Orbit Checking for Invertible Transducers

Evan Bergeron & Klaus Sutner

Carnegie Mellon Computer Science Department

Abstract

We study iterated transductions defined by a class of invertible transducers over the binary alphabet. We present polynomial time orbit checking algorithms for a subclass of automata associated with Abelien free groups of finite rank.

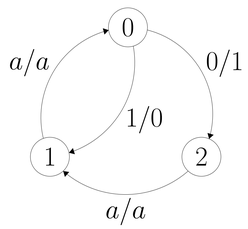
Flipping Pebbles

Suppose we're given a sequence of pebbles, black on one side, white on the other. Starting at the left, flip the current pebble. If the resulting color is black, skip ahead two pebbles. Else, skip ahead one. Repeat until the end of the string.

For example, given the string 0000, we have

$$0000 \to 1001 \to 0011 \to 1010 \to 0000$$

This can be modeled with the following finite state machine A:



When we have two states p and q with the transition $p^{a/b} \to q$, this means "read character a and output character b". The algorithm previously described starts on state 0.

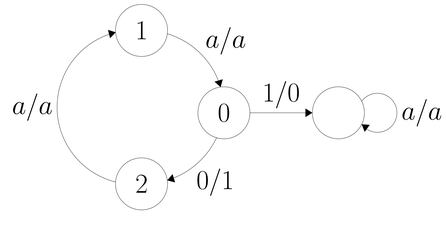
Starting at the 1st state ignores the first character, then proceeds as normal. We can view these pebble flipping algorithm as a function from string to string. These functions form a semigroup $\mathcal{S}(A)$ under composition (associative and closed).

Definition 1. *Given some function $f \in \mathcal{S}(A)$ and some string x, the set of all strings reachable from x by repeated application of f is called the* orbit of x under f.

The central question: given f and two strings x and y, is x in the orbit of y under f? Can we answer this question efficiently?

1-Tree Transducers

Definition 2. *Take a directed acyclic graph with exactly one directed cycle (excluding a copy state self-loop) and exactly one vertex v of outdegree two. Let v be the sole toggle state and every other state be a copy state. The resulting automaton is a 1-tree transducer.*



Proposition 1. *For a 1TT with a cycle of length n, on input x, state i adds (or subtracts) one to the number $x(i) = \{x_j\}_{j \equiv i \mod n}$ interpreted in reverse binary.*

Theorem 1. *Orbit checking for 1-tree transducers can be done in polynomial time.*

Proof. The above proposition reduces orbit checking to a system of equations. Given two strings x, y and a word $f \in \mathcal{S}(A)$, compute which "step size" with which we add to $x(i)$ for all $i \in [n-1]$.

Then simply verify that each $x(i)$ is the same multiple away from $y(i)$ for all i. All of this arithmetic is performed on numbers polynomial in the length of the input. □

Theorem 2. *The semigroup of a 1TT with cycle length n is the free semigroup of rank n.*

Definition 3. *A relation is* rational *if there is some Mealy automaton recognizing the relation.*

Theorem 3. *The orbit relation of a 1TT is rational.*

A Small CCC

Definition 4. *A Cycle-Cum-Chord automaton (CCC) has state set $\{0, 1, \ldots n-1\}$ and transitions $p^{a/a} \to p-1$, $0^{1/0} \to m-1$, $0^{0/1} \to n-1$, where $1 \le m \le n$. We write A_m^n for this transducer.*

The leftmost diagram on this poster is A_2^3.

Theorem 4. *Orbit checking for A_2^3 can be done in polynomial time.*

Theorem 5. *The orbit relation for A_2^3 is rational.*

Theorem 6. *$\mathcal{S}(A_2^3)$ is already a group, ismorphic to $\mathbb{Z}^2$.*

Proof. Here's a first step: We claim that $\underline{0}^2\underline{1}^1\underline{2} = I$. Fix some input string s. We claim each bit is flipped exactly twice.

If c_i is the number of times bit i is flipped, we have the recurrence

$$\begin{aligned} c_i = &\lfloor (c_{i-3}/2) \rfloor + (c_{i-3} \mod 2) \cdot (1 - s_{i-3}) \\ &+ \lfloor (c_{i-2}/2) \rfloor + (c_{i-2} \mod 2) \cdot s_{i-2} \end{aligned}$$

The claim holds for the first two bits trivially, the third is flipped once by $\underline{0}$ and once by $\underline{2}$. Then induct across s.

So we have $\mathcal{S}(A_2^3)$ is already a group (as $\underline{0}^{-1} = \underline{01}^2\underline{2}$ and so on).

Further, since $\underline{2}$ is expressible in terms of $\underline{0}$ and $\underline{1}$, we have that $\mathcal{S}(A_2^3) = \{\underline{0}^i\underline{1}^j \mid i, j \in \mathbb{Z}\}$, giving us a concise data structure to represent elements of $\mathcal{S}(A_2^3)$.

It takes a bit of work to show no other such identities exist. □

Cycle-Cum-Chord Transducers

Theorem 7. *Orbit checking for A_m^n can be done in polynomial time.*

Question 1. *For which n, m is the orbit relation of A_m^n rational?*

Theorem 8. *$\mathcal{S}(A_m^n)$ is already a group, ismorphic to $\mathbb{Z}^{n-gcd(n,m)}$.*

Acknowledgements

Thanks to Klaus Sutner for his guidance and to Tim Becker for his continued interest in the project.