Iterating Invertible Binary Transducers

Klaus Sutner[1] and Kevin Lewi[2,⋆]

[1] Carnegie Mellon University,
Pittsburgh, PA 15213
sutner@cmu.edu
[2] Stanford University,
Stanford, CA 94305
klewi@cs.standford.edu

Abstract. We study iterated transductions defined by a class of invertible 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.

1 Motivation

An *invertible transducer* is a type of Mealy automaton where all transitions are of the form $p \xrightarrow{a/\pi(a)} q$; here π 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 [9,15] 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 invertible transducer. Automata groups should not be confused with *automatic groups* as introduced in [6] or *automatic structures*, see [11,13]. The former are characterized by the group operations being described directly by finite state machines operating on words over the generators. The latter are first-order structures whose carrier sets and relations are represented by finite state machines. A comparison of the two models can be found in [10].

We are here interested in both connections between automata theory and group theory as discussed in [1]. 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

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

M. Kutrib, N. Moreira, and R. Reis (Eds.): DCFS 2012, LNCS 7386, pp. 294–306, 2012.

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 invertible 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, [5] 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 [22]; 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 [14] 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 [4]. 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 invertible 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 Invertible 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 [2,18,12] for background. We are here only interested in *invertible 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 functions; $\mathcal{S}(\mathcal{A})$ 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 [19], we can interpret our transductions as automorphisms of this tree, see [15,20]. 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. The automorphisms f such that $f = (f_0, f_1)\sigma$ are *odd*, the others *even*. 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 [17]. It was shown by Gluškov that the residuals of a sequential map are sufficient to construct a corresponding Mealy automaton, see [7] and [15]. 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

$$\partial_{xy} f = \partial_y \partial_x f$$
$$\partial_x fg = \partial_x f\, \partial_{f(x)} g$$

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 $f \xrightarrow{s/f(s)} \partial_s f$. 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 [15]. 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 invertible transducers. For example, 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 [15]. 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 [22], 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 the Orbit Automaton

Consider an automorphism f in $\mathsf{Aut}(\mathbf{2}^*)$. The iterate f^* is an equivalence relation on $\mathbf{2}^*$, the *orbit relation* of f, written $\equiv_f$. Two automorphism f and g are *star equivalent* if they have the same orbit relation. It is easy to see that any orbit $xa\, f^*$ either has the same length as $x\, f^*$, or twice that length. We will say correspondingly that x *splits* or *doubles* under f: in the first case the orbits of $x0$ and $x1$ are distinct, in the second case they coincide (as sets). 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 are star equivalent.

In order to show that some orbit relations are rational, it is useful to generalize the notion of orbit slightly. Given two automorphisms f and h and a word u, define the *orbit of u under f with translation h* to be $u\,f^*h = \{\, u\,f^ih \mid i \geq 0\,\}$. Correspondingly, the relation $\mathbf{R}(f,h)$ holds on u and v if $v \in u\,f^*h$. When h is the identity then $\mathbf{R}(f,I)$ is simply the orbit relation of f. In general, $\mathbf{R}(f,h)$ 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 Brzozowski [3] quotients. Here we interpret $\mathbf{R}(f,h)$ as a language over $(\mathbf{2} \times \mathbf{2})^*$.

Lemma 1. *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

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

All other quotients are empty.

Proof. In the first case we get $ax\,f^*h = b\,(x\,{f_a}^*h_a)$. In the second case note that $f^2 = (f_0 f_1, f_1 f_0)$. Since the first bit alternates along the orbit of ax under f, it follows that $ax\,f^* = a\,(x\,(f_a f_{\overline{a}})^*) \cup \overline{a}\,(x\,(f_a f_{\overline{a}})^* f_a)$. Our claim follows by applying the translation h to this equation. □

The lemma provides a way to construct a transition system over the alphabet $\mathbf{2} \times \mathbf{2}$ that decides the orbit relation $\equiv_f$ of an automorphism f: starting at (f, I), generate all quotients according to the lemma and record transitions $\mathbf{R}(f,h) \xrightarrow{a/b} (a{:}b)^{-1}\,\mathbf{R}(f,h)$. The initial state is (f, I) and all states other than $\emptyset$ are accepting. Clearly, the system accepts the convolution $x{:}y$ of two words x and y of equal length if, and only if, $x \equiv_f y$. To obtain a minimal transition system $\mathcal{M}_f$ in the sense of Eilenberg [4], we have to adjust the notion of star equivalence to pairs: (f,h) and (g,h') are *star equivalent* if $\mathbf{R}(f,h) = \mathbf{R}(g,h')$. We write $(f,h) \approx (g,h')$ to indicate star equivalence. From the definitions we have the following sufficient condition for star equivalence.

Proposition 1. *Let f and h be automorphisms. Then for any odd r and any integer s: $(f,h) \approx (f^r, f^s h)$.*

Of course, in general $\mathcal{M}_f$ will be infinite. For some automorphisms given by an invertible 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" SA_n in [15], generalizations of the adding machine from above. In wreath notation they are given by

$$\underline{1} = (0, \underline{n})\,\sigma \qquad \text{and} \qquad \underline{k} = (\underline{k-1}, \underline{k-1}), \quad 2 \leq k \leq n$$

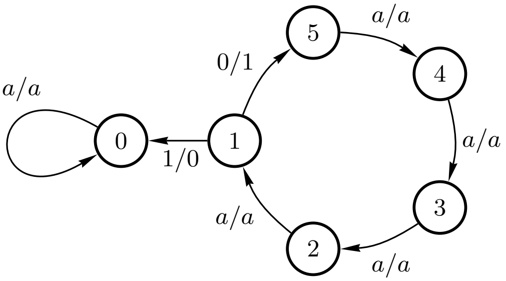


Fig. 1. The "sausage automaton" $\mathcal{A}_5$, an invertible transducer that generates $\mathbb{Z}^5$

where we ignore the identity I, as customary. Figure 1 shows $\mathcal{A}_5$.

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 $x^i \in \mathbf{2}^r$, $1 \leq i \leq n$, and $1 \leq k \leq n$. Then

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

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

$$\mathsf{shf}(x^1, x^2, \ldots, x^s) = x^1_1 x^2_1 \ldots x^s_1\, x^1_2 x^2_2 \ldots x^s_2\, \ldots\, x^1_r x^2_r \ldots x^s_r.$$

Note that automatic relations are closed under perfect shuffle. With a little bit of effort one can show that the orbit relation $\equiv_f$ is automatic for any transduction f in $\mathcal{S}(\mathcal{A}_n)$

2.3 Cycle-Cum-Chord Transducers

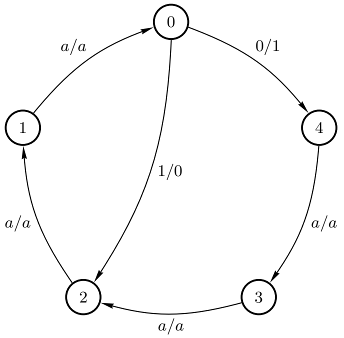
We now introduce a simple class of invertible transducers whose associated semigroups will turn out to be free Abelian groups. Unlike with the sausage automata from above, the orbits of words under the corresponding transductions are fairly complicated. A *cycle-cum-chord (CCC)* transducer has state 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 $1 \leq m \leq n$. We will write $\mathcal{A}^n_m$ for this transducer. The diagram of $\mathcal{A}^5_3$ is shown in figure 2. The source node of the chord is the sole toggle state in these transducers. As we will see shortly, $\mathcal{S}(\mathcal{A}^n_m) = \mathcal{G}(\mathcal{A}^n_m)$.

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

Lemma 2. *The transduction semigroup of $\mathcal{A}^n_m$ is Abelian.*



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

Fig. 2. The cycle-cum-chord transducer $\mathcal{A}_3^5$, an invertible transducer on 5 states with one toggle state

Proof. Let $0 \leq r, s < n-1$. Then

$$\begin{aligned}
\underline{0}\;\underline{r+1} &= (\underline{n-1}, \underline{m-1})\;\sigma\;(\underline{r}, \underline{r}) = (\underline{n-1}\;\underline{r}, \underline{m-1}\;\underline{r})\;\sigma \\
\underline{r+1}\;\underline{0} &= (\underline{r}, \underline{r})\;(\underline{n-1}, \underline{m-1})\;\sigma = (\underline{r}\;\underline{n-1}, \underline{r}\;\underline{m-1})\;\sigma \\
\underline{r+1}\;\underline{s+1} &= (\underline{r}, \underline{r})\;(\underline{s}, \underline{s}) \qquad\qquad\quad = (\underline{r}\;\underline{s}, \underline{r}\;\underline{s}) \\
\underline{s+1}\;\underline{r+1} &= (\underline{s}, \underline{s})\;(\underline{r}, \underline{r}) \qquad\qquad\quad = (\underline{s}\;\underline{r}, \underline{s}\;\underline{r})
\end{aligned}$$

and we are done by induction. □

Lemma 3. *Cancellation Identities*
Consider $\mathcal{A}_m^n$ where $1 \leq m \leq n$ and let $s = \gcd(n,m)$, $r = m/s$. Then the following identities hold in the transduction semigroup of $\mathcal{A}_m^n$, for $0 \leq i < s$:

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

Proof. For $i = 0$ we have

$$\begin{aligned}
&\partial_a \underline{0}^2\;(\underline{s})^2 \ldots (\underline{(r{-}1)s})^2\;\underline{m}\;\underline{m+s} \ldots \underline{n-s} = \\
&\underline{s-1}^2\;(\underline{2s}-1)^2 \ldots (\underline{(r{-}1)s-1})^2\;\;\underline{m+s} \ldots \underline{n-s-1}\;\underline{n-1}
\end{aligned}$$

Noting that, for $i > 0$, each term $\underline{r}$ in the equation is replaced by $\underline{r-1}$ under residuation we are done by induction. □

3 Orbit Rationality

3.1 Knuth Normal Form

From the two lemmata it follows that $\mathcal{S}(\mathcal{A}_m^n) = \mathcal{G}(\mathcal{A}_m^n)$ is an Abelian group: by the cancellation identities the inverse of each monoid generator lies already in $\mathcal{S}(\mathcal{A}_m^n)$. Also, by the cancellation identities, the resulting group is a quotient of $\mathbb{Z}^{n-s}$. To show that the group is in fact isomorphic to $\mathbb{Z}^{n-s}$ we use a method suggested by D. Knuth [14]: we add a new state n to the transducer with transitions $n \xrightarrow{a/a} n-1$ for $a \in \mathbf{2}$. By repeating this extension step, we can enlarge the state set to $\mathbb{N}$ where for all $i > 0$ we have $\underline{i} = (\underline{i{-}1}, \underline{i{-}1})$. We write $\mathcal{K}^n_m$ for the new transducer.

Lemma 4. *Shift Identities*
In the transduction semigroup of $\mathcal{K}^n_m$ we have, for $m < n$ and all $k \geq 0$, the identities

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

Proof. It suffices to prove the result for $k = 0$. Both $\underline{0}^2$ and $\underline{m}\;\underline{n}$ are even and we have residuals $\underline{m-1}\;\underline{n-1}$. □

According to the shift identities, the transduction semigroups of $\mathcal{A}^n_m$ and $\mathcal{K}^n_m$ coincide. Likewise, the cancellation identities generalize to all transductions in $\mathcal{K}^n_m$. Since $\mathcal{S}(\mathcal{A}^n_m) = \mathcal{S}(\mathcal{K}^n_m)$ we have an alternative representation as $f = \underline{k_1}^{e_1}\,\underline{k_2}^{e_2}\ldots\underline{k_r}^{e_r}$ where $k_1 < k_2 < \ldots < k_r$ and $e_i \geq 1$. We allow $r = 0$ for the identity map. 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. To generate the KNF of f we interpret the identities from lemma 4 as rewrite rules. For example, in $\mathcal{K}^3_2$ 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 3 immediately terminates the process. Thus, the rewrite system is weakly terminating.

Theorem 1. *Knuth Normal Form*
Every transduction over $\mathcal{A}^n_m$ 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 $\mathcal{S}(\mathcal{A}^n_m)$ 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 3 in the first place possible. If none of these identities apply, use the shift rule derived from lemma 4, 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 leftmost $m-1$ entries in the vector must then all be even and positive. Hence we can apply cancellation and we have the desired contradiction. Uniqueness is clear from the construction. □

We can now pin down the structure of the transductions semigroups $\mathcal{S}(\mathcal{A}^n_m)$.

Corollary 1. *The transduction semigroup of $\mathcal{A}^n_n$ is isomorphic to the Boolean group $\mathbf{2}^n$. For $m < n$, the transduction semigroup of $\mathcal{A}^n_m$ is isomorphic to $\mathbb{Z}^{n-\gcd(n,m)}$.*

Knuth normal form can be used to establish other properties of the group of $\mathcal{A}^n_m$. For example, the group can be shown to act transitively on all the level sets $\mathbf{2}^\ell$, $\ell \geq 0$. Here is another important property of the transduction group.

Lemma 5. *Let $f \neq I$ be a transduction over a CCC transducer $\mathcal{A}^n_m$ and $\underline{r}$ the first term in the KNF of f. Then exactly all words of length $r + m\mathbb{N}$ double for $m < n$. For $n = m$, only words of length r double.*

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 $k_i + m\mathbb{N}$.

Suppose $m < n$ 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 the first term in the KNF of f^{2^k} is $\underline{km}$ 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. □

Lemma 6. *For any CCC transducer $\mathcal{A}^n_m$ 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 transduction f and consider arbitrary bits $a_0, \dots, a_{m-1}$ and $b_0, \dots, b_{m-1}$. Note that $xa_0\, f\underline{0}^{e_0} = yb_0$ for $e_0 = 0$ or $e_0 = 2^k$. Proceeding inductively, we can find $e_i \in \left\{0, 2^k\right\}$ such that $xa_0 \dots a_{m-1}\, f\underline{0}^{e_0} \dots \underline{m{-}1}^{e_{m-1}} = yb_0 \dots b_{m-1}$.

Since the coefficients are uniquely determined modulo 2^{k+1}, the second claim also follows. □

3.2 Orbit Geometry and Rationality

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

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

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: $\langle\, w \,\rangle_\ell = (a_0, \dots, a_{m-1})$ if, and only if, $w = 0^\ell\, \underline{0}^{a_0}\underline{1}^{a_1} \dots \underline{m{-}1}^{a_{m-1}}$. In terms of this coordinate system, orbits can be described as affine subspaces of $(\mathbb{Z}/(2^k))^m$:

$$\langle\, w\, f^* \,\rangle_\ell = \langle\, w \,\rangle_\ell + \mathbb{N} \cdot \langle\, f \,\rangle_\ell \pmod{2^k}$$

In fact, all these orbits are translations of the basic linear subspace $0^\ell\, f^*$. But then two transductions f and g are star equivalent for words of length $\ell = km$ if, and only if, for some odd integer z depending on ℓ we have $\langle\, f \,\rangle_\ell = z \cdot \langle\, g \,\rangle_\ell \pmod{2^k}$. Thus, for fixed ℓ, simple modular arithmetic suffices to determine star equivalence, given the coordinates. To deal with the general case, recall that a sequence (a_i) of integers is *coherent* if $a_i = a_{i+1} \pmod{2^i}$, and likewise for vectors of integers, see [8]. For any word x let $x[i]$ be the prefix of x of length i. It is easy to check that the sequence $(\langle\, f \,\rangle_\ell)$ 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 example, in $\mathcal{A}_2^3$, letting $f = \underline{0}^{-1}\underline{1}^3$ we get

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

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 $\mathbb{Z}_2$.

Theorem 2. *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 star 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 star equivalent if, and only if, the following two conditions hold:

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

There is an interesting special case where we can obtain a better description. Call a CCC transducer $\mathcal{A}^n_m$ *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 $n - \gcd(n, m) = m$. It is easy to see that $\mathcal{A}^n_m$ is amenable if, and only if, $m = n - d$ where $d < n$ divides n.

Corollary 2. *For amenable cycle-cum-chord transducers, star equivalence is decidable in polynomial time.*

For any odd integer s and a transduction f, define the fractional power $f^{1/s}$ as follows: $x\, f^{1/s} = y$ iff $x = y\, f^s$. This yields the following characterization of star equivalence for CCC transducers.

Corollary 3. *In any amenable cycle-cum-chord transducer, the following are equivalent for transductions f and g:*

- *f and g are star equivalent,*
- *there are odd integers r and s such that $f^{r/s} = g$,*
- *there are odd integers r and s and a transduction h such that $f = h^r$ and $g = h^s$.*

Call an invertible transducer $\mathcal{A}$ *orbit rational* if f^* is rational for all f in $\mathcal{S}(\mathcal{A})$. To simplify the discussion, consider $\mathcal{A}^n_m$ and let $s = \gcd(n, m)$ and $n' = n/s$, $m' = m/s$. We refer to $\mathcal{A}^{n'}_{m'}$ as the *reduct* of $\mathcal{A}^n_m$. The transition diagram of the reduct is s-partite and the orbits can be described via shuffle as follows.

Lemma 7. *Let $\mathcal{A}^n_m$ be a CCC transducer, $s = \gcd(n, m)$ and $\mathcal{A}^{n'}_{m'}$ its reduct; write $f = \mathcal{A}^n_m(0)$ and $g = \mathcal{A}^{n'}_{m'}(0)$. Then for words $x^i \in \mathbf{2}^k$ we have*

$$f(\mathsf{shf}(x^1, x^2, \ldots, x^s)) = \mathsf{shf}(g(x^1), x^2, \ldots, x^s)$$

As a consequence it suffices to determine orbit rationality for reducts only.

Lemma 8. *A transducer $\mathcal{A}^n_m$ is orbit rational if, and only if, its reduct $\mathcal{A}^{n'}_{m'}$ is orbit rational.*

3.3 Rational Orbit Relations

Theorem 3. *All transducers $\mathcal{A}^n_1$ 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 5: let $\underline{k}$ be the leading term of the KNF of f, then $x \equiv_f y$ iff $x[k] = y[k]$. 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 4. *Every transducer of the form $\mathcal{A}_m^{mt}$ is orbit rational for $m, t \geq 1$.*

By using lemma 1 and corollary 2 one can construct a minimal finite state machine on 36 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 4. *Every transducer of the form $\mathcal{A}_{2t}^{3t}$ is orbit rational for $t \geq 1$.*

Proof. It 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 1. 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 star 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. □

A careful discussion of so-called 1/2-homomorphisms can be found in [16].

4 Summary and Open Problems

We have characterized the transduction semigroups associated with a class of invertible 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 $\mathcal{A}^4_m$. 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. We are able to show that $\mathcal{A}^4_3$ indeed fails to be orbit rational, but the proof uses field theory in combination with symbolic computation and does not easily generalize to any other situation. In view of the quotient algorithm from above, it would be interesting to know whether star 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 invertible transducers are also open, see [9, 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. For example, in the case of $\mathcal{A}^3_2$ the complete automaton mentioned in section 2.1 has 8 non-trivial strongly connected components that are all finite. As a consequence, we can compute $x\,f$ in time $O(|x| \log^2 w)$ where w is the weight of f. As we have seen, for $\mathcal{A}^3_2$ the elementary decision problem of determining orbit equivalence can be handled by a finite state machine. A slightly stronger version of the decision problem 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. Surprisingly, for $\mathcal{A}^3_2$, there is a finite transducer that computes the minimal t given input $x{:}y$. Knuth normal form is a critical tool in the corresponding correctness proofs. Lastly, in light of the description of orbits in terms of the coordinate system introduced in section 3.2, it is natural to ask how difficult it is to compute the coordinates of a given word. Again for $\mathcal{A}^3_2$, 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 $0 \leq s, t < 2^k$, see [21]. Note that based on the geometric description of orbits from section 3.2 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.

References

1. Bartholdi, L., Silva, P.V.: Groups defined by automata. CoRR, abs/1012.1531 (2010)
2. Berstel, J.: Transductions and context-free languages (2009), `http://www-igm.univ-mlv.fr/~berstel/LivreTransductions/LivreTransductions.html`
3. Brzozowski, J.A.: Derivatives of regular expressions. Journal Assoc. for Comp. Machinery 11 (1964)
4. Eilenberg, S.: Automata, Languages and Machines, vol. A. Academic Press (1974)
5. Elgot, C.C., Mezei, J.E.: On relations defined by generalized finite automata. IBM J. Res. Dev. 9, 47–68 (1965)
6. Epstein, D.B.A., Cannon, J.W., Holt, D.F., Levy, S.V.F., Patterson, M.S., Thurston, W.P.: Word Processing in Groups. Jones and Bartlett (1992)
7. Gluškov, V.M.: Abstract theory of automata. Uspehi Mat. Nauk 16(5(101)), 3–62 (1961)
8. Gouvêa, F.Q.: p-Adic Numbers: An Introduction, 2nd edn. Springer (1997)
9. Grigorchuk, R.R., Nekrashevich, V.V., Sushchanski, V.I.: Automata, dynamical systems and groups. Proc. Steklov Institute of Math. 231, 128–203 (2000)
10. Kharlampovich, O., Khoussainov, B.: A Miasnikov. From automatic structures to automatic groups. ArXiv e-prints (July 2011)
11. Khoussainov, B., Nerode, A.: Automatic Presentations of Structures. In: Leivant, D. (ed.) LCC 1994. LNCS, vol. 960, pp. 367–392. Springer, Heidelberg (1995)
12. Khoussainov, B., Nerode, A.: Automata Theory and its Applications. Birkhäuser (2001)
13. Khoussainov, B., Rubin, S.: Automatic structures: overview and future directions. J. Autom. Lang. Comb. 8(2), 287–301 (2003)
14. Knuth, D.: Private communication (2010)
15. Nekrashevych, V.: Self-Similar Groups. Math. Surveys and Monographs, vol. 117. AMS (2005)
16. Nekrashevych, V., Sidki, S.: Automorphisms of the binary tree: state-closed subgroups and dynamics of 1/2-endomorphisms. Cambridge University Press (2004)
17. Raney, G.N.: Sequential functions. J. Assoc. Comp. Mach. 5(2), 177–180 (1958)
18. Sakarovitch, J.: Elements of Automata Theory. Cambridge University Press (2009)
19. Serre, J.-P.: Arbres, Amalgames, SL_2. Number 46 in Astérisque. Société Mathématique de France, Paris (1977)
20. Sidki, S.: Automorphisms of one-rooted trees: Growth, circuit structure, and acyclicity. J. Math. Sciences 100(1), 1925–1943 (2000)
21. Sutner, K., Devanny, W.: Timestamps in iterated invertible transducers (in preparation, 2012)
22. Vuillemin, J.: On circuits and numbers. IEEE Transactions on Computers 43, 868–879 (1994)