groups." Proc. Steklov Inst. Math. **231** (2000), 128–203.
8. R. I. Grigorchuk and A. Żuk, *The lamplighter group as a group generated by a 2-state automaton, and its spectrum*, Geom. Dedicata **87** (2001), 209–244.
9. R. I. Grigorchuk and A. Żuk, *The Ihara zeta function of infinite graphs, the KNS spectral measure and integrable maps*, in: "Random Walks and Geometry", Berlin, 2004, 141–180.
10. M. Kambites, P. V. Silva and B. Steinberg, *The spectra of lamplighter groups and Cayley machines*, Geom. Dedicata, to appear.
11. K. Krohn, J. Rhodes and B. Tilson, *Lectures on the algebraic theory of finite semigroups and finite-state machines*, Chapters 1, 5, 7-9 of "Algebraic Theory of Machines, Languages, and Semigroups", M. A. Arbib, (ed.), Academic Press, New York, 1968.
12. O. Macedońska, V. Nekrashevych and V. Sushchansky, *Commensurators of groups and reversible automata*, Dopov. Nats. Akad. Nauk Ukr., Mat. Pryr. Tekh. Nauky (2000), 36–39.
13. V. Nekrashevych, "Self-similar groups," Mathematical Surveys and Monographs, 117. American Mathematical Society, Providence, RI, 2005.
14. J. Rhodes, *Monoids acting on trees: elliptic and wreath products and the holonomy theorem for arbitrary monoids with applications to infinite groups*, Internat. J. Algebra Comput. **1** (1991), 253–279.
15. P. V. Silva and B. Steinberg, *On a class of automata groups generalizing lamplighter groups*, Internat. J. Algebra Comput. **15** (2005), 1213–1234.
16. M. Vorobets and Y. Vorobets, *On a free group of transformations defined by an automaton*, Geom. Dedicata, to appear.
17. M. Vorobets and Y. Vorobets, *On a series of finite automata defining free transformations groups*, preprint, 2006 (arXiv.org/math.GR/0604328).

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, Ontario K1S 5B6, Canada
E-mail address: bsteinbg@math.carleton.ca

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

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