Journal of Automata, Languages and Combinatorics **u** (v) w, x–y

ITERATING INVERSE BINARY TRANSDUCERS

Klaus Sutner
Computer Science Department, Carnegie Mellon University
Pittsburgh, PA 15213, USA
e-mail: sutner@cs.cmu.edu

and

Kevin Lewi
Computer Science Department, Stanford University
Stanford, CA 94305, USA[1]
e-mail: klewi@cs.stanford.edu

ABSTRACT

We study iterated transductions defined by a class of inverse transducers over the binary alphabet. The transduction semigroups of these automata turn out to be free Abelian groups and the orbits of finite words can be described as affine subspaces in a suitable geometry defined by the generators of these groups. We show that iterated transductions are rational for a subclass of our automata.

Keywords: Inverse transducers, transduction group, iteration, rationality.

1. Motivation

An *inverse transducer* is a type of Mealy automaton where all transitions are of the form $p \xrightarrow{a/\pi_p(a)} q$; here π_p is a permutation of the alphabet depending on the source state p. We only consider $\mathbf{2} = \{0, 1\}$ as input and output alphabet. Selecting an arbitrary state p as the initial state, we obtain a transduction $\mathcal{A}(p)$ from $\mathbf{2}^*$ to $\mathbf{2}^*$. These transductions can be viewed as automorphisms of the complete binary tree $\mathbf{2}^*$ and the collection of all transductions generates a subsemigroup $\mathcal{S}(\mathcal{A})$ of the full automorphism group $\mathsf{Aut}(\mathbf{2}^*)$. Similarly one can associate a group $\mathcal{G}(\mathcal{A})$ with $\mathcal{A}$ by including the inverses of all transductions. These groups are called *automata groups* or *self-similar groups* and have been studied in great detail in group theory and symbolic dynamics, see [11, 17] for extensive pointers to the literature. Automata groups have many interesting properties and have lead to elegant solutions to several outstanding problems. For example, Grigorchuk's well-known example of a group of intermediate growth has a description in terms of a 5-state inverse transducer.

[1] This work was done at Carnegie Mellon University.

Automata groups should not be confused with *automatic groups* as introduced in [7] or *automatic structures*, see [13, 15]. The former are characterized by the group operations being described directly by finite state machines operating on words over the generators; the latter are relational first-order structures where the carrier set and right-multiplication by generators is by finite state machines.

We are here interested in both connections between automata theory and group theory as discussed in [2]. More precisely, we study the effect of iteration on transductions: given a transduction $f \in \mathcal{S}(\mathcal{A})$, write $f^* \subseteq \mathbf{2}^* \times \mathbf{2}^*$ for the binary relation obtained by iterating f. Note that f^* is a length-preserving equivalence relation on $\mathbf{2}^*$. While the first-order structure $\langle\, \mathbf{2}^*, f \,\rangle$ is clearly automatic and thus has decidable first-order theory, it is difficult to determine when $\langle\, \mathbf{2}^*, f, f^* \,\rangle$ is automatic. We introduce a class of inverse transducers called *cycle-cum-chord (CCC)* transducers in section 2 and characterize their transduction semigroups as free Abelian groups. Moreover, for some CCC transducers the orbit relations f^* turn out to be automatic for all transductions f in the semigroup. Since f^* is length-preserving, it follows from a result by Elgot and Mezei, [6] that this is equivalent to f being rational. To show that f^* is automatic we construct a canonical transition system, which turns out to be finite for some of the automata under consideration. This scenario is somewhat similar to the discussion of digital circuits computing functions on the dyadic numbers in [24]; note that we are dealing with relations rather than functions, though.

The construction of the transition system is based on a normal form for transductions proposed by Knuth [16] that allows one to show that $\mathcal{S}(\mathcal{A})$ is in fact a free Abelian group. The normal form is also useful to define a natural geometry on $\mathbf{2}^*$ that describes the orbits of words under f as affine subspaces. As a consequence, it is polynomial-time decidable whether two transductions give rise to the same equivalence relation and we can in fact construct the minimal transition system for f^* in the sense of Eilenberg [5]. In addition, we obtain fast algorithms to compute $x\, f^t$, to test whether two words belong to the same orbit under f and the calculate coordinates in the geometry introduced below.

This paper is organized as follows. In section 2 we introduce inverse transducers and define cycle-cum-chord transducers. We also show how to construct the canonical transition system that tests orbit equivalence. In the next section, we discuss Knuth normal form, characterizes the transduction semigroups of CCC transducers and determine the rationality of orbits of some of these machines. Section 4 contains comments on related decision problems and mentions open problems.

2. Inverse Transducers

2.1. Transduction Semigroups

We consider Mealy machines of the form $\mathcal{A} = \langle\, Q, \mathbf{2}, \delta, \lambda \,\rangle$ where Q is a finite set, $\mathbf{2} = \{0, 1\}$ is the input and output alphabet, $\delta : Q \times \mathbf{2} \to Q$ the transition function and $\lambda : Q \times \mathbf{2} \to \mathbf{2}$ the output function. We can think of $\mathbf{2}^*$ as acting on Q via δ, see [3, 20, 14] for background. We are here only interested in *inverse transducers* where $\lambda(p, .) : \mathbf{2} \to \mathbf{2}$ is a permutation for each state p. When this permutation is

the transposition in the symmetric group $\mathfrak{S}_2$ on two letters, we refer to p as a *toggle state* and as a *copy state*, otherwise. Fixing a state p as initial state, we obtain a transduction $\mathcal{A}(p) : \mathbf{2}^* \to \mathbf{2}^*$ that is easily seen to be a length-preserving permutation. If the automaton is clear from context we write $\underline{p}$ for this function; $\mathcal{S}(\mathcal{A})$ denotes the semigroup and $\mathcal{G}(\mathcal{A})$ denotes the group generated by all these functions.

If we think of $\mathbf{2}^*$ as an infinite, complete binary tree in the spirit of [21], we can interpret our transductions as automorphisms of this tree, see [17, 22]. Clearly any automorphism f of $\mathbf{2}^*$ can be written in the form $f = (f_0, f_1)s$ where $s \in \mathfrak{S}_2$: s describes the action of f on $\mathbf{2}$, and f_0 and f_1 are the automorphisms induced by f on the two subtrees of the root. Write σ for the transposition in $\mathfrak{S}_2$. The automorphisms f such that $f = (f_0, f_1)\sigma$ are *odd*, the others *even*. Needless to say, $\mathcal{A}(p)$ is odd whenever p is a toggle state and even, otherwise. The whole automorphism group can be described in terms of wreath products thus:

$$\mathsf{Aut}(\mathbf{2}^*) \simeq \mathsf{Aut}(\mathbf{2}^*) \wr \mathfrak{S}_2 = (\mathsf{Aut}(\mathbf{2}^*) \times \mathsf{Aut}(\mathbf{2}^*)) \rtimes \mathfrak{S}_2$$

The components f_i arise naturally as the *left residuals* of f, first introduced by Raney [19]. It was shown by Gluškov that the residuals of a sequential map are sufficient to construct a corresponding Mealy automaton, see [8] and [17]. More precisely, for any word x, define the function $\partial_x f$ by $(x\, f)\,(z\, \partial_x f) = (xz)\, f$ for all words z (for transductions, we write function application on the right and use diagrammatic composition for consistency with relational composition). It follows that

$$\begin{aligned} \partial_{xy} f &= \partial_y \partial_x f, \\ \partial_x f g &= \partial_x f \, \partial_{x\, f} g. \end{aligned}$$

The transduction semigroup $\mathcal{S}(\mathcal{A})$ is naturally closed under residuals. In fact, we can describe the behavior of all the transductions by a transition system $\mathcal{C}$, much the way $\mathcal{A}$ describes the basic transductions: the states are $\mathcal{S}(\mathcal{A})$ and the transitions are $f \xrightarrow{s/s\, f} \partial_s f$. Thus $\mathcal{C}$ contains $\mathcal{A}$ as a subautomaton. Of course, this system is infinite in general; it is referred to as the *complete automaton* in [17]. Also note that, in terms of residuals, the group operation in the wreath product has the form

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

This provides a convenient notation system for inverse transducers. For example, again writing σ for the transposition in $\mathfrak{S}_2$, $\alpha = (I, \alpha)\,\sigma$ and $I = (I, I)$ specifies an automaton $\mathcal{A}$ known as the "adding machine," see figure 1 and [17]. The transduction semigroup generated by $\mathcal{A}$ is isomorphic to $\mathbb{N}$, and the group is isomorphic to $\mathbb{Z}$. If we think of automorphism α as a map on $\mathbb{Z}_2$, the ring of dyadic numbers, as in [24], we have $x\,\alpha = x + 1$ and the orbit of 0^ω under α is dense in $\mathbb{Z}_2$.

2.2. Orbit Equivalence and Orbit Trees

Iterating an automorphism f of $\mathbf{2}^*$ we obtain an equivalence relation f^*, the *orbit relation* or *orbit equivalence* of f, in symbols $\equiv_f$. The group $\mathsf{Aut}(\mathbf{2}^*)$ naturally acts

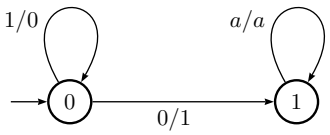


Figure 1: The adding machine over the alphabet **2**.

on $\mathbf{2}^*$, so we can think of the partition induced by orbit equivalence as given by the subgroup generated by f acting on $\mathbf{2}^*$. Since all orbits are finite we could also consider the semigroup generated by f. The classes of $\equiv_f$ saturate the level sets $\mathbf{2}^n$ and their sizes are tightly constrained, as shown in the next proposition. Suppose $u_0, u_1, \ldots, u_{n-1}$ is the length n orbit of $u = u_0$ under f. If f^n is the identity on the extended word $u0$ then we obtain two disjoint cycles $u_0 0, u_1 b_1, \ldots, u_{n-1} b_{n-1}$ and $u_0 1, u_1 \overline{b_1}, \ldots, u_{n-1} \overline{b_{n-1}}$ under f. Otherwise there is a single cycle of the form $u_0 0, \ldots, u_{n-1} b_{n-1}, u_0 1, \ldots, u_{n-1} \overline{b_{n-1}}$. We will say that u *splits* or *doubles* under f, correspondingly.

Proposition 1 *Let f be an automorphism and u an arbitrary word, write n for the length of the orbit of u under f. Then either the orbits of $u0$ and $u1$ under f are disjoint and have length n, or they are identical (up to a shift) and have length $2n$.*

Hence, any orbit has length 2^k for some $k \geq 0$ and it follows that for any odd integer r the maps f and f^r generate the same orbits. To describe transductions acting on the infinite binary tree $\mathbf{2}^*$ it is natural to consider the *orbit tree* of f, the quotient structure induced on $\mathbf{2}^*$ by orbit equivalence. It is easy to see that the quotient is another infinite tree which we denote $\mathfrak{T}_f$. The *root* of an orbit is the lexicographically least element of the orbit, which we denote $\mathsf{root}(u)$ for any element u of the orbit; this corresponds to the first canonical form in [12]. Note that the root function is length-preserving and prefix-preserving: $\mathsf{root}(x) \sqsubseteq \mathsf{root}(xy)$ for all words x and y. For our purposes it is convenient to think of the nodes of the orbit tree as being the roots of the corresponding orbits. We refer to the collection of all roots as the *root language* of f. Thus, a node u in $\mathfrak{T}_f$ either has a single successor $u0$ or two successors $u0$ and $u1$. We call a tree *homogeneous* if all nodes at the same level have the same out-degree. Note that a homogeneous orbit tree is characterized uniquely by the sequence of these out-degrees. For example, the orbit tree of the adding machine has degree sequence 1^ω. We call a tree *regular* if it has only finitely many subtrees, up to isomorphism.

Lemma 2 *Let f be an automorphism. Then the orbit tree $\mathfrak{T}_f$ of f is regular if, and only if, the root language of f is regular.*

Proof. First assume the orbit tree is regular. If the tree is the full infinite binary tree the root language is $\mathbf{2}^*$ and we are done. Otherwise we construct a DFA for the root

language as follows. Let Q be the set of subtrees, up to isomorphism, augmented by a sink $\perp$ and define a transition function on Q as follows. If p has two direct subtrees q_0 and q_1 in this order, introduce transitions $\delta(p, i) = q_i$. If there is only one direct subtree q let $\delta(p, 0) = q$ and $\delta(p, 1) = \perp$. The initial state is the whole orbit tree and all states other than the sink are final.

Now suppose the root language R is regular. As in the preceding argument we may assume that $R \neq \mathbf{2}^*$, so the minimal automaton for R is a sink automaton. Clearly R is prefix-closed and a root x is doubling iff $x1 \notin R$. But then the number of subtrees is just the number of left quotients of R minus 1, corresponding to the non-sink states in the minimal DFA for R. □

Lemma 3 *Let f be an automorphism. Then the root function of f is rational if, and only if, the orbit relation of f is rational.*

Proof. Since the orbit relation is none other than the relational composition of root and the converse root^{-1}, rationality of the root function implies rationality of the orbit relation. For the opposite direction note that root is the standard length-lex uniformization of the orbit relation, see [1] and [12]. □

For example, the orbit tree of the map associated with state 0 in the inverse transducer in figure 4 has the form shown in figure 2. The tree is homogeneous and 3-regular with type $(122)^\omega$.

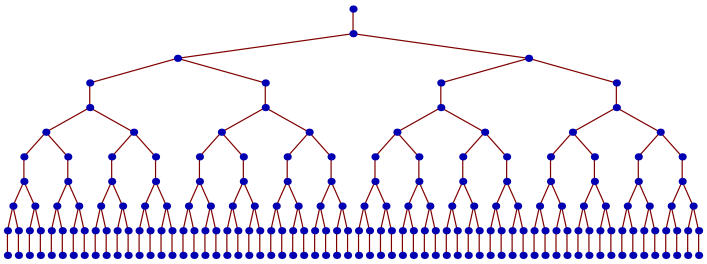


Figure 2: The orbit tree of an automorphism defined by an inverse transducer.

The last two lemmata also immediately imply the following.

Lemma 4 *Any automorphism with a rational orbit relation has a regular orbit tree.*

Unsurprisingly, the converse is false. For example, one can show that transduction $\underline{0}$ in the cycle-cum-chord transducer $\mathcal{A}_3^4$ fails to have rational orbit relation, see section 2.4 for definitions and section 4 for a more detailed description. Yet the orbit tree of $\underline{0}$ is isomorphic to the the tree in figure 2.

2.3. The Orbit Automaton

For a general "automaton mapping" it is shown in [8] how to construct the *free automaton*, a Moore automaton that represents the mapping. The free automaton is infinite and it is pointed out in the reference that for specific maps better constructions exist, in particular when the map is given by a finite state machine. We will now show how to construct a transition system that recognizes the orbit relation of an automorphism and is finite precisely when the orbit relation is rational.

Suppose R is a length-preserving binary relation on $\mathbf{2}^*$. We can define an associated language

$$\mathcal{L}(R) = \{\, x{:}y \mid x\ R\ y \,\} \subseteq (\mathbf{2} \times \mathbf{2})^*.$$

where the *convolution* $x{:}y$ of two words $x, y \in \mathbf{2}^k$ is defined by

$$x{:}y = \begin{array}{|c|c|c|c|}\hline x_1 & x_2 & \ldots & x_k \\ \hline y_1 & y_2 & \ldots & y_k \\ \hline \end{array} \in (\mathbf{2} \times \mathbf{2})^k$$

(since R is length-preserving there is no need for a padding symbol as in [15]). Clearly, the relation R is rational if, and only if, the language $\mathcal{L}(R)$ is regular. Following Brzozowski [4], the latter condition is equivalent to $\mathcal{L}(R)$ having only finitely many *left quotients*. In this case, the quotients take the form

$$(a{:}b)^{-1}\, R = \{\, x{:}y \in (\mathbf{2} \times \mathbf{2})^* \mid ax{:}by \in R \,\}$$

The map $u \mapsto u^{-1}\, R$ defines an equivalence relation ρ on $(\mathbf{2} \times \mathbf{2})^*$ that is easily seen to be the coarsest right congruence that saturates R. Hence we can construct a minimal deterministic recognizer for $\mathcal{L}(R)$ by using the set of all quotients as the state set.

If we think of a transduction $\underline{p}$ as a binary relation, then this relation is recognized by the transducer, interpreted as a standard acceptor over the alphabet $\mathbf{2} \times \mathbf{2}$ and with p as the initial state. The relations we are interested in here are the orbit relations of automorphisms represented by an inverse transducer. To describe the orbit relation in terms of Brzozowski [4] style quotients we need to generalize slightly. Given two automorphisms $f, g : \mathbf{2}^* \to \mathbf{2}^*$ define the *orbit of u under f with translation g* to be $u\, f^* g = \{\, u\, f^i g \mid i \geq 0 \,\}$. For clarity we will sometimes write $\mathsf{orb}(u; f, g)$. Correspondingly, the relation $\mathbf{R}(f, g)$ holds on u and v if $v \in \mathsf{orb}(u; f, g)$. Note that $\mathbf{R}(f, I)$ is simply the orbit relation of f. In general, $\mathbf{R}(f, g)$ fails to be an equivalence relation (and even to be reflexive), but, as we will show in the following lemma, orbits with translation are closed under quotients.

Lemma 5 *Quotient Lemma*

Let f and h be two automorphisms and set $b = a\, h$. For $f = (f_0, f_1)$ we have

$$(a{:}b)^{-1}\, \mathbf{R}(f, h) = \mathbf{R}(f_a, h_a)$$

Otherwise, for $f = (f_0, f_1)\, \sigma$, we have

$$(a{:}b)^{-1}\, \mathbf{R}(f, h) = \mathbf{R}(f_a f_{\overline{a}}, h_a)$$
$$(a{:}\overline{b})^{-1}\, \mathbf{R}(f, h) = \mathbf{R}(f_a f_{\overline{a}}, f_a h_{\overline{a}})$$

All other quotients are empty.

Proof. First assume f is even. Then $\mathsf{orb}(au; f, I) = a\,\mathsf{orb}(u; f_a, I)$ and our claim follows by applying the translation g:

$$\begin{aligned}\mathsf{orb}(au; f, g) &= (a\,\mathsf{orb}(u; f_a, I))g \\ &= b\,(\mathsf{orb}(u; f_a, I))g_a \\ &= b\,\mathsf{orb}(u; f_a, g_a)\end{aligned}$$

For $f = (f_0, f_1)\,\sigma$ we have $f^2 = (f_0 f_1, f_1 f_0)$. It now follows that

$$\mathsf{orb}(au; f, I) = a\,\mathsf{orb}(u; f_a f_{\overline{a}}, I) \cup\ \overline{a}\,\mathsf{orb}(u; f_a f_{\overline{a}}, f_a)$$

Our claim follows by applying g to this equation. □

Given an automorphism F and the corresponding orbit relation F^*, the lemma determines the collection of all quotients. Thus we obtain a transition system $\mathcal{M}_F$ over alphabet $\mathbf{2} \times \mathbf{2}$ with transitions

$$\mathbf{R}(f, g) \xrightarrow{a:b} (a{:}b)^{-1}\,\mathbf{R}(f, g).$$

In this case, all non-empty quotients are final and the behavior of a state $\mathbf{R}(f, g)$ in $\mathcal{M}$ is none other than

$$\{\, x{:}y \mid y \in \mathsf{orb}(x; f, g) \,\}.$$

Thus F^* is rational if, and only if, $\mathcal{M}_F$ is finite, in which case we will refer to $\mathcal{M}_F$ as the *orbit automaton* for F.

As a step towards implementation, suppose the original automorphism F lies in the transduction semigroup of some inverse transducer $\mathcal{A}$. Since all the functions that occur in the quotients of F are compositions of residuals of F, they also lie in the transduction semigroup $\mathcal{S}(\mathcal{A})$. This leads to a simple representation system: quotient $\mathbf{R}(f, g)$ can be represented by a pair $(\boldsymbol{p}, \boldsymbol{q})$ of state vectors in $\mathcal{A}$. In this context we refer to the pair (f, g) as a *star pair*, f as its *star part* and g as its *translation part*. Residuals on state vectors $\boldsymbol{p}$ and $\boldsymbol{q}$ can be computed via

$$\partial_a \boldsymbol{p} = \boldsymbol{q} \iff \exists\, a_i \in \mathbf{2}\,(a = a_1 \wedge q_i = p_i \cdot a_i \wedge a_{i+1} = p_i * a_i)$$

Here we have written $p \cdot a = q$ for the transition function and $p * a = b$ for the output function, for $p, q \in Q$ and $a, b \in \mathbf{2}$. Note that multiple state vectors can represent the same transduction; however, there is a simple algorithm to test for equivalence in this sense: we can compute the compound transducer and minimize it as a deterministic machine over $\mathbf{2} \times \mathbf{2}$. In fact we will see that the transducers introduced in section 2.4 admit a simple normal form.

Of course, there is another problem to contend with: different transductions may have the same orbit relation. Let us say that two automorphisms are *orbit equivalent* if they induce the same orbit relation. Likewise, two star pairs (f, g) and (f', g') are *orbit equivalent* if $\mathbf{R}(f, g) = \mathbf{R}(f', g')$; correspondingly we write $f \approx f'$ or $(f, g) \approx (f', g')$ for orbit equivalence. Thus, the automorphism f and g are orbit equivalent if the star pairs (f, I) and (g, I) are orbit equivalent. Multiple star pairs can represent the same generalized orbit. In particular, since cycle lengths are always powers of 2 for inverse binary transducers, we have the following proposition.

Proposition 6 *Let f and h be automorphisms. Then for any odd r and any integer s: $f \approx f^r$ and $(f,h) \approx (f^r, f^s h)$.*

Of course, in general $\mathcal{M}_f$ will be infinite. For some automorphisms given by an inverse transducer, $\mathcal{M}_f$ turns out to be finite, so that the orbit relation of f is rational. One well-known example are the so-called "sausage automata" $\mathcal{A}_n$ in [17], generalizations of the adding machine from above. In wreath notation they are given by

$$\underline{0} = (\underline{0}, \underline{0}) \qquad \underline{1} = (\underline{n}, 0)\,\sigma \qquad \underline{k} = (\underline{k-1}, \underline{k-1}), \quad 2 \le k \le n.$$

Figure 3 shows $\mathcal{A}_5$. The orbit tree of transduction $\underline{0}$ in $\mathcal{A}_5$ is homogeneous with type $(12222)^\omega$.

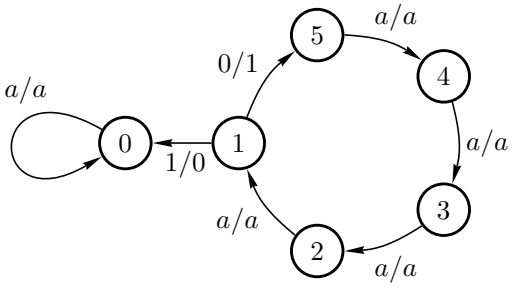


Figure 3: The "sausage automaton" $\mathcal{A}_5$, an inverse transducer that generates $\mathbb{Z}^5$.

The group generated by $\mathcal{A}_n$ is $\mathbb{Z}^n$ and the basic transductions are given by a combination of the successor function of the adding machine and a polyadic version of perfect shuffle. Let $x^i \in \mathbf{2}^r$, $1 \le i \le n$, and $1 \le k \le n$. Then

$$\mathsf{shf}(x^1, x^2, \ldots, x^n)\,\underline{k} = \mathsf{shf}(x^1, \ldots, x^k\alpha, \ldots, x^n)$$

Here α is again the successor operation defined by the adding machine from section 2.1 and shf is the natural generalization of binary perfect shuffle to a variable number of arguments of the same length:

$$\mathsf{shf}(x^1, x^2, \ldots, x^s) = x_1^1 x_1^2 \ldots x_1^s\, x_2^1 x_2^2 \ldots x_2^s \;\ldots\; x_r^1 x_r^2 \ldots x_r^s.$$

It follows that any transduction f in $\mathcal{S}(\mathcal{A}_n)$ can be written as

$$\mathsf{shf}(x^1, x^2, \ldots, x^n)\, f = \mathsf{shf}(x^1\alpha^{e_1}, \ldots, x^n\alpha^{e_n})$$

Accordingly, it is not hard to see that for any transduction f in $\mathcal{S}(\mathcal{A}_n)$ the orbit relation $\equiv_f$ is automatic. However, see lemma 18 for a slightly more complicated situation in the context of cycle-cum-chord transducers.

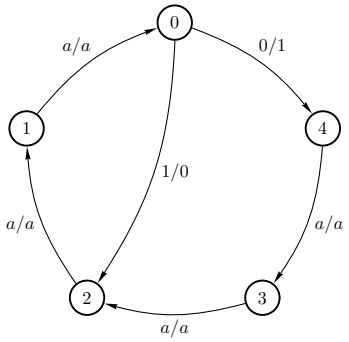
2.4. Cycle-cum-Chord Transducers

We now introduce a simple class of inverse transducers whose associated semigroups will turn out to be free Abelian groups. Unlike with the sausage automata from above,

the orbits of words under the corresponding transductions can be fairly complicated. A *cycle-cum-chord (CCC)* transducer has state set $\{0, 1, \ldots, n-1\}$ and transitions

$$p \xrightarrow{a/a} p-1, \quad p>0 \qquad \text{and} \qquad 0 \xrightarrow{0/1} n-1, \quad 0 \xrightarrow{1/0} m-1$$

where $1 \le m \le n$. We will write $\mathcal{A}_m^n$ for this transducer. The diagram of $\mathcal{A}_3^5$ is shown in figure 4. The source node of the chord is the sole toggle state in these transducers. As we will see shortly, $\mathcal{S}(\mathcal{A}_m^n) = \mathcal{G}(\mathcal{A}_m^n)$.



$$\underline{0} = (\underline{4}, \underline{2})\,\sigma$$
$$\underline{k} = (\underline{k-1}, \underline{k-1}) \quad 0 < k < 5$$

Figure 4: The cycle-cum-chord transducer $\mathcal{A}_3^5$, an inverse transducer on 5 states with one toggle state.

Using wreath representations it is easy to verify algebraically that $\mathcal{S}(\mathcal{A}_m^n)$ is an Abelian group. More precisely, we can establish the following two lemmata.

Lemma 7 *The transduction semigroup of $\mathcal{A}_m^n$ is Abelian.*

Proof. Using wreath representations we have

$$\underline{0}\,\underline{i} = (\underline{n-1}, \underline{m-1})\,\sigma\,(\underline{i-1}, \underline{i-1}) = (\underline{n-1}\,\underline{i-1}, \underline{m-1}\,\underline{i-1})\,\sigma$$
$$\underline{i}\,\underline{0} = (\underline{i-1}, \underline{i-1})\,(\underline{n-1}, \underline{m-1})\,\sigma = (\underline{i-1}\,\underline{n-1}, \underline{i-1}\,\underline{m-1})\,\sigma$$

and likewise for all other pairwise products not involving $\underline{0}$. Done by induction. □

Lemma 8 *Cancellation Identities*
Consider $\mathcal{A}_m^n$ where $1 \le m \le n$ and let $s = \gcd(n, m)$, $r = m/s$. Then the following identities hold in the transduction semigroup of $\mathcal{A}_m^n$, for $0 \le i < s$:

$$\underline{i}^2\,\underline{s+i}^2 \ldots \underline{(r-1)s+i}^2\,\underline{m+i}\,\underline{m+s+i} \ldots \underline{n-s+i} = I$$

As a consequence, the transduction semigroup $\mathcal{S}(\mathcal{A}_m^n)$ is already a group.

Proof. Write g_i for the left-hand side of these identities, $0 \le i < s$. It is easy to see that for $0 < i$ the wreath form of g_i is (g_{i-1}, g_{i-1}). Furthermore,

$g_0 = \underline{0}^2\,\underline{s}^2 \ldots \underline{(r{-}1)s}^2\ \underline{m}\,\underline{m+s} \ldots \underline{n-s}$ and it follows that $g_0 = (g_{s-1}, g_{s-1})$. Simultaneous induction finishes the argument. □

Note that for $n = m$ we have the identities $\underline{k}^2 = I$ for $0 \leq k < n$. Hence $\mathcal{S}(\mathcal{A}_n^n)$ is finite and isomorphic to the Boolean group $\mathbf{2}^n$.

3. Orbit Rationality

3.1. Knuth Normal Form

According to the preceding remark we can safely ignore the case $n = m$ and assume that $m < n$. From the two lemmata it follows that $\mathcal{S}(\mathcal{A}_m^n) = \mathcal{G}(\mathcal{A}_m^n)$ is a quotient of $\mathbb{Z}^{n-s}$. To show that the transduction group is in fact isomorphic to $\mathbb{Z}^{n-s}$ we use a method suggested by D. Knuth [16]: since $\underline{0}^2\underline{m}^{-1} = (\underline{n{-}1}, \underline{n{-}1})$ we can add a new copy state n to the transducer with both transitions leading to state $n-1$, without changing the semigroup. By repeating this extension step, we can enlarge the state set to all of $\mathbb{N}$ where for all $i > 0$ we have $\underline{i} = (\underline{i{-}1}, \underline{i{-}1})$. We write $\mathcal{K}_m^n$ for the new transducer.

Lemma 9 *Shift Identities*
In the transduction semigroup of $\mathcal{K}_m^n$, $m < n$, we have, for all $k \geq 0$, the identities

$$\underline{k}^2 = \underline{k+m}\ \underline{k+n}$$

Proof. Since $\underline{0}^2\underline{m}^{-1} = (\underline{n{-}1}, \underline{n{-}1})$ the case $k = 0$ holds by our definition of state n. By induction, $\underline{k+1}^2\,\underline{m+k+1}^{-1} = (\underline{k}^2, \underline{k}^2)(\underline{m+k}^{-1}, \underline{m+k}^{-1}) = (\underline{n+k}, \underline{n+k})$, so we can add a new copy state $n+k+1$ with transitions to $n+k$, without changing the semigroup. □

According to our definition of $\mathcal{K}_m^n$ we have for all $k \geq 0$

$$x\,\underline{k} = \begin{cases} x & \text{if } |x| \leq k, \\ x_1 \ldots x_k\,(x_{k+1} \ldots x_\ell)\,\underline{0} & \text{otherwise.} \end{cases}$$

for any word x.

Write shift_k for the natural shift-by-k operation that replaces a term $\underline{i}$ by $\underline{i+k}$. More precisely, in the Knuth extension we can consider a term $f = \underline{k_1}^{e_1}\,\underline{k_2}^{e_2} \ldots \underline{k_r}^{e_r}$ where $0 \leq k_1 < k_2 < \ldots < k_r$ and $e_i \geq 1$. Then $\mathrm{shift}_k(f) = \underline{k_1+k}^{e_1}\,\underline{k_2+k}^{e_2} \ldots \underline{k_r+k}^{e_r}$ for any $k \geq -k_1$. Observe that any identity $f = I$ is then equivalent to $\mathrm{shift}_k(f) = I$. If we select $k = -k_1$ we obtain a normal form: $\underline{0}^{e_1}\,\underline{k_2-k_1}^{e_2} \ldots \underline{k_r-k_1}^{e_r} = I$. For example, the cancellation identities from lemma 8 are all shifts of the basic identity

$$\underline{0}^2\,\underline{s}^2 \ldots \underline{(r{-}1)s}^2\ \underline{m}\,\underline{m+s} \ldots \underline{n-s} = I$$

In a similar fashion it follows that the cancellation identities generalize to all transductions in $\mathcal{K}_m^n$.

Of particular interest is the case where $e_i = 1$ for all i; we will refer to this flat representation $f = \underline{k_1}\,\underline{k_2} \ldots \underline{k_r}$ as the *Knuth normal form (KNF)* of f; we allow $r = 0$ for the identity map. To generate the KNF of f we interpret the identities from lemma 9 as rewrite rules. For example, in $\mathcal{K}_2^3$ we have the shift rule $\underline{k}^2 \to \underline{k+2}\,\underline{k+3}$. Alas, application of the shift rule alone can lead to infinite loops as in $\underline{0}^2\ \underline{1}^2\ \underline{2} \to \underline{1}^2\ \underline{2}^2\ \underline{3} \to \underline{2}^2\ \underline{3}^2\ \underline{4} \to \ldots$ However, in this case, a single application of the cancellation identity from lemma 8 immediately terminates the process. Thus, the rewrite system is weakly terminating.

Theorem 10 *Knuth Normal Form*
Every transduction over $\mathcal{A}_m^n$ has a unique Knuth normal form.

Proof. For $n = m$ the cancellation identities have the form $\underline{k}^2 = I$ and it follows immediately that every transduction can be written uniquely in the required form. So assume $m < n$. For any transduction f in $\mathcal{S}(\mathcal{A}_m^n)$ consider the standard semigroup representation

$$f = \underline{k_1}^{e_{k_1}}\ \underline{k_2}^{e_{k_2}}\ \ldots \underline{k_r}^{e_{k_r}}$$

where $e_{k_i} \geq 1$ and $0 \leq k_i < k_{i+1} < n$. If all exponents are equal 1, or if $r = 0$, we are done. Otherwise rewrite the expression as follows. First, apply cancellation according to the identities from lemma 8 in the leftmost place possible. If none of these identities apply, use the shift rule derived from lemma 9, again in the leftmost possible position. Thus we obtain a sequence of expressions (f_i) with $f_0 = f$ that all denote f. We claim that the sequence is finite and thus ends in the desired flat representation.

Define the *weight* of f to be $\sum e_i$. Note that the shift rule preserves weight whereas a reduction reduces weight. Suppose for the sake of a contradiction that our rewrite process continues indefinitely for some initial f. Since weights are non-negative we may safely assume that the weight remains constant. Thus, no reductions apply and we only use shift rules. For the sake of simplicity let us assume that $s = \gcd(n, m) = 1$ so there is only a single reduction to deal with. The general argument is more tedious but entirely similar.

Observe that there must be a minimal critical index c such that $e_c > 1$. Define the *essential weight* of the expression as the sum $\sum_{i \geq c} e_i$. Again we may assume that the essential weight of the expression is non-decreasing. Hence e_c must always be even and the shift operation adds $e_c/2$ to e_{c+m} and e_{c+n}. But then, after a sufficiently large number of steps, there will be a critical block of exponents $e_c, e_{c+1}, \ldots, e_{c+n-1}$ with the property that $e_i \leq 1$ for $i < c$ and $e_i = 0$ for $i \geq c + n$; c increases by 1 at each step. Since e_c is even we are essentially operating on an n-tuple of natural numbers:

$$(a_0, \ldots, a_{n-1}) \mapsto (a_1, a_2, \ldots, a_m + a_0/2, \ldots, a_{n-1}, a_0/2)$$

We may safely assume a_0 to be positive. Since n and m are coprime all entries in the vector will be positive after at most $m(n-1)+1$ steps. But note that the first $m-1$ entries in the vector must then all be even and positive. Hence we can apply cancellation and we have the desired contradiction.

Now suppose that f has two KNFs, say, $f = \underline{k_1}\,\underline{k_2}\ldots\underline{k_r}$ and $f = \underline{\ell_1}\,\underline{\ell_2}\ldots\underline{\ell_s}$. Assume for the sake of a contradiction that $k_1 < \ell_1$. Then for any word x of length k_1 we have $xa\,f = x\overline{a}$ according to the first description, but $xa\,f = xa$ according to the second. By a symmetric argument, $k_1 = \ell_1$. Proceeding by induction we find $r = s$ and $k_i = \ell_i$, as required. □

We will write $\mathsf{KNF}(f)$ for the Knuth normal form of a transduction in $\mathcal{G}(\mathcal{A}_m^n)$, $\mathsf{KNF}_{\leq k}(f)$ for the first k terms in $\mathsf{KNF}(f)$ and $\mathsf{KNF}_1(f)$ for the first term (assuming $f \neq I$). Note that $\mathsf{KNF}(\underline{k}) = \mathrm{shift}_k(\mathsf{KNF}(\underline{0}))$ where shift_k is the shift-by-k operation from above. Orbit equivalence of two transductions f and g implies that $\mathsf{KNF}_1(f) = \mathsf{KNF}_1(g)$. It is easy to see that $\mathsf{KNF}_{\leq k}(f) = \mathsf{KNF}_{\leq k}(g)$ whenever $0^k\,f = 0^k\,g$. Hence $f = g$ if, and only if, $0^\omega\,f = 0^\omega\,g$.

We mention that a Knuth extension and Knuth normal form also exists for sausage automata, the shift identities here take the form $\underline{k}^2 = \underline{k+n}$. However, there are no cancellation identities, the semigroup is distinct from the group generated by these automata. At any rate, we can now pin down the structure of the transductions semigroups $\mathcal{S}(\mathcal{A}_m^n)$.

Corollary 11 *For $m < n$, the transduction semigroup of $\mathcal{A}_m^n$ is isomorphic to $\mathbb{Z}^{n-\gcd(n,m)}$.*

Proof. For $m < n$, by lemmata 7 and 8, we have that $\mathcal{S}(\mathcal{A}_m^n)$ must be a quotient of $\mathbb{Z}^{n-\gcd(n,m)}$. For simplicity assume that n and m are coprime and consider the group epimorphism $\Phi : \mathbb{Z}^{n-1} \to \mathcal{S}(\mathcal{A}_m^n)$. By the theorem, any element $\boldsymbol{e}$ in the kernel of Φ defines a transduction $f = \Phi(\boldsymbol{e})$ that has trivial KNF and whose reduction requires only the cancellation identities from lemma 8. But none of the identities apply to f, so f must in fact be the identity. Thus Φ is an isomorphism. □

The theorem also shows that for any ℓ the stabilizer Stab_x of $x \in \mathbf{2}^\ell$ is non-empty. In fact, there are transductions that fix every word of length ℓ, but have no fixed points among words of length $\ell+1$. Another important consequence is that the whole group acts transitively on all the level sets.

Corollary 12 *The transduction semigroup of $\mathcal{A}_m^n$ acts transitively on all the level sets $\mathbf{2}^\ell$, $\ell \geq 0$.*

Proof. By induction assume that $\mathcal{S}(\mathcal{A}_m^n)$ acts transitively on $\mathbf{2}^\ell$. Hence, given $u, v \in \mathbf{2}^\ell$ there is some transduction f such that $u\,f = v$. By the theorem there is a transduction h such that h is the identity on $\mathbf{2}^{\leq \ell}$ but h toggles the last bit in any word in $\mathbf{2}^{\ell+1}$. But then $ua\,f = vb$ and $ua\,fh = v\overline{b}$. □

It follows that the orbit of 0^ω under $\mathcal{S}(\mathcal{A}_m^n)$ is dense. We write $f =_\ell g$ if $x\,f = x\,g$ for all words $x \in \mathbf{2}^\ell$.

Corollary 13 *For any two transductions f and g of $\mathcal{A}_m^n$ we have $f =_\ell g$ if, and only if, $\mathsf{KNF}_{<\ell}(f) = \mathsf{KNF}_{<\ell}(g)$.*

Proof. Since the terms of the normal form of f outside of $\mathsf{KNF}_{<\ell}(f)$ all lie in the stabilizer of $\mathbf{2}^\ell$ the implication from right to left is immediate. For the opposite direction let ℓ be minimal such that $f =_\ell g$ but $\mathsf{KNF}_{<\ell}(f) \neq \mathsf{KNF}_{<\ell}(g)$, say, $\mathsf{KNF}_{<\ell-1}(f) = \alpha$ and $\mathsf{KNF}_{<\ell}(g) = \alpha\,\underline{\ell-1}$. But then $0^\ell f \neq 0^\ell g$, contradiction. □

3.2. Orbit Geometry

In this section we will show that the orbits of a cycle-cum-chord transducer have a simple geometric interpretation.

Lemma 14 *Let f be a transduction over a CCC transducer $\mathcal{A}_m^n$. Then the orbit tree of f is homogeneous and regular. More precisely, letting $\mathsf{KNF}_1(f) = \underline{r}$, the orbit tree of f doubles exactly at levels $r + m\mathbb{N}$ for $m < n$, and at level r for $n = m$.*

Proof. For $m = n$ the orbit of a word x has length 1 when $|x| \leq r$ and length 2 otherwise: letting $f = \underline{k_1}\,\underline{k_2} \ldots \underline{k_s}$ where $r = k_1$, $0 \leq k_i < k_{i+1} < n$, we can see that f toggles exactly the bits in positions $k_i + m\mathbb{N}$.

Assume $m < n$ and consider the case $r = 0$. Assume by induction that x is a word of length $\ell = km$ such that the f-orbit of x has length 2^k. Then $\mathsf{KNF}_1(f^{2^k}) = \underline{km}$ so that $xa\,f^{2^k} = x\overline{a}$. Similarly $xv\,f^{2^{k+1}} = xv$ for all $v \in \mathbf{2}^m$ and our claim follows. Lastly, for $r > 0$, note that f is the identity on all words up to length r and, for $x = uv$ where $|u| = r$, we have $x\,f = u(v\,g)$ where $g = \partial_u f$ and g is odd. □

It follows that the root language of $\mathcal{A}_m^n$ consists of all prefixes of

$$\bigcup_{x \in \mathbf{2}^r} x(0\mathbf{2}^{m-1})^*$$

for $m < n$ and $\bigcup_{x\in\mathbf{2}^r} x0\mathbf{2}^*$ for $m = n$.

For transducers of the form $\mathcal{A}_1^n$ it follows that $\underline{0}$ acts transitively on all level sets $\mathbf{2}^k$ of $\mathbf{2}^*$: all nodes in the orbit tree double. Hence, in $\mathcal{S}(\mathcal{A}_1^n)$ two transductions f and g are orbit equivalent if, and only if, $\mathsf{KNF}_1(f) = \mathsf{KNF}_1(g)$. The orbit tree of $\mathcal{A}_1^n$ coincides with that of the adding machine in figure 1: the tree degenerates into a one-way infinite path. However, the successor function computed by $\mathcal{A}_1^n$ is more complicated and we are not aware of a simple combinatorial description. The corresponding automorphisms are conjugate in the group of all automorphisms, see [10]. In the general case we also need m of the basic transductions to obtain a transitive action of the level sets.

Lemma 15 *For any CCC transducer $\mathcal{A}_m^n$ let H be the group of transductions generated by $\underline{i}$, $0 \leq i < m$. Then H acts transitively on the level sets $\mathbf{2}^\ell$. For $\ell = km$ the quotient group H' obtained by factoring with respect to $\underline{i}^{2^k}$ acts simply transitively on $\mathbf{2}^\ell$.*

Proof. Since our transductions are sequential it suffices to consider only levels $\ell = km$. Consider two words x and y of length ℓ. Suppose by induction that

$x\,f = y$ for some f in H and consider arbitrary bit sequences $a_0, \ldots, a_{m-1}$ and $b_0, \ldots, b_{m-1}$ of length m. Note that $xa_0\, f\underline{0}^{e_0} = yb_0$ for $e_0 = 0$ or $e_0 = 2^k$ according to the last lemma. Proceeding inductively we can find $e_i \in \{0, 2^k\}$ such that $xa_0 \ldots a_{m-1}\, f\underline{0}^{e_0} \ldots \underline{m{-}1}^{e_{m-1}} = yb_0 \ldots b_{m-1}$. Thus H also acts transitively on $\mathbf{2}^{(k+1)m}$, as required. Since the coefficients are uniquely determined modulo 2^{k+1}, the second claim also follows. □

3.3. Intrinsic Coordinates and Amenable Transducers

One important consequence of the last lemma is that it provides a natural coordinate system for the level set $\mathbf{2}^{km}$: for every $\ell = km$ there is a coordinate map, a bijection

$$\mathbf{2}^\ell \to \mathbb{Z}/(2^k) \times \ldots \times \mathbb{Z}/(2^k)$$

where the product on the right has m terms. We will write $\langle\, w \,\rangle_\ell \in (\mathbb{Z}/(2^k))^m$ for the coordinates of a word w: $\langle\, w \,\rangle_\ell = (a_0, \ldots, a_{m-1})$ if, and only if, $w = 0^\ell\, \underline{0}^{a_0}\, \underline{1}^{a_1} \ldots \underline{m{-}1}^{a_{m-1}}$. We use the notation $x \equiv y$ to express that two integer vectors of length m are componentwise congruent modulo 2^k. Also, for a transduction f, define the ℓ-coordinates of f by $\langle\, f \,\rangle_\ell = \langle\, 0^\ell\, f \,\rangle_\ell$. For example, in $\mathcal{A}_2^3$, letting $f = \underline{0}^{-1}\underline{1}^3$ we get $\langle\, f \,\rangle_{2k} = (2^k - 1, 3)$ for $k \geq 2$. By commutativity it follows that $\langle\, 0^\ell\, f^i \,\rangle_\ell \equiv i \cdot \langle\, f \,\rangle_\ell$ and $\langle\, 0^\ell\, f^* \,\rangle_\ell \equiv \mathbb{N} \cdot \langle\, f \,\rangle_\ell$, so that the orbit of 0^ℓ is a linear subspace of $(\mathbb{Z}/(2^k))^m$. Again by commutativity general orbits can be described as affine subspaces of $(\mathbb{Z}/(2^k))^m$:

$$\langle\, w\, f^* \,\rangle_\ell \equiv \langle\, w \,\rangle_\ell + \mathbb{N} \cdot \langle\, f \,\rangle_\ell$$

In fact, all these orbits are translations of the basic linear subspace $0^\ell\, f^*$. Since our transductions are sequential maps it suffices to consider only words of length $\ell = km$ where $k \geq 0$: two transductions f and g are orbit equivalent if they are orbit equivalent for words of length $\ell = km$. It follows from the coordinate representation of orbits that f and g are orbit equivalent for words of length ℓ if, and only if, for some odd integer $z = z_\ell$, possibly depending on ℓ, we have $\langle\, f \,\rangle_\ell \equiv z \cdot \langle\, g \,\rangle_\ell$. Thus, for fixed ℓ, simple modular arithmetic suffices to determine orbit equivalence, given the ℓ-coordinates of the two transductions.

To deal with the general case, recall that a sequence (a_i) of integers is *coherent* if $a_i = a_{i+1} \pmod{2^i}$. A sequence of vectors of integers is coherent if the corresponding component sequences are, see [9]. It is easy to check that the vector sequence $(\langle\, f \,\rangle_{km})_{k \geq 0}$ is coherent. Thus, the local coordinates $\langle\, w\, f \,\rangle_{km}$ define a vector $\langle\, f \,\rangle \in \mathbb{Z}_2^m$ of m dyadic numbers. For the example $f = \underline{0}^{-1}\underline{1}^3$ in $\mathcal{A}_2^3$ from above we get

$$\langle\, f \,\rangle = (0.1111\ldots, 0.11000\ldots) \in \mathbb{Z}_2^2$$

using the standard digit notation for $\mathbb{Z}_2$. Note, though, that for $\mathcal{A}_2^3$ the dimension of the coordinate system coincides with the number of generators of the transduction group; in general the situation is more complicated. Write $\nu_2(x)$ for the dyadic valuation of x in $\mathbb{Z}_2$ and similarly $\nu_2(\boldsymbol{x})$ for a vector $\boldsymbol{x}$ over $\mathbb{Z}_2$, see [9]. Then the projection

of $0^\ell f^*$ onto the ith component has cardinality $2^{k-\nu_2(e_i)}$ where e_i is the ith component of the ℓ-coordinates of f as long as $k \geq \nu_2(e_i)$. Hence, for two transductions to be orbit equivalent on $\mathbf{2}^\ell$ their ℓ-coordinates have to have the same dyadic valuations. This can be strengthened to a characterization of orbit equivalence as follows.

Theorem 16 *Let $\mathcal{A}$ be a cycle-cum-chord transducer and f and g two transductions in $\mathcal{S}(\mathcal{A})$. Then f and g are orbit equivalent if, and only if, the following two conditions hold:*

1. $\nu_2(\langle f \rangle) = \nu_2(\langle g \rangle)$, *and*
2. $\langle f \rangle = \zeta \langle g \rangle$ *for some unit* $\zeta \in \mathbb{Z}_2$.

Likewise, (f, h_1) and (g, h_2) are orbit equivalent if, and only if, the following two conditions hold:

1. f *and* g *are orbit equivalent, and*
2. $\langle h_1^{-1} h_2 \rangle = \zeta \langle f \rangle$ *for some* $\zeta \in \mathbb{Z}_2$.

Proof. Let $f, g \in \mathcal{S}(\mathcal{A}_m^n)$ be two transductions and consider a word w of length km. Write $(e_0, \ldots, e_{m-1})$ and $(e'_0, \ldots, e'_{m-1})$, respectively, for the ℓ-coordinates of f and g. As already mentioned, the projection of an orbit $w f^*$ onto the ith axis, $0 \leq i < m$, has cardinality $2^{k-\nu_2(e_i)}$ for $k \geq \nu_2(e_i)$, so a necessary condition for f and g to be orbit equivalent is that $\nu_2(\langle f \rangle) = \nu_2(\langle g \rangle)$. Suppose that this condition holds. If f and g are orbit equivalent then for all k there exists a unit z_ℓ in $\mathbb{Z}/(2^k)$, such that

$$\langle f \rangle_\ell \equiv z_\ell \cdot \langle g \rangle_\ell .$$

By Hensel's lemma, the sequence (z_ℓ) is coherent and thus defines $\zeta \in \mathbb{Z}_2$, as required. For the opposite direction note that ζ gives rise to a coherent sequence (z_ℓ) of odd integers, see [9], which solve the preceding equations.

For the second part consider two star pairs (f, h_1) and (g, h_2) and let $h = h_1^{-1} h_2$. In this case orbit equivalence means that for all k we have

$$\mathbb{N} \langle f \rangle_\ell \equiv \mathbb{N} \langle g \rangle_\ell + \langle h \rangle_\ell .$$

But then $\langle h \rangle_\ell$ lies in the linear subspace $\mathbb{N} \langle g \rangle_\ell$ and we must have $\mathbb{N} \langle f \rangle_\ell \equiv \mathbb{N} \langle g \rangle_\ell$ so that f and g orbit equivalent. Hence, for all k there must exist a z_ℓ in $\mathbb{Z}/(2^k)$, not necessarily a unit, such that

$$\langle h \rangle_\ell \equiv z_\ell \langle f \rangle_\ell$$

Our claim follows. The opposite direction is entirely similar. □

There is an interesting special case where we can obtain a better description. Call a CCC transducer $\mathcal{A}_m^n$ *amenable* if the dimension of the coordinate system for words coincides with the number of free generators. In other words, the transduction group is isomorphic to $\mathbb{Z}^m$, which is equivalent to $n - \gcd(n, m) = m$. It is easy to see that $\mathcal{A}_m^n$ is amenable if, and only if, $m = n - d$ where $d < n$ divides n.

In an amenable transducer we can express ℓ-coordinates directly in terms of the group representation. To keep notation manageable, assume that n and m are coprime, so that $m = n - 1$. Letting $f = (a_0, \ldots, a_{m-1}) \in \mathbb{Z}^m$ and $\ell = km$ we have

$$\langle\, f \,\rangle_\ell \equiv (a_0, \ldots, a_{m-1})$$

In other words, there is no need to recompute the ℓ-coordinates for each ℓ separately.

In this setting we can also express residuals conveniently as follows.

$$\begin{aligned}
\partial_s(f) &= (a_1 - a_0, \ldots, a_{m-2} - a_0, -a_0/2) && \text{if } a_0 \text{ is even,}\\
\partial_0(f) &= (a_1 - a_0 - 1, \ldots, a_{m-2} - a_0 - 1, -\lceil a_0/2 \rceil - 1) && \text{if } a_0 \text{ is odd,}\\
\partial_1(f) &= (a_1 - a_0 + 1, \ldots, a_{m-2} - a_0 + 1, -\lceil a_0/2 \rceil + 1) && \text{if } a_0 \text{ is odd.}
\end{aligned}$$

In the general case these operations are applied to the first terms in m/s blocks of length s, followed by a cyclic rotation to the left. Amenability also yields the next theorem.

Corollary 17 *For amenable cycle-cum-chord transducers, orbit equivalence is decidable in polynomial time.*

Proof. First consider two transductions f and g. By amenability, $\langle\, f \,\rangle$ is a vector of integers and likewise for g. By the theorem, we have $f \approx g$ if, and only if, $\nu_2(\langle\, f \,\rangle) = \nu_2(\langle\, g \,\rangle)$ and the system $\langle\, f \,\rangle = z \cdot \langle\, g \,\rangle$ has a solution, a dyadic rational. The latter condition is equivalent to $f_i g_j = f_j g_i$ for all i, j where f_i and g_i denote the group representation of f and g, respectively. For two star pairs (f, h_1) and (g, h_2) let again $h = h_1^{-1} h_2$. For orbit equivalence we need This time, apart from testing orbit equivalence of f and g, we have to check the solvability of the equations $\langle\, h \,\rangle = z \cdot \langle\, f \,\rangle$.

It is clear that the arithmetic operations required to test orbit equivalence are all polynomial in the size of the input. □

The position of point $\langle\, h \,\rangle$ in the orbit of f in the last proof may be fractional in the sense that the solutions z define a dyadic rational. As an example, consider $\mathcal{A}_2^3$ and let $h = (1, 3)$ and $f = (3, 9)$. Then the first few positions of the point for increasing ℓ-values are given by $1, 3, 3, 11, 11, 43, 43, 171, 171, 683, 683, 2731, \ldots$ which is the standard sequence representation of $1/3$ in $\mathbb{Z}_2$.

Call an inverse transducer $\mathcal{A}$ *orbit rational* if f^* is rational for all f in $\mathcal{S}(\mathcal{A})$. To determine orbit rationality of a CCC transducer $\mathcal{A}_m^n$ let $s = \gcd(n, m)$ and set $n' = n/s$, $m' = m/s$. We refer to $\mathcal{A}_{m'}^{n'}$ as the *reduct* of $\mathcal{A}_m^n$. It is clear from the definitions that the transition diagram of the reduct is s-partite. As a consequence, the orbits of $\mathcal{A}_m^n$ can be described in terms of the orbits of the reduct and the shuffle operation defined in section 2.3 as follows.

Lemma 18 *Let $\mathcal{A}_m^n$ be a CCC transducer, $s = \gcd(n, m)$ and $\mathcal{A}_{m'}^{n'}$ its reduct. For $0 \le k < m$ let $k_0 = k \operatorname{div} s$, $k_1 = k \bmod s$ and write $f = \mathcal{A}_m^n(k)$ and $g = \mathcal{A}_{m'}^{n'}(k_0)$. Then for words $x^i \in \mathbf{2}^k$ we have*

$$\mathsf{shf}(x^0, x^1, \ldots, x^{s-1})\, f = \mathsf{shf}(x^0, \ldots, x^{k_1}\, g, \ldots, x^{s-1})$$

The proof is straightforward from the definitions and will be omitted. As an example, consider $\mathcal{A}_2^6$ so that $s = 2$, $n' = 3$ and $n' = 1$. Write g_i for $\mathcal{A}_1^3(i)$, $i = 0, 1$ and let $\underline{k} = \mathcal{A}_2^6(k)$. Since we are in the binary case we write the customary $x \parallel y$ instead of $\mathsf{shf}(x, y)$. Then $(x \parallel y)\,\underline{0} = x\,g_0 \parallel y$, $(x \parallel y)\,\underline{1} = x \parallel y\,g_0$, $(x \parallel y)\,\underline{2} = x\,g_1 \parallel y$ and $(x \parallel y)\,\underline{3} = x \parallel y\,g_1$.

The lemma generalizes to other generators $\underline{p}$ to composite transitions in the following way. Suppose f is an arbitrary transduction over $\mathcal{A}_m^n$. It follows from the lemma that there are transductions g_i over $\mathcal{A}_{m'}^{n'}$ such that

$$\mathsf{shf}(x^0, x^1, \ldots, x^{s-1})\, f = \mathsf{shf}(x^0\, g_0, \ldots, x^{s-1}\, g_{s-1})$$

Conversely, given the g_i's there is a corresponding f. As an immediate consequence we have that the reduct $\mathcal{A}_{m'}^{n'}$ must be orbit rational whenever $\mathcal{A}_m^n$ is orbit rational. The converse requires a stronger property than just orbit rationality, we have to be able to determine the position of a word in an orbit. The problem of determining $t \geq 0$ such that $y = x\, f^t$ is referred to as the Timestamp Problem in [23]. Surprisingly, for some CCC transducers such as $\mathcal{A}_2^3$, the Timestamp Problem can be solved by a finite state machine in the sense that there is a transducer that, given x and y, will output the appropriate t in reverse binary (or determine that no such t exists). One can combine the timestamp transducers for the g_i to test orbit equivalence for f.

3.4. Rational Orbit Relations

Theorem 19 *All transducers $\mathcal{A}_1^n$ and $\mathcal{A}_n^n$ are orbit rational, $n \geq 1$.*

Proof. First consider $\mathcal{A}_1^n$. We have seen that $\underline{0}$ acts transitively on all level sets, so $\equiv_{\underline{0}}$ is universal in the sense that two words are equivalent iff they have the same length. In the general case, our claim follows similarly from lemma 14: let $\underline{k}$ be the leading term of the KNF of f, then $x \equiv_f y$ iff the prefix of length k of x agrees with the corresponding prefix of y. Hence, $\equiv_f$ can be decided by a finite state machine of size 1 when $k = 0$, and $k + 2$ otherwise.

For transducers of the form $\mathcal{A}_n^n$ recall that every transduction in $\mathcal{S}(\mathcal{A}_n^n)$ can be written uniquely in the form $f = \underline{k_1}\,\underline{k_2} \ldots \underline{k_r}$ where $0 \leq k_i < k_{i+1} < n$. Thus, f toggles exactly the bits in positions $k_i + n\mathbb{N}$ and the orbit of any word of length at least k_1 is a 2-cycle. Clearly, $\equiv_f$ can be decided by a finite state machine of size at most n. □

Corollary 20 *Every transducer of the form $\mathcal{A}_m^{mt}$ is orbit rational for $m, t \geq 1$.*

By using lemma 5 and corollary 17 one can construct a minimal finite state machine on 35 states decides orbit equivalence of $\underline{0}$ for $\mathcal{A}_2^3$. The following theorem explains why this construction terminates; a similar argument also provides a plausibility argument for the state complexity of the machine.

Theorem 21 *Every transducer of the form $\mathcal{A}_{2t}^{3t}$ is orbit rational for $t \geq 1$.*

Proof. It is shown in [23] that for $\mathcal{A}_2^3$ timestamps can be determined by transducers. Together with the comment following lemma 18 it therefore suffices to show that the common reduct $\mathcal{A} = \mathcal{A}_2^3$ is orbit rational. As we have seen, the transduction group of $\mathcal{A}$ is isomorphic to $\mathbb{Z}^2$. Consider the set $\mathcal{Q} \subseteq \mathbb{Z}^2$ obtained by closing (f, I) under quotients as in lemma 5. For the time being, let us focus on $\mathcal{Q}_0$, the projection on the first component. Note that $\mathcal{Q}_0$ is the orbit of f under the map $\pi(g) = \partial_0 g$ when g is even and $\pi(g) = \partial_0 g^2$ otherwise. It is not hard to see that the orbit of f must contain on odd function, say, $\pi^r(f) = (a, b) \in \mathbb{Z}^2$. Then the π-orbit of (a, b), modulo orbit equivalence, is

$$(a,b), (2b-2a,-a), (a-2b,a-b), (2b,2b-a), (-a,-b) \approx (a,b)$$

Here odd and even steps alternate. At any rate, $\mathcal{Q}_0$ is finite.

To see that the second component of $\mathcal{Q}$ is also finite note that, using the group representation, we can compute residuals like so:

$$\partial_s \boldsymbol{u} = \begin{cases} A \cdot \boldsymbol{u} & \text{if } \boldsymbol{u} \text{ is even,} \\ A \cdot \boldsymbol{u} - (-1)^s \boldsymbol{a} & \text{otherwise.} \end{cases}$$

where

$$A = \begin{pmatrix} -1 & 1 \\ -1/2 & 0 \end{pmatrix} \quad \text{and} \quad \boldsymbol{a} = (1, 3/2)$$

The rational matrix A has complex eigenvalues of norm $1/\sqrt{2} < 1$ and gives rise to a contraction $\mathbb{Q}^2 \to \mathbb{Q}^2$. We can over-approximate the operations required for the second components of $\mathcal{Q}$ by a map $\Phi : \mathbb{Q}^2 \to \mathfrak{P}(\mathbb{Q}^2)$ defined by

$$\Phi(\boldsymbol{u}) = \{\, A \cdot \boldsymbol{u} + c\, \boldsymbol{a} + \boldsymbol{w} \mid c \in \{0, \pm 1\}, \boldsymbol{w} \in W \,\}.$$

Here W is a set of residuals obtained from the transductions in $\mathcal{Q}_0$. Since A is a contraction the closure of h under Φ is a bounded set in $\mathbb{Q}^2$, containing only finitely many integral points. □

The fact that the matrix A in the last proof induces a contraction has the consequence that the complete automaton of $\mathcal{A}_2^3$ has 8 non-trivial strongly connected components all of which are all finite. Note that the complete automaton admits an involution that sends $f \xrightarrow{s/t} g$ to $f^{-1} \xrightarrow{\overline{s}/\overline{t}} g^{-1}$. Omitting the component of the identity, the strong components modulo this involution are listed in figure 5. The transductions are given in group notation. A copy of the original transducer appears as the bottom left component.

A careful discussion of so-called 1/2-homomorphisms can be found in [18]. In the special case $f = \underline{0}$ the π orbit has the form $(1, 0), (2, 1), (1, 1), (0, 1)$ so we can exploit orbit equivalence to rewrite the translations into a form where only one component is non-zero. We are left essentially with a one-dimensional problem and one can show that the corresponding contraction has the form

$$\widehat{\Phi}(x) = \{\, -(i + x)/4 \mid -11 \leq i \leq 13 \,\}$$

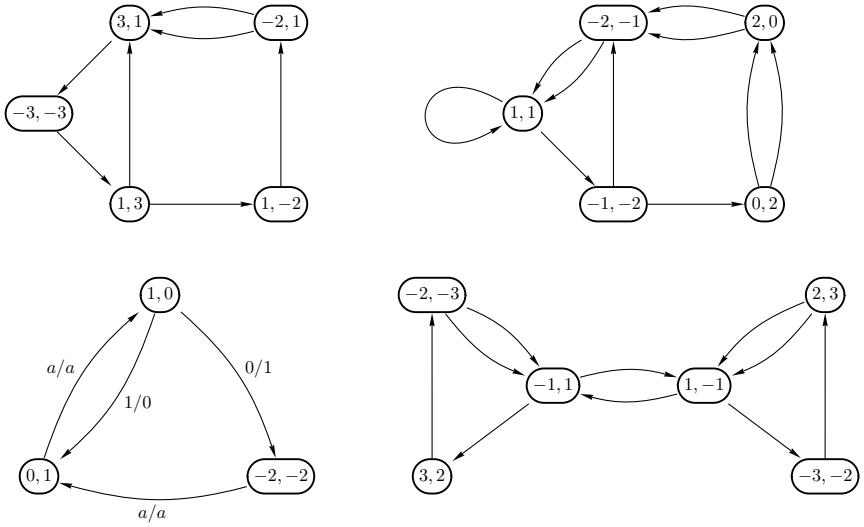


Figure 5: Strong components in the complete automaton for $\mathcal{A}_2^3$. The last component is invariant under the involution.

Hence all closures under $\widehat{\Phi}$ starting at $|x| \leq 13/3$ will stay in the interval $[-13/3, 13/3]$. There are 9 integral points in the interval and, since there are 4 rounds in the quotient process, an upper bound for the number of states in $\mathcal{M}$ is 36, surprisingly close to the actual value of 35.

4. Summary and Open Problems

We have characterized the transduction semigroups associated with a class of inverse transducers over the binary alphabet as free Abelian groups. For a subclass of these transducers we can show that the iterates f^* of any transduction is rational and hence automatic. We do not know how to decide rationality in general, and, in fact, not even for the class of amenable cycle-cum-chord transducers. As a concrete example, consider the transducers $\mathcal{A}_m^4$. It follows from our results that they are orbit rational for $m = 1, 2, 4$. In the case $m = 3$ the transducer is amenable and reduced. Following a suggestion by Cummings and Devanney, we have been able to show that $\mathcal{A}_3^4$ has non-rational orbit relation. Briefly, one can show that no power of a certain 3×3 rational matrix, corresponding to matrix A in the proof of theorem 21, has any rational eigenvalue. The first step in the argument exploits field theory to reduce the number of cases that need to be checked to about 500. The second step then relies on brute-force computation in a computer algebra system to establish that the critical matrices all fail to have rational eigenvalues. It is far from clear how this method could be generalized to other cases. In view of the quotient algorithm from above, it would be interesting to know whether orbit equivalence is decidable in general. As a special case, one can consider transduction that produce only orbits of bounded

size. Again, we are currently unable to answer these questions even for non-amenable cycle-cum-chord transducers.

It is straightforward to check whether $\mathcal{S}(\mathcal{A})$ is commutative, using standard automata-theoretic methods. Similarly it is semidecidable whether $\mathcal{S}(\mathcal{A})$ is a group, though the exponential growth in the size of the corresponding automata makes it difficult to investigate even fairly small transducers. We do not know whether it is decidable whether $\mathcal{S}(\mathcal{A})$ is a group. Unsurprisingly, many other decidability questions regarding transduction semigroups or groups of inverse transducers are also open, see [11, chap. 7] for an extensive list.

Lastly, there are several computational problems that arise naturally in the context of $\mathcal{S}(\mathcal{A})$. The most basic one is the Iteration Problem: for a given transduction $f \in \mathcal{S}(\mathcal{A})$, compute $x\,f$ for a word x. As already mentioned, in the case of $\mathcal{A}_2^3$ the complete automaton has only finite non-trivial strongly connected components. As a consequence, we can compute $x\,f$ in time $O(|x| \log^2 w)$ where w is the weight of f. Closely related is the Timestamp Problem: given two words $x, y \in \mathbf{2}^k$, find a witness t such that $x\,f^t = y$ or determine that they are not on the same f-orbit. Again for $\mathcal{A}_2^3$, there is a finite transducer that computes the minimal t given input $x{:}y$, see [23]. Knuth normal form is a critical tool in the corresponding correctness proofs. In light of the description of orbits in terms of the coordinate system introduced in section 3.3 it is natural to ask how difficult it is to compute the coordinates of a given word. Again for $\mathcal{A}_2^3$, there is a finite transducer that solves the Coordinate Problem: given $x \in \mathbf{2}^{2k}$ as input, outputs the coordinates (s, t) of x, where $0 \le s, t < 2^k$, see [23]. Note that based on the geometric description of orbits from section 3.3 the Timestamp Problem can be reduced to the Coordinate Problem. We do not know whether these problems can be solved in polynomial time in general for cycle-cum-chord transducers.

Acknowledgments: We would like to thank W. Devanney and J. Cummings for helpful discussions. The anonymous referees have helped greatly to improve the presentation.

References

[1] P.-Y. Angrand and J. Sakarovitch. Radix enumeration of rational languages. *RAIRO-Theor. Inf. Appl.*, 44(1):19–36, 2010.

[2] L. Bartholdi and P. V. Silva. Groups defined by automata. *CoRR*, abs/1012.1531, 2010.

[3] J. Berstel. Transductions and context-free languages. `http://www-igm.univ-mlv.fr/~berstel/LivreTransductions/LivreTransductions.html`, 2009.

[4] J. A. Brzozowski. Derivatives of regular expressions. *Journal Assoc. for Comp. Machinery*, 11, 1964.

[5] S. Eilenberg. *Automata, Languages and Machines*, volume A. Academic Press, 1974.

[6] C. C. Elgot and J. E. Mezei. On relations defined by generalized finite automata. *IBM J. Res. Dev.*, 9:47–68, January 1965.

[7] D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Patterson, and W. P. Thurston. *Word Processing in Groups*. Jones and Bartlett, Burlington, 1992.

[8] V. M. Gluškov. Abstract theory of automata. *Uspehi Mat. Nauk*, 16(5(101)):3–62, 1961.

[9] F. Q. Gouvêa. *p-Adic Numbers: An Introduction*. Springer Verlag, 2nd edition, 1997.

[10] R. Grigorchuk and Z. Šunić. *Groups St. Andrews 2005*, volume 339 of *London Math. Soc. Lec. Notes*, chapter Self-Similarity and Branching in Group Theory. Cambridge University Press, 2007.

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

[12] J. Howard Johnson. Rational equivalence relations. *Theoretical Computer Science*, 47:167–176, 1986.

[13] B. Khoussainov and A. Nerode. Automatic presentations of structures. In *LCC '94: Int. Workshop on Logical and Computational Complexity*, pages 367–392, London, UK, 1995. Springer-Verlag.

[14] B. Khoussainov and A. Nerode. *Automata Theory and its Applications*. Birkhäuser, 2001.

[15] B. Khoussainov and S. Rubin. Automatic structures: overview and future directions. *J. Autom. Lang. Comb.*, 8(2):287–301, 2003.

[16] D. Knuth. Private communication, 2010.

[17] V. Nekrashevych. *Self-Similar Groups*, volume 117 of *Math. Surveys and Monographs*. AMS, 2005.

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

[19] G. N. Raney. Sequential functions. *J. Assoc. Comp. Mach.*, 5(2):177–180, 1958.

[20] J. Sakarovitch. *Elements of Automata Theory*. Cambridge University Press, 2009.

[21] J.-P. Serre. *Arbres, Amalgames, SL_2*. Number 46 in Astérisque. Société Mathématique de France, Paris, 1977.

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

[23] K. Sutner. Invertible transducers, iteration and coordinates. Submitted, 2013.

[24] J. Vuillemin. On circuits and numbers. *IEEE Transactions on Computers*, 43:868–879, 1994.