Matrix Representations of Abelian Automaton Groups

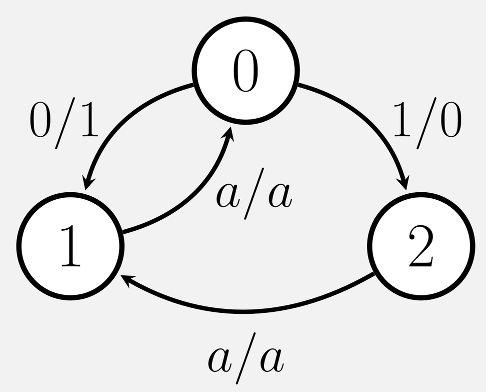
Tim Becker & Klaus Sutner
Carnegie Mellon Computer Science Department

Abstract

Representing groups concretely may aid in solving group-theoretic computational problems, and some representations will provide more insight than others. In this poster, we give an efficient algorithm to compute a linear-algebraic representation of abelian automaton groups, along with a basis of identites that hold in the transduction group.

Automaton Groups

A *binary invertible transducer* is a Mealy machine of the form show below.



For each state q we have length-preserving transduction $\underline{q}$. These transductions (along with their inverses) form a group under composition, denoted $\mathcal{G}(A)$. A transduction $f \in \mathcal{G}(A)$ is called *odd* if it flips the first bit of its input; otherwise f is called *even*. We also have the *residuation* maps $\partial_a : \mathcal{G}(\mathcal{A}) \to \mathcal{G}(\mathcal{A})$ for $a \in \{0,1\}$. In the example above, $\partial_0\,\underline{0} = \underline{1}$ and $\partial_1\,\underline{0} = \underline{2}$.

Let $\mathcal{A}$ be a transducer with n states $\{s_1, \dots, s_n\}$ whose transduction group is abelian.

Proposition 1. *There is an epimorphism $\psi : \mathbb{Z}^n \to \mathcal{G}(\mathcal{A})$ given by $\psi(a_1, \dots, a_n) = \underline{s_1}^{a_1} \cdots \underline{s_n}^{a_n}$*

Proposition 2. *Define the* 1/2-transition matrix *as follows:*

$$B_{i,j} = \begin{cases} 1 & \text{if } \partial_0\,\underline{s_i} = \partial_1\,\underline{s_j} \\ \frac{1}{2} & \text{if } s_i \text{ is a toggle state and } \partial_0\,\underline{s_i} = \underline{s_j} \text{ or } \partial_1\,\underline{s_i} = \underline{s_j} \\ 0 & \text{otherwise} \end{cases}$$

Then B performs residuation on even states. That is, for any $v \in \mathbb{Z}^m$ such that $\psi(v)$ is even, $\partial_a\,\psi(v) = \psi(Bv)$.

Matrix Representations

In [1], Nekrashevych and Sidki proved the following:

Theorem 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 $m \times m$ matrix A, and a vector r which satisfy*

$$\phi(\partial_a\,\underline{p}) = \begin{cases} A \cdot \phi(\underline{p}) & \text{if } \underline{p} \text{ is even} \\ A \cdot \phi(\underline{p}) + (-1)^a r & \text{if } \underline{p} \text{ is odd} \end{cases}$$

Also, the matrix A satisfies several interesting properties:

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

We call this A and r the *residuation pair* for the automaton $\mathcal{A}$. We prove some additional properties of A.

Lemma 1. *The map $R = \psi \circ \phi$ is a surjective linear map $\mathbb{Z}^n \to \mathbb{Z}^m$, and for all $k \geq 1$, $RB^k = A^k R$.*

Proof. ψ is surjective and ϕ is bijective, so R is surjective. Since $\psi \circ B = \partial_a \circ \psi$, we have $RB = AR$. The claim follows by induction. □

Lemma 2. *The characteristic polynomial of A divides the characteristic polynomial of B.*

Proof. By the previous lemma, for any polynomial P, $RP(B) = P(A)R$. Apply Cayley-Hamilton. □

Lemma 3. *Let A' be the companion matrix of χ_A. We say A is well-behaved if A is $GL(m,\mathbb{Z})$-similar to A', i.e. if there exists an invertible $m \times m$ integral matrix T such that $TAT^{-1} = A'$. If A is well-behaved, then (A', Tr) is a residual pair.*

Proof. For all $v \in \mathbb{Z}^m$ and $c \in \{0, \pm 1\}$,

$$T(Av + cr) = T(T^{-1}A'Tv + cr) = A'(Tv) + cr'$$

□

An Algorithm

Theorem 2. *There is a polynomial time algorithm to compute a residuation pair A, r for a well-behaved abelian automaton $\mathcal{A}$.*

Proof. For each irreducible factor f of $\chi_B(x)$ of the form $x^k + \frac{1}{2}g(x)$ where $g(x) \in \mathbb{Z}[x]$ has degree less than k, let C_f be the companion matrix of f. Solve the matrix equation $RB = C_f R$ for R, which can be done using Kronecker Products. Such a solution is guaranteed to exist because C_f and B share eigenvalues. Once R is computed, we can compute r as follows. Let s_a be an odd state in $\mathcal{A}$ and let $s_b = \partial_0\,s_a$. Let e_i denote the ith standard basis vector, such that $\psi(e_i) = \underline{s_i}$, and compute $r = Re_b - A'Re_a$. We can now simply check if (C_f, r) is a residuation pair for $\mathcal{A}$.
By Lemma 2, one of these factors must be χ_A, and since $\mathcal{A}$ is well-behaved, (C_f, r) will be a residuation pair for some factor f. □

Theorem 3. *The matrix R computed in the above algorithm gives a basis of identites holding in $\mathcal{G}(\mathcal{A})$.*

Proof. Since A' is a contraction, A'^k has no nontrivial fixed points for all $k > 0$. Thus the only identity in $R(\mathbb{Z}^n)$ is $\vec{0}$, and computing the null space of R gives the basis of identites. □

References

[1] 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.

Acknowledgements

Thanks to Klaus Sutner for his guidance on this project. Also, thanks to Evan Bergeron for helpful discussions.