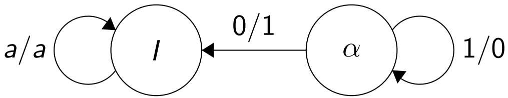
Abelian Automata and their Groups

Chris Grossack

July 20, 2018

Finite State Automata

- Combinatorial Objects
- Encode functions as graphs
  - states
  - transitions



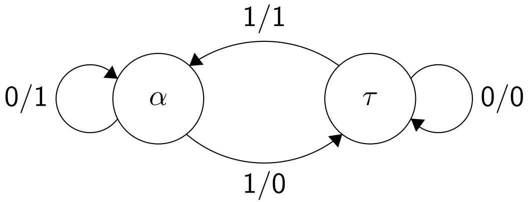
- $\forall w \in \mathbf{2}^* \ . \ I(w) = w$
- $\forall w \in \mathbf{2}^\omega \ . \ I(w) = w$
- $\forall w \in \mathbf{2}^* \ . \ \alpha(w) = w + 1$

Groups

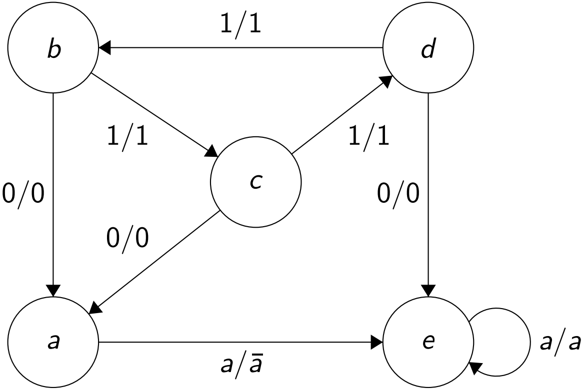
- Where we have functions, we have groups
- Interesting to automata theorists
  - Study automata groups for their own structure
- Interesting to group theorists
  - Rich source of counterexamples
  - Compact way of encoding extremely complex groups

Definition

If $\mathcal{A}$ is an automaton with states $\{s_i\}$, then $\mathcal{G}(\mathcal{A})$ is $\langle s_i \rangle$



- This automaton generates the **Lamplighter Group** $\mathbb{Z}_2 \wr \mathbb{Z}$
- Finitely generated, not finitely presented



- This automaton generates the **Grigorchuk Group**, the first constructive example of a group of intermediate growth

Definition

For $f \in \mathcal{A}$, f_0 is the state after following a 0 transition. Similarly f_1 is the state after following a 1 transition. This extends naturally to functions $f \in \mathcal{G}(\mathcal{A})$.

Definition

A function $f \in \mathcal{G}(\mathcal{A})$ is called **odd** *if it toggles the first bit it reads, and* **even** *otherwise.*

Definition

An automaton $\mathcal{A}$ is called **Abelian** *if the group it generates is*

Theorem (Sutner)

$\mathcal{A}$ is abelian iff $\exists \gamma$ such that $\forall f \in \mathcal{G}(\mathcal{A})$

$$f_0^{-1} f_1 = \begin{cases} I & f \text{ is even} \\ \gamma & f \text{ is odd} \end{cases}$$

Theorem (Nekrashevich and Sidki (paraphrased))

Every abelian automaton group is isomorphic to either an integer lattice or a boolean group. Further, when isomorphic to an integer lattice, residuation lifts to a matrix operation.

- This means we can consider $\mathcal{G}(\mathcal{A}) \cong \mathbb{Z}^m$, equipped with a matrix A which encodes residuation in the following way:
- $\partial_0 : f \mapsto f_0$ lifts to an affine function:

$$v_0 = \begin{cases} A(v) & v \text{ is even} \\ A(v-r) & v \text{ is odd} \end{cases}$$

- $\partial_1 : f \mapsto f_1$ is similar:

$$v_1 = \begin{cases} A(v) & v \text{ is even} \\ A(v+r) & v \text{ is odd} \end{cases}$$

- Somewhat annoyingly, r can be any odd vector...
  - Infinitely many linear algebraic interpretations of one machine

Theorem (N+S (paraphrased))

χ_A is Q-irreducible exactly when your automata use prime many digits

Lemma

2 is prime

Corollary

For the matrices of interest to us, χ_A is Q-irreducible.

Module Theory

- $\mathbb{Z}^m$ looks kind of like $\mathbb{Q}^m$
- $\mathbb{Z}^m$ comes equipped with a matrix A of irreducible character...
- This may remind you of viewing $\mathbb{Q}^m$ as a cyclic $\mathbb{Q}[x]$ module

Definition

A **module** *M over a ring R is a really bad vector space. Just like you can scale vectors by coefficients coming from some field, we can scale module elements by coefficients coming from some ring.*

If $r_1, r_2 \in R$ and $x, y \in M$, then we require things be nice:

- $r_1 \cdot (x + y) = r_1 \cdot x + r_1 \cdot y$
- $(r_1 + r_2) \cdot x = r_1 \cdot x + r_2 \cdot x$
- $(r_1 r_2) \cdot x = r_1 \cdot (r_2 \cdot x)$

Theorem

If $\mathcal{A}$ is an abelian automaton, then $\mathcal{G}(\mathcal{A}) \cong \mathbb{Z}^m$ is a $\mathbb{Z}[x]$ module, where $p \cdot v = p(A^{-1})v$

Theorem

$\mathcal{G}(\mathcal{A})$ is actually a **cyclic** *$\mathbb{Z}[x]$ module, namely:*

$$\forall v \in \mathbb{Z}^m, \exists p \in \mathbb{Z}[x] \text{ such that } v = p \cdot e_1$$

- Now we can characterize the different residuation vectors!
- Recall for any odd vector r:
  - $\partial_0 : f \mapsto f_0$ lifts to an affine function:

$$v_0 = \begin{cases} A(v) & v \text{ is even} \\ A(v-r) & v \text{ is odd} \end{cases}$$

- But our group is a cyclic module, so instead of $A(v-r)$, consider $A(v - p \cdot e_1)$
- Then if $v = p \cdot u$, $A(p \cdot u - p \cdot e_1) = p \cdot A(u - e_1)$
- So really, different residuation vectors correspond to various extensions of some initial group, $\mathfrak{A}$ generated when $r = e_1$.

extensions?

Definition

Denote by $p \cdot \mathfrak{A}$ *the automaton group* $\mathbb{Z}^m$ *whose residuation is given by*

$$v_0 = \begin{cases} A(v) & v \text{ is even} \\ A(v-r) & v \text{ is odd} \end{cases}$$

Note that since r *must be an odd vector,* p *must have odd constant term.*

Theorem

If $p|q$ *then* $p \cdot \mathfrak{A} \leq q \cdot \mathfrak{A}$. *In particular,* $\forall p\ .\ \mathfrak{A} \leq p \cdot \mathfrak{A}$

Hand-Wavy Proof™.

Let $f \in p \cdot \mathfrak{A}$. It suffices to find $g \in q \cdot \mathfrak{A}$ such that f and g have the same parity and have equal residuals.

Let $q = mp$ by assumption. Then $g = m \cdot f$ works.

Since q and p have odd constant term, so must m
"odd times even is even, odd times odd is odd"
Clearly, then, g and f have the same parity.

If f is even, then $f_0 = Af$ and
$g_0 = (m \cdot f)_0 = A(m \cdot f) = m \cdot (Af) = m \cdot f_0$

If f is odd, then $f_0 = A(f - p \cdot e_1)$ and
$g_0 = (m \cdot f)_0 = A(m \cdot f - q \cdot e_1) = m \cdot A(f - p \cdot e_1) = m \cdot f_0$

So, by induction we are done. □

What about other vectors?

- $p \cdot v \in p \cdot \mathfrak{A}$ is the same function as $v \in \mathfrak{A}$
- What about vectors which can NOT be written as $p \cdot v$?
- They are **Fractional**. They correspond to vectors $v \in \mathbb{Q}^m$ such that $p \cdot v \in \mathbb{Z}^m$.
- This justifies the idea of an *extension* of $\mathfrak{A}$. Every time we scale by a polynomial, we introduce new group elements, which are fractions of the original group elements.

- What we've seen so far is a cool characterization of these groups
- Can we solve problems with it, though?

Definition (Orbit Problem)

Given a function f from some abelian automaton group, and words $x, y \in \mathbf{2}^*$ (or polite words in $\mathbf{2}^\omega$), does there exist a $t \in \mathbb{Z}$ such that $f^t(x) = y$?

- We start with the finite case.
- Identify f with a vector in $p \cdot \mathfrak{A}$ for some principal group $\mathfrak{A}$.

Definition

For $u \in \mathbf{2}^*$ let $\langle u \rangle = v \in p \cdot \mathfrak{A}$ such that $v(0^{|u|}) = u$

Theorem

$\langle u \rangle$ always exists, and is unique mod $\textbf{Stab}(0^{|u|})$

Lemma

Denote $p \cdot e_1 \in p \cdot \mathfrak{A}$ by δ, and let $u0v$ be a word in $\mathbf{2}^*$ (or $\mathbf{2}^\omega$) with $|u| = n$.

$$(x^n \cdot \delta)(u0v) = u1v$$

Proof.

When $n = 0$, notice $\delta(0v) = 1v$ since δ is odd and $\delta_0 = A(\delta - p \cdot e_1) = 0$.

Otherwise, $x^{n+1} \cdot \delta = x \cdot x^n \cdot \delta$.
One can check $(x^{n+1} \cdot \delta)$ is even and further $(x^{n+1} \cdot \delta)_0 = (x^n \cdot \delta)$

Then $(x \cdot x^n \cdot \delta)(u_0 u0v) = u_0(x^n \cdot \delta)(u0v) = u_0(u1v)$ $\square$

Proof.

For $u \in \mathbf{2}^*$, $\langle u \rangle = (\sum_{i=0}^{|u|-1} u_i x^i) \cdot \delta$ works

(Recall we want $\langle u \rangle(0^{|u|}) = u$)

By the lemma, each $x^i \cdot \delta$ flips the *ith*0 to a 1, and leaves everything else unchanged. Since each u_i is a 1 iff it needs to be flipped, the polynomial works.

Uniqueness mod $\mathbf{Stab}(0^{|u|})$ follows from basic group theory. □

Theorem (Finite Orbit Problem)

The orbits of f corresopnd precisely to lines in $\mathbb{Z}^m$.

Proof.

Let $u \in \mathbf{2}^*$. Then $\langle (tf)u \rangle = tf + \langle u \rangle$

Thus, the orbit of u under f is precisely $(\mathbb{Z}f + \langle u \rangle)(0^{|u|})$ $\square$

What about when $u \in \mathbf{2}^\omega$?

- The above proof breaks becase $\langle u \rangle$ is not well defined on $\mathbf{2}^\omega$
- However we can approximate $u \in \mathbf{2}^\omega$ as a sequence of strings of increasing length.
- If we can create a sequence of functions which sends each 0 string to the appropriate u approximation, then our sum will converge in the cantor topology, and we can run the same orbit argument.

Theorem

$\langle u \rangle = (\sum_i u_i x^i) \cdot \delta$ *works.*

- For cardinality reasons, however, this clearly can't always converge in our group.
- $\mathbf{2}^\omega$ is uncountable, $p \cdot \mathfrak{A}$ is clearly countable for all p.

Definition

$u \in \mathbf{2}^\omega$ is called **ultimately periodic** *iff $u = tv^*$ for some $|t|, |v| < \infty$*

- Does every ultimately periodic word u have a well defined $\langle u \rangle$?
- Is every word u with well defined $\langle u \rangle$ ultimately periodic?

Theorem

Yes.

Proof.

let $u = tv^*$, then the polynomial we would associate to $\langle u \rangle$ is

$$\begin{aligned}
\langle u \rangle &= (\sum_i u_i x^i) \cdot \delta \\
&= \left(\sum_{i<|t|} t_i x^i + x^{|t|} \frac{\sum_{i<|v|} v_i x^i}{1 - x^{|v|}} \right) \cdot \delta \\
&= \left(\langle t \rangle + x^{|t|} \frac{\langle v \rangle}{1 - x^{|v|}} \right) \cdot \delta \\
&= \frac{p_1}{p_2} \cdot \delta \\
&= p_1 \cdot \delta \in p_2 \cdot \mathfrak{A}
\end{aligned}$$

It is easy to see that any function applied to 0^ω gives a ultimately periodic string, completing the proof. □