Representations and Complexity of Abelian Automaton Groups

Tim Becker
tjbecker@cmu.edu

Advised by
Klaus Sutner
sutner@cs.cmu.edu

Abstract

Automaton groups are a class of groups generated by invertible finite-state transducers. We study representations of abelian automaton groups and their applications to the complexity of computational problems arising within these groups. We demonstrate a correspondence between abelian automaton groups and a class of ideals of a corresponding algebraic number field. Properties of this number field are utilized to construct efficient algorithms for problems related to orbits of finite state transductions. The algorithms developed within are implemented in the Sage computer algebra system and are publicly available.

Contents

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 [11, 4] 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 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, 1-toggle invertible binary transducer shown in Figure 1. In fact, even 3-state invertible binary transducers generate groups which are exceedingly complicated, see [2] for a classification of all such automata.

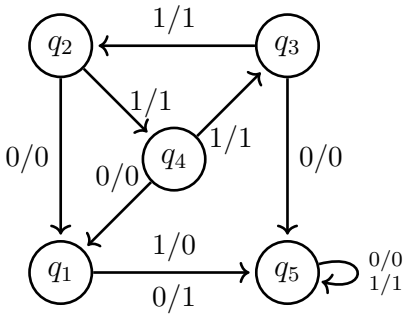


Figure 1: An invertible binary transducer generating Grigorchuk's group

Here, we will be primarily concerned with a simpler class of transducers: those which generate abelian groups. This situation has been previously studied in [13, 17]. It is known that all abelian automaton groups are either boolean or free abelian [13], and in the free abelian case, one can show that the underlying automata have nice structural properties. We will summarize and build upon these results in Section 2.2. A running example in this thesis 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 representations

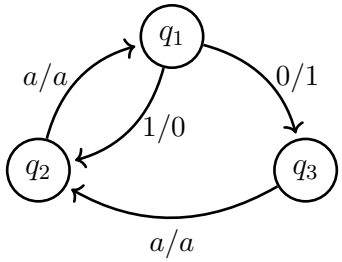


Figure 2: The cycle-cum-chord transducer CC_2^3

where transitions in the transducer correspond to affine maps on $\mathbb{Z}^m$ [12]. In this thesis, we describe a related representation of abelian automaton groups as fractional ideals of an associated algebraic number field and describe how these may be efficiently computed.

Properties of this representation 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 binary relation obtained by iterating f. Note that f^* is a length-preserving equivalence relation on $\mathbf{2}^*$. The complexity of this relation was first studied in [18], 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 [18] that CC_2^3 is orbit-rational. In this thesis, we answer a more general question by giving a precise characterization of orbit-rational abelian transducers and a corresponding decision procedure.

The algorithms developed in this thesis are implemented in the Sage computer algebra system and are available online at

`https://github.com/tim-becker/thesis-code`.

Throughout this thesis, we will utilize the theory of free abelian groups, linear algebra, field theory, and some algebraic number theory. See [5] for the necessary material on the latter subjects, and [6, 16] for background on algebraic number theory.

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 [18] 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 $f = (f_{\mathbf{0}}, f_{\mathbf{1}})$. 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 [13]:

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 $\gamma_{\mathcal{A}}$. 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 $\mathcal{A} \times \mathcal{A}^{-1}$. The minimization can be computed using a partition-refinement algorithm, where

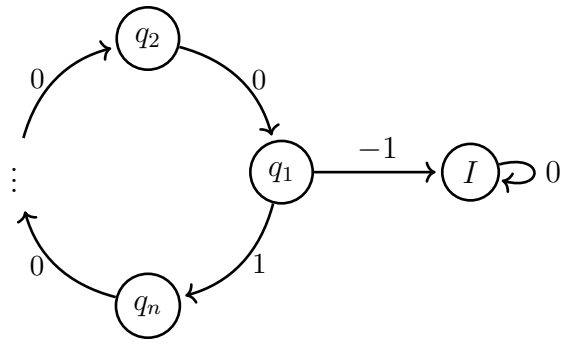


Figure 3: The sausage automaton of rank n.

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 $\mathcal{B}$.

As a result of Lemma 2.1, each state in a minimal abelian automata has in-degree at most 3. Otherwise, for some state q, there would exist two states p_1, p_2 with edges $p_1 \xrightarrow{\mathbf{a/b}} q$ and $p_2 \xrightarrow{\mathbf{a/b}} q$. But then, because the gap value is fixed, the $\overline{\mathbf{a}}$-residuals of p_1 and p_2 must also be equal, implying that $p_1 = p_2$ and contracting minimality. Thus we have proven the following proposition.

Proposition 2.2. *If $\mathcal{A}$ is a minimal abelian automaton, then each state in $\mathcal{A}$ has at most one in-edge of each label (hence has in-degree at most 3).*

Because there are only three types of edges in abelian automata, it is convenient to have a shorthand notation for edge labels. For reasons that will become clear in Section 3.3, we will adopt the following notation:

$$p \xrightarrow{0/1} q \text{ is denoted } p \xrightarrow{1} q$$
$$p \xrightarrow{1/0} q \text{ is denoted } p \xrightarrow{-1} q$$
$$p \xrightarrow{a/a} q \text{ is denoted } p \xrightarrow{0} q$$

This the first example of a combinatorial property of $\mathcal{A}$ that can be deduced from algebraic properties of $\mathcal{G}(\mathcal{A})$. Similar results will be explored further in Section 3.3.

2.2.1 One-Toggle Automata

The simplest class of Abelian automata are those with only one toggle state. Let q_1 be the toggle state. Then each residual of q_1 is either the identity, or it is a copy chain leading back to q_1. Restricting ourselves to only free abelian, where $\gamma \neq I$, rules out having both residuals be the identity, and thus we have two basic topologies for these machines: the sausage automata (Figure 3) and the cycle-cum-chord (CCC) automata (Figure 4).

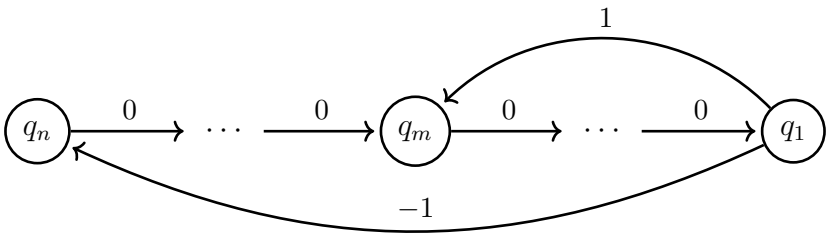


Figure 4: The CCC automaton CC_m^n.

The sausage automaton of rank n is easily seen to generate $\mathbb{Z}^n$ (the generators $q_1, \ldots, q_n$ are independent). The groups generated by the CCC automata are less obvious, however. These were studied in [18], where it was shown that $\mathcal{G}(\mathsf{CC}_m^n) \cong \mathbb{Z}^{n-\gcd(n,m)}$. Furthermore, the authors proved that CC_m^n is orbit-rational in a few cases. The general case of this question will be handled in Section 4.2.

Example 2.3. CC_2^3 *is perhaps the simplest nontrivial abelian automaton. Here we have* $\mathcal{G}(\mathsf{CC}_2^3) \cong \mathbb{Z}^2$ *with the identity* $\underline{q_1}^2 \underline{q_2}^2 = \underline{q_3}^{-1}$.

2.3 SCC Automata

We now examine the case when $\mathcal{A}$ is a minimal abelian automaton which is a single strongly connected component. We will exclude the case when $\mathcal{A}$ is simply the identity state. Let $t \geq 1$ denote the number of toggle states in $\mathcal{A}$. Write $q_1, \ldots, q_n$ for states of $\mathcal{A}$, where q_i is odd if $i \leq t$. Define $\delta_{\mathcal{A}} \in \mathbf{Aut}(\mathbf{2}^*)$ as $\delta_{\mathcal{A}} = (\gamma_{\mathcal{A}}, I)\sigma$. Like with γ, when the automaton is clear we will denote $\delta_{\mathcal{A}}$ as δ.

Lemma 2.4. $\delta \in \mathcal{G}(\mathcal{A})$.

Proof. Note that it suffices to show that there exists a state in $\mathcal{A}$ with both an even and odd in-edge. Indeed, if f is odd, and g is even with $f_{\mathbf{1}} = g_{\mathbf{0}}$, then $fg^{-1} = \delta$. Likewise if h is odd with $h_{\mathbf{0}} = g_{\mathbf{0}}$ then $gh^{-1} = \delta$. This is shown in Figure 5.

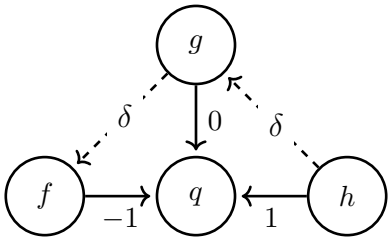
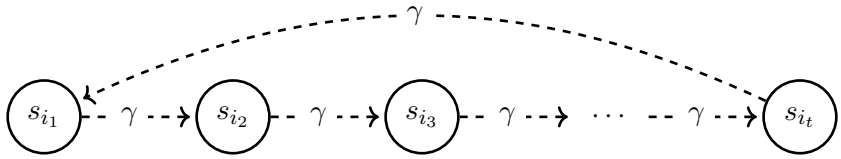


Figure 5: The three possible parents of a state q. Dashed lines denotes applying the group operation with the label.

We proceed by contradiction. Suppose no state in $\mathcal{A}$ has both an even and an odd in-edge. Let T denote the set of states with odd in-edges, and E denote the set with even in-edges. By assumption these sets are disjoint. By minimality of $\mathcal{A}$, we know $|E| = n - t$, and thus $|T| = t$. Then T must have $2t$ total in-edges. By minimality, each state $q \in T$ has in-degree exactly 2. It follows that the action of the multiplication by the gap value on the states of T forms a cycle, shown below.



Thus we have $\gamma^k = I$ for some positive integer k, contradicting the fact that $\mathcal{G}(\mathcal{A})$ is free abelian. □

The above proof is sufficient to show $\delta \in \mathcal{G}(\mathcal{A})$, but computational evidence suggests an even stronger topological property in $\mathcal{A}$.

Conjecture 2.5. *For every state q in $\mathcal{A}$, if q has two odd in-edges, then q also has an even in-edge.*

This conjecture would imply that δ may be expressed in exactly t distinct ways as differences of generators of $\mathcal{A}$. We suspect this may be proven in a similar manner as Lemma 2.4.

We now show that attaching a copy chain to state of $\mathcal{A}$ does not change the generated group. For any $f \in \mathbf{Aut}(\mathbf{2}^*)$, let $\tau(f)$ denote the automorphism which copies one bit and then applies f, that is $\tau(f) = (f, f)$.

Proposition 2.6. *$\mathcal{G}(\mathcal{A})$ is recurrent. That is, for all $f \in \mathcal{G}(\mathcal{A})$, $\tau(f) \in \mathcal{G}(\mathcal{A})$.*

Proof. Because τ is a homomorphism, it suffices to prove the claim for the generators of $\mathcal{A}$. Because $\mathcal{A}$ is an SCC, each state in $\mathcal{A}$ has in-degree at least 1. Let $p \xrightarrow{c} q$ be an edge in $\mathcal{A}$. By the preceding lemma, $\delta \in \mathcal{G}(\mathcal{A})$ and thus $p\delta^c = \tau(q) \in \mathcal{G}(\mathcal{A})$. □

Corollary 2.7. *If $f \in \mathbf{Aut}(\mathbf{2}^*)$ and $f_{\mathbf{w}}$ is a state in $\mathcal{A}$, then $f \in \mathcal{G}(\mathcal{A})$.*

Proof. If q is a state in $\mathcal{A}$, then Proposition 2.6 implies $\tau(q) \in \mathcal{G}(\mathcal{A})$. Hence, $\delta^{\pm 1}\tau(q) \in \mathcal{G}(\mathcal{A})$, so all possible predecessors of q are in $\mathcal{G}(\mathcal{A})$. Induction on $\mathbf{w}$ gives the desired result. □

Note that studying SCC automata does not severely restrict the class of automaton groups. Let $\mathcal{A}$ be any connected abelian automaton. Let D denote the condensation of $\mathcal{A}$, i.e. the directed graph induced by the SCCs of $\mathcal{A}$. D will always have at least one sink, so $\mathcal{A}$ will always have at least one terminal SCC $\mathcal{A}'$. If this SCC is nontrivial, then by Corollary 2.7, any element of an SCC of $\mathcal{A}$ which can reach $\mathcal{A}'$ is contained in $\mathcal{G}(\mathcal{A})$. Hence, by residuating, we see $\mathcal{G}(\mathcal{A}) = \mathcal{G}(\mathcal{A}')$. This proves the following proposition.

Proposition 2.8. *If $\mathcal{A}$ has a nontrivial SCC $\mathcal{A}'$, then $\mathcal{G}(\mathcal{A}) = \mathcal{G}(\mathcal{A}')$.*

We conclude by stating a lemma which will not be proven entirely until Section 3.3. It provides futher justification to the separate study of SCC transducers.

Lemma 2.9. *Every abelian automaton has only one terminal SCC.*

2.4 Principal Automata

We now move to a class of abelian automata which will play a crucial role the classification of abelian automaton groups discussed in Section 3.4.

Definition 2.10. *For any abelian automaton $\mathcal{A}$ we call the subautomaton of $\mathfrak{C}(\mathcal{A})$ generated by $\delta_{\mathcal{A}}$ the principal automaton of $\mathcal{A}$, denoted $\mathfrak{A}(\mathcal{A})$.*

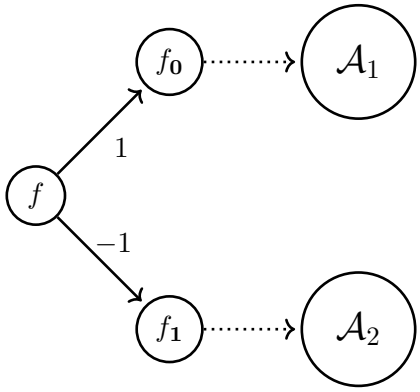
Note that $\mathfrak{A}(\mathcal{A})$ is a subautomaton of $\mathcal{A} \times \mathcal{A}^{-1}$, and thus is finite. Also, since $\delta = (\gamma, I)\sigma$, the principal automata of two machines are isomorphic if and only if their gap values are equal.

Principal automata may be the only machines not generated by a terminal SCC. Indeed, principal automata always have the trivial SCC I, and by Lemma 2.9 this is its only terminal SCC.

In fact, proving this property of principal automata would be sufficient to prove Lemma 2.9, as shown in the following proposition.

Proposition 2.11. *If in every principal automaton, there exists a path from γ to I, then Lemma 2.9 holds.*

Proof. Let $\mathcal{A}$ be a connected abelian automaton. We'll proceed by contradiction. Assume there exists two distinct terminal SCCs $\mathcal{A}_0$ and $\mathcal{A}_1$. Let f be the lowest common ancestor of $\mathcal{A}_0$ and $\mathcal{A}_1$; i.e. f is the state closest to $\mathcal{A}_0$ and $\mathcal{A}_1$ which can reach both $\mathcal{A}_0$ and $\mathcal{A}_1$. Thus without loss of generality, f is odd, $f_{\mathbf{0}}$ leads into $\mathcal{A}_0$ and $f_{\mathbf{1}}$ leads into $\mathcal{A}_1$.



Thus we have $\gamma = f_{\mathbf{0}} {f_{\mathbf{1}}}^{-1}$. Now if for some word $\mathbf{w}$, $\gamma_{\mathbf{w}} = I$, then we have $\gamma_{\mathbf{w}} = f_{\mathbf{0}\cdot\mathbf{w}} {f_{\mathbf{1}\cdot\mathbf{w}}}^{-1} = I$, and hence $f_{\mathbf{0}\cdot\mathbf{w}} = f_{\mathbf{1}\cdot\mathbf{w}}$, a contradiction. □

In Section 3.3 we will prove the preconditions to Proposition 2.11, completing the proof of Lemma 2.9. We expect that the existence of a path from γ to I admits an easier proof than the one given in given in Section 3.3, but finding such a proof is left as an open problem.

Shown in Figure 6 is the principal automaton for CC_2^3. Note that the machine is skew-symmetric, i.e. that it is its own inverse machine. This appears to be typical for principal automata, with only one exception: the sausage automata. Computational evidence supports the following conjecture:

Conjecture 2.12. *Every principal automaton other than the sausage automata is skew-symmetric.*

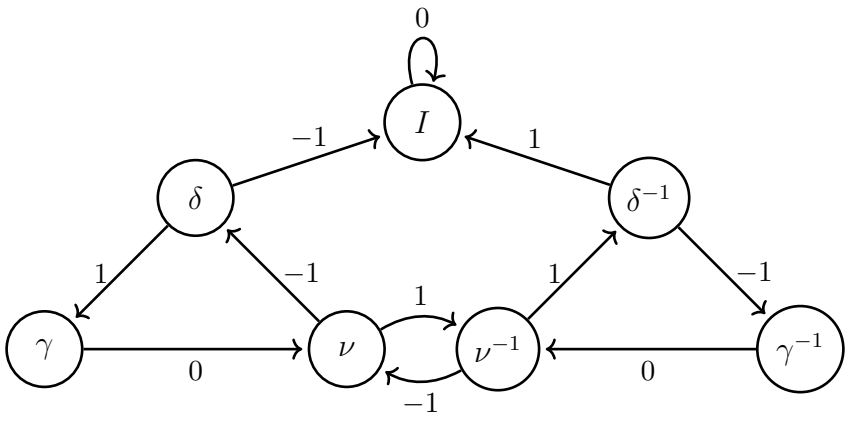


Figure 6: The principal automaton $\mathfrak{A}(\mathsf{CC}_2^3)$. Note the skew-symmetry.

3 Representations of Automaton Groups

In this section we will discuss algebraic representations of automaton groups and make connections between algebraic properties of $\mathcal{G}(\mathcal{A})$ and the structure of its generating automata.

3.1 Matrix Representation

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 [12]. 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 $m-1$.*

This theorem gives rise to the *matrix representation* of the group $\mathcal{G}(\mathcal{A})$, parameterized by the matrix A and vector r. The fact that ϕ is an isomorphism implies that this representation is faithful.

Example 3.2. CC_2^3 *admits the following matrix representation:*

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

The representation of the 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 representation is a useful tool for performing computations in $\mathcal{G}(\mathcal{A})$. Transduction composition is reduced to vector addition and residuation is reduced to an affine map over $\mathbb{Z}^m$.

However, the matrix representation is not unique. First and foremost, for any integer vector e, let $r' = r + e$. Then one can take a cycle in $\mathcal{A}$ on some state q_i and translate it into a matrix equation using Equation (1). If solving this equation for $\Psi(q_i)$ gives an integer vector, then we have a new matrix representation for $\mathcal{A}$. For instance, for $\mathcal{A}_2^3$, if we take

$$r' = r + \begin{pmatrix} -1 \\ 1 \end{pmatrix},$$

then a cycle on q_1 gives the equation

$$A(A\Psi(q_1) - r') = \Psi(q_1).$$

Solving this yields

$$\Psi(q_1) = \begin{pmatrix} 3 \\ 1 \end{pmatrix},$$

and the other states are then uniquely determined by Equation (1).

Furthermore, the matrix A is 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 $\mathbb{Z}[z](\chi_A(z))$ [9]. Utilizing computer algebra, we can find an example with multiple similarity classes.

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

Furthermore, it is unclear how one may compute a matrix representation for a general abelian automaton.

3.2 Number Field Representation

We now introduce a representation which addresses the above concerns. We will show that $\mathcal{G}(\mathcal{A})$ can be represented 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 [6, 16] 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 $s_i \xrightarrow{c} s_j$ in $\mathcal{A}$, we define the polynomial $p_{i,j} \in R$ as $p_{i,j} = zx_i - x_j + c$, where we are interpreting a and b as integers for convenience. Let $\mathcal{I}$ be the ideal of R generated by the set of all such polynomials. 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 matrix representation 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 matrix representation 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 $\mathcal{S}$. 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 $\Psi(q_i) = \beta_i$. We first show that residuation behaves as in Equation (2).

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. □

The preceding lemma shows that residuation is preserved under Ψ. This is a crucially important property that will make the field representation useful for analyzing $\mathcal{G}(\mathcal{A})$. What follows is a sequence of results which shows Ψ faithfully represents $\mathcal{G}(\mathcal{A})$, i.e. Ψ is an isomorphism.

Lemma 3.6. *If α is a solution for z in $\mathcal{S}$, then $|\alpha| < 1$.*

Proof. We proceed by contradiction. Let β_i be such that $|\beta_i|$ is largest. If q_i is even, there would exist an odd state q_j with $\beta_j = \alpha^k \beta_i$, $|\beta_j| \geq |\beta_i|$. Thus without loss of generality, we may assume q_i is odd. Then one of the residuals $\alpha\beta_i \pm 1$ will have absolute value larger than β_i, a contradiction. Thus $|\alpha| < 1$. □

Lemma 3.7. *Let $\mathcal{L}$ be the image of $\mathcal{G}(\mathcal{A})$ under Ψ. Then $\Psi : \mathcal{G}(\mathcal{A}) \to \mathcal{L}$ is an isomorphism.*

Proof. We will use results from algebraic number theory to show that the norm of elements in $\mathcal{L}$ can be lower bounded. Because the polynomials $p_{i,j}$ are linear with respect to z, we know $\beta_i \in \mathbb{Q}(\alpha)$ for each i. We write $F = \mathbb{Q}(\alpha)$ and $\mathcal{O}_F$ for the ring of integers in F, and let J be the fractional ideal of $\mathcal{O}_F$ generated by $\beta_1, \ldots, \beta_n$. Note that since $\mathcal{L}$ is the $\mathbb{Z}$-module generated by $\beta_1, \ldots, \beta_n$, $\mathcal{L}$ is contained in J. Well-known results from algebraic number theory show that there exists a nonzero $\zeta \in F$ such that $\zeta J \subset \mathcal{O}_F$ [16]. Since each element in $\mathcal{O}_F$ has integral norm, it follows each $\lambda \in \mathcal{L}$ satisfies $|\lambda| \geq \frac{1}{|\zeta|}$.

We use this fact to show that Ψ is an isomorphism. 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, by Lemma 3.6, there are arbitrarily small nonzero elements in $\mathcal{L}$, which contradicts the preceding paragraph. Thus, if $\Psi(f) = 0$, then f must be the identity, implying that Ψ is an isomorphism. □

The preceding lemma shows that each solution to $\mathcal{S}$ is capable of faithfully representing $\mathcal{G}(\mathcal{A})$ in its corresponding number field $\mathbb{Q}[z]/(\mu(z))$, where $\mu(z)$ is the minimal polynomial of α in this solution. The following theorem proves that these solutions are equivalent up to conjugates of α, and thus α has a unique minimal polynomial.

Theorem 3.8. *There exists a unique irreducible polynomial $\chi(z)$ such that $\mathcal{A}$ admits a field representation in $F(\mathcal{A}) = \mathbb{Q}[z]/(\chi(z))$. Specifically, there exists an injective homomorphism $\Psi : \mathcal{G}(\mathcal{A}) \to F(\mathcal{A})$ such that for all $f \in \mathcal{G}(\mathcal{A})$,*

$$\Psi(f_{\mathbf{a}}) = \begin{cases} z\Psi(f) & \text{if } f \text{ is even,} \\ z\Psi(f) + (-1)^a & \text{if } f \text{ is odd.} \end{cases} \tag{3}$$

Proof. Let $\alpha, \beta_1, \ldots, \beta_n$ be solutions to $\mathcal{S}$ for the unknowns $z, x_1, \ldots, x_n$ respectively. Let γ be the gap value for $\mathcal{A}$ discussed in Section 3.1. From Lemma 3.5, it is clear that $\Psi(\gamma) = 2$. Let ζ_k be any length-k residual of γ, so that $\Psi(\zeta_i)$ is a polynomial in α of degree k. Thus, if $\mathcal{G}(\mathcal{A})$ has rank m, then $\gamma, \zeta_1, \ldots, \zeta_m$

are linearly dependent. Under Ψ, this shows that α is a root of a degree m polynomial. This polynomial has the same degree as the irreducible $\chi(z)$ from Lemma 3.4, proving that α satisfies $\chi(\alpha) = 0$. Hence, all solutions to $\mathcal{S}$ are equivalent up to conjugates of α, which implies there is a unique solution in $F(\mathcal{A}) = \mathbb{Q}[z]/(\chi(z))$. □

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

Theorem 3.9. *The field representation 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 [10]. 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 $\mathcal{I}$ [10]. In general, Gröbner basis calculation is known to be EXPSPACE-complete. However, the nearly-linear structure of the equations in $\mathcal{I}$ allow for better upper bounds on the complexity. It follows from [3] 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

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

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

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

3.3 Algebraic Structure of Principal Automata

In this section we will examine the structure of the principal automata from the lens of its algebraic number field.

Unlike the previous section, here we will let α denote the reciprocal of the solution for z in $\mathcal{S}$. Note that we still have $F(\mathcal{A}) = \mathbb{Q}(\alpha)$. It follows from Theorem 3.1 that the minimal polynomial of α is of the form $\chi^{-1}(z) = z^m + c_{m-1}z^{m-1} + \cdots + c_1 z \pm 2$ where $c_i \in \mathbb{Z}$, so α is an algebraic integer. Let $\Psi : \mathcal{G}(\mathcal{A}) \to F(\mathcal{A})$ be the map constructed in the previous section.

Proposition 3.11. $\Psi(\delta) = \alpha$.

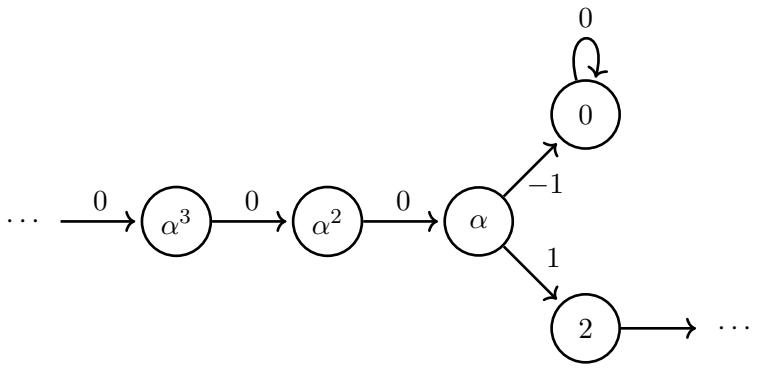


Figure 7: The copy chain attached to α, leading into $\mathfrak{A}(\mathcal{A})$.

Proof. Since $\delta_{\mathbf{1}} = I$, by Equation (2) we have $\alpha^{-1}\Psi(\delta) - 1 = 0$. □

Consider the copy chain in $\mathfrak{C}(\mathcal{A})$ rooted at δ. This is shown in Figure 7 with the states labeled with their image under Ψ.

Lemma 3.12. *$\mathcal{G}(\mathfrak{A}(\mathcal{A}))$ is generated by $\delta, \tau(\delta), \ldots, \tau^{m-1}(\delta)$.*

Proof. Let $G = \langle \tau^i(\delta) \mid 0 \leq i < m \rangle$. We have $\Psi(\tau^i(\delta)) = \alpha^i$. Evaluating α at its minimal polynomial shows

$$\pm 2 = \alpha^m + c_{m-1}\alpha^{m-1} + \cdots + c_1\alpha$$

and hence $\gamma \in G$. Thus for $\mathbf{a} \in \mathbf{2}$, $\gamma_{\mathbf{a}} \in \langle \gamma, G \rangle = G$, and by induction every state of $\mathfrak{A}(\mathcal{A})$ is contained in G. Thus $\mathcal{G}(\mathfrak{A}(\mathcal{A})) \subseteq G$. The other containment follows from Corollary 2.7. □

Example 3.13. *The diagram of $\mathfrak{A}(\mathsf{CC}_2^3)$ is shown in Figure 6. We have $\nu = \tau(\delta)\delta^{-1}$ and $\gamma = \tau(\delta)^{-1}\tau(\delta)^{-2}$, so $\mathcal{G}(\mathfrak{A}(\mathsf{CC}_2^3)) = \langle \delta, \tau(\delta) \rangle$.*

Recall that Proposition 2.11 shows that, in order to prove Lemma 2.9, it suffices to show that $\mathfrak{A}(\mathcal{A})$ must contain a path from γ to I. We will use the concept of Knuth normal form for elements of $\mathcal{G}(\mathcal{A})$ explained in [17] and summarized below.

Definition 3.14. *A (weak) Knuth normal form for an element $f \in \mathcal{G}(\mathfrak{A}(\mathcal{A}))$ is an expansion*

$$\Psi(f) = \sum_{i=1}^{k} d_i \alpha^i$$

where each $d_i \in \{-1, 0, 1\}$. We call k the length of the Knuth normal form for f.

Recall from the proof of Lemma 3.7 that ± 1 cannot be in the image of $\mathcal{G}(\mathcal{A})$ under Ψ. Therefore, in a Knuth normal form, we could never have a constant term, and thus the sum starts at index 1. We make the following observation.

Proposition 3.15. *f admits a Knuth normal form if and only if f has a path to I.*

Proof. We will show that the digits of the Knuth normal form of f specify the path from f to I. Suppose $\Psi(f) = \sum_{i=1}^{k} d_i \alpha^i$. Then the map

$$f \mapsto \begin{cases} f_{\mathbf{0}} & \text{if } d_1 \in \{-1, 0\}, \\ f_{\mathbf{1}} & \text{otherwise.} \end{cases}$$

reduces the length of the Knuth normal form by 1, in particular by shifting the coefficients as follows:

$$(d_k, d_{k-1}, \ldots, d_2, d_1) \mapsto (0, d_k, \ldots, d_3, d_2)$$

Iterating the above map k times (using the trailing coefficient as d_0 on each iteration) yields all zero coefficients, and hence we have constructed a path to the identity state.

Conversely, if f has a path to I of length k, then let $d_1, \ldots, d_k$ be the edge labels traversed on the path. It follows that

$$f = \delta^{d_1} \cdots \tau^k(\delta)^{d_k},$$

and thus f admits the Knuth normal form $\Psi(f) = \sum_{i=1}^{k} d_i \alpha^i$. □

Thus, to prove Lemma 2.9 it suffices to show γ admits a Knuth normal form. We will achieve this by invoking a result from the study of numeration systems in algebraic number fields. For background, see [14] and the references therein.

The following result follows from [8, 7].

Theorem 3.16. *Let α be an expanding algebraic integer of norm 2. Then for every $\beta \in \mathbb{Z}[\alpha]$ may be written as $\beta = \sum_{i<k} d_i \alpha^i$, where $d_i \in \{-1, 0, 1\}$.*

Corollary 3.17. *Every element of $\mathcal{G}(\mathfrak{A}(\mathcal{A}))$ admits a Knuth normal form.*

Proof. By Lemma 3.12, the image of $\mathcal{G}(\mathfrak{A}(\mathcal{A}))$ under Ψ is contained in $\mathbb{Z}[\alpha]$, satisfying the preconditions for Theorem 3.16. □

The above corollary finishes the proof of Lemma 2.9.

3.4 Ideal Classification

In this section we will classify abelian automaton groups as fractional ideals of particular form in their corresponding field. We refer the reader to [16] for background on ideal arithmetic and fractional ideals.

We will work under the assumption of a conjecture which is well supported by computational evidence. Let α be such that $F(\mathcal{A}) = \mathbb{Q}(\alpha)$, and let $\mathcal{O}_{\mathcal{A}}$ be the ring of integers of $F(\mathcal{A})$.

Conjecture 3.18. *$F(\mathcal{A})$ is monogenic. That is, $\mathcal{O}_{\mathcal{A}} = \mathbb{Z}[\alpha]$.*

As in Section 3.2, let $\beta_1, \ldots, \beta_n$ be the images of the states of $\mathcal{A}$ in $F(\mathcal{A})$. Let L be the integral span of $\beta_1, \ldots, \beta_n$, so $L \cong \mathcal{G}(\mathcal{A})$. Let J be the fractional ideal of $\mathcal{O}_\mathcal{A}$ generated by $\beta_1, \ldots, \beta_n$. The above conjecture, if true, implies that $L = J$.

Corollary 3.19. $L = J$

Proof. It's clear that $L \subseteq J$, because $\mathbb{Z} \subset \mathcal{O}_\mathcal{A}$. By Conjecture 3.18, to show $J \subseteq L$, it suffices to show that $\beta \in L \implies \alpha\beta \in L$. This follows from the fact that $\mathcal{G}(\mathcal{A})$ is recurrent, i.e. Proposition 2.6. □

This shows that we may associate to $\mathcal{G}(\mathcal{A})$ a fractional ideal of $\mathcal{O}_\mathcal{A}$. Let $\mathfrak{I}(\mathcal{A})$ denote this map from abelian automata to fractional ideals. Let $\mathfrak{A}$ be the principal automaton of $\mathcal{A}$, and recall that $\mathcal{G}(\mathfrak{A}) \subseteq \mathcal{G}(\mathcal{A})$. As one would expect, this fact holds for the fractional ideals as well. We first characterize the fractional ideal $\mathfrak{I}(\mathfrak{A})$.

Lemma 3.20. $\mathfrak{I}(\mathfrak{A}) = (\alpha)$*, the principal ideal generated by* α*.*

Proof. By Lemma 3.12, $\Psi(\mathcal{G}(\mathfrak{A})) = \alpha\mathbb{Z}[\alpha]$, and Conjecture 3.18 implies $\alpha\mathbb{Z}[\alpha] = (\alpha)$. □

Lemma 3.21. *The ideal* (α) *has norm two. That is,* $[\mathcal{O}_\mathcal{A} : (\alpha)] = 2$*.*

Proof. Because the gap value is in $\mathcal{G}(\mathfrak{A})$, we have $2 \in \Psi(\mathcal{G}(\mathfrak{A}))$. Hence all even rational integers are in (α). By Conjecture 3.18, it follows that (α) contains all elements of the form

$$\alpha\mathbb{Z}[\alpha] + 2\mathbb{Z}$$

and hence (α) has norm 2. □

Corollary 3.22. (α) *is a prime ideal of* $\mathcal{O}_\mathcal{A}$*.*

Proof. The norm of (α) is prime, and ideal norms are multiplicative. □

Recall that $\mathcal{O}_\mathcal{A}$ is a Dedekind domain, and hence we have unique factorization of any fractional ideal J as

$$J = (\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_k^{a_k}) \cdot (\mathfrak{p}_{k+1}^{a_{k+1}} \cdots \mathfrak{p}_n^{a_n})^{-1}$$

where the ideals $\mathfrak{p}_i$ are distinct.

Definition 3.23. *A fractional ideal* J *of* $\mathcal{O}_\mathcal{A}$ *is called residually closed if*

$$J = (\alpha)J + (\alpha) \tag{4}$$

Theorem 3.24. *A fractional ideal* J *is the image of an abelian automaton group if and only if it is residually closed. In this case, we have that for some* $\mathcal{A}$*,*

$$J = \mathfrak{I}(\mathcal{A}) = (\alpha) \cdot \mathfrak{b}^{-1}$$

for a unique ideal $\mathfrak{b}$ *of* $\mathcal{O}_\mathcal{A}$ *which is relatively prime to* (α)*.*

Proof. First note that $\mathfrak{I}(\mathfrak{A})$ is always residually closed. The set $(\alpha)\mathfrak{I}(\mathfrak{A}) + (\alpha)$ contains the image of all possible predecessors of an element of $\mathcal{G}(\mathcal{A})$, and hence is equal to $\mathfrak{I}(\mathfrak{A})$.

Conversely suppose J is a residually closed fractional ideal. Then $J = (\alpha)(J + \mathcal{O}_\mathcal{A})$, so (α) divides J. Thus J contains the image of a principal automaton group and is closed under backwards residuation, so J is the image of an abelian automaton group.

For any residually closed ideal J, by unique factorization we have $\mathfrak{I}(\mathcal{A}) = (\alpha)\mathfrak{a}\cdot\mathfrak{b}^{-1}$, where either $\mathfrak{a} = \mathcal{O}_\mathcal{A}$ or else $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime. We will show that only $\mathfrak{a} = \mathcal{O}_\mathcal{A}$ is possible. Suppose otherwise. Then, we divide Equation (4) by J to find

$$(\alpha) + (\alpha)J^{-1} = \mathcal{O}_\mathcal{A}$$

and thus

$$(\alpha) + \mathfrak{b}\mathfrak{a}^{-1} = \mathcal{O}_\mathcal{A}$$

Because $(\alpha) \subset \mathcal{O}_A$, we must have $\mathfrak{b}\mathfrak{a}^{-1} \subseteq \mathcal{O}_\mathcal{A}$, contradicting the fact that $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime. Thus we conclude $J = (\alpha)\mathfrak{b}^{-1}$. □

Theorem 3.24 implies that we may apply unique factorization of ideals to observe properties of automaton groups. In particular, we have the following corollaries:

Corollary 3.25. *Let $J_1, \ldots, J_k$ be fractional ideals such that*

$$(\alpha) = J_1 \subsetneq \cdots \subsetneq J_k = \mathfrak{I}(\mathcal{A})$$

where all $J_i \subsetneq J_{i+1}$. Then for all i with $1 \leq i \leq k$ there there exists an abelian automaton $\mathcal{A}_i$ such $J_i = \mathfrak{I}(\mathcal{A}_i)$ and

$$\mathcal{G}(\mathfrak{A}(\mathcal{A})) = \mathcal{G}(\mathcal{A}_1) \subsetneq \cdots \subsetneq \mathcal{G}(\mathcal{A}_k) = \mathcal{G}(\mathcal{A})$$

where all $\mathcal{G}(\mathcal{A}_i) \subsetneq \mathcal{G}(\mathcal{A}_{i+1})$.

Corollary 3.26. *Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be two abelian automata. If $\mathfrak{A}(\mathcal{A}_1) \cong \mathfrak{A}(\mathcal{A}_2)$, then $\mathfrak{I}(\mathcal{A}_1) = \mathfrak{q}\mathfrak{I}(\mathcal{A}_2)$ for some fractional ideal $\mathfrak{q}$.*

Proof. By Theorem 3.24, we have $\mathfrak{I}(\mathcal{A}_1) = (\alpha)\mathfrak{b}_1^{-1}$ and $\mathfrak{I}(\mathcal{A}_2) = (\alpha)\mathfrak{b}_2^{-1}$. Then

$$\mathfrak{I}(\mathcal{A}_1)\mathfrak{I}(\mathcal{A}_2)^{-1} = \mathfrak{b}_2\mathfrak{b}_1^{-1}$$

□

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* of f as

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

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 [18]:

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

It was shown that $\mathbf{R}$ is closed under quotients. Precisely, 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

$$\varphi(f) = \begin{cases} f_{\mathbf{0}} & \text{if } f \text{ is even,} \\ \gamma {f_{\mathbf{1}}}^2 & \text{if } f \text{ is odd.} \end{cases} \tag{5}$$

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 field representation of the group. 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 (5) 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 [15] 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 [13] lists the 6 polynomials over $\mathbb{Q}$ of degree 2 which are monic, irreducible, and have constant term $\pm\frac{1}{2}$:

$$P_1(z) = z^2 - \frac{1}{2}, \qquad P_2(z) = z^2 + \frac{1}{2},$$
$$P_3(z) = z^2 - z + \frac{1}{2}, \qquad P_4(z) = z^2 + z + \frac{1}{2},$$
$$P_5(z) = z^2 - \frac{1}{2}z + \frac{1}{2}, \qquad P_6(z) = z^2 + \frac{1}{2}z + \frac{1}{2}.$$

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 representation of $\mathcal{A}$ to 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 introduced several classes of abelian transducers. The simplest nontrivial automata are the CCC transducers, which have are SCC transducers with one toggle state. We showed that the study of SCC transducers excludes only groups generated by principal automata. The largest open problem in this area is to prove the skew-symmetry conjecture: that every principal automaton except for the sausage automata is skew-symmetric and self-inverse.

We also studied representations of abelian automaton groups, and extended the results of Nekrashevych and Sidki in [12]. This yielded a representation as fractional ideals of an algebraic number field $F(\mathcal{A})$ where residuation in $\mathcal{A}$ corresponds to an affine map in $F(\mathcal{A})$. This representation removes redundancies present in the parameterization of matrix representations, giving each automorphism in an abelian automaton group a unique element in a number field. Additionally, we have demonstrated that this representation is computable in polynomial time.

In Section 3.4, we conjectured that $F(\mathcal{A})$ is always monogenic, which would have consequences for unique factorization of abelian automaton groups. Proving this precondition remains an open problem.

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 many 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 discussed in this thesis were implemented in Sage. Field representations for abelian automata of size under 40 may be computed in only a few seconds, and hence orbit-rationality may be checked for a large class of automata. Our code is available at

`https://github.com/tim-becker/thesis-code`.

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] 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]`.

[3] 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.

[4] 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.

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

[6] 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.

[7] J. C. Lagarias and Y. Wang. "Integral Self-Affine Tiles in $\mathbf{R}^n$ II. Lattice Tilings". In: *J. Fourier Anal. Appl.* 3.1 (1997), pp. 83–102.

[8] J. C. Lagarias and Y. Wang. "Self-Affine Tiles in $\mathbf{R}^n$". In: *Adv. Math.* 121 (1996), pp. 21–49.

[9] 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.

[10] 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.

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

[12] 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.

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

[14] A. Pethö. *Connections between power integral bases and radix representations in alebraic number fields*. https://arato.inf.unideb.hu/petho.attila/cikkek/cnsnagoya_paper_110.pdf. 2009.

[15] 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.

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

[17] 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.

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