Orbits of Abelian Automaton Groups

Tim Becker
tbecker@cs.wisc.edu

Klaus Sutner
sutner@cs.cmu.edu

Abstract

Automaton groups are a class of self-similar groups generated by invertible finite-state transducers [10]. Extending the results of Nekrashevych and Sidki [11], we describe a useful embedding of abelian automaton groups into a corresponding algebraic number field, and give a polynomial time algorithm to compute this embedding. We apply this technique to study iteration of transductions in abelian automaton groups. Specifically, properties of this number field lead to a polynomial-time algorithm for deciding when the orbits of a transduction are a rational relation. These algorithms were implemented in the SageMath computer algebra system and are available online [2].

1 Introduction

An *invertible binary transducer* $\mathcal{A}$ is a Mealy automaton over the binary alphabet where each state has an invertible output function. The transductions of $\mathcal{A}$ are therefore length-preserving invertible functions on binary strings. These transductions (along with their inverses) naturally generate a group under composition, denoted $\mathcal{G}(\mathcal{A})$. Such groups, over a general alphabet, are called automaton groups or self-similar groups; these groups have been studied in great detail, see [10, 5] for extensive studies.

Automaton groups have many interesting properties and are capable of surprising complexity. A number of well-known groups can be generated by fairly simple transducers, indicating that transducers may be a useful semantic interpretation for many groups. Bartholdi's recent book review in the Bulletin of the AMS about the relationship between syntactic and semantic approaches to algebra gives some examples where transducers play such a role [1]. For instance, after Grigorchuk famously solved the long-open problem of finding a group of intermediate growth, it was realized that his group can be generated by the 5-state invertible binary transducer shown in Figure 1. In fact, even 3-state invertible binary transducers generate groups which are exceedingly complicated, see [3] for a classification of all such automata.

Here, we will be primarily concerned with a simpler class of transducers: those which generate abelian groups. This situation has been previously studied in [12, 16]. It is known that all abelian automaton groups are either boolean or free abelian [12], and in the free abelian case, one can show that the underlying automata have nice

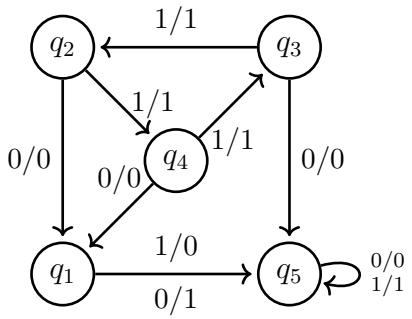

Figure 1: An invertible binary transducer generating Grigorchuk's group

structural properties. We will summarize and build upon these results in Section 2.2. A running example in this paper will be the transducer CC_2^3, shown in Figure 2. This transducer generates a group isomorphic to $\mathbb{Z}^2$ and is perhaps the simplest nontrivial transducer generating an abelian group.

We will make connections between abelian automaton groups and other areas of algebra that will provide useful insight into their structure and complexity. A result of Nekrashevych and Sidki shows that the groups admit embeddings into $\mathbb{Z}^m$ where transitions in the transducer correspond to affine maps [11]. In this paper, we describe a related embedding of abelian automaton groups into associated algebraic number fields and describe how these may be efficiently computed.

Properties of this embedding can be used to study computational problems arising in automaton groups. Given a transduction $f \in \mathcal{G}(\mathcal{A})$, we write $f^* \subseteq \mathbf{2}^* \times \mathbf{2}^*$ for the transitive closure of f. Note that f^* is a length-preserving equivalence relation on $\mathbf{2}^*$. The complexity of this relation was first studied in [17], where it was shown that for a certain class of abelian transductions f, f^* is rational. We will refer to such transductions as *orbit-rational*. For instance, it was shown in [17] that CC_2^3 is orbit-rational. In this paper, we answer a more general question by giving a precise characterization of orbit-rational abelian transducers and a corresponding decision procedure.

Throughout this paper, we will utilize the theory of free abelian groups, linear algebra, field theory, and some algebraic number theory. See [6] for the necessary material on the latter subjects, and [7, 15] for background on algebraic number theory.

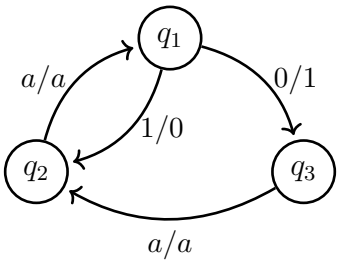

Figure 2: The cycle-cum-chord transducer CC_2^3

2 Background

2.1 Automata and Automaton Groups

A *binary transducer* is a Mealy automaton of the form $\mathcal{A} = \langle Q, \mathbf{2}, \delta, \lambda \rangle$ where Q is a finite state set, $\delta : Q \times \mathbf{2} \to Q$ is the transition function, and $\lambda : Q \times \mathbf{2} \to \mathbf{2}$ is the output function. Such a machine is *invertible* if for each state $q \in Q$, the output function $\lambda(q, \cdot)$ is a permutation of $\mathbf{2}$. A state q is called a *toggle* state if $\lambda(q, \cdot)$ is the transposition and a *copy* state otherwise. We define the transduction of q, $\underline{q} : \mathbf{2}^* \to \mathbf{2}^*$ recursively as follows: $\underline{q}(\epsilon) = \epsilon$ and $\underline{q}(a \cdot w) = \lambda(q, a) \cdot \underline{\delta(q, a)}(w)$, where ϵ denotes the empty string, $\cdot$ denotes concatenation, and $a \in \mathbf{2}$. Note that invertibility of transductions follows from invertibility of the transition functions. The inverse machine $\mathcal{A}^{-1}$ is computed by simply flipping the edge labels of $\mathcal{A}$: if $p \xrightarrow{\mathbf{a/b}} q$ in $\mathcal{A}$ then $p^{-1} \xrightarrow{\mathbf{b/a}} q^{-1}$ in $\mathcal{A}^{-1}$.

Invertible transducers define a subclass of automaton groups. The group $\mathcal{G}(\mathcal{A})$ is formed by taking all transductions and their inverses under composition. As described in [17] the group $\mathcal{G}(\mathcal{A})$ can be seen as a subgroup of the automorphism group of the infinite binary tree, denoted $\mathbf{Aut}(\mathbf{2}^*)$. Clearly any automorphism $f \in \mathbf{Aut}(\mathbf{2}^*)$ can be written in the form $f = (f_\mathbf{0}, f_\mathbf{1})\pi$ where $\pi \in S_2$. Here π describes the action of f on the root, and $f_\mathbf{0}$ and $f_\mathbf{1}$ are the automorphisms induced by f on the two subtrees. We call $(f_\mathbf{0}, f_\mathbf{1})\pi$ the *wreath representation* of f; this name is derived from the fact that $\mathbf{Aut}(\mathbf{2}^*) \cong \mathbf{Aut}(\mathbf{2}^*) \wr S_2$, where $\wr$ denotes the wreath product. Let $\sigma \in S_2$ denote the transposition. A transduction f is called *odd* if $f = (f_\mathbf{0}, f_\mathbf{1})\sigma$ and *even* otherwise. In the even case, we'll write $f = (f_\mathbf{0}, f_\mathbf{1})$. Here $f_\mathbf{0}$ and $f_\mathbf{1}$ are called the *residuals* of f, a concept first introduced by Raney [13]. We call the maps $f \mapsto f_\mathbf{a}$ for $\mathbf{a} \in \mathbf{2}$ the *residuation maps*. Residuals can be extended to arbitrary length words by $f_\epsilon = f$ and $f_{\mathbf{w}\cdot\mathbf{a}} = (f_\mathbf{w})_\mathbf{a}$, where $w \in \mathbf{2}^*$ and $a \in \mathbf{2}$. The complete group automaton for $\mathcal{A}$, denoted $\mathfrak{C}(\mathcal{A})$, has as its state set $\mathcal{G}(\mathcal{A})$ with transitions of the form $f \xrightarrow{\mathbf{a/b}} f_\mathbf{a}$, where $\mathbf{b} = f\mathbf{a}$.

2.2 Abelian Automata

For any automorphism $f \in \mathcal{G}(\mathcal{A})$, define its gap to be $\gamma_f = (f_\mathbf{0})(f_\mathbf{1})^{-1}$, so that $f_\mathbf{0} = \gamma_f f_\mathbf{1}$. An easy induction on the wreath product shows the following [12]:

Lemma 2.1. *An automaton group $\mathcal{G}(\mathcal{A})$ is abelian if, and only if, all even elements of G have gap value I, where I denotes the identity automorphism, and all odd elements have the same gap.*

Thus, for abelian groups, we may denote the shared gap value by $\gamma_\mathcal{A}$, and when the underlying automaton is clear from context, we will simply denote the gap value by γ. It follows that every odd f satisfies $f = (\gamma f_\mathbf{1}, f_\mathbf{1})\sigma$ and every even f satisfies $f = (f_\mathbf{1}, f_\mathbf{1})$.

If $\mathcal{G}(\mathcal{A})$ is abelian, we will call $\mathcal{A}$ an *abelian automaton*. It should be noted that Lemma 2.1 gives an easy decision procedure to determine if a given machine $\mathcal{A}$ is abelian. Let $\mathcal{B}$ be the minimization of the product machine $\mathcal{A} \times \mathcal{A}^{-1}$, which can be computed using a partition-refinement algorithm, where the initial partition is induced by even and odd states. Then $\mathcal{A}$ is abelian if and only if the gap of each even state is collapsed to the identity state in $\mathcal{B}$ and if the gap of each odd state is collapsed to the same state in $\mathcal{B}$.

3 Affine Residuation Parametrization

In this section we will discuss embeddings of abelian automaton groups where residuation corresponds to an affine map.

3.1 Residuation Pairs

When $\mathcal{G}(\mathcal{A}) \cong \mathbb{Z}^m$, elements of the group may be represented as integer vectors in $\mathbb{Z}^m$. This section will use this interpretation, and explore the linear-algebraic properties of the residuation maps. Let $H \leq \mathcal{G}(\mathcal{A})$ be the subgroup of even automorphisms. It's clear that H is a subgroup of index 2 and that the residuation maps restricted to H are homomorphisms into $\mathcal{G}(\mathcal{A})$. Maps of this form are known as 1/2-endomorphisms and were studied by Nekrashevych and Sidki in [11]. The authors proved that when $\mathcal{G}(\mathcal{A})$ is free abelian, the residuation maps take the form of an affine map.

Theorem 3.1. *If $\mathcal{G}(\mathcal{A}) \cong \mathbb{Z}^m$, then there exists an isomorphism $\phi : \mathcal{G}(\mathcal{A}) \to \mathbb{Z}^m$, an $m \times m$ rational matrix A, and a rational vector r which satisfy*

$$\phi(f_{\mathbf{a}}) = \begin{cases} A \cdot \phi(f) & \text{if } f \text{ is even,} \\ A \cdot \phi(f) + (-1)^a r & \text{if } f \text{ is odd.} \end{cases} \tag{1}$$

Also, the matrix A satisfies several interesting properties:

- *A is contracting, i.e., its spectral radius is less than 1.*
- *The characteristic polynomial $\chi(z)$ of A is irreducible over $\mathbb{Q}$, and has the form $\chi(z) = z^m + \frac{1}{2}g(z)$, where $g(z) \in \mathbb{Z}[z]$ is of degree at most $m-1$.*

We'll call the pair A, r a *residuation pair* for $\mathcal{A}$. Then $\mathcal{G}(\mathcal{A})$ (and its residuation relations) is completely determined by the image of one state under ϕ and a residuation pair.

Example 3.2. CC_2^3 *admits the following resiudation pair:*

$$A = \begin{pmatrix} -1 & 1 \\ -1/2 & 0 \end{pmatrix} \qquad r = \begin{pmatrix} -1 \\ -3/2 \end{pmatrix} \qquad \phi(s_1) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

The image of other states may be obtained by residuation:

$$\phi(s_2) = A\phi(s_1) - r = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \phi(s_3) = A\phi(s_1) + r = \begin{pmatrix} -2 \\ -2 \end{pmatrix}$$

This parameterization is a useful tool for performing computations in $\mathcal{G}(\mathcal{A})$. Transduction composition becomes vector addition and residuation becomes an affine map over $\mathbb{Z}^m$. However, the residuation pair is not unique. In fact, the matrix A may not be unique even up to $GL(m, \mathbb{Z})$ similarity. A theorem of Latimer and MacDuffee implies that the $GL(m, \mathbb{Z})$ similarity classes of matrices with characteristic polynomial $\chi_A(z)$ are in one-to-one correspondence with the ideal classes of $\mathbb{Z}[z]/(\chi_A(z))$ [8]. Utilizing computer algebra, we can find an example with multiple similarity classes.

Example 3.3. *The residuation matrices of the automaton CC_8^{15} have 2 $GL(m, \mathbb{Z})$ similarity classes.*

Furthermore, it is unclear at this point how one may compute a residuation pair for a general abelian automaton.

3.2 Number Field Embedding

We introduce a parametrization which addresses the above concerns, i.e. it will be unique for $\mathcal{A}$, and we will give a method to compute it efficiently. We will show that $\mathcal{G}(\mathcal{A})$ can be embedded as an additive subgroup of an algebraic number field $F(\mathcal{A})$. At this point, it is not clear that $F(\mathcal{A})$ is unique, but this will indeed be the case, as shown in Theorem 3.8. In this section, we will use some basic results from algebraic number theory, see [7, 15] for the requisite background.

Suppose $\mathcal{A}$ has states $q_1, \ldots, q_n$. For each state q_i, we introduce an unknown x_i, and let $R = \mathbb{Q}[z, x_1, \ldots, x_n]$. For each transition $q_i \xrightarrow{c} q_j$ in $\mathcal{A}$, we define the polynomial $p_{i,j} \in R$ as $p_{i,j} = zx_i - x_j + c$. Let $\mathcal{I}$ be the ideal of R generated by the set of all such polynomials, and let $\mathcal{S}$ be the system of equations defined by $\mathcal{I}$, i.e. by setting each $p_{i,j} = 0$.

Lemma 3.4. *The polynomial system $\mathcal{S}$ has a solution.*

Proof. Let A, r be a residuation pair of $\mathcal{A}$ and let $\chi(z)$ be the characteristic polynomial of A. Define $F = \mathbb{Q}(\alpha)$, where α is any root of $\chi(z)$, and let $\phi : \mathcal{G}(\mathcal{A}) \to \mathbb{Z}^m$ be the isomorphism from Theorem 3.1. We will construct a map $\psi : \mathbb{Z}^m \to F$ such that applying $\psi \circ \phi$ to the states of $\mathcal{A}$ yields a solution to $\mathcal{S}$.

Since $\chi(z)$ is irreducible, it's clear that $\mathcal{B} = \{r, Ar, \ldots, A^{m-1}r\}$ is a basis for $\mathbb{Q}^m$. Define $\psi : \mathbb{Q}^m \to F$ on $\mathcal{B}$ as $\psi(A^k r) = \alpha^k$. Then we have an injective homomorphism $\Psi : \mathcal{G}(\mathcal{A}) \to F$, where $\Psi = \psi \circ \phi$. Now applying ψ to the terms in Equation (1) gives

$$\Psi(f_{\mathbf{a}}) = \begin{cases} \alpha\Psi(f) & \text{if } f \text{ is even,} \\ \alpha\Psi(f) + (-1)^a & \text{if } f \text{ is odd.} \end{cases} \tag{2}$$

It follows that $\alpha, \Psi(q_1), \ldots, \Psi(q_n)$ is a solution to $\mathcal{S}$. □

We now analyze the structure of a general solution to $\mathcal{S}$, and show that up to conjugates, the above solution is unique. For an example of such a solution, look forward to Example 3.10. For the following results, let $\alpha, \beta_1, \ldots, \beta_n \in \mathbb{C}$ be solutions for $z, x_1, \ldots, x_n$ respectively. Define the map Ψ on the generators of $\mathcal{G}(\mathcal{A})$ as $\Psi(q_i) = \beta_i$.

Lemma 3.5. *For each $f \in \mathcal{G}(\mathcal{A})$, Equation (2) holds.*

Proof. The definition of the generators of $\mathcal{I}$ ensures that it holds for the generators of $\mathcal{G}(\mathcal{A})$. This can be extended to arbitrary products by induction on the length of the product. Let $f \in \mathcal{G}(\mathcal{A})$, and write $f = s \cdot g$, where s is a generator and $g \neq I$. By induction we have that both s and g obey Equation (2). Consider the possible parities of s and g; if both are even, then we have

$$\alpha\Psi(f) = \alpha(\Psi(s) + \Psi(g)) = \alpha\Psi(s) + \alpha\Psi(g) = \Psi(s_{\mathbf{a}}) + \Psi(g_{\mathbf{a}}) = \Psi(f_{\mathbf{a}}).$$

Likewise, if s is odd and g is even, then note $\alpha\Psi(s) = \Psi(s_{\mathbf{a}}) - (-1)^a$, and so

$$\alpha\Psi(f) + (-1)^a = \alpha\Psi(s) + \alpha\Psi(g) + (-1)^a = \Psi(s_{\mathbf{a}}) + \Psi(g_{\overline{\mathbf{a}}}) = \Psi(f_{\mathbf{a}}).$$

The final case follows similarly. □

Lemma 3.6. *α is unique up to conjugates, i.e. it is a root of $\chi(z)$, the characteristic polynomial of a residuation matrix of $\mathcal{A}$.*

Proof. Let γ be the gap value for $\mathcal{A}$ discussed in Section 3.1. From Lemma 3.5, we see $\Psi(\gamma) = 2$. Let m be the rank of $\mathcal{G}(\mathcal{A})$, and let ζ_k be a non-identity length-k residual of γ, so that for $k = 1, \ldots, m$, $\Psi(\zeta_i)$ is a polynomial in α of degree k. Then $\gamma, \zeta_1, \ldots, \zeta_m$ are linearly dependent in $\mathcal{G}(\mathcal{A})$, and hence are also under Ψ. This shows that α is a root of a degree m polynomial, which is the the same degree as the irreducible $\chi(z)$ from Lemma 3.4, implying that α satisfies $\chi(\alpha) = 0$. □

Lemma 3.7. *Let $\mathcal{L}$ be the integral span of $\beta_1, \ldots, \beta_n$, and let $\Psi : \mathcal{G}(\mathcal{A}) \to \mathcal{L}$ be the homomorphism defined on the generators as $q_i \mapsto \beta_i$. Then Ψ is an isomorphism.*

Proof. Suppose for the sake of contradiction that there is a non-identity $f \in \mathcal{G}(\mathcal{A})$ such that $\Psi(f) = 0$. If f is even, then some finite residual $f_{\mathbf{w}}$ must be odd (because f is non-identity), and $\Psi(f_{\mathbf{w}}) = \alpha^{|\mathbf{w}|}\Psi(f) = 0$. Thus without loss of generality, we may assume f is odd. It follows from Lemma 3.5 that $\Psi(f_{\mathbf{0}}) = 1$, and thus $1 \in \mathcal{L}$.

Then, by induction, we can show that $\alpha^k \in \mathcal{L}$ for all $k \in \mathbb{N}$. The base case of $k = 0$ follows from the above, and for the inductive case let us assume $\alpha^k = \sum_{i=1}^n c_i\beta_i$. Let $\partial_{\mathbf{0}}\,\beta_i$ denote the $\mathbf{0}$-residual of β_i. Then, if q_i is even, we have $\alpha q_i = \partial_{\mathbf{0}}\, q_i$ and if q_i is odd, we have $\alpha q_i = \partial_{\mathbf{0}}\, q_i - 1$. It follows that

$$\alpha^{k+1} = \alpha \sum_{i=1}^{n} c_i\beta_i = \sum_{i=1}^{n} c_i \partial_{\mathbf{0}}\, \beta_i - \sum_{i=1}^{n} c_i,$$

Because $1 \in \mathcal{L}$, we conclude that the constant term $\sum_{i=1}^n c_i \in \mathcal{L}$, implying that $\alpha^{k+1} \in \mathcal{L}$. Thus, since $|\alpha| < 1$, there are arbitrarily small nonzero elements in $\mathcal{L}$. But $\mathcal{L}$ is a discrete subgroup of a number field, and hence has a smallest nonzero element [15], so we have a contradiction. □

We summarize these results in the following theorem:

Theorem 3.8. *There exists a unique (up to conjugates) algebraic number α such that $\mathcal{G}(\mathcal{A})$ embeds into the field $F(\mathcal{A}) = \mathbb{Q}(\alpha)$, such that if $\Psi : \mathcal{G}(\mathcal{A}) \to F(\mathcal{A})$ is the embedding, then for all $f \in \mathcal{G}(\mathcal{A})$,*

$$\Psi(f_{\mathbf{a}}) = \begin{cases} \alpha\Psi(f) & \text{if } f \text{ is even,} \\ \alpha\Psi(f) + (-1)^a & \text{if } f \text{ is odd.} \end{cases}$$

The existence of a unique solution addresses one of the issues mentioned with the residuation matrix. What remains is to show the number field embedding is efficiently computable.

Theorem 3.9. *$F(\mathcal{A})$ and the embedding $\Psi : \mathcal{G}(\mathcal{A}) \to F(\mathcal{A})$ from Theorem 3.9 can be computed in time $O(n^6)$.*

Proof. We seek to compute $\chi(z)$ along with the unique solution to $\mathcal{S}$ as elements of $F(\mathcal{A})$. By Theorem 3.8, computing a triangular decomposition of $\mathcal{I}$, with respect to the lexicographic monomial ordering on $x_1 < \cdots < x_n < z$, would yield $\chi(z)$ as the first element [9]. The values for x_i may then be computed by solving the linear system in $F(\mathcal{A})$. The work required to compute a triangular decomposition is dominated by the calculation of a Gröbner basis for $\mathcal{I}$ [9]. In general, Gröbner basis calculation is known to be EXPSPACE-complete. However, the nearly-linear structure of the equations allow for better upper bounds on the complexity. It follows from [4] that the F_5 algorithm can compute a Gröbner basis for $\mathcal{I}$ in time $O(n^6)$. □

Example 3.10. *The polynomial ideal for* CC_2^3 *is*

$$\mathcal{I} = (zx_1 + 1 - x_3, zx_1 - 1 - x_2, zx_3 - x_2, zx_2 - x_1).$$

A triangular decomposition gives

$$\mathcal{I} = (z^2 + z + 1/2, 5x_1 - 4z - 8, 5x_2 + 6z + 2, 5x_3 - 4z + 2).$$

Thus $\chi(z) = z^2 + z + 1/2$*. Letting* α *denote a root of* $\chi(z)$*, we have*

$$\Psi(q_1) = \frac{1}{5}(-6\alpha - 2), \qquad \Psi(q_2) = \frac{1}{5}(4\alpha - 2), \qquad \Psi(q_3) = \frac{1}{5}(4\alpha + 8).$$

4 Orbit Rationality

4.1 Background

We briefly return to the case of a general (possibly nonabelian) automaton group. For $f \in \mathcal{G}(\mathcal{A})$ and $\mathbf{x} \in \mathbf{2}^*$, we define the *orbit* of $\mathbf{x}$ under f, denoted $f^*(\mathbf{x})$, as the set of iterates of f applied to $\mathbf{x}$, $\{f^t\mathbf{x} \mid t \in \mathbb{Z}\}$. Following this, we define the *orbit language*,

$$\mathbf{orb}(f) = \{\mathbf{x}{:}\mathbf{y} \mid \exists t \in \mathbb{Z} \text{ such that } f^t\mathbf{x} = \mathbf{y}\},$$

where the *convolution* $\mathbf{x}{:}\mathbf{y}$ of two words $\mathbf{x}, \mathbf{y} \in \mathbf{2}^k$ is defined by

$$\mathbf{x}{:}\mathbf{y} = \begin{array}{|c|c|c|c|}\hline \mathbf{x_1} & \mathbf{x_2} & \cdots & \mathbf{x_k} \\ \hline \mathbf{y_1} & \mathbf{y_2} & \cdots & \mathbf{y_k} \\ \hline \end{array} \in (\mathbf{2} \times \mathbf{2})^k.$$

We concern ourselves with the following question: Given $\mathbf{x}, \mathbf{y} \in \mathbf{2}^*$, is $\mathbf{x}{:}\mathbf{y} \in \mathbf{orb}(f)$? We'll call automorphisms *orbit-rational* if their orbit language is regular (and hence their orbit relation is rational). Consider the *orbit with translation language* as defined in [17]:

$$\mathbf{R}(f, g) = \{\mathbf{x}{:}\mathbf{y} \mid \exists t \in \mathbb{Z} \text{ such that } gf^t\mathbf{x} = \mathbf{y}\}.$$

It was shown that $\mathbf{R}$ is closed under quotients. If $f, g \in \mathcal{G}(\mathcal{A})$ and $\mathbf{b} = g\mathbf{a}$, then

$$(a{:}b)^{-1}\mathbf{R}(f, g) = \begin{cases} \mathbf{R}(f_\mathbf{a}, g_\mathbf{a}) & \text{if } f \text{ is even,} \\ \mathbf{R}(f_\mathbf{a} f_{\overline{\mathbf{a}}}, g_\mathbf{a}) & \text{if } f \text{ is odd.} \end{cases}$$

$$(a{:}\overline{b})^{-1}\mathbf{R}(f, g) = \begin{cases} \emptyset & \text{if } f \text{ is even,} \\ \mathbf{R}(f_\mathbf{a} f_{\overline{\mathbf{a}}}, f_\mathbf{a} g_{\overline{\mathbf{a}}}) & \text{if } f \text{ is odd.} \end{cases}$$

Consider the infinite transition system $M_\mathcal{A}$ over $\mathbf{2} \times \mathbf{2}$ and with transitions

$$\mathbf{R}(f, g) \xrightarrow{\mathbf{a}:\mathbf{b}} (\mathbf{a}{:}\mathbf{b})^{-1}\mathbf{R}(f, g).$$

For any $f \in \mathcal{G}(\mathcal{A})$, $\mathbf{R}(f, I)$ is the orbit language for f, and thus f is orbit-rational if and only if the subautomaton of $M_\mathcal{A}$ reachable from (f, I) is finite. Because $\mathcal{G}(\mathcal{A})$ is contracting (see Section 3.1), this occurs if and only if finitely many first arguments to $\mathbf{R}$ appear in the closure of $\mathbf{R}(f, I)$ under residuation. The first arguments of the quotients depend only on the input bit $\mathbf{a}$, which leads us to consider the maps

$$\varphi_\mathbf{a}(f) = \begin{cases} f_\mathbf{a} & \text{if } f \text{ is even,} \\ f_\mathbf{a} f_{\overline{\mathbf{a}}} & \text{if } f \text{ is odd.} \end{cases}$$

Thus, to determine if f is orbit-rational, it suffices to determine the cardinality of the set resulting from iterating $\varphi_\mathbf{0}$, $\varphi_\mathbf{1}$ starting at f.

4.2 The Abelian Case

Throughout this section we will assume $\mathcal{A}$ is abelian. In this case, we have $\varphi_a = \varphi_{\overline{a}}$, so we will drop the subscript and simply refer to φ. If f is odd, then $f = (\gamma f_{\mathbf{1}}, f_{\mathbf{1}})\sigma$, where γ is the gap value of $\mathcal{A}$. Then, $\varphi(f) = \gamma {f_{\mathbf{1}}}^2$, and

$$\varphi(f) = \begin{cases} f_{\mathbf{0}} & \text{if } f \text{ is even,} \\ \gamma {f_{\mathbf{1}}}^2 & \text{if } f \text{ is odd.} \end{cases} \tag{3}$$

We seek to understand the behavior of iterating φ on an automorphism, and in particular, determine when $\varphi^*(f) = \{\varphi^t(f) \mid t \in \mathbb{N}\}$ is finite. To accomplish this, will return to the wreath representation for automorphisms and relate φ to an extension of parity for automorphisms in $\mathcal{G}(\mathcal{A})$.

Definition 4.1. *The even rank of an automorphism $f \in \mathcal{G}(\mathcal{A})$, denoted $|f|$, is defined as the minimum integer k such that $\varphi^k(f)$ is odd. If there is no such integer, then $|f| = \infty$.*

When the context is clear, we will abbreviate "even rank" as "rank". It is clear that when f is even, $\varphi(f) = f_{\mathbf{0}} = f_{\mathbf{1}}$, so the rank equivalently measures the distance from f to its first odd residual. If f has infinite rank, then for every $w \in \mathbf{2}^*$, the residual $f_{\mathbf{w}}$ is even. Thus $f\mathbf{x} = \mathbf{x}$ for all $\mathbf{x} \in \mathbf{2}^*$, implying that the only automorphism with infinite rank is the identity. We will now prove the primary connection between rank and φ: that rank equality is preserved under φ.

Lemma 4.2. *If $f, g \in \mathcal{G}(\mathcal{A})$ with $|f| = |g|$, then $|\varphi(f)| = |\varphi(g)|$.*

Proof. The case when $|f| > 0$ is clear, but if $|f| = 0$, then we may write f in wreath representation as $f = (\gamma h, h)\sigma$, where γ is the gap value discussed in Section 3.1, and it follows that $\varphi(f) = \gamma h^2$. If we had $|\gamma| < \left|h^2\right|$, it would follow that $|\varphi(f)| = |\gamma|$, so it suffices to show this inequality. Indeed, since h^2 is even and $h^2 = (\gamma {h_{\mathbf{1}}}^2, \gamma {h_{\mathbf{1}}}^2)$, we have

$$\left|h^2\right| \geq 1 + \min(|\gamma|, \left|{h_{\mathbf{1}}}^2\right|).$$

This inequality would hold for any square h^2; in particular, it also holds for ${h_{\mathbf{1}}}^2$. It follows that the min takes value $|\gamma|$, so $\left|h^2\right| \geq 1 + |\gamma|$. Thus, for any odd f, $|\varphi(f)| = |\gamma|$, which completes the proof. □

This result allows us to begin to understand the conditions under which $\varphi^*(f)$ will be finite. We first show that φ-orbits are periodic when f is odd.

Corollary 4.3. *If f is an odd automorphism and $t = |\varphi^*(f)|$ is finite, then $\varphi^t(f) = f$.*

Proof. Because $|\varphi^*(f)|$ is finite, the sequence $\{\varphi^n(f) | n \geq 0\}$ is eventually periodic. Lemma 4.2 shows iterating φ on f produces a cyclic sequence of ranks of the form $0, |\gamma|, |\gamma| - 1, \ldots, 0, \ldots$. We note that φ is invertible when restricted to the automorphisms of rank at most $|\gamma|$. Indeed, for any automorphism g, if $|g| < |\gamma|$, then the unique inverse is $\varphi^{-1}(g) = (g, g)$. If instead $|g| = |\gamma|$, there is a unique odd h such that $g = \varphi(h) = \gamma {h_{\mathbf{1}}}^2$. It follows that the first repeated automorphism in $\varphi^*(f)$ is f itself, so $\varphi^t(f) = f$. □

The preceding results can be interpreted in the corresponding number field. Recall the map $\Psi : \mathcal{G}(\mathcal{A}) \to F(\mathcal{A})$ satisfying the properties described in Section 3.2. Let $\chi(z)$ be the unique characteristic polynomial for $\mathcal{A}$, and let α be a root of χ such that $F(\mathcal{A}) = \mathbb{Q}(\alpha)$. Let $\mathcal{L} = \Psi(\mathcal{G}(\mathcal{A}))$ be the image of the group elements in $F(\mathcal{A})$. Then $\Gamma = \Psi\varphi\Psi^{-1}$ is the orbit residuation map in $\mathcal{L}$, so $|\varphi^*(f)| = |\Gamma^*(\Psi(f))|$, and it follows from Equation (3) that for any $\beta \in \mathcal{L}$,

$$\Gamma(\beta) = \begin{cases} \alpha\beta & \text{if } \Psi^{-1}(\beta) \text{ is even,} \\ 2\alpha\beta & \text{if } \Psi^{-1}(\beta) \text{ is odd.} \end{cases}$$

Lemma 4.4. *If $f \in \mathcal{G}(\mathcal{A})$, $f \neq I$, and $\varphi^*(f)$ is finite, then $(2\alpha^k)^n = 1$ for some $k, n \in \mathbb{N}$. Furthermore, $\varphi^*(g)$ is finite for any $g \in \mathcal{G}(\mathcal{A})$.*

Proof. Suppose $\varphi^*(f)$ is finite. Because any non-identity f has finite rank, if we let $f' = \varphi^{|f|}(f)$, then f' is odd and $\varphi^*(f')$ is finite.

By Corollary 4.3, we may write $\varphi^t(f') = f'$. Let h be the first odd automorphism after f' in the sequence $\{\varphi^n(f') \mid n \geq 0\}$, say $\varphi^k(f') = h$. So in $F(\mathcal{A})$,

$$\Gamma^k\Psi(f') = 2\alpha^k\Psi(h).$$

Then by Lemma 4.2, the sequence of parities starting from f' and h are identical, meaning that any odd state reachable by f' must be of the form $\varphi^{kn}(f')$. Thus taking $n = \frac{t}{k}$ shows $(2\alpha^k)^n \Psi(f') = \Psi(f')$. Since $f' \neq I$, it follows that $\Psi(f') \neq 0$, and so $(2\alpha^k)^n = 1$ in $F(\mathcal{A})$. Now if $g \in \mathcal{G}(\mathcal{A})$ with $g \neq I$, then $g' = \varphi^{|g|}$ is odd, and

$$\Gamma^{kn}(\Psi(g)) = (2\alpha^k)^n \Psi(g) = \Psi(g),$$

so $\varphi^{kn}(g) = g$, and hence $\varphi^*(g)$ is finite. □

Lemma 4.5. *Some power of α is rational if and only if for some $k, n \in \mathbb{N}$, $(2\alpha^k)^n = 1$. In this case, α has magnitude $2^{-\frac{1}{m}}$, where m is the rank of the free abelian group $\mathcal{G}(\mathcal{A})$.*

Proof. First assume that $(2\alpha^k)^n = 1$ for some integers k and n. Then $\alpha^{kn} = 2^{-n}$. Conversely let ℓ be smallest such that $\alpha^\ell = r$ is rational. Then α is a root of $p(z) = z^\ell - r$. Let $\chi(z)$ be the irreducible characteristic polynomial of $\mathcal{A}$. Since χ is the minimal polynomial of λ_0, then $\chi(z) \mid p(z)$. Thus all roots of χ have equal magnitude, and since the constant term of $\chi(z)$ is $\pm\frac{1}{2}$, this magnitude is $|\alpha| = \pm 2^{-\frac{1}{m}}$, where m is the rank of $\mathcal{G}(\mathcal{A})$. Since $\lambda^\ell = r$ has rational norm, m divides ℓ. Setting $k = m$ and $n = \frac{2\ell}{m}$ guarantees that $(2\alpha^k)^n = 1$. □

The preceding lemmas directly imply our main result concerning orbit rationality:

Theorem 4.6. *Let $\chi(z)$ be the unique characteristic polynomial for $\mathcal{A}$, and let α be a root of χ such that $F(\mathcal{A}) = \mathbb{Q}(\alpha)$. Then for any $f \in \mathcal{G}(\mathcal{A})$, f is orbit-rational if and only if some power of α is rational.*

Example 4.7. *CC_2^3 is orbit rational. Recall from Example 3.10 that $F(\mathsf{CC}_2^3) = \mathbb{Q}[z]/(\chi(z))$ for $\chi(z) = z^2 + z + 1/2$. If α is a root of $\chi(z)$, then $\alpha^4 = -1/4$.*

4.3 Decision Procedure

We aim to turn Theorem 4.6 into a decision procedure for orbit rationality. Computationally, we must decide if some power of α is rational. The following result shows that it suffices to check only one power of α.

Lemma 4.8. *Some power of α is rational if and only if $\alpha^{4\ell}$ is rational, where*

$$\ell = \begin{cases} \frac{m}{2} & \text{if } m \text{ is odd,} \\ m & \text{otherwise.} \end{cases}$$

Proof. By Lemma 4.5, all roots of $\chi(z)$ have norm $2^{-\frac{1}{m}}$ and therefore lie on the complex disk of radius $2^{-\frac{1}{m}}$. We will follow a technique of Robinson in [14] to show $\chi(z)$ is of the form $P(z^\ell)$, where P has degree at most 2. We write

$$\chi(z) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0,$$

where $a_m = 1$ and $a_0 = \pm\frac{1}{2}$. Now if β is any root of $\chi(z)$, then the conjugate $\overline{\beta} = 2^{-2m}\beta^{-1}$ is also a root of $\chi(z)$. Consider the polynomial $p(z) = z^m \chi\left(\frac{2^{-2m}}{z}\right)$. Then, $p(z)$ has the same roots and same degree as $\chi(z)$, so $\chi(z)$ is a constant multiple of $p(z)$. Computing the leading coefficient shows $a_0\chi(z) = p(z)$, and equating the remaining coefficients gives for all $k \leq m$, $a_0 a_{m-k} = a_k 2^{-\frac{2k}{m}}$. Thus $2^{-\frac{2k}{m}}$ is rational when $a_k \neq 0$. Let ℓ be the smallest integer such that $2^{-\frac{2\ell}{m}}$ is rational:

$$\ell = \begin{cases} m & \text{if } m \text{ is odd,} \\ \frac{m}{2} & \text{if } m \text{ is even.} \end{cases}$$

Then a_k is nonzero only if $\ell \mid k$, so there exists a degree $\frac{m}{\ell}$ polynomial $P(z)$ such that $\chi(z) = P\left(z^\ell\right)$. That is, the roots of $\chi(z)$ are of the form $\sqrt[\ell]{\beta}$ for β a root of P. Note that $P(z)$ is monic and irreducible, has constant term $\pm\frac{1}{2}$, and all of its roots have norm $2^{-\frac{\ell}{m}}$. This process reduces $\chi(z)$ to a degree 1 or 2 polynomial, depending on the parity of m. If m is odd, then the only possible polynomials are $P(z) = z \pm \frac{1}{2}$, both of which have a single rational root. Thus the only interesting case is if m is even, where we claim there are only 4 possibilities for $P(z)$. The appendix of [12] lists the 6 polynomials over $\mathbb{Q}$ of degree 2 which are monic, irreducible, with constant term $\pm\frac{1}{2}$:

$$P_1(z) = z^2 - \frac{1}{2}, \qquad P_2(z) = z^2 + \frac{1}{2}, \qquad P_3(z) = z^2 - z + \frac{1}{2}$$

$$P_4(z) = z^2 + z + \frac{1}{2}, \qquad P_5(z) = z^2 - \frac{1}{2}z + \frac{1}{2}, \qquad P_6(z) = z^2 + \frac{1}{2}z + \frac{1}{2}.$$

We claim that, in orbit-rational case, $P(z)$ cannot be $P_5(z)$ or $P_6(z)$. The polynomial $P_5(z)P_6(z)$ has roots $\beta = \pm\frac{i}{4}(\sqrt{7} \pm i)$, which live in the degree 2 extension $\mathbb{Q}(\sqrt{-7})$. If one of these roots satisfied $\beta^k = r$ for some integer k and rational number r, then $\mathbb{Q}(\sqrt{-7})$ would contain an kth root of unity. Recall that a kth root of unity has degree $\varphi(k)$ over $\mathbb{Q}$, where φ is Euler's totient function. Thus we would have $\varphi(k) = 2$, so $k = 3$ or $k = 4$. It's straightforward to check that β^k is not rational for any of the above roots β where $k = 3, 4$. Thus, $P_5(z)$ and $P_6(z)$ are not possible. One can also verify any root β of $P_1(z)$, $P_2(z)$, $P_3(z)$, or $P_4(z)$ satisfies $\beta^4 = \pm\frac{1}{4}$. Thus, since the roots of $\chi(z)$ satisfy $\lambda^\ell = \beta$ for a root β of $P(z)$, it follows that $\lambda^{4\ell}$ is rational. □

Theorem 4.9. *Given an abelian binary invertible transducer $\mathcal{A}$, we can decide if $\mathcal{G}(\mathcal{A})$ is orbit-rational in polynomial time.*

Proof. By Theorem 3.9, we can compute the number field of $\mathcal{A}$ and find $\chi(z)$ in time $O(n^6)$. Let ℓ be as in Lemma 4.8. Using standard number field arithmetic techniques, we compute $z^{4\ell}$ in the field $\mathbb{Q}[z]/(\chi(z))$ and check if it is rational, which by Lemma 4.8 is equivalent to $\mathcal{G}(\mathcal{A})$ being orbit rational. □

5 Discussion and Open Problems

We extended the results of Nekrashevych and Sidki in [11]. This yielded an embedding of $\mathcal{G}(\mathcal{A})$ into a number field where residuation in $\mathcal{A}$ became an affine map in $F(\mathcal{A})$. This removed redundancies present in the residuation pairs, giving each automorphism in an abelian automaton group a unique element in a number field. Additionally, we have demonstrated that this embedding is computable in polynomial time.

Phrasing computational problems about $\mathcal{A}$ in terms of $F(\mathcal{A})$ may yield efficient solutions. We demonstrated this with the question of deciding orbit-rationality, where the problem reduces to a simple computation in $F(\mathcal{A})$. We expect other computational problems in $\mathcal{A}$ can exploit the algebraic structure of $F(\mathcal{A})$ in a similar way to yield efficient solutions. It is not clear how these results may be generalized to non-abelian automaton groups, and this is the largest open question we raise. At this time we are not aware of any nonabelian orbit-rational automaton groups.

The algorithms presented in this paper were implemented in the SageMath computer algebra system, and the code is available online [2].

6 Acknowlegements

The authors would like to thank Eric Bach for his helpful feedback on a draft of this paper. We also thank Evan Bergeron and Chris Grossack for many helpful conversations on the results presented.

References

[1] Laurent Bartholdi. "Book Review: Combinatorial algebra: syntax and semantics". In: *Bulletin of the AMS* 54.4 (2017). Great discussion of syntactic vs semantic approach to algebra, listing automata as useful semantic views of groups., pp. 681–686.

[2] Tim Becker. *Embeddings and Orbits of Abelian Automaton Groups*. `https://github.com/tim-becker/thesis-code`. 2018.

[3] I. Bondarenko et al. "Classification of groups generated by 3-state automata over a 2-letter alphabet". In: *ArXiv e-prints* (Mar. 2008). arXiv: `0803.3555 [math.GR]`.

[4] Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. "Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1, 1): Algorithms and complexity". In: *Journal of Symbolic Computation* 46.4 (2011), pp. 406–437.

[5] Rostislav I Grigorchuk, Volodymyr V Nekrashevich, and Vitali I Sushchanskii. "Automata, dynamical systems and groups". In: *Proc. Steklov Inst. Math.* Vol. 231. 4. 2000, pp. 128–203.

[6] T. W. Hungerford. *Algebra*. New York: Springer-Verlag, 1974.

[7] K. Ireland, M. Rosen, and M.I. Rosen. *A Classical Introduction to Modern Number Theory*. Graduate Texts in Mathematics. Springer, 1990. ISBN: 9780387973296. URL: https://books.google.com/books?id=jhAXHuP2y04C.

[8] Claiborne G. Latimer and C. C. MacDuffee. "A Correspondence Between Classes of Ideals and Classes of Matrices". In: *Annals of Mathematics* 34.2 (1933), pp. 313–316. ISSN: 0003486X. URL: http://www.jstor.org/stable/1968204.

[9] D. Lazard. "Solving zero-dimensional algebraic systems". In: *Journal of Symbolic Computation* 13.2 (1992), pp. 117 –131. ISSN: 0747-7171. DOI: https://doi.org/10.1016/S0747-7171(08)80086-7. URL: http://www.sciencedirect.com/science/article/pii/S0747717108800867.

[10] V. Nekrashevych. *Self-Similar Groups*. Mathematical Surveys and Monographs. American Mathematical Society, 2014. ISBN: 9781470413446. URL: https://books.google.com/books?id=amfqoQEACAAJ.

[11] Volodymyr Nekrashevych and Said Sidki. "Automorphisms of the binary tree: state-closed subgroups and dynamics of 1/2-endomorphisms". In: *London Mathematical Society Lecture Note Series* 311 (2004), pp. 375–404.

[12] Tsutomu Okano. "Invertible Binary Transducers and Automorphisms of the Binary Tree". MA thesis. Carnegie Mellon University, 2015.

[13] George N Raney. "Sequential functions". In: *Journal of the ACM (JACM)* 5.2 (1958), pp. 177–180.

[14] Raphael M. Robinson. "Conjugate algebraic integers on a circle". In: *Mathematische Zeitschrift* 110.1 (Feb. 1969), pp. 41–51. ISSN: 1432-1823. DOI: 10.1007/BF01114639. URL: https://doi.org/10.1007/BF01114639.

[15] William Stein. "Algebraic number theory, a computational approach". In: *Harvard, Massachusetts* (2012).

[16] K. Sutner. "Abelian Invertible Automata". In: *Reversibility and Universality*. Ed. by A. Adamatzky. Springer Verlag, 2018. DOI: https://doi.org/10.1007/978-3-319-73216-9_3.

[17] Klaus Sutner and Kevin Lewi. "Iterating Inverse Binary Transducers". In: *jalc* 17.2–4 (2012), pp. 293–313.