Extensions of Abelian Automata Groups

Chris Grossack
Advised by Klaus Sutner

May 3, 2019

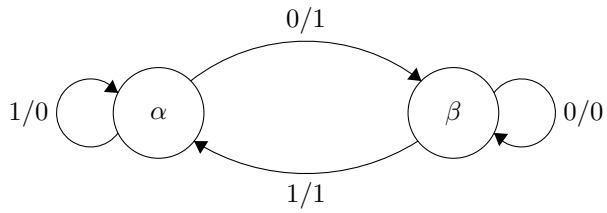
Abstract

A longstanding problem in understanding abelian automata groups comes from a seemingly unnecessary parameter in the classification given by Nekrashevych and Sidki. In this paper, we show that this parameter corresponds to the presence of certain fractional group elements. Further, we show the existence of a computable universal object which removes the need for this parameter entirely.

1 Background

Finite State Automata are combinatorial objects which encode relations between words over some alphabet. Automata provide deep connections between combinatorics, algebra, and logic, and are essential tools in contemporary computer science. One such link is in the decidability of truth in a structure whose relations are all computable by automata. One can combine these automata into more complicated automata representing logical sentences in such a way that a sentence is true if and only if a simple reachability condition holds [2]. This gives a simple proof that the theory of $\mathbb{N}$ with $+$ and $<$, for example, is decidable.

While the most common automata one encounters are Deterministic Finite State Automata (DFAs), and Turing Machines, providing a characterization of the complexity of certain languages, automata can encode functions, and therefore groups, as well. These groups are surprisingly complicated, and indeed a classification of all groups generated by three state automata over the alphabet $\mathbf{2} = \{0, 1\}$ is an extremely difficult problem, though much impressive progress has been made [4]. This complexity can be extremely useful, as automaton groups have become a rich source of examples and counterexamples [15, 19, 7]. Automaton groups provide examples of finitely generated infinite torsion groups, with application to Burnside's Problem [10], and automata groups have provided the only examples of groups of intermediate growth, providing counterexamples to Milnor's Conjecture regarding the existence of such groups [9]. In fact, one of the simplest conceivable automata (shown below) already generates the lamplighter group $\mathbb{Z}/2\mathbb{Z} \wr \mathbb{Z}$ [8].



Because of the complexity of general automaton groups, in this paper we restrict our attention to the abelian case, over the alphabet $\mathbf{2}$. For our purposes, then, a **Mealy Automaton** is a tuple $\mathcal{A} = (S, \tau)$ where S is the **State Set**, and $\tau : S \times \mathbf{2} \to S \times \mathbf{2}$ is the **transition function**. Given a state $s \in S$, we can treat it as a length preserving function $\underline{s} : \mathbf{2}^* \to \mathbf{2}^*$ as follows:

$$\begin{aligned} \underline{s}(\varepsilon) &= \varepsilon \\ \underline{s}(ax) &= a'\underline{s'}(x) \quad (\text{where } (s', a') = \tau(s, a)) \end{aligned}$$

Here juxtaposition is concatenation, and the empty word ε is the identity in $\mathbf{2}^*$. Clearly we can treat $\underline{s}$ as a function on $\mathbf{2}^\omega$, the set of infinite words, instead. In this case, automata provide a computable way of encoding complicated continuous functions from cantor space to itself, with ties to descriptive set theory

[20]. If all of these functions are invertible, we let $\mathcal{G}(\mathcal{A})$ denote the group generated by these functions, with extra structure given by residuation (we write our groups additively, and denote the identity element by I).

Definition 1. The **0-residual** (resp. **1-residual**) of a function $f \in \mathcal{G}(\mathcal{A})$ is the unique function $\partial_0 f$ such that for all w, $f(0w) = f(0)\partial_0 f(w)$ (resp. $f(1w) = f(1)\partial_1 f(w)$).

For a state $s \in S$, it is clear that $\partial_a \underline{s} = \underline{s'}$, where $(s', a') = \tau(s, a)$. Since the generators are closed under residuation, so is the group.

Definition 2. A function $f \in \mathcal{G}(\mathcal{A})$ is called **Odd** if it flips its first bit and **Even** otherwise.

We call an automaton **Abelian** or **Trivial** exactly when its group is. We represent τ graphically by labeling an edge from s_1 to s_2 by a/b exactly when $\tau(s_1, a) = (s_2, b)$.

In the above automaton, $\underline{\alpha}$ is odd, $\underline{\beta}$ is even, $\partial_0\underline{\alpha} = \underline{\beta}$, and $\partial_1\underline{\alpha} = \underline{\alpha}$. Further, $\underline{\alpha}(011) = 1\underline{\beta}(11) = 11\underline{\alpha}(1) = 110$. For a more in depth description of Mealy Automata and their properties, see [18, 11].

Of great importance to abelian automata theory is the result of Nekrashevych and Sidki that every such group is either torsion free abelian or boolean [16]. Because of this classification, much of the interesting structure of these groups comes from the residuation functions. To that end, for the duration of this paper, homomorphisms and isomorphisms are all restricted to those which preserve the residuation structure in addition to the group structure. We now restrict ourselves further to the case where $\mathcal{G}(\mathcal{A})$ is free abelian, that is to say $\mathcal{G}(\mathcal{A}) \cong \mathbb{Z}^m$ for some m. [1]

1.1 Prior Results

This thesis leans heavily on prior results in the theory of abelian automata, and in the interest of self-containedness, we will sumamrize the relevant results and their proofs in this section. Everything in this section can be atributed to one of [16, 21, 17], and we will name the theorems accordingly.

Definition 3. A vector $\bar{v} \in \mathbb{Z}^m$ is called **Odd** (resp. **Even**) when its first component is odd (resp. even).

Theorem 1 (Nekrashevych and Sidki)**.** *If $\mathcal{G}$ is an automaton group and $\varphi : \mathcal{G} \to \mathbb{Z}^m$ is a group isomorphism, then there is a matrix $\boldsymbol{A}$ of $\mathbb{Q}$-irreducible character and an odd vector $\bar{e}$ such that if $\mathbb{Z}^m$ is equipped with the following residuation structure, then φ preserves residuation:*

If $\bar{v}$ is even:

$$\partial_0\bar{v} = \partial_1\bar{v} = \boldsymbol{A}\bar{v}$$

[1] For historical reasons we use $\mathbb{Z}^m$ instead of $\mathbb{Z}^n$ because traditionally n is reserved for the size of the state set of an automaton.

If $\bar{v}$ is odd:

$$\partial_0 \bar{v} = \boldsymbol{A}(\bar{v} - \bar{e})$$
$$\partial_1 \bar{v} = \boldsymbol{A}(\bar{v} + \bar{e})$$

Further, $\boldsymbol{A}$ is unique up to conjugation, and can always be taken to be "$\frac{1}{2}$ − integral", meaning $\boldsymbol{A}$ is of the form

$$\begin{pmatrix} \frac{a_{11}}{2} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{a_{n1}}{2} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

where each $a_{ij} \in \mathbb{Z}$.

Finally, these matrices all have characteristic polynomial $\chi = x^n + \frac{1}{2}g(x)$, where $g \in \mathbb{Z}[x]$ and has constant term ± 1, and if $\mathcal{G}$ is generated by a finite state automaton, then $\boldsymbol{A}$ is a contraction. That is, all of its complex eigenvalues have norm < 1.

Definition 4. Following Sutner [21], we call $\mathbb{Z}^m$ equipped with this residuation structure **The Complete Automaton** $\mathfrak{C}(\mathbf{A}, \bar{e})$.

Definition 5. The $\mathbf{A}$ so that $\mathcal{G}(\mathcal{A}) \cong \mathfrak{C}(\mathbf{A}, \bar{e})$ is called the **Associated Matrix** of $\mathcal{A}$.

Definition 6. Given an automaton group $\mathcal{G}$, define the **Gap Value** of a function f to be $\gamma_f = \partial_1 f - \partial_0 f$.

Theorem 2 (Okano)**.** *An automaton group $\mathcal{G}$ is Abelian if and only if for every even function $f \in \mathcal{G}$ has gap value I, and every odd function f has the same gap value.*

Proof. The forward direction follows from the characterization of Nekrashevych and Sidki, since for $\bar{v} \in \mathbb{Z}^m$ odd, $\partial_1 \bar{v} - \partial_0 \bar{v} = \mathbf{A}(\bar{v} + \bar{e}) - \mathbf{A}(\bar{v} - \bar{e}) = 2\mathbf{A}\bar{e}$ by linearity. For $\bar{v} \in \mathbb{Z}^m$ even, $\partial_1 \bar{v} - \partial_0 \bar{v} = \mathbf{A}\bar{v} - \mathbf{A}\bar{v} = I$

For the backwards direction, let $f, g \in \mathcal{G}$ be odd, and let $\gamma = \partial_1 f - \partial_0 f = \partial_1 g - \partial_0 g$. Note $f + g = g + f$ if and only if $\forall w \in \mathbf{2}^*.(f+g)(w) = (g+f)(w)$. We induct on the length of w. $(f+g)(\varepsilon) = \varepsilon = (g+f)(\varepsilon)$, and

$$\begin{aligned} (f+g)(0w) &= 0(\partial_0 f + \partial_1 g)(w) \\ &= 0(\partial_1 g + \partial_0 f)(w) \\ &= 0((\gamma + \partial_0 g) + (\partial_1 f - \gamma))(w) \\ &= 0(\partial_0 g + \partial_1 f)(w) \\ &= (g+f)(0w) \end{aligned}$$

Here all rearranging is done by induction, and the cases for $1w$ and for f or g even are similar. □

Each $\mathcal{G}(\mathcal{A})$ can also be viewed as an automaton, by taking $\mathcal{G}(\mathcal{A})$ as states, and defining $\tau(f, i) = \partial_i f$. $\mathcal{A}$ is a natural subautomaton of $\mathcal{G}(\mathcal{A})$ by identifying $s \in \mathcal{A}$ with $\underline{s} \in \mathcal{G}(\mathcal{A})$.

Theorem 3. *For each $\mathcal{G}(\mathcal{A})$, there is $\boldsymbol{A}$ and $\bar{e}$ so that $\mathcal{G}(\mathcal{A})$ and $\mathfrak{C}(\boldsymbol{A}, \bar{e})$ are isomorphic as automata.*

Proof. This is a restatement of Nekrashevych and Sidki's result above. □

Nekrashevych and Sidki's theorem gives us a purely linear algebraic method of discussing these automaton groups, since the above theorem shows that every abelian automaton $\mathcal{A}$ is a subautomaton of some $\mathfrak{C}(\mathbf{A}, \bar{e})$. However there are infinitely many valid choices for $\bar{e}$, and classifying these is the goal this paper.

Definition 7. We say a function $f \in \mathcal{G}(\mathcal{A})$ is **Located at** $\bar{v} \in \mathfrak{C}(\mathbf{A}, \bar{e})$ iff the isomorphism between $\mathcal{G}(\mathcal{A})$ and $\mathfrak{C}(\mathbf{A}, \bar{e})$ sends f to $\bar{v}$. Further, if $\mathcal{A}$ was finite state, then given any state $\bar{v} \in \mathfrak{C}(\mathbf{A}, \bar{e})$, closing $\{\bar{v}\}$ under residuation will result in a finite automaton $\mathcal{A}_{\bar{v}}$ since $\mathbf{A}$ is a contraction. So we say an automaton $\mathcal{A}$ is **Located At** $\bar{v} \in \mathfrak{C}(\mathbf{A}, \bar{e})$ iff the isomorphism sends $\mathcal{A}$ to $\mathcal{A}_{\bar{v}} \subseteq \mathfrak{C}(\mathbf{A}, \bar{e})$.

Note that the location of a function or an automaton, and indeed whether a location exists or not, will depend on the choice of $\bar{e}$. For a more detailed discussion of these linear algebraic methods and their origins, see [15, 16]

Definition 8. The **Copy Chain** at a state $s \in \mathcal{A}$ is a chain of even states s_i such that $s_0 = s$ and $\partial_0 s_{i+1} = \partial_1 s_{i+1} = s_i$.

Such a chain always exists, as if we consider $\mathcal{A}$ as a subset of $\mathfrak{C}(\mathbf{A}, \bar{e})$, then for any $s \in \mathcal{A}$, $\mathbf{A}^{-i}\varphi(s)$ forms a copy chain. This is because $\mathbf{A} : 2\mathbb{Z} \oplus \mathbb{Z}^{m-1} \to \mathbb{Z}^m$, so $\mathbf{A}^{-1} : \mathbb{Z}^m \to 2\mathbb{Z} \oplus \mathbb{Z}^{m-1}$, and always gives an even vector. Then residuating $\mathbf{A}^{-(i+1)}\bar{v}$ is $\mathbf{A}\mathbf{A}^{-(i+1)}\bar{v} = \mathbf{A}^{-1}\bar{v}$.

Definition 9. If $x \in \mathbf{2}^*$, then $\partial_x f$ is defined inductively as follows:

$$\partial_\epsilon f = f$$
$$\partial_{wa} f = \partial_a(\partial_w f)$$

Theorem 4 (Sutner)**.** *Let $\mathcal{A} \subseteq \mathfrak{C}(\boldsymbol{A}, \bar{e})$ be a nontrivial automaton, and for $f \in \mathfrak{C}(\boldsymbol{A}, \bar{e})$ with $\partial_x f \in \mathcal{A}$ for some $x \in \boldsymbol{2}^*$, let $\mathcal{A}_+$ be the smallest subautomaton of $\mathfrak{C}(\boldsymbol{A}, \bar{e})$ containing $\mathcal{A}$ and f. Then $\mathcal{G}(\mathcal{A}) = \mathcal{G}(\mathcal{A}_+)$.*

Proof. Fix $q \in \mathcal{A} \subseteq \mathfrak{C}(\mathbf{A}, \bar{e})$ with $\partial_x f = q$.

First, let f be even. Consider the copy chain $q_i = \mathbf{A}^{-i}q$ with $q_0 = q$. Then by Cayley-Hamilton, $\mathbf{A}^{-1}$ satisfies its own characteristic polynomial χ^*. Thus $\chi^*(\mathbf{A}^{-}1)q = I$, and so we see some $\mathbb{Z}-$linear combination of the q_i sum to the identity. By repeatedly residuating both sides of this equation, we obtain $f \in \mathcal{G}(\mathcal{A})$.

If instead f is odd, then without loss of generality $\partial_0 f \in \mathcal{A}$. The ∂_1 case is clearly symmetric, and if the path from f to $\mathcal{A}$ is of length > 1, then we can induct on the length of the path to get the desired result. A similar residuation argument works to show $f \in \mathcal{G}(\mathcal{A})$, however since f is odd, we also need to know that $\partial_1 f \in \mathcal{G}(\mathcal{A})$. Thankfully, $\mathcal{A}$ is nontrivial, and so $\gamma \in \mathcal{G}(\mathcal{A})$. But $\partial_1 f = \gamma + \partial_0 f = \gamma + q \in \mathcal{G}(\mathcal{A})$. The claim follows. □

1.2 Principal Automata

To each abelian automaton we can associate a matrix as above, however each matrix can be associated to infinitely many automata. It was shown by Okano [17] that there is a distinguished automaton, now called the **Principal Automaton** $\mathfrak{A}$, associated to each matrix.

Definition 10. $\mathfrak{A}(\mathbf{A})$ is defined to be $\mathfrak{A} = \mathcal{A}_{\bar{e}_1} \cup \mathcal{A}_{-\bar{e}_1} \subseteq \mathfrak{C}(\mathbf{A}, \bar{e}_1)$, though there is a longstanding conjecture that in most cases this is the same machine as $\mathcal{A}_{\bar{e}_1} \subseteq \mathfrak{C}(\mathbf{A}, \bar{e}_1)$. We will write $\mathfrak{A}$ when the matrix is clear from context.

We shall soon see that the same element of $\mathfrak{A}$ is located at $\bar{e}$ in $\mathfrak{C}(\mathbf{A}, \bar{e})$ for all $\bar{e}$, and so we call this group element $\delta \in \mathcal{G}(\mathfrak{A})$. Notice that for all $\bar{e}$, $\partial_0 \delta = \mathbf{A}(\bar{e} - \bar{e}) = \bar{0} = I$, and so $\partial_1 \delta = \gamma$, since for any odd vector $\partial_1 \bar{v} - \partial_0 \bar{v} = \gamma$. Thus, γ depends on only the matrix $\mathbf{A}$, rather than on individual automata.

$\mathfrak{A}$ is clearly minimal in terms of state complexity, as its states are distinct group elements of $\mathfrak{C}(\mathbf{A}, \bar{e}_1)$ and therefore have different behavior. However, $\mathfrak{A}$ is also minimal in the subgroup relation for nontrivial automata sharing its matrix. While there are proofs of this claim which rely heavily on the ambient linear algebraic structure [17], we present here a difference construction which uses only the given automaton $\mathcal{A}$ to construct $\mathfrak{A}$. Thus every $s \in \mathfrak{A}$ is already in $\mathcal{G}(\mathcal{A})$, and the subgroup relation follows.

Theorem 5. *For each nontrivial $\mathcal{A}$ with associated matrix $\boldsymbol{A}$, $\mathcal{G}(\mathfrak{A}(\boldsymbol{A})) \leq \mathcal{G}(\mathcal{A})$.*

Proof. Let $\mathcal{A}$ be an abelian automaton with at least one odd state. Note that if $\mathcal{A}$ has no odd states, its group is trivial, so we may safely ignore it.

Put $\gamma = \partial_1 f - \partial_0 f$ for $f \in \mathcal{A}$ odd, and construct a new automaton by closing γ under residuation. Note that this can be done using only information contained in $\mathcal{A}$, since it is easy to check that:

$$\partial_0(f+g) = \begin{cases} \partial_0 f + \partial_1 g & \text{both odd} \\ \partial_0 f + \partial_0 g & \text{otherwise} \end{cases}$$

$$\partial_1(f+g) = \begin{cases} \partial_1 f + \partial_0 g & \text{both odd} \\ \partial_1 f + \partial_1 g & \text{otherwise} \end{cases}$$

$$\partial_0(-f) = -\partial_1 f$$

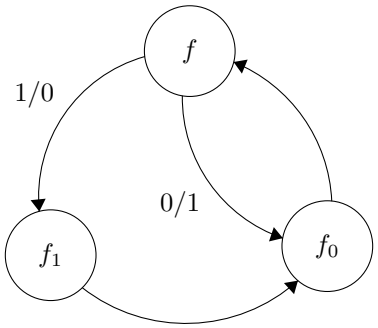
$$\partial_1(-f) = -\partial_0 f$$

Thus using the characterization by Sutner [21], that a state is odd iff it has distinct residuals, we can close γ under residuation using only information in $\mathcal{A}$. Since $\gamma \in \mathcal{G}(\mathcal{A})$ and $\mathcal{G}(\mathcal{A})$ is residuation closed, this entire closure is a subset of $\mathcal{G}(\mathcal{A})$.

But we know that adding a state which residuates into an existing automaton does not change the group. To that end, the above closure generates the same group as the above closure with an additional state δ residuating into γ and a self loop I. This new machine is exactly $\mathcal{A}_{\bar{e}_1} \subseteq \mathfrak{C}(\mathbf{A}, \bar{e}_1)$. Any state in $\mathcal{A}_{e_1}$ is the negation of a state in $\mathcal{A}_{e_1}$, and so $\mathfrak{A}(\mathbf{A}) = \mathcal{A}_{\bar{e}_1} \cup \mathcal{A}_{-\bar{e}_1} \subseteq \mathcal{G}(\mathcal{A})$. Then $\mathcal{G}(\mathfrak{A}(\mathbf{A})) \leq \mathcal{G}(\mathcal{A})$, as desired. □

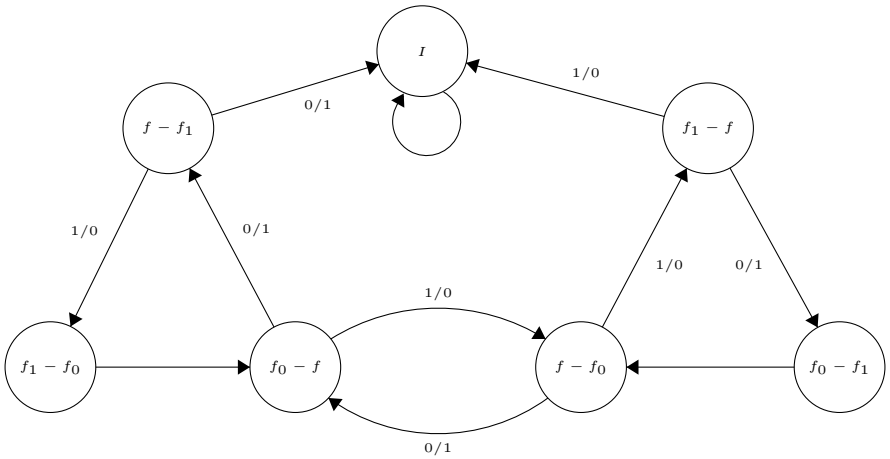
1.3 An Example

Consider the following machine, $\mathcal{A}_2^3$:



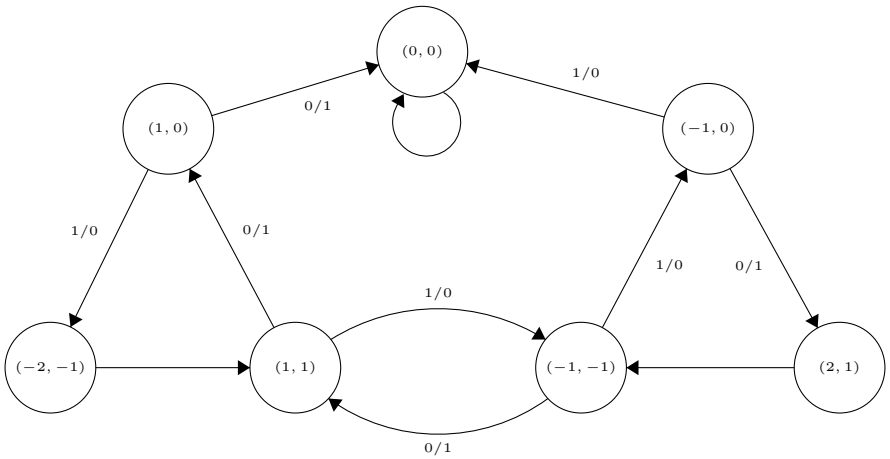
Here the unlabeled transitions both copy the input bit, however these have been omitted for cleanliness.

Then by letting $\gamma = \partial_1 f - \partial_0 f = f_1 - f_0$, and closing under residuation using the above algorithm, we construct the following machine (γ is shown at the bottom left):



When running the algorithm in this case, we do not need to separately add $\pm\delta$ or the inverse machine. Here $\delta = f - f_1$, and the machine is already closed under negation. The Strongly Connected Component Conjecture predicts that this will be the case whenever $\mathbf{A}$ has characteristic polynomial other than $x^m - \frac{1}{2}$, which corresponds to the so called sausage automata. Unfortunately, however, this conjecture is yet unproven, and so in the above proof we had to explicitly add in these extra states.

Relatedly, the following is $\mathfrak{A}(\mathbf{A})$ for $\mathbf{A} = \begin{pmatrix} -1 & 1 \\ -\frac{1}{2} & 0 \end{pmatrix}$:



So, for example, $\partial_1(1,0) = \mathbf{A}((1,0)+(1,0)) = (-2,-1)$, and indeed we see a 1/0 transition from (1,0) to (-2,-1).

Further, $\mathcal{A}_2^3$ as above is located at $\bar{e}_1 \in \mathfrak{C}(\mathbf{A},(3,2))$, and taking $f = (1,0)$ gives $f_0 = \partial_0 f = \mathbf{A}((1,0)-(3,2)) = (0,1)$ and $f_1 = \partial_1 f = \mathbf{A}((1,0)+(3,2)) = (-2,-2)$. It is readily checked, for instance, that $\partial_0 f_1 = \partial_1 f_1 = f_0$.

One can also check that $\mathfrak{A}$ is located at $(3,2) \in \mathfrak{C}(\mathbf{A},(3,2))$, a pattern which we will see continues for all $\bar{e}$.

Finally, in $\mathfrak{A}$ as shown above, $\gamma = (-2,-1)$, since we see $\partial_1(1,0) - \partial_0(1,0) = \gamma$. In $\mathcal{A}_2^3$, however, we see $\gamma = (-2,-3)$. Notice that even though numerically the vectors are different, due to the different values of $\bar{e}$, both versions of γ compute the same function. This is a manifestation of the fact that δ is located at different positions in the two machines, and $\gamma = 2\mathbf{A}\delta$.

2 Group Extensions

Going forward, $\mathcal{G} = \mathbb{Z}^m$ will denote $\mathcal{G}(\mathfrak{A})$ for some principal machine $\mathfrak{A}$.

$\mathcal{G}$ admits representation as a $\mathbb{Z}[x]$ module where $x \cdot \bar{v} = \mathbf{A}^{-1}\bar{v}$, extended linearly. Further, since $\mathbf{A}$ has irreducible character so does $\mathbf{A}^{-1}$. Thus this module is cyclic, and is generated by $\bar{e}_1 = \delta$. (Note that since $\mathbf{A}$ sends $2\mathbb{Z}\oplus\mathbb{Z}^{m-1}$ to $\mathbb{Z}^m$, and therefore has multiples of $\frac{1}{2}$ in general, $\mathbf{A}^{-1}$ sends $\mathbb{Z}^m$ to $2\mathbb{Z}\oplus\mathbb{Z}^{m-1}$, and so has only integer entries).

Now for $p \in \mathbb{Z}[x]$ with odd constant term, we write $p \cdot \mathcal{G}$ in place of $\mathcal{G}(\mathfrak{C}(\mathbf{A}, p\cdot\bar{e}_1))$. That is to say, $p\cdot\mathcal{G}$ has as its states $\mathbb{Z}^m$ and as its odd residuations $\partial_0\bar{v} = \mathbf{A}(\bar{v} - p\cdot\bar{e}_1)$, and $\partial_1\bar{v} = \mathbf{A}(\bar{v} + p\cdot\bar{e}_1)$. Since this module is cyclic, every $\bar{v}$ arises as $p_{\bar{v}}\cdot\bar{e}_1$ where $p_{\bar{v}} = \bar{v}_0 + \bar{v}_1 x + \ldots + \bar{v}_{m-1}x^{m-1}$. We will only discuss polynomials p with an odd constant term, as this ensures $p\cdot\bar{e}_1$, our residuation vector, is odd.

Definition 11. $p\cdot\mathcal{G}$ is called the **Group Extension** of $\mathcal{G}$ by p

To justify this nomenclature, we first notice $\mathcal{G} \hookrightarrow p\cdot\mathcal{G}$ for all p by the homomorphism $\bar{v} \mapsto p\cdot\bar{v}$. Further, we recognize that if p is not a unit in $\mathrm{End}_{\mathcal{G}} \cong \mathbb{Z}^m/\chi^*$, this homomorphism is *not* surjective. That is to say $\mathcal{G}$ is a proper subgroup of $p\cdot\mathcal{G}$. Here, $\mathrm{End}_{\mathcal{G}}$ is the ring of all group endomorphisms, not necessarily preserving the residuation structure, and χ^* is the characteristic polynomial of $\mathbf{A}^{-1}$. This observation is true in more generality, as shown below.

Theorem 6. *If $rp = q$ in $\mathbb{Z}[x]$, then $p\cdot\mathcal{G} \hookrightarrow q\cdot\mathcal{G}$, with a canonical injection $\varphi_r : \bar{v} \mapsto r\cdot\bar{v}$. In particular, if r is a unit, then $p\cdot\mathcal{G} \cong q\cdot\mathcal{G}$.*

Proof. Let $rp = q$, $f \in p\cdot\mathcal{G}$ located at $\bar{v}$. Consider $f' \in q\cdot\mathcal{G}$ located at $r\cdot\bar{v}$.

First note f and f' have the same parity, since r has odd constant term, and so $\bar{v}$ and $r\cdot\bar{v}$ have the same parity. Now, consider the residuals of f and f'.

If f is even, then

$$\partial_0 f' = \mathbf{A}(r\cdot\bar{v}) = r\cdot\mathbf{A}\bar{v} = r\cdot\partial_0 f$$

If f is odd, then

$$\partial_0 f' = \mathbf{A}(r\cdot\bar{v} - q\cdot\bar{e}_1) = r\cdot\mathbf{A}(\bar{v} - p\cdot\bar{e}_1) = r\cdot\partial_0 f$$

A similar argument shows $\partial_1 f' = r\cdot\partial_1 f$

If r is a unit, then r^{-1} also has odd constant term (since $r * r^{-1} = 1$ has odd constant term) and so φ_r is an isomorphism with inverse $\varphi_{r^{-1}}$. □

2.1 Fractional Elements

As the previous proof shows, $p\cdot\bar{v} \in p\cdot\mathcal{G}$, computes exactly the same function as $\bar{v} \in \mathcal{G}$. However, most vectors cannot be written as $p\cdot\bar{v}$. What do they do as functions? We call such vectors (and their corresponding functions) **Fractional**, due to the following observation and theorem:

Consider $\bar{e}_1 \in 3 \cdot \mathcal{G}$. By the above theorem, $3\bar{e}_1 = \delta$, and so we should expect $\bar{e}_1$ to behave like "$\frac{1}{3}\delta$", and in fact it does.

In general, $\bar{v} \in p \cdot \mathcal{G}$ behaves like $p^{-1} \cdot \bar{v} \in \mathcal{G}$, (where p^{-1} comes from $\mathbb{Q}[x]$ and so $p^{-1} \cdot \bar{v} \in \mathbb{Q}^m$) and so Group Extensions give us access to fractions of functions from our base group $\mathcal{G}$.

We will consider $p^{-1} \cdot \mathbb{Z}^m = \{p^{-1} \cdot \bar{v} \mid \bar{v} \in \mathbb{Z}^m\}$ as a subgroup of $\mathbb{Q}^m$. Residuation in this setting is given by $\partial_0 \bar{v} = \mathbf{A}(\bar{v} - \bar{e}_1)$ and $\partial_1 \bar{v} = \mathbf{A}(\bar{v} + \bar{e}_1)$. Here, instead of scaling *up* our residuation vector, we scale *down* all of our other vectors. Then we have access to certain elements of $\mathbb{Q}^m$, which are exactly the factional elements as noted before. Now δ is always located at $\bar{e}_1$.

Morally, however, this is just a different way of looking at the group extension construction. We justify this with the following theorem:

Theorem 7. *For $p \in \mathbb{Z}[x]$ with odd constant term, $p^{-1} \cdot \mathbb{Z}^m \cong p \cdot \mathcal{G}$.*

Proof. Consider $\varphi : p^{-1} \cdot \mathbb{Z}^m \to p \cdot \mathcal{G}$ by $\varphi(p^{-1} \cdot \bar{v}) = \bar{v}$.
φ is clearly bijective, and is a homomorphism since:

$$\begin{aligned}\varphi(p^{-1} \cdot \bar{v}_1 + p^{-1} \cdot \bar{v}_2) &= \varphi(p^{-1} \cdot (\bar{v}_1 + \bar{v}_2)) \\ &= \bar{v}_1 + \bar{v}_2 \\ &= \varphi(p^{-1} \cdot \bar{v}_1) + \varphi(p^{-1} \cdot \bar{v}_2)\end{aligned}$$

Further, if $\bar{v}$ is even, then:

$$\begin{aligned}\varphi(\partial_0(p^{-1} \cdot \bar{v})) &= \varphi(\mathbf{A}(p^{-1} \cdot \bar{v})) \\ &= \varphi(p^{-1} \cdot \mathbf{A}\bar{v}) \\ &= \mathbf{A}\bar{v} \\ &= \partial_0(\varphi(p^{-1} \cdot \bar{v}))\end{aligned}$$

If $\bar{v}$ is odd, then:

$$\begin{aligned}\varphi(\partial_0(p^{-1} \cdot \bar{v})) &= \varphi(\mathbf{A}(p^{-1} \cdot \bar{v} - \bar{e}_1)) \\ &= \varphi(p^{-1} \cdot \mathbf{A}(\bar{v} - p \cdot \bar{e}_1)) \\ &= \mathbf{A}(\bar{v} - p \cdot \bar{e}_1) \\ &= \partial_0(\varphi(p^{-1} \cdot \bar{v}))\end{aligned}$$

The proof for ∂_1 is similar. □

Thus we can view functions in $p \cdot \mathcal{G}$ as fractions of functions in $\mathcal{G}$. It is a natural question to ask which fractions are attainable in this way.

Clearly, for any $f \in \mathcal{G}$, we can attain $\frac{1}{k} f$ for any odd k. Simply take $\bar{v} \in k \cdot \mathcal{G}$ for f located at $\bar{v}$. However, fractions with even denominator are, in general, unattainable. $2\frac{1}{2}\delta = \delta$ should be an odd function, but no function, when doubled, is odd.

2.2 Characterizing Automata

Since each automaton $\mathcal{A}$ is a subautomaton of some $\mathfrak{C}(\mathbf{A}, \bar{e})$, equivalently some $p \cdot \mathcal{G}$, there should be a minimal $\bar{e}$ (up to multiplication by units) which still has $\mathcal{A}$ as a subautomaton.

Notice that if we locate $\mathcal{A}$ at $\bar{e}_1 \in p \cdot \mathcal{G}$, then there can be no smaller polynomial q (in the division ordering) which also places $\mathcal{A}$ at an integral position. The following theorem shows this is always possible.

Theorem 8. *Every nontrivial abelian automaton $\mathcal{A}$ can be located at $\bar{e}_1$ in $p \cdot \mathcal{G}$ for some p.*

Proof. It is a theorem by Sutner [21] that every finite state abelian automaton residuates into a strongly connected component, and further that this component generates the same group as the entire machine. So we may, with no loss of generality, assume our machine is strongly connected (that is, every state except possibly I has a path to every other state).

Let f be an odd state in $\mathcal{A}$. Then at least one of $\partial_0 f$ and $\partial_1 f$ is not equal to f. So there is some nontrivial cycle from f to itself, which we can represent by a matrix equation relating $\bar{v}_f$, and $\bar{e}$. (Here $\bar{v}_f$ is where f will be located, and $\bar{e}$ will be the residuation vector). We can then rearrange this equation to obtain $p_1(\mathbf{A})\bar{v}_f = p_2(\mathbf{A})\bar{e}$.

$p_1, p_2 \in \mathbb{Z}[x]$, and $\mathbf{A}$ has irreducible character over $\mathbb{Z}$. It is well known that the eigenvalues of $p(\mathbf{A})$ are precisely $p(\lambda)$ where λ is an eigenvalue of $\mathbf{A}$, so $\mathbf{A}$'s invertibility implies the invertibility of both $p_1(\mathbf{A})$ and $p_2(\mathbf{A})$. Thus

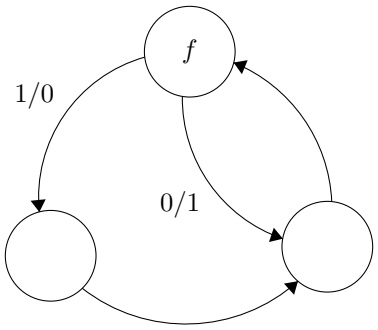
$$\bar{e} = p_2(\mathbf{A})^{-1} p_1(\mathbf{A}) \bar{v}_f$$

Choosing $\bar{v}_f = \bar{e}_1$ gives a value for the residuation vector $\bar{e}$, and (since $\mathcal{G}$ is cyclic as a $\mathbb{Z}[x]$ module) a value $\bar{e}$ induces a polynomial $p_{\bar{e}}$ such that $p_{\bar{e}} \cdot \bar{e}_1 = \bar{e}$. Then, by construction, $\mathcal{A}$ is a subautomaton of $p_e \cdot \mathcal{G}$, and is anchored with f at $\bar{e}_1$. As desired. □

For any automaton $\mathcal{A}$, we can now completely characterize in which $\mathfrak{C}(\mathbf{A}, \bar{e})$ it can be located, and at what vectors. Simply locate $\mathcal{A}$ at $\bar{e}_1 \in p \cdot \mathcal{G}$, and then to locate it at any odd vector $\bar{v}$, scale both sides by $p_{\bar{v}}$ to see $\mathcal{A}$ located at $\bar{v} \in p_{\bar{v}} p \cdot \mathcal{G}$. In the above proof, the choice of $\bar{v}_f = \bar{e}_1$ was arbitrary, and we can directly locate $\mathcal{A}$ at a different odd vector $\bar{v}'$ by setting $\bar{v}_f = \bar{v}'$. This will give the same result as locating it at $\bar{e}_1$ and then multiplying by $p_{\bar{v}'}$, again, by cyclicity. The same observation shows that, given some polynomial q (equivalently some vector $q \cdot \bar{e}_1$) $\mathcal{A}$ is located somewhere in $q \cdot \mathcal{G} = \mathfrak{C}(\mathbf{A}, q \cdot \bar{e}_1)$ if and only if $p \mid q$. Further, it will be located at exactly $p^{-1} q \cdot e_1$.

2.3 An Example

Recall the abelian automaton $\mathcal{A}_2^3$ from earlier in the paper:



Say we want to find $\bar{v}$ and $\bar{e}$ such that $\mathcal{A}_2^3$ is located at $\bar{v} \in \mathfrak{C}(\mathbf{A}, \bar{e})$.
Using the algorithm described by Becker [3] gives $\mathbf{A} = \begin{pmatrix} -1 & 1 \\ -\frac{1}{2} & 0 \end{pmatrix}$.
Then notice $\partial_0 \partial_0 f = f$. So $\mathbf{A}^2(\bar{v}_f - \bar{e}) = \bar{v}_f$, and $\mathbf{A}^2 \bar{v}_f - \bar{v}_f = \mathbf{A}^2 \bar{e}$. Thus

$$\bar{e} = \mathbf{A}^{-2}(\mathbf{A}^2 - I)\bar{v}_f$$

Choosing $\bar{v}_f = \bar{e}_1$ gives $\bar{e} = (3, 2)$.
Then $f = (1, 0) \in (3 + 2x) \cdot \mathcal{G}$

2.4 Limiting Object

Since each $p \cdot \mathcal{G}$ can be viewed as $p^{-1} \cdot \mathbb{Z}^m \subseteq \mathbb{Q}^m$ with residuation vector $\bar{e}_1$, it is reasonable to consider the subgroup of $\mathbb{Q}^m$

$$\widetilde{\mathcal{G}} = \bigcup_p p^{-1} \cdot \mathbb{Z}^m$$

(Recall we only include polynomials with odd constant term in this union)

Notice that this group is universal, in the sense that it contains as subgroups each $p \cdot \mathcal{G}$. Further, it concretely shows the relationships between the various automata. In this setting, we see exactly why automata show up in multiple group extensions, and why the division ordering of polynomials is the characterizing factor. $p \cdot \mathcal{G}$ is an approximation of $\widetilde{\mathcal{G}}$, where we scale up by a factor of p and take only the integral vectors (residuation is necessarily scaled up to match). In this structure, then, there is no unnecessary duplication of the location of automata, and there is no extra parameter $\bar{e}$.

3 Characterizing Orbits

Recall an **Orbit** of $f \in \mathcal{G}(\mathcal{A})$ at $u \in \mathbf{2}^\omega$ is $\{f^t u \mid t \in \mathbb{Z}\}$, or, additively, $\{tfu \mid t \in \mathbb{Z}\}$. It is a reasonable question to wonder what these orbits look like for an arbitrary function f. We will soon see they look like lines with slope f and "intercept" given by $\langle u \rangle$, which sends $0^{|u|}$ to u.

We begin with a useful lemma: we can flip just the ith bit.

Theorem 9. $(x^n \cdot \delta)(u0v) = u1v$ *(when* $|u| = n$*, and* $v \in \mathbf{2}^*$ *or* $\mathbf{2}^\omega$*)*

Proof. If $n = 0$ the theorem is clear, since $\delta 0v = 1(\partial_0 \delta v) = 1(Iv) = 1v$

Further, $\mathbf{A}^{-1} f$ is always even (since $\mathbf{A}^{-1} : 2\mathbb{Z} \oplus \mathbb{Z}^{m-1}$), and so copies the first bit, then applies f. The claim follows by induction.

□

We will first prove the result in the finite case.

Theorem 10. *For every word* $u \in \mathbf{2}^n$*, there exists a unique function (mod* $Stab(0^n)$*) sending* 0^n *to* u*. Following Sutner and Lewi [22], we call this function* $\langle u \rangle$*.*

Proof. The existance of such a function is a direct consequence of the lemma, and is given by $\sum_{i=0}^{n-1} u_i x^i \delta$. Uniqueness mod $Stab(0^n)$ is immediate. □

Theorem 11. *The orbit of* f *at* u *is given by the line* $\mathbb{Z}f + \langle u \rangle$

Proof. Let $w = tfu$ be in the orbit of u. Then $\langle w \rangle$ sends 0^n to w, but so does $tf + \langle u \rangle$. By uniqueness, then, $\langle w \rangle = tf + \langle u \rangle$ and the theorem follows. □

Note that this argument works in the infinite case as well (it arguably works better, since $\mathrm{Stab}(0^\omega)$ is trivial), though the obvious extension $\langle u \rangle = \sum_{i=0}^{\infty} u_i x^i \delta$ for $u \in \mathbf{2}^\omega$ cannot be effective in general for cardinality reasons. We clearly cannot send 0^ω to any u without working in the topological closure $\widehat{\mathcal{G}}$, where we may lose finiteness of our automata. Further, since every f residuates into a strongly connected component, every f sends 0^ω to an ultimately periodic string. This is the only obstruction.

Theorem 12. *For* $u \in \mathbf{2}^\omega$*,* $\langle u \rangle$ *exists in some group extension iff* u *is ultimately periodic.*

Proof. Since every function $f \in p \cdot \mathcal{G}$ eventualy residuates into a finite strongly connected component, $f0^\omega$ is ultimately periodic for every such f.

Further, if we have an ultimately periodic string $u = tv^\omega$, then $\sum_{i=0}^{\infty} u_i x^i \delta$ works if it exists in some group extension. It does, since:

$$\begin{aligned}
\sum_{i=0}^{\infty} u_i x^i \delta &= \sum_{i=0}^{|t|} t_i x^i \delta + \sum_{i=|t|}^{\infty} v_i^* x^i \delta \\
&= \sum_{i=0}^{|t|} t_i x^i \delta + x^{|t|} \sum_{i=0}^{\infty} v_i^* x^i \delta \\
&= \sum_{i=0}^{|t|} t_i x^i \delta + x^{|t|} \frac{\sum_{i=0}^{|v|} v_i x^i \delta}{1 - x^{|v|}} \\
&= \left(\sum_{i=0}^{|t|} t_i x^i + x^{|t|} \frac{\sum_{i=0}^{|v|} v_i x^i}{1 - x^{|v|}} \right) \cdot \delta \\
&= \frac{\left(1 - x^{|v|}\right) \sum_{i=0}^{|t|} t_i x^i + x^{|t|} \sum_{i=0}^{|v|} v_i x^i}{1 - x^{|v|}} \cdot \delta
\end{aligned}$$

This last sum is of the form $\frac{q}{1-x^{|v|}} \cdot \delta$, Thus, this sum is equal to $q \cdot \delta \in (1 - x^{|v|}) \cdot \mathcal{G}$. (Or, equivalently, $\frac{q}{1-x^{|v|}} \cdot \delta \in \widetilde{\mathcal{G}}$) $\square$

4 Conclusion

We have shown that the residuation vector $\bar{e}$ corresponds to how fine an approximation of $\widetilde{\mathcal{G}}$ one wants. This is because each $\mathfrak{C}(\mathbf{A}, \bar{e})$ corresponds to $p_{\bar{e}} \cdot \mathcal{G}$, with progressively larger $\bar{e}$ corresponding to progressively more complicated fractional elements, which approximate $\widetilde{\mathcal{G}}$. Thus, the parameter really provides a way of interacting with these elements living in $\mathbb{Q}^m$ as though they were in $\mathbb{Z}^m$, and so by computing in $\widetilde{\mathcal{G}}$ (or a suitably large approximation) directly, we can remove the need for this parameter.

Further, the existence of the universal object $\widetilde{\mathcal{G}}$ sheds new light on the connection between affine tiles [12, 13] and abelian automata noted by Sutner [21]. Indeed it is easy to see that in $\widetilde{\mathcal{G}}$ every strongly connected component (and thus every subautomaton of interest) has each vector in the attractor of the iterated function system given by the residuation functions $\{\bar{v} \mapsto \mathbf{A}\bar{v}, \bar{v} \mapsto \mathbf{A}(\bar{v} \pm \bar{e}_1)\}$. Thus, in particular, the size of the principal machine is bounded by the number of integral points in this attractor. Even in $\mathbb{Z}^2$, however, there are examples where this bound is not tight.

The relation between automata and polynomials discussed in this paper also provides a new take on a proof technique for the longstanding Strongly Connected Component Conjecture. This conjecture asserts that principal machines $\mathfrak{A}$ have only one strongly connected component (plus the self looping identity state) whenever their matrix has a characteristic polynomial that is *not* of the form $x^n + \frac{1}{2}$. The new way of looking at residuation vectors allows us to rewrite the residual functions as $\partial_i \bar{v} = \mathbf{A}(\bar{v} - (-1)^i \delta)$ for $\bar{v}$ odd. It is easy to see, then, that the following polynomials correspond to paths ending in δ, since they undo residuation:

$$\begin{aligned} P_\epsilon(x) &= 1 \\ P_{w0}(x) &= xP_w(x) + 0 \\ P_{w1}(x) &= xP_w(x) + 1 \\ P_{w\bar{1}}(x) &= xP_w(x) - 1 \end{aligned}$$

Sutner made a similar observation, and described Path Polynomials [21] which allow us to reason about the existence of directed paths between states in an automaton by purely algebraic means. However, these polynomials are clunky and not always defined, since they correspond to paths *starting* at δ, and so $P'_{w0} \cdot \delta$ is only well defined if $P'_w \cdot \delta$ is even (and P'_{w1} and $P'_{w\bar{1}}$ are only well defined if $P_w \cdot \delta$ is odd). Since the polynomials defined above move *backwards* along transitions instead of forwards, they are always well defined.

These path polynomials are certainly useful, as at the very least they give a lower bound on the size of the principal machine. We know that any nontrivial path polynomial connecting δ to δ must be 1 mod χ^*, and cannot be 1. Thus it has degree at least that of χ^*, which is m. With this, we gain a (weak) lower bound on the size of the principal machine of roughly $2m$, as there is also a path of length m from $-\delta$ to $-\delta$ by linearity. This bound is approximate, because it

is a priori possible for these two paths to intersect. However, path polynomials seem to be much more useful than this wimpy bound would lead us to believe.

The existence of a path polynomial p which is congruent to $-1 \bmod \chi^*$ then shows the existence of a path from $-\delta$ to δ. Then to prove the SCC conjecture, it suffices to prove that whenever $\mathbf{A}$ does not have characteristic $x^n + \frac{1}{2}$ there is a polynomial $p \in \{-1, 0, 1\}[x]$ which is congruent to $-1 \bmod \chi^*$.

In fact, the set $\{-1, 0, 1\}[x]$ is sometimes called $\mathcal{B}$, the set of **Borwein Polynomials** (named after [5]). These polynomials are related to multiple open problems in number theory, most notably in a conjecture regarding the existance a minimal non-trivial mahler measure [14]. This strengthens the ties to number theory which Becker noted in his thesis, and gives new ties to extremely diverse branches of math, including extremely recent results of the dynamics of binary substitution systems [1].

These substitution systems give rise to similar tilings to the ones mentioned above from [12, 13]. Indeed, there are deep ties between Borwein Polynomials, the iterated function system given by residuation, and Complex Analysis. One exploration of these connections comes in the form of generalized mandelbrot sets [6].

These path polynomials seem like the correct approach to solving the SCC Conjecture, as the naive algorithm for finding a path from $-\delta$ to δ seemes to always work. By "the naive algorithm", we mean the following (in pseudo-python):

```
def tryToGetPathPoly(A):
    aut = PrincipalAutomaton(A)

    if aut.isSausage(): # charpoly = z^m - 2
        print "No path -delta to delta in sausage!"
        return None

    sgn = aut.chi(0)/abs(aut.chi(0)) # sign of constant term of charpoly

    p = -1
    while not isPathPoly(p):
        flag = False # only add one multiple of chi per iteration
        for a_i in coeffs(p):
            if abs(a_i) > 1 and not flag:
                p = p - z^i * sgn * (a / abs(a)) * aut.chi
                flag = True

        if not flag: # p must be Borwein with leading coeff -1
            p = p + (z^(len(list(p))-1) * sgn * aut.chii)

    return p
```

This algorithm halts on all of the abelian automata we have access to, and efforts are underway to prove the SCC Conjecture using this approach.

Acknowledgements

This paper would not exist without the advice of my advisor Dr Klaus Sutner. There aren't enough thanks for the hours of conversation I enjoyed. I would also like to thank Dr Clinton Conley and Dr Kate Thompson, both of whom were a wealth of knowledge. Their patience and kindness in the face of my constant pestering is an inspiration to the kind of professor I hope to one day be.

References

[1] Baake, M., Coons, M., Mañibo, N.: Binary constant-length substitutions and mahler measures of borwein polynomials (11 2017)

[2] Bárány, V.: Automatic presentations of infinite structures (2007)

[3] Becker, T.: Representations and complexity of abelian automaton groups. Senior Thesis, CMU. `http://tjbecker.me/files/thesis.pdf` (may 2018)

[4] Bondarenko, I., Grigorchuk, R., Kravchenko, R., Muntyan, Y., Nekrashevych, V., Savchuk, D., Šunić, Z.: Groups generated by 3-state automata over a 2-letter alphabet. ii. Journal of Mathematical Sciences **156**(1), 187–208 (Jan 2009), `https://doi.org/10.1007/s10958-008-9262-5`

[5] Borwein, P., Erdélyi, T.: On the zeros of polynomials with restricted coefficients. Illinois J. Math **46**, 667–675 (1997)

[6] CALEGARI, D., KOCH, S., WALKER, A.: Roots, schottky semigroups, and a proof of bandt's conjecture. Ergodic Theory and Dynamical Systems **37**(8), 2487–2555 (2017). https://doi.org/10.1017/etds.2016.17

[7] Grigorchuk, R.R., Nekrashevich, V.V., Sushchanski, V.I.: Automata, dynamical systems and groups. Proc. Steklov Institute of Math. **231**, 128–203 (2000)

[8] Grigorchuk, R.R., Zuk, A.: The lamplighter group as a group generated by a a 2-state automaton, and its spectrum. Geom. Dedicata **87**, 209–244 (2001)

[9] Grigorchuk, R.: Milnor's problem on the growth of groups and its consequences (2011)

[10] Gupta, N., Sidki, S.: On the burnside problem for periodic groups. Mathematische Zeitschrift **182**(3), 385–388 (Sep 1983). https://doi.org/10.1007/BF01179757, `https://doi.org/10.1007/BF01179757`

[11] Holcombe, W.M.L.: Algebraic Automata Theory. Cambridge University Press (1982)

[12] Lagarias, J.C., Wang, Y.: Self-affine tiles in $\mathbb{R}^n$. Adv. Math. **121**, 21–49 (1996)

[13] Lagarias, J.C., Wang, Y.: Integral self-affine tiles in $\mathbb{R}^n$ ii. lattice tilings. J. Fourier Anal. Appl. **3**(1), 83–102 (1997)

[14] Mossinghoff, M.: Algorithms For The Determination Of Polynomials With Small Mahler Measure. Ph.D. thesis (01 1995)

[15] Nekrashevych, V.: Self-Similar Groups, Math. Surveys and Monographs, vol. 117. AMS (2005)

[16] Nekrashevych, V., Sidki, S.: Automorphisms of the binary tree: state-closed subgroups and dynamics of 1/2-endomorphisms. Cambridge University Press (2004)

[17] Okano, T.: Invertible binary transducers and automorphisms of the binary tree. MS Thesis, CMU (may 2015)

[18] Sakarovitch, J.: Elements of Automata Theory. Cambridge University Press (2009)

[19] Sidki, S.: Automorphisms of one-rooted trees: Growth, circuit structure, and acyclicity. J. Math. Sciences **100**(1), 1925–1943 (2000)

[20] Skrzypczak, M.: Descriptive Set Theoretic Methods in Automata Theory. Springer-Verlag Berlin Heidelberg (2016)

[21] Sutner, K.: Abelian Invertible Automata

[22] Sutner, K., Lewi, K.: Iterating invertible binary transducers. In: Kutrib, M., Moreira, N., Reis, R. (eds.) Descriptional Complexity of Formal Systems, Lecture Notes in Computer Science, vol. 7386, pp. 294–306. Springer Berlin (2012)