Abelian Mealy Automata

Klaus Sutner

Carnegie Mellon University

March 2026

Burnside 1902

Is there an infinite, finitely generated group where every element has finite order?

Milnor 1968

Are there groups of intermediate growth?

Grigorchuk 1980/83

Yes and yes.

Grigorchuk's Construction

Define 4 transformations $\alpha, \beta, \gamma, \delta$ on $[0,1] \subseteq \mathbb{R}$.

Use Cantor space $\mathbf{2}^\omega$, $\mathbf{2} = \{0,1\}$, as representation.

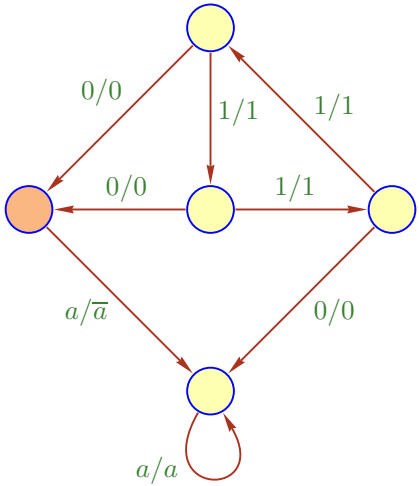
Let $a \in \mathbf{2}$, $x \in \mathbf{2}^\omega$ and define recursively

$$\alpha(a\,x) = \overline{a}\,x$$

$$\beta(a\,x) = \mathbf{if}(a = 0)\ \mathbf{then}\ a\,\alpha(x)\ \mathbf{else}\ a\,\beta(x)$$

$$\gamma(a\,x) = \mathbf{if}(a = 0)\ \mathbf{then}\ a\,\alpha(x)\ \mathbf{else}\ a\,\delta(x)$$

$$\delta(a\,x) = \mathbf{if}(a = 0)\ \mathbf{then}\ a\,x\ \mathbf{else}\ a\,\beta(x)$$


0/0
1/1
1/1
0/0
1/1
a/ā
0/0
a/a

Mealy machine

$$\delta : Q \times \mathbf{2} \longrightarrow \mathbf{2} \times Q$$

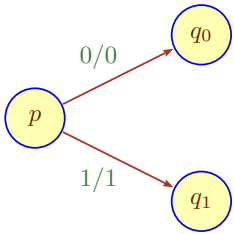
The residual is $\partial_a\, p = \mathsf{snd}\big(\delta(p, a)\big)$.

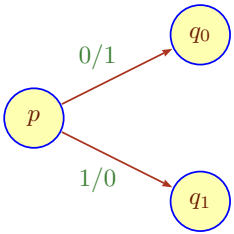
No initial and final states; Eilenberg referred to these machines as output modules.

For any state p in $\mathcal{A}$ we get a length-preserving transduction $\mathcal{A}(p)$ or simply

$$\underline{p} : \mathbf{2}^\star \to \mathbf{2}^\star$$

Invertible Mealy Machines





Two types of states: parity even/copy and odd/toggle.

In this case, $\underline{p}$ is a bijection on $\mathbf{2}^n$.

Automaton (Semi-) Groups

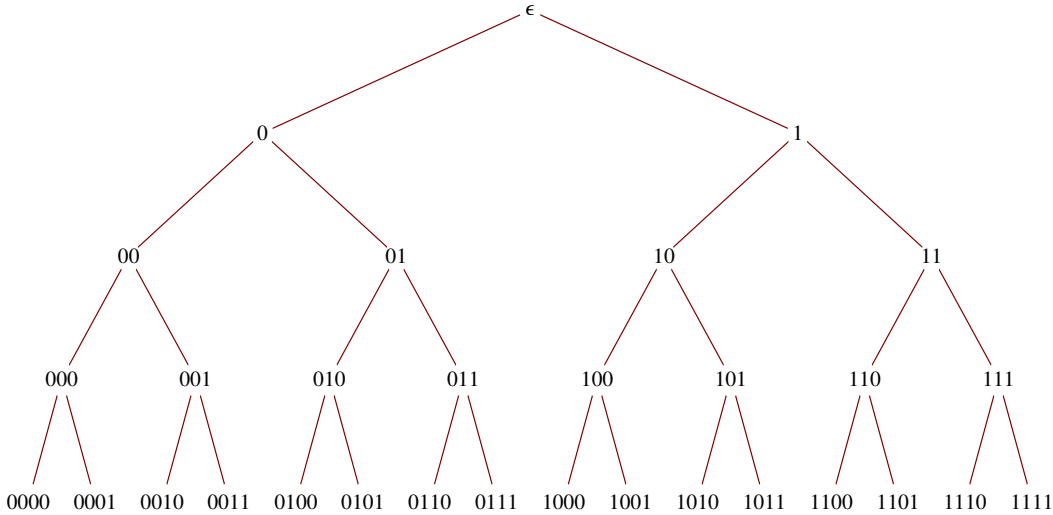
Let $\mathcal{A}$ be an invertible Mealy machine.

$$\begin{aligned} \operatorname{Sgrp}\mathcal{A} &= \text{ the semigroup generated by the } \underline{p} \\ \operatorname{Grp}\mathcal{A} &= \text{ the group generated by the } \underline{p} \end{aligned}$$

Typically $\operatorname{Sgrp}\mathcal{A}$ fails to be a group; one needs the inverse automaton $\mathcal{A}^{-1}$:

change transition $p \xrightarrow{a/b} q$ to $p \xrightarrow{b/a} q$.

Think of automorphisms of the tree $\mathbf{2}^\star$


ϵ
0
1
00
01
10
11
000
001
010
011
100
101
110
111
0000
0001
0010
0011
0100
0101
0110
0111
1000
1001
1010
1011
1100
1101
1110
1111

Wreath Products

The full automorphism group $\mathrm{Aut}(\mathbf{2}^\star)$ of $\mathbf{2}^\star$ has a nice recursive structure:

$$\mathrm{Aut}(\mathbf{2}^\star) \simeq \mathrm{Aut}(\mathbf{2}^\star) \wr \mathfrak{S}_2 = \big(\mathrm{Aut}(\mathbf{2}^\star) \times \mathrm{Aut}(\mathbf{2}^\star)\big) \rtimes \mathfrak{S}_2$$

The elements are triples $f = (f_0, f_1)s$, $f_i \in \mathrm{Aut}(\mathbf{2}^\star)$, $s \in \mathfrak{S}_2$.

The f_i are the residuals of f and s is its parity.

The group operation is

$$(f_0, f_1)\, s * (g_0, g_1)\, t = (f_0 g_{s(0)}, f_1 g_{s(1)})\, st$$

Classification 3 States

On classification of groups generated by 3-state automata over a 2-letter alphabet

I. Bondarenko, R. Grigorchuk, R. Kravchenko, Y. Muntyan,
V. Nekrashevych, D. Savchuk and Z. Šunić

Algebra and Discrete Mathematics, 1 (2008) 1–163

Up to symmetry, 5832 automata. Many produce the same group.

Theorem

There are at most 122 distinct groups generated by 3-state automata.

Abelian Mealy Automata

Define the gap value of state p to be

$$\gamma_p = (\underline{\partial_0 p})^{-1} \underline{\partial_1 p} \in \mathsf{Grp}\,\mathcal{A}$$

Lemma

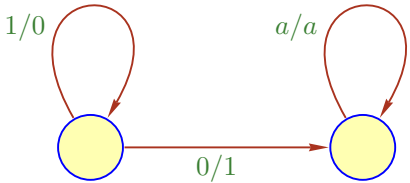
Let $\mathcal{A}$ be minimal. Then $\mathsf{Sgrp}\,\mathcal{A}$ *is commutative iff*

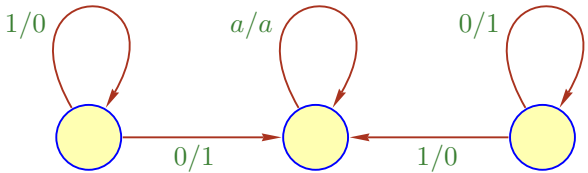
p even implies $\gamma_p = I$ and p odd implies $\gamma_p = f$ constant

Only consider only Abelian Mealy automata: odd gap value is different from I, generate a free Abelian group $\mathbb{Z}^m$.

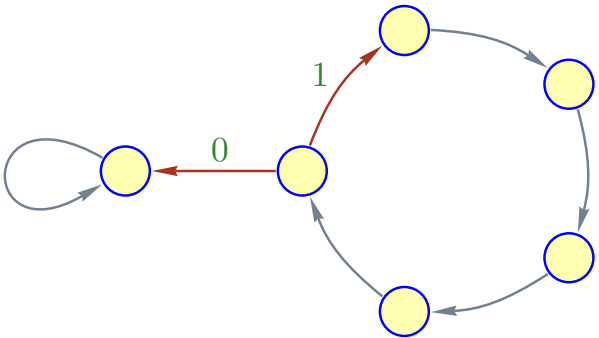
Checkable in polynomial time using standard automata-theoretic algorithms.

Adding Machine

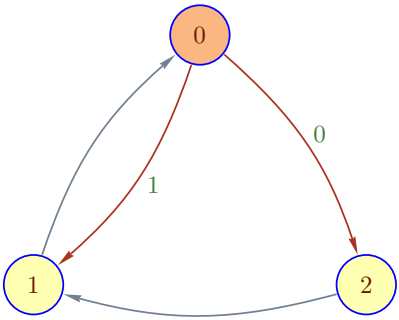




Sausage Automaton



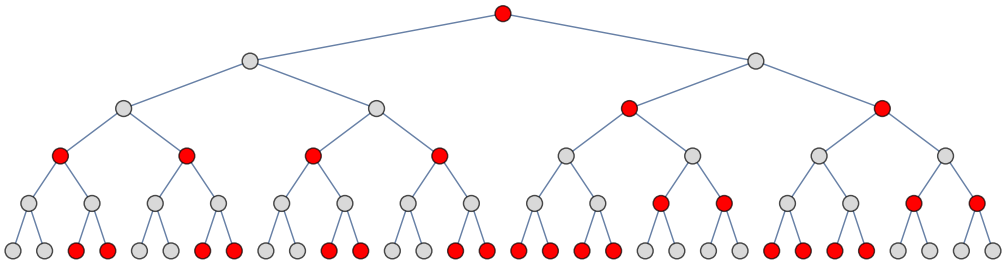
Running Example



automaton $\mathcal{A}_2^3$

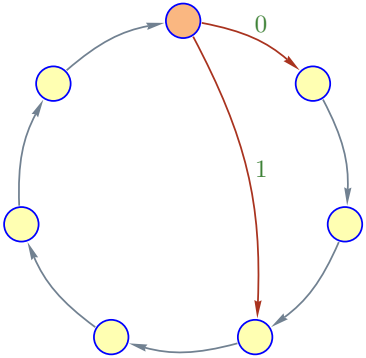
Claim: $\mathsf{Sgrp}(\mathcal{A}_2^3) = \mathsf{Grp}(\mathcal{A}_2^3) \simeq \mathbb{Z}^2$

Tree Action



The automorphism $\underline{0}$ acting on the infinite binary tree.

Cycle-Cum-Chord



automaton $\mathcal{A}_3^7$

Claim: $\mathsf{Grp}(\mathcal{A}_m^n) \simeq \mathbb{Z}^{n-\gcd(n,m)}$

Searching for Identities

Want a basis for the identities in Sgrp $\mathcal{A}_2^3$.
One-toggle machine, hence commutative, so basis is modulo AC.

Can use standard automata-theoretic algorithms to construct minimal machines for automorphisms in the semigroup. But beware of exponential blow-up (number of words over generators, size of product automata).

$$\underline{0}^{\,2}\,\underline{1}^{\,2}\,\underline{2} = I$$

Verify

$$\begin{aligned}
\underline{0}^{\,2}\,\underline{1}^{\,2}\,\underline{2} &= \big((\underline{2},\underline{1})\sigma\big)^2(\underline{0},\underline{0})^2(\underline{1},\underline{1}) \\
&= (\underline{2}\,\underline{1},\underline{1}\,\underline{2})(\underline{0},\underline{0})(\underline{0},\underline{0})(\underline{1},\underline{1}) \\
&= \big(\underline{0}^{\,2}\,\underline{1}^{\,2}\,\underline{2},\underline{0}^{\,2}\,\underline{1}^{\,2}\,\underline{2}\big)
\end{aligned}$$

Hard part: show that there are no other identities (up to associativity/commutativity).

Theorem (Nekrashevych, Sidki)

- *There is an isomorphism* $\Phi : \mathrm{Grp}\,\mathcal{A} \to \mathbb{Z}^m$, *a* $m \times m$ *rational matrix* A *and a rational vector* $\boldsymbol{r}$ *such that*

$$\Phi(\partial_a f) = \begin{cases} \mathrm{A}\,\Phi(f) & f \text{ even} \\ \mathrm{A}\,\Phi(f) + (-1)^a \boldsymbol{r} & f \text{ odd} \end{cases}$$

- A *is invertible and contracting.*
- *The characteristic polynomial of* A *is* $\mathbb{Q}$*-irreducible and has the form* $z^m + \frac{1}{2}\, g(z)$*;* $g \in \mathbb{Z}[z]$ *has degree at most* $m-1$ *and constant term* ± 1.

The groups $\mathbb{Z}^m$ here are also referred to as m-lattices.

Tile Perspective

affine	$\mathsf{A}\boldsymbol{v} \pm \boldsymbol{r}$	$\boldsymbol{r} = \mathsf{A}\boldsymbol{e}$
tiling	$\mathsf{A}\big(\boldsymbol{v} \pm \boldsymbol{e}\big)$	$\boldsymbol{e} = \mathsf{A}^{-1}\boldsymbol{r}$

Both A^{-1} and $\boldsymbol{e}$ are integral ($\boldsymbol{e}$ is odd in the first component).

1/2-Matrices

$$\mathsf{A} = \begin{pmatrix} \frac{a_{11}}{2} & a_{12} & \dots & a_{1m} \\ \frac{a_{21}}{2} & a_{22} & \dots & a_{2m} \\ \vdots & & & \vdots \\ \frac{a_{m1}}{2} & a_{m2} & \dots & a_{mm} \end{pmatrix}$$

Up to $\mathsf{GL}(m, \mathbb{Z})$ equivalence, the residuation matrices look like so: companion matrices for the g polynomials.

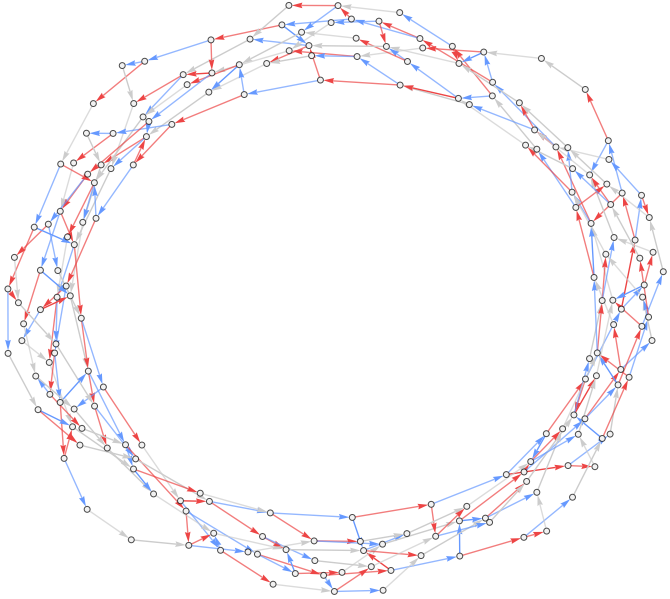
Claim: There are only finitely many $1/2$-matrices for each m-lattice.

$$\begin{pmatrix} 0 & 1 \\ 1/2 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 \\ -1/2 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1/2 & 1 \\ -1/2 & 0 \end{pmatrix}$$

$$z^2 - 1/2 \qquad z^2 - z + 1/2 \qquad z^2 - z/2 + 1/2$$

$$\begin{pmatrix} 0 & 1 \\ -1/2 & 0 \end{pmatrix} \qquad \begin{pmatrix} -1 & 1 \\ -1/2 & 0 \end{pmatrix} \qquad \begin{pmatrix} -1/2 & 1 \\ -1/2 & 0 \end{pmatrix}$$

$$z^2 + 1/2 \qquad z^2 + z + 1/2 \qquad z^2 + z/2 + 1/2$$



Residuation Matrix

Theorem

Given an Abelian automaton $\mathcal{A}$, one can construct the corresponding residuation matrix in polynomial time.

Moreover, one can construct a basis for the identities in $\mathsf{Grp}\,\mathcal{A}$.

$$\begin{array}{ccccc} \mathbb{Z}^n & \xrightarrow{\phi} & \mathcal{G} & \xrightarrow{\psi} & \mathbb{Z}^m \\ \uparrow B & & \uparrow \partial_0 & & \uparrow A \\ U & \xrightarrow{\phi} & E & \xrightarrow{\psi} & V \end{array}$$

$U = (2\mathbb{Z})^t \oplus \mathbb{Z}^{n-t}$, E even automorphisms, $V = \psi(E)$

B is an $n \times n$ matrix over $\{0, 1/2, 1\}$ encoding $\mathcal{A}$.

Requires factoring char_B to obtain char_{A}.

Gröbner

Translate transitions $p \xrightarrow{a/b} q$ into polynomials $P(p,q)$ in $\mathbb{Q}[z, x_1, \ldots, x_n]$.

$$P(p,q) = z\,x_p - x_q + (a - b)$$

The constant term $a - b$ is just a symmetric binary digit.

A specialized Gröbner basis algorithm produces the characteristic polynomial in time $O(n^6)$.

Taxonomy

A residuation pair is a residuation matrix A together with an odd vector $\boldsymbol{e} \in \mathbb{Z}^m$.

The complete automaton or ambient automaton $\mathfrak{C}(\mathsf{A}, \boldsymbol{e})$ has state set $\mathbb{Z}^m$ and transitions

$$\boldsymbol{p} \xrightarrow{a/b} \boldsymbol{q} \iff \boldsymbol{q} = \mathsf{A}\big(\boldsymbol{p} + (b{-}a)\boldsymbol{e}\big)$$

$\mathfrak{A}(\mathsf{A}, \boldsymbol{e}, \boldsymbol{v})$ is the finite subautomaton of $\mathfrak{C}(\mathsf{A}, \boldsymbol{e})$ generated by $\boldsymbol{v} \in \mathbb{Z}^m$.

$\boldsymbol{v}$ realizes $\mathcal{A}$ in $\mathfrak{C}(\mathsf{A}, \boldsymbol{e})$ iff $\mathcal{A} \simeq \mathfrak{A}(\mathsf{A}, \boldsymbol{e}, \boldsymbol{v})$.

The principal automaton is $\mathfrak{A}(\mathsf{A}) = \mathfrak{A}(\mathsf{A}, \boldsymbol{e}_1, \boldsymbol{e}_1)$.

Theorem

Let $\mathcal{A}$ be an Abelian subautomaton of $\mathfrak{C}(\mathrm{A}, e)$, $p \longrightarrow q$ a transition with $q \in \mathcal{A}$.
Let $\mathcal{A}_+$ be the smallest subautomaton containing $\mathcal{A}$ and p.

Then $\mathrm{Grp}\,\mathcal{A} = \mathrm{Grp}\,\mathcal{A}_+$.

As a consequence, there are two interesting types of subautomata of $\mathfrak{C}(\mathrm{A}, e)$:

- the principal automaton
- strongly connected automata

These are all situated in a bounded region around the origin for each ambient automaton.

Theorem

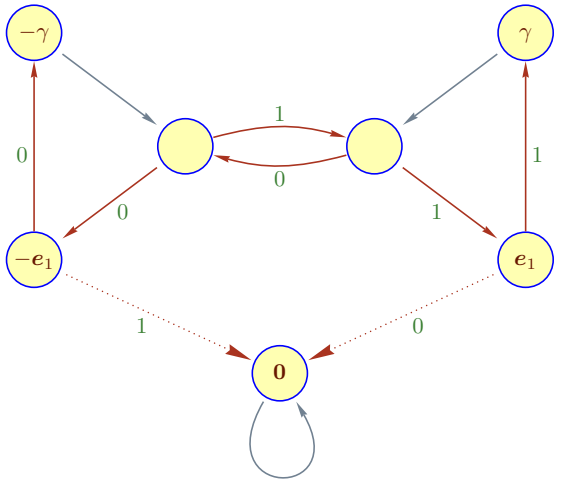
Each complete automaton $\mathfrak{C}(\mathrm{A}, \boldsymbol{e})$ has the principal automaton $\mathfrak{A}(\mathrm{A})$ as a subautomaton.

Hence the gap value depends only on the residuation matrix.

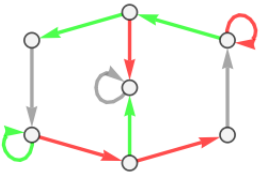
The principal automaton contains the state $\mathbf{0} \in \mathbb{Z}^m$ as a trap:

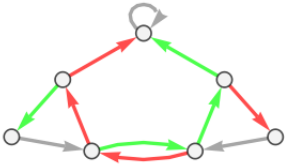
$\mathbf{0}$ is one of the successors for $\boldsymbol{e}_1$, the other is the gap value.

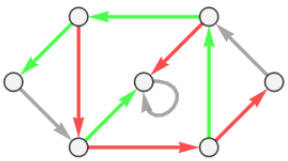
Running Example

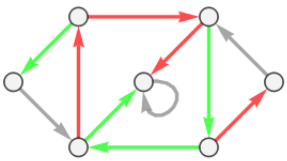


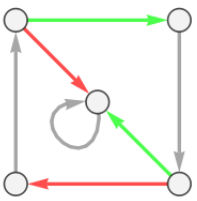
All Principals











Constructing Principals

Lemma

Given any Abelian $\mathcal{A}$, one can directly construct the corresponding principal automaton.

Clearly can obtain γ. The closure of γ can be computed directly using just $\mathcal{A}$.

$$\partial_a (fg) = \begin{cases} \partial_a f \; \partial_{\overline{a}} g & \text{if both are odd} \\ \partial_a f \; \partial_a g & \text{otherwise} \end{cases}$$

$$\partial_a f^{-1} = (\partial_{\overline{a}} f)^{-1}$$

Question:
Given some SCC automaton $\mathcal{A}$, can we realize it at $\boldsymbol{v}$ in $\mathfrak{C}(\mathsf{A}, \boldsymbol{e})$?

Find a residuation cycle anchored at an odd state

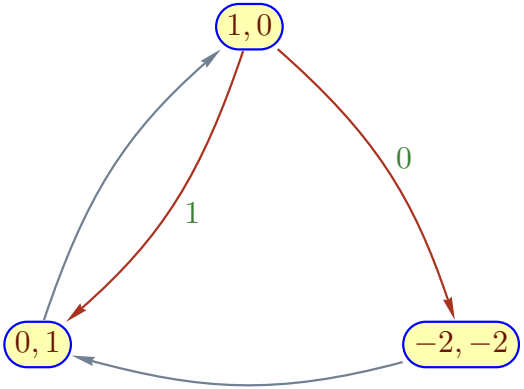
$$\partial_{a_1}\partial_{a_2}\ldots\partial_{a_r}\boldsymbol{v} = \boldsymbol{v}$$

and use it get linear equations for $\boldsymbol{v}$ and $\boldsymbol{e}$.

E.g., for $\mathcal{A}_2^3$ there is a cycle $\partial_1\,\partial_1\,\underline{0} = \underline{0}$, so

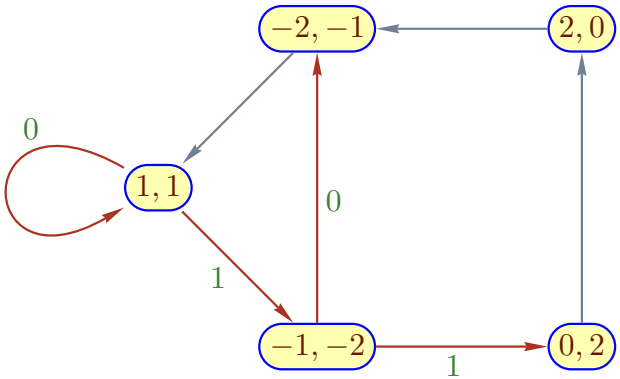
$$\boldsymbol{e} = \mathsf{A}^{-2}\big(\mathsf{A}^2 - I\big)\boldsymbol{v}$$

It follows that $\mathcal{A}_2^3$ embeds in $\mathfrak{C}\big(\mathsf{A}, (3,2)\big)$ at $\boldsymbol{e}_1$.



$\mathfrak{A}\big(\mathsf{A}, (3,2), \boldsymbol{e}_1\big)$

And Another



$\mathfrak{A}\big(\mathsf{A}, (3,2), (1,1)\big)$

Minimal Embeddings

Think of $\mathbb{Z}^m$ as $\mathbb{Z}[z]$-module with $z \cdot \boldsymbol{v} = \mathsf{A}^{-1}\boldsymbol{v}$, so $p(z) \cdot \boldsymbol{v} = \sum a_k \mathsf{A}^{-k}\boldsymbol{v}$.

Suppose p has odd constant term. Since $\mathsf{A}^{-1} : \mathbb{Z}^m \to 2\mathbb{Z} \oplus \mathbb{Z}^{m-1}$ is surjective, we get all odd residuation vectors as $p(z) \cdot \boldsymbol{e}_1$.

Theorem

Every Abelian automaton can be realized by $\boldsymbol{e}_1$ in the ambient automaton A *and $\boldsymbol{e} = p(z) \cdot \boldsymbol{e}_1$ for some $p \in \mathbb{Z}[z]$.*

Provides a sort of canonical representation by choosing p minimal with respect to divisibility.

Open Problems

- **Principal Automaton Conjecture**

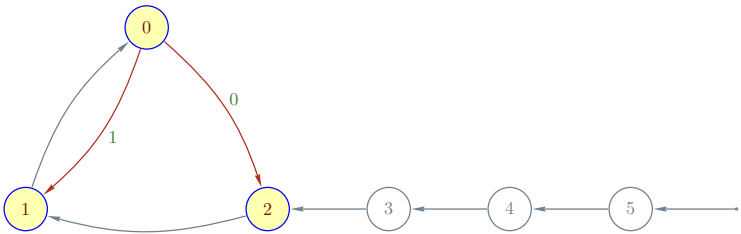
  The principal automaton is always a single strongly connected component plus the identity—except for sausage automata.

- Is there reasonable way to count SCC automata, given $(\mathsf{A}, \boldsymbol{e})$.

- Is there reasonable way to compute the smallest SCC automaton, given A.

Extension

Establishing $\underline{0}^{\,2}\,\underline{1}^{\,2}\,\underline{2} = I$ as basis for identities.



Adding an infinite copy-chain $\underline{k{+}1} = (\underline{k}\,, \underline{k}\,)$.

$\underline{k}\,(x) = x_1 \ldots x_k\, \underline{0}\,(x_{k+1} x_{k+2} \ldots)$

More Identities

cancellation identity

$$\underline{k}^{\,2}\,\underline{k{+}1}^{\,2}\,\underline{k{+}2} = I$$

shift identity

$$\underline{k}^{\,2} = \underline{k{+}2}\;\underline{k{+}3}$$

As a rewrite system, prefer cancellation over shift to get termination.

Rewrite

0	1	2	3	4	5	6	7	8	9
15	10								
-14	-14	-7							
	4	4	2						
		4	4	2					
			-6	-6	-3				
				4	4	2			
						-2	-2	-1	
							2	2	1
1	0	1	0	0	1	0	0	1	1

Theorem (Knuth Normal Form)

Every automorphism f of $\mathcal{G}$ has a unique normal form

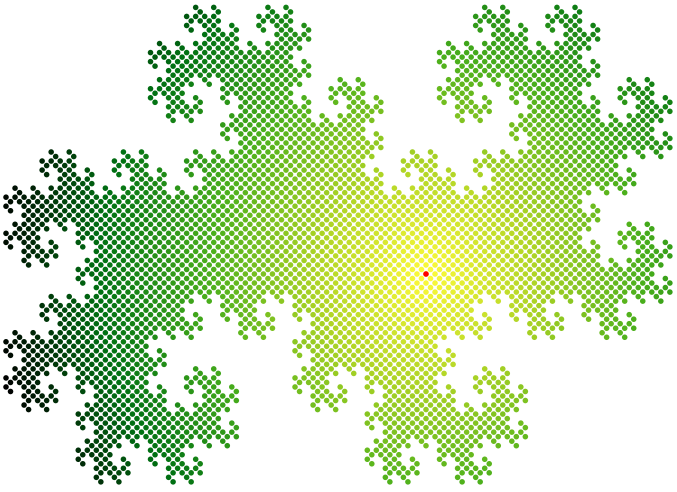
$$f = \underline{k_1}\ \underline{k_2}\ \ldots\ \underline{k_n}$$

where $k_i < k_{i+1}$, $n \geq 0$.

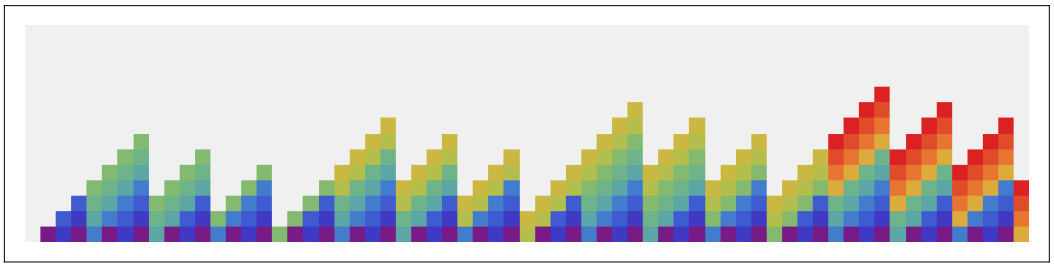
Corollary

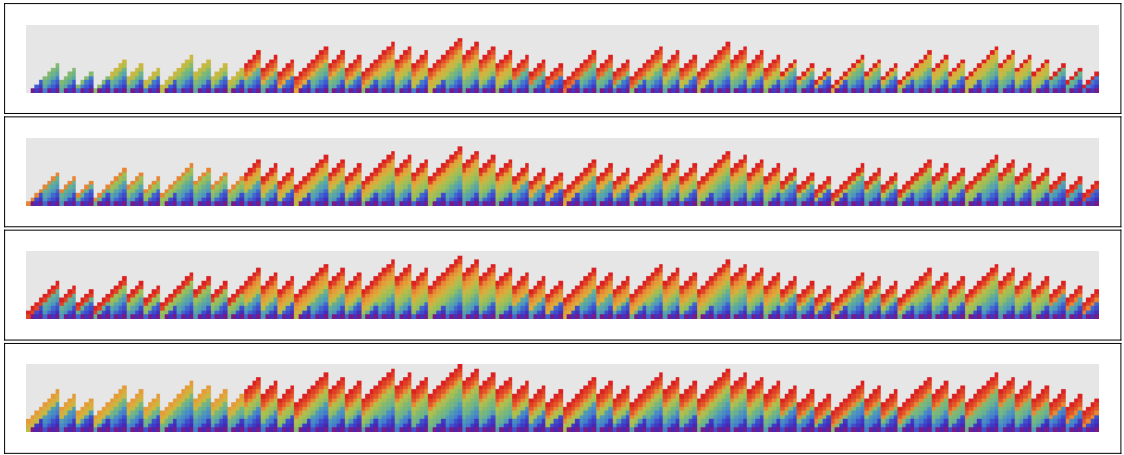
$\mathcal{G}$ is isomorphic to $\mathbb{Z}[\mathbf{i}]$ via $f \mapsto \rho^{k_1} + \rho^{k_2} + \ldots + \rho^{k_t} \in \mathbb{Z}[\mathbf{i}]$ where $\rho = \mathbf{i} - 1 \in \mathbb{C}$.

Dragon Curve



KNF for $\underline{0}^{\ell}$, $\ell < 64$

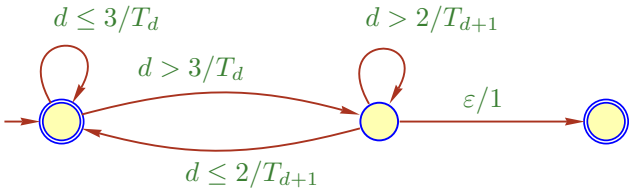




Rationality

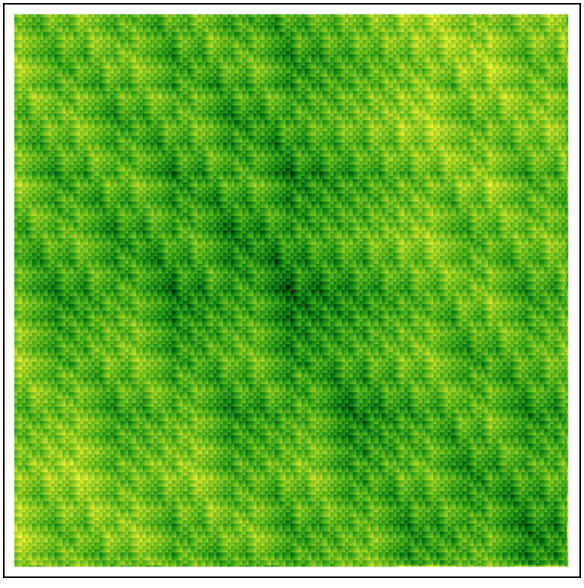
Claim

The map $k \mapsto \mathsf{KNF}(\underline{0}^{\,k})$ is rational.



Input is reverse base-16, output binary.

$\mathsf{KNF}\left(\underline{0}^{\,16^k}\right) = \underline{8k}$



A digit set is a subset $\mathcal{D} \subseteq \mathbb{Z}^m$.

A self-affine tile is a compact set $T \subseteq \mathbb{R}^m$ such that

- $T = \mathsf{A}(T + \mathcal{D})$
- T has positive Lebesgue measure

$$T = \left\{ \sum\nolimits_{i \geq 0} \mathsf{A}^{-i} d_i \mid d_i \in \mathcal{D} \right\} \subseteq \mathbb{R}^m$$

Digit Sets

A^{-1} and $\mathcal{D}$ define a $\mathbb{Z}$-module

$$\mathbb{Z}[\mathsf{A}^{-1}, \mathcal{D}] = \mathbb{Z}[\mathcal{D}, \mathsf{A}^{-1}\,\mathcal{D}, \ldots, \mathsf{A}^{-m+1}\mathcal{D}]$$

For the standard digit set $\mathcal{D} = \{\mathbf{0}, \boldsymbol{e}_1\}$, this is the $\mathbb{Z}$-linear closure of the points co-reachable from the origin in the ambient automaton $\mathfrak{C}(\mathsf{A}, \boldsymbol{e}_1)$.

$\mathcal{D}$ is primitive if $\mathbb{Z}[\mathsf{A}^{-1}, \mathcal{D}] = \mathbb{Z}^m$.

We need $\mathcal{D}$ primitive whose digits form a complete residue system of $\mathbb{Z}^m/\mathsf{A}^{-1}\mathbb{Z}^m$.

KNF for $m = 2$

A	root	KNF
$\left(\begin{smallmatrix} 0 & 1 \\ 1/2 & 0 \end{smallmatrix}\right)$	$\sqrt{2}$	no
$\left(\begin{smallmatrix} 1 & 1 \\ -1/2 & 0 \end{smallmatrix}\right)$	$1 + \mathbf{i}$	no
$\left(\begin{smallmatrix} 1/2 & 1 \\ -1/2 & 0 \end{smallmatrix}\right)$	$\left(1 + \mathbf{i}\sqrt{7}\right)/2$	yes
$\left(\begin{smallmatrix} 0 & 1 \\ -1/2 & 0 \end{smallmatrix}\right)$	$\mathbf{i}\sqrt{2}$	yes
$\left(\begin{smallmatrix} -1/2 & 1 \\ -1/2 & 0 \end{smallmatrix}\right)$	$\left(-1 + \mathbf{i}\sqrt{7}\right)/2$	yes
$\left(\begin{smallmatrix} -1 & 1 \\ -1/2 & 0 \end{smallmatrix}\right)$	$-1 + \mathbf{i}$	yes

Number Field Representation

Let α be a root of the reciprocal $\mathrm{char}_{\mathsf{A}}^{\star}$ of $\mathrm{char}_{\mathsf{A}}$ and consider the field extension $\mathbb{F} = \mathbb{Q}[\alpha]$.

Since α is an algebraic integer this is preferable over adjoining a root of $\mathrm{char}_{\mathsf{A}}$.

α is expanding: all its conjugates have modulus larger than 1.

This produces a representation of the m-lattice as a lattice of algebraic integers $\sum a_i \alpha^i$ in $\mathbb{F}$.

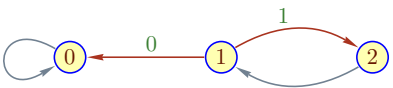
Alternatives

Define weak Knuth normal form analogously but with symmetric digit set $\{-1, 0, +1\}$.

A theorem by Lagarias and Wang shows that every Abelian automaton admits a weak KNF.

Alternatively, one can consider infinite versions of KNF over the standard digit set.

E.g., for the sausage machine of order 2, the inverse of $\underline{1}$ has infinite KNF $101010\ldots$



Orbit Problems

Problem: **Orbit Rationality**
Instance: A length-preserving transduction f on $\mathbf{2}^\star$.
Question: Are the orbits of f rational?

Problem: **Timestamp Problem**
Instance: A length-preserving transduction f, two words $x, y \in \mathbf{2}^k$.
Solution: The least $t \geq 0$ such that $y = x\, f^t$, if it exists; `No` otherwise.

Problem: **Coordinate Problem**
Instance: A word $x \in \mathbf{2}^\ell$ where $\ell = km$.
Solution: The coordinates of x in $(2^k)^m$.

Proposition

The CCC automaton $\mathcal{A}_2^3$ is orbit rational.

The CCC automaton $\mathcal{A}_3^4$ fails to be orbit rational.

The non-rationality depends on the the field extension $\mathbb{Q}[\alpha]$.

One needs to show that α^k is irrational for all $k > 0$; can be reduced to finitely many tests.

Open Problems

- When does an Abelian automaton admit Knuth normal form?
- Characterize orbit-rational Abelian automata.
- Are there interesting examples of orbit rationality for non-Abelian automata?
- Study automorphisms with infinite KNF such as $101010\ldots$.