Monoids that map onto the Thompson-Higman groups

Jean-Camille Birget

September 3, 2010

Abstract

A slight modification of the definition of the Thompson-Higman groups $G_{k,1}$ and $F_{k,1}$ leads to inverse monoids that map onto $G_{k,1}$ (respectively $F_{k,1}$), and that have interesting properties: they are finitely generated, and residually finite. These inverse monoids are closely related to the suffix expansion of $G_{k,1}$ (respectively $F_{k,1}$).

1 Introduction

The groups $G_{k,1}$ and $F_{k,1}$ ($k \geq 2$) of Thompson and Higman \cite{17,14,18,11} are well known in combinatorial group theory (see e.g. the references in \cite{4,2}). A classical survey is \cite{7}. The group $G_{2,1}$ is usually called $V$, and $F_{2,1}$ is called $F$.

The group $G_{k,1}$ can be defined as consisting of all maximally extended right-ideal isomorphisms between finitely generated essential right ideals of a free monoid $A^*$ (where $A$ is a $k$-letter alphabet). An important fact about isomorphisms between essential right ideals of $A^*$ is that they have a unique maximal essential extension. Multiplication in $G_{k,1}$ is composition, followed by maximum extension. Details appear in the Background definitions below. In \cite{7} $G_{k,1}$ is defined (differently, but isomorphically) as consisting of all continuous, increasing, piecewise-linear bijections (with finitely many pieces), from the real interval $[0,1]$ onto itself, where only base-$k$ rationals are allowed as coordinates of articulation points. A base-$k$ rational is a rational number of the form $a/k^n$ with $a, n$ integers and $n \geq 0$. In this definition of $G_{k,1}$, maximum extension is achieved by repeatedly combining certain adjacent linear pieces into one linear piece if these pieces have the same slope, and if the domain intervals of these pieces are of the form $[a/k^n, a/k^{n+1}]$, $[a/k^{n+1}, a/k^{n+2}]$, \ldots, $[a/k^n, a/k]$; then $[a/k^n, a/k]$ is the domain interval of the corresponding combined piece.

In order to gain a better understanding of the role of the maximum essential extension one can look at what happens if maximum essential extension is simply left out in the definition of the Thompson-Higman groups. The structure that is obtained then is the inverse monoid $\tilde{\text{riAut}}(k)$, consisting of all isomorphisms between finitely generated essential right ideals of $A^*$, where $|A| = k$. Multiplication is now just composition. In relation to the group $F_{k,1}$ one can also define the inverse monoid $\tilde{\text{riAut}}_{\text{dict}}(k)$, consisting of all dictionary order preserving isomorphisms between finitely generated essential right ideals of $A^*$.

The monoids $\tilde{\text{riAut}}(k)$ and $\tilde{\text{riAut}}_{\text{dict}}(k)$ are not groups but they nevertheless have interesting, sometimes surprising properties. In summary, $\tilde{\text{riAut}}(k)$ maps homomorphically onto $G_{k,1}$, and $G_{k,1}$ is the maximum group-homomorphic image. Similarly, $\tilde{\text{riAut}}_{\text{dict}}(k)$ maps onto $F_{k,1}$, and the latter is the maximum group-homomorphic image. Both $\tilde{\text{riAut}}(k)$ and $\tilde{\text{riAut}}_{\text{dict}}(k)$ are finitely generated as monoids, their word problem is in $\mathsf{P}$, they are residually finite, and they are $F$-inverse.

Another way to obtain $G_{k,1}$ as a homomorphic image of a residually finite $F$-inverse monoid is to take the $\Gamma$-generated suffix expansion $(G_{k,1}^\Gamma)_\Gamma$ of $G_{k,1}$, where $\Gamma$ is a generating set of $G_{k,1}$. This will be defined in Section 4; the suffix and the prefix expansions were introduced in the early 1980’s and had a priori no special connection with the Thompson-Higman groups. We show that $(G_{k,1}^\Gamma)_\Gamma$ maps
homomorphically into \( riAut(k) \), that the map is finite-to-one, and that it is surjective for certain (finite and infinite) choices of \( \Gamma \). Thus, the relationship between \( riAut(k) \) and the prefix expansion \( (G_{k,1}^+)_f \) reveals that certain finite generating sets \( \Gamma \) of \( G_{k,1} \) have special properties. In combinatorial group theory it is very rare that some finite generating sets of a group behave very differently than others (in non-trivial ways). Similar results hold for \( F_{k,1} \).

Background definitions and facts

We will define the Thompson-Higman groups \( G_{k,1} \) and \( F_{k,1} \), as well as the inverse monoids \( riAut(k) \) and \( riAut_{dict}(k) \) but we need some preliminary definitions; we follow [4] and [2] (and indirectly [13]).

Let \( A = \{a_1, \ldots , a_k\} \) be a finite alphabet of cardinality \( |A| = k \). The free monoid over \( A \) (consisting of all finite strings over \( A \)) is denoted by \( A^* \). The length of \( w \in A^* \) is denoted by \( |w| \), and the empty word is denoted by \( \varepsilon \), where \( |\varepsilon| = 0 \). The concatenation of \( x, y \in A^* \) is denoted by \( xy \) or by \( x \cdot y \), and for \( B, C \subseteq A^* \) the concatenation is defined by \( BC = \{xy : x \in B, y \in C\} \). For \( x, y \in A^* \) we say that \( x \) is a prefix of \( y \) iff \( xs = y \) for some \( s \in A^* \). For \( S \subseteq A^* \), \( \text{pref}(S) \) denotes the set of all prefixes of the strings in \( S \), including the elements of \( S \) and \( \varepsilon \). We say that \( x, y \in A^* \) are prefix-comparable iff \( x \in \text{pref}(y) \) or \( y \in \text{pref}(x) \). A prefix code \( C \) is a subset \( C \subseteq A^* \) whose elements are two-by-two prefix-incomparable. A prefix code \( C \) is maximal iff \( C \) is not a strict subset of any other prefix code.

A set \( R \subseteq A^* \) is called a right ideal iff \( RA^* \subseteq R \), and \( R \) is called an essential right ideal iff \( R \) intersects every right ideal of \( A^* \). We say that a right ideal \( R \) is generated by a set \( C \subseteq A^* \) iff \( R \) is the intersection of all right ideals that contain \( C \); equivalently, \( R = CA^* \). One can prove that a right ideal \( R \) has a unique minimal (under inclusion) generating set, and that this minimal generating set is a prefix code, and that this prefix code is maximal iff \( R \) is an essential right ideal. Here we will only consider finitely generated right ideals, and finite prefix codes.

For a partial function \( f : A^* \rightarrow A^* \) the domain is denoted by \( \text{Dom}(f) \) and the image by \( \text{Im}(f) \). A right ideal homomorphism of \( A^* \) is a function \( \varphi : R_1 \rightarrow A^* \) such that \( \text{Dom}(\varphi) = R_1 \) is a right ideal, and for all \( x_1 \in R_1 \) and all \( w \in A^* \) : \( \varphi(x_1w) = \varphi(x_1)w \). Then one can prove that \( \text{Im}(\varphi) \) is also a right ideal, and if \( R_1 \) is a finitely generated right ideal then \( \text{Im}(\varphi) \) is also finitely generated. We write the action of partial functions on the left of the argument; equivalently, functions are composed from right to left. When \( \varphi : \text{Dom}(f) \rightarrow A^* \) is injective we call \( \varphi \) a right ideal isomorphism between the right ideals \( \text{Dom}(f) \) and \( \text{Im}(\varphi) \).

In this paper we only deal with right ideal isomorphisms for which both \( \text{Dom}(\varphi) \) and \( \text{Im}(\varphi) \) are essential, i.e., their prefix codes are maximal. We call such an isomorphism a right ideal automorphism of \( A^* \). This does not mean that \( \text{Dom}(\varphi) = \text{Im}(\varphi) \); however, \( \text{Dom}(\varphi) \) and \( \text{Im}(\varphi) \) are “essentially equal”, in the sense that every ideal that intersects one also intersects the other and vice versa; equivalently, \( \text{Dom}(\varphi) \) and \( \text{Im}(\varphi) \) have the same ends (see section 1 of [1]).

A right ideal automorphism \( \varphi : R_1 \rightarrow R_2 \) is uniquely determined by its restriction \( P_1 \rightarrow P_2 \), where \( P_i \) is the finite maximal prefix code that generates \( R_i \) \( (i = 1, 2) \). This finite bijection \( P_1 \rightarrow P_2 \) is called the table of \( \varphi \). The prefix code \( P_1 \) is called the domain code of \( \varphi \) and is denoted by \( \text{domC}(\varphi) \); \( P_2 \) is called the image code, denoted by \( \text{imC}(\varphi) \). We can write the table of \( \varphi \) in the form \( \{(x_1, y_1), \ldots , (x_n, y_n)\} \) where \( \{x_1, \ldots , x_n\} = P_1 \) and \( \{y_1, \ldots , y_n\} = P_2 \).

The set of right ideal automorphisms with finite tables, called \( riAut(k) \), is closed under composition, and the identity map on \( A^* \) serves as an identity for this multiplication; hence, \( riAut(k) \) is a monoid. Every \( \varphi \in riAut(k) \) is injective, and its inverse \( \varphi^{-1} : \text{Im}(\varphi) \rightarrow \text{Dom}(\varphi) \) belongs to \( riAut(k) \), and satisfies \( \varphi \circ \varphi^{-1} \circ \varphi = \varphi \) and \( \varphi^{-1} \circ \varphi \circ \varphi^{-1} = \varphi^{-1} \). Moreover, \( \varphi^{-1} \) is the only element \( \psi \in riAut(k) \) that satisfies \( \varphi \circ \psi \circ \varphi = \varphi \) and \( \psi \circ \varphi \circ \psi = \psi \), by injectiveness of \( \varphi \) and \( \psi \). Hence, \( riAut(k) \) is an inverse monoid. We have \( \varphi^{-1} \circ \varphi = \text{id}_{\text{dom}(\varphi)} \) (i.e., the identity map, restricted to \( \text{Dom}(\varphi) \)), and \( \varphi \circ \varphi^{-1} = \text{id}_{\text{im}(\varphi)} \). Recall again that in this paper, maps act on the left.

An interesting submonoid of \( riAut(k) \) is \( riAut_{dict}(k) \), the dictionary order preserving automorphisms. The dictionary order \( \leq_{\text{dict}} \) is a well-order on \( A^* \) derived from an order \( a_1 < \ldots < a_k \) of the alphabet \( A \):
For \( u, v \in A^* \) the dictionary order between them is the prefix order, if \( u \) and \( v \) are prefix-comparable. If \( u, v \) are not prefix-comparable we can write \( u = pa_1x \) and \( v = pa_jy \) where \( p \in A^* \) is the longest common prefix of \( u \) and \( v \), where \( a_1, a_j \in A \) with \( a_1 \neq a_j \), and \( x, y \in A^* \); then the dictionary order between \( u \) and \( v \) is the same as the order between \( a_1 \) and \( a_j \). An injective partial function \( f : A^* \to A^* \) is dictionary order preserving if for all \( u, v \in \text{Dom}(f) : u \leq_{\text{dict}} v \) implies \( f(u) \leq_{\text{dict}} f(v) \). One easily proves that if \( f \) is dictionary order preserving then \( f^{-1} \) is also dictionary order preserving. The composition of dictionary order preserving maps yields a dictionary order preserving map. Thus \( \text{riAut}_{\text{dict}}(k) \) is an inverse submonoid of \( \text{riAut}(k) \).

We now proceed to the definition of the Thompson-Higman groups \( G_{k,1} \) and \( F_{k,1} \). For a right ideal automorphism \( \varphi : R_1 \to R_2 \), an essential restriction of \( \varphi \) is a right ideal automorphism \( \Phi : R'_1 \to R'_2 \) such that \( R'_1, R'_2 \) are finitely generated right ideals with \( R'_1 \subseteq R_1 \) and \( R'_2 \subseteq R_2 \). We also say that \( \varphi \) is an essential extension of \( \Phi \). Thompson [18] (see also [15] and [4]) proved that every \( \varphi \in \text{riAut}(k) \) has a unique maximal essential extension in \( \text{riAut}(k) \); we call it \( \text{max}(\varphi) \). He showed that an essential restriction (and, inversely, an essential extension) can be obtained by a finite number of steps of the following form: In the table \( \{(x_1, y_1), \ldots, (x_n, y_n)\} \) of \( \varphi \), replace some entry \( (x_i, y_i) \) by \( (x_ia_j, y_ia_j) : a_j \in A \). It follows that \( \text{max}(\varphi) \in \text{riAut}_{\text{dict}}(k) \) if \( \varphi \in \text{riAut}_{\text{dict}}(k) \). We now define \( G_{k,1} \) by

\[
G_{k,1} = \{ \text{max}(\varphi) : \varphi \in \text{riAut}(k) \}
\]

with multiplication

\[
\psi \cdot \varphi = \text{max}(\psi \circ \varphi).
\]

This multiplication is associative and turns \( G_{k,1} \) into a group whose identity is the identity map on \( A^* \). The map \( \eta : \varphi \mapsto \text{max}(\varphi) \) is a homomorphism from \( \text{riAut}(k) \) onto \( G_{k,1} \) (see [4]). We define \( F_{k,1} \) by

\[
F_{k,1} = \{ \text{max}(\varphi) : \varphi \in \text{riAut}_{\text{dict}}(k) \}.
\]

Then \( F_{k,1} \) is a subgroup of \( G_{k,1} \) and it is the homomorphic image of \( \text{riAut}_{\text{dict}}(k) \) by \( \eta \).

## 2 Basic properties of \( \text{riAut}(k) \) and \( \text{riAut}_{\text{dict}}(k) \)

We need some more facts about prefix codes. Recall that for any set \( S \subseteq A^* \), \( \text{pref}(S) \) is the set of all prefixes of strings in \( S \). When \( S \) is a prefix code we also define \( \text{spref}(S) = \text{pref}(S) \backslash S \), i.e., the set of strict prefixes of the strings in \( S \).

With any prefix code \( P \subseteq A^* \) one can associate a rooted tree, called the prefix tree of \( P \), whose vertex set is \( \text{pref}(P) \), whose edge set is \( \{(v, va_i) : a_i \in A, va_i \in \text{pref}(P)\} \), and whose root is \( \varepsilon \). The set of leaves of this tree is \( P \) itself. The non-leaves are called inner vertices of the prefix tree, so this set is \( \text{spref}(P) \). The subtree spanned by \( \text{spref}(P) \) is called the inner tree of \( P \), and the leaves of the inner tree are called the inner leaves.

It is well-known that for any maximal prefix code \( P \subseteq A^* \), \( |P| = 1 + (k - 1) \cdot i \), where \( i \) is the number of inner vertices of the prefix tree of \( P \) (see e.g. Lemma 6.1(0) in [3] for a proof and references). Conversely, for any integer \( i \geq 0 \) there exists a maximal prefix code \( P \subseteq A^* \) such that \( |P| = 1 + (k - 1) \cdot i \). To summarize:

**Lemma 2.1** Let \( A \) be a finite alphabet with \( |A| = k \), let \( P \subseteq A^* \) be any finite maximal prefix code, let \( V = \text{pref}(P) \) be the set of vertices of the prefix tree of \( P \), and let \( i \) be the number of inner vertices the prefix tree. Then the elements of \( P \) are the leaves of the prefix tree, so \( |V| = i + |P| \). Moreover,

\[
|P| = 1 + (k - 1) \cdot i,
\]

\[
|V| = 1 + ki = \frac{k}{k-1} \cdot |P|.
\]

\[ \square \]

**Lemma 2.2** If \( P_1, P_2 \subseteq A^* \) are finite maximal prefix codes and if \( P_2 A^* \subseteq P_1 A^* \) then \( |P_2| \geq |P_1| \).
Proof. If $P_2A^* \subseteq P_1A^*$, the prefix tree of $P_1$ is contained in the prefix tree of $P_2$, hence the prefix tree of $P_2$ has at least as many vertices as as the prefix tree of $P_1$. For maximal prefix codes, the number of leaves grows monotonically with the number of vertices (by Lemma 2.1), so the prefix tree of $P_2$ has at least as many leaves as the prefix tree of $P_1$. □

Lemma 2.3 For all $\varphi, \psi \in \riAut(k)$ : $|\domC(\psi \circ \varphi)| \geq \max\{|\domC(\varphi)|, |\domC(\psi)|\}$.

Proof. For any $\varphi, \psi \in \riAut(k)$ we have $\dom(\psi \circ \varphi) \subseteq \dom(\varphi) \cap \varphi^{-1}(\dom(\psi))$. Since $\dom(\psi \circ \varphi) \subseteq \dom(\varphi)$ it follows (by Lemma 2.2) that $|\domC(\psi \circ \varphi)| \geq |\domC(\varphi)|$. And since $\dom(\psi \circ \varphi) \subseteq \varphi^{-1}(\dom(\psi))$ it follows that $|\domC(\psi \circ \varphi)| \geq |\varphi^{-1}(\domC(\psi))| = |\domC(\psi)|$. □

In semigroup theory the Green relations play an important role in the structure of a semigroup. In a monoid $M$, the Green relations $\leq_J, \leq_R, \leq_L$ are preorders, defined as follows (see [8, 10, 12] for more details). For $s,t \in M$, we have $t \leq_J s$ iff $t = xsy$ for some $x,y \in M$; equivalently, every ideal that contains $s$ also contains $t$. Similarly, we have $t \leq_R s$ iff $t = sy$ for some $y \in M$, and $t \leq_L s$ iff $t = xs$ for some $x \in M$.

Proposition 2.4 The $J$-orders of $\riAut(k)$ and $\riAut_{dict}(k)$ are as follows, for all $\varphi_1, \varphi_2$ :

$\varphi_2 \leq_J \varphi_1 \iff |\domC(\varphi_2)| \geq |\domC(\varphi_1)|$.

Proof. $[\Rightarrow]$ If $\varphi_2 \leq_J \varphi_1$ then $\varphi_2 = \beta \varphi_1 \alpha$ for some $\beta, \alpha \in \riAut(k)$. This implies (by Lemma 2.3) that $|\domC(\varphi_2)| \geq |\domC(\varphi_1)|$.

$[\Leftarrow]$ Let $\varphi_1$ have table $P_i \rightarrow Q_i$ ($i = 1, 2$), with $|Q_2| = |P_2| \geq |P_1| = |Q_1|$. Since $P_1, Q_1, P_2, Q_2$ are maximal prefix codes, all have cardinalities of the form $|P_i| = |Q_i| = 1 + (k-1)n_i$, where $k = |A|$ and $n_i$ is the number of inner vertices of $P_i$ (which is the same as the number of inner vertices of $Q_i$).

For $\varphi \in \riAut(k)$ with table $P \rightarrow Q$, consider a restriction step; this consists of replacing some entry $(x,y)$ in the table of $\varphi$ by the set of entries $\{(x_{a_1}, y_{a_1}), \ldots, (x_{a_k}, y_{a_k})\}$. This is equivalent to replacing $\varphi$ by $\id_Q \circ \varphi \circ \id_P$ where $P' = (P - \{x\}) \cup xA$ and $Q' = (Q - \{y\}) \cup yA$.

By applying restriction steps to $\varphi_1$ we obtain $\Phi_1 = \id_{Q'_1} \circ \varphi_1 \circ \id_{P'_1}$ such that $|P'_1| = |Q'_1| = |P_2| = |Q_2|$. Let $[P_2 \rightarrow P'_1]$ and $[P'_1 \rightarrow P_2]$ be the dictionary-order preserving bijections from $P_2$ to $P'_1$, respectively from $P'_1$ to $P_2$. Then $\varphi_2 = \varphi_2 \circ \id_{P_1A^*} = \varphi_2 \circ [P'_1 \rightarrow P_2] \circ \Phi_1^{-1} \circ \Phi_1 \circ [P_2 \rightarrow P'_1]$. Hence $\varphi_2 \leq_J \Phi_1 \leq_J \varphi_1$.

When $\varphi_1, \varphi_2 \in \riAut_{dict}(k)$, the multipliers $\id_{P'_1}, \id_{Q'_1}, [P_1 \rightarrow P'_1], [P'_1 \rightarrow P_2], \varphi_2$, used in the proof, belong to $\riAut_{dict}(k)$, so the result holds for $\riAut_{dict}(k)$ too. □

By definition, a semigroup $S$ is finite-$J$-above iff each $s \in S$ the set $\{x \in S : x \geq_J s\}$ is finite. In $A^*$ there are only finitely many maximal prefix codes $P$ with a given cardinality $n = |P|$; precisely, it is the number of trees of degree $\leq k$ with $i = \frac{n-1}{k-1}$ vertices. Thus we have:

Corollary 2.5 The monoids $\riAut(k)$ and $\riAut_{dict}(k)$ are finite-$J$-above. □

Corollary 2.6 The monoid $\riAut(k)$ is a projective limit of finite inverse monoids, hence $\riAut(k)$ is residually finite.

Proof. Every semigroup $S$ is the projective limit of the Rees quotients $R_s = \{x \in S : x \geq_J s\} \cup \{0\}$, as $s$ ranges over $S$. By definition, the semigroup $R_s$ is the set $\{x \in S : x \geq_J s\}$ with a zero $0$ added. The multiplication in $R_s$ is $x \cdot y = xy$ (product in $S$) if $xy \geq_J s$, and $x \cdot y = 0$ if $xy \not{\geq_J} s$. So, $S$ maps homomorphically onto $R_s$ by mapping the ideal $\{x \in S : x \not{\geq_J} s\}$ to 0. (see [8, 10]). Clearly, $S$ is finite-$J$-above iff each Rees quotient semigroup $R_s$ is finite. □

The formula $|P| = 1 + i \cdot (|A| - 1)$, and the characterization of the $J$-order yield the following.
Corollary 2.7 The $\mathcal{J}$-classes of $\text{riAut}(k)$ form an $\omega$-chain $(J_i : i \in \omega)$, where $J_i = \{ \varphi : |\text{dom}(\varphi)| = 1 + i \cdot (|A| - 1) \}$ (and similarly for $\text{riAut}_{\text{dict}}(k)$).

All maximal subgroups of the $\mathcal{J}$-class $J_i \subset \text{riAut}(k)$ are isomorphic to the symmetric group $\mathfrak{S}_n$, where $n = 1 + i \cdot (|A| - 1)$. The group of units of $\text{riAut}(k)$ is $J_0$, and $|J_0| = 1$.

In $\text{riAut}_{\text{dict}}(k)$ all subgroups are trivial. \hfill \Box

The $\mathcal{R}$-order of $\text{riAut}(k)$ corresponds to the inclusion relation between finitely generated right ideal. We have for all $\varphi_1, \varphi_2 \in \text{riAut}(k)$: $\varphi_2 \leq_{\mathcal{R}} \varphi_1$ iff $\text{im}(\varphi_2) \subseteq \text{im}(\varphi_1)$ iff $\text{im}(\varphi_1) \subseteq \text{pref}(\text{im}(\varphi_2))$.

The $\mathcal{L}$-order of $\text{riAut}(k)$ corresponds to the refinement of right-congruences on $A^*$; for injective functions, this is equivalent to an inclusion of domains, i.e., we have for all $\varphi_1, \varphi_2 \in \text{riAut}(k)$: $\varphi_2 \leq_{\mathcal{L}} \varphi_1$ iff $\text{Dom}(\varphi_2) \subseteq \text{Dom}(\varphi_1)$ iff $\text{dom}(\varphi_1) \subseteq \text{pref}(\text{dom}(\varphi_2))$.

The set of idempotents of $\text{riAut}(k)$ is the set of partial identities $\text{id}_{P,A}^*$, where $P$ ranges over all maximal finite prefix codes. Hence, $\eta^{-1}(1)$ is the set of idempotents of $\text{riAut}(k)$.

For a semigroup $S$ a group homomorphism is, by definition, any homomorphism from $S$ onto a group. A group homomorphism $h_0 : S \to G_0$ is called maximum iff every group homomorphism $h : S \to G$ factors through $h_0$. For every inverse semigroup $S$, a maximum group homomorphism $h_0$ exists; $h_0$ is unique, except that $G_0$ is only determined up to isomorphism. The congruence on $S$ determined by $h_0$ is unique (see [10] 8).

In an inverse semigroup the natural partial order is defined by $t \leq s$ iff there exist idempotents $e, e'$ such that $t = se = e's$. A semigroup $S$ is called F-inverse iff $S$ is inverse, and every congruence class of the maximum group homomorphism of $S$ has exactly one maximum element (in the natural order). The uniqueness of maximum essential extension of right ideal isomorphisms of $A^*$ means that $\text{riAut}(k)$ and $\text{riAut}_{\text{dict}}(k)$ are F-inverse.

Proposition 2.8 The map $\eta : \text{riAut}(k) \to G_{k,1}$ and its restriction $\text{riAut}_{\text{dict}}(k) \to F_{k,1}$ are maximum group homomorphisms.

Proof. (1) Let $h : \text{riAut}(k) \to G$ be any group homomorphism. We want to show that for any $h : \text{riAut}(k) \to H$, if $\eta(\varphi) = \eta(\psi)$ then $h(\varphi) = h(\psi)$.

Let $P = \text{dom}(\varphi), P' = \text{im}(\varphi), Q = \text{dom}(\psi), Q' = \text{im}(\psi)$. The assumption $\eta(\varphi) = \eta(\psi)$ is equivalent to $\text{max}(\varphi) = \text{max}(\psi)$; let $g$ be this element of $G_{k,1}$. Then $\varphi = \text{id}_{P,A}^* \circ g \circ \text{id}_{P,A}^*$ and $\psi = \text{id}_{Q,A}^* \circ g \circ \text{id}_{Q,A}^*$. Hence $h(\varphi) = h(g) = h(\psi)$, since $h$ maps idempotents to the identity of $H$. \hfill \Box

Besides the maximum group homomorphism $\eta : \text{riAut}(k) \to G_{k,1}$ there are other homomorphisms on $\text{riAut}(k)$. For example, for any $i > 0$ let us define $\eta_i$ as the identity map on the $\mathcal{J}$-classes $J_0, \ldots, J_{i-1}$ of $\text{riAut}(k)$, and let $\eta_i$ be defined to be $\eta$ on all $J_j$ for $j \geq i$. Then the image monoid of $\eta_i$ is $\text{riAut}(k)_{i} = J_0 \cup \ldots \cup J_{i-1} \cup G'_{k,1}$, where $G'_{k,1}$ is an isomorphic copy of $G_{k,1}$, disjoint from $J_0 \cup \ldots \cup J_{i-1}$. This leads to an $\omega$-chain of homomorphisms

$\text{riAut}(k) \to \text{riAut}(k)_0 \to \text{riAut}(k)_1 \to \ldots \to \text{riAut}(k)_i \to \text{riAut}(k)_{i+1} \to \ldots$;

the direct limit of this chain is $G_{k,1}$. Correspondingly, there exists an $\omega$-chain of progressively finer congruences on $\text{riAut}(k)$ whose union is the congruence of the maximum group homomorphism.

3 Finite generation

Higman’s method for proving finite generation of $G_{k,1}$ ([11] p. 24-28) can be adapted to prove the following.

Theorem 3.1 The monoids $\text{riAut}(k)$ and $\text{riAut}_{\text{dict}}(k)$ are finitely generated.
A remark before we prove the Theorem: We saw in Lemma 2.1 that for any maximal prefix code \( P \subset A^* \) we have \( |P| = 1 + (k - 1) \cdot i \), where \( i \) is the number of inner vertices of the prefix tree of \( P \). Conversely, for any \( i \geq 3 \) there exists a maximal prefix code \( P \subset A^* \) such that \( |P| = 1 + (k - 1) \cdot i \). It follows that for all \( i \geq 3 \) there exists a maximal prefix code with at least two inner leaves. This means that for any \( n \) of the form \( n = 1 + (k - 1) \cdot i \) with \( i \geq 3 \) there exists a prefix code \( P \) of the form \( P = \{ ra_1, \ldots, ra_k, sa_1, \ldots, sa_k, z_{2k+1}, \ldots, z_n \} \). E.g., the tree with set of inner vertices \{ \varepsilon, a_1, a_2 \} has inner leaves \( a_1 \) and \( a_2 \); the corresponding maximal prefix code is \( \{ a_1, a_2 \} A \cup \{ a_3, \ldots, a_k \} \).

**Proof that \( riAut(k) \) is finitely generated:** The following Lemma provides a finite generating set.

**Lemma 3.2** The monoid \( riAut(k) \) is generated by the set of elements of \( riAut(k) \) whose domain codes have prefix trees with \( \leq 3 \) inner vertices.

**Proof.** Let \( \varphi \) be an element of \( riAut(k) \) with table \( \{ (x_1, y_1), \ldots, (x_n, y_n) \} \), where \( n = 1 + (k - 1) \cdot i \) with \( i \geq 4 \). Since \( i \geq 4 > 0 \) the prefix codes \( \text{domC}(\varphi) = \{ x_1, \ldots, x_n \} \) and \( \text{imC}(\varphi) = \{ y_1, \ldots, y_n \} \) each have at least one inner leaf in their respective prefix tree. Hence \( \text{domC}(\varphi) \) is of the form \( \{ ua_1, \ldots, ua_k, x_{i+1}, \ldots, x_n \} = \{ x_1, \ldots, x_n \} \), and \( \text{imC}(\varphi) \) is of the form \( \{ va_1, \ldots, va_k, y_{j+1}, \ldots, y_n \} = \{ y_1, \ldots, y_n \} \).

We say that the positions of \( \{ ua_1, \ldots, ua_k \} \) and \( \{ va_1, \ldots, va_k \} \) in the table of \( \varphi \) overlap iff the table contains \( (ua_i, va_j) \) for some \( i, j \).

**Case 1:** The positions of \( \{ ua_1, \ldots, ua_k \} \) and \( \{ va_1, \ldots, va_k \} \) in the table of \( \varphi \) do not overlap.

Then (for some ordering of the columns) the table of \( \varphi \) has the form

\[
\begin{bmatrix}
ua_1 & \ldots & ua_k & x_{k+1} & \ldots & x_{2k} & x_{2k+1} & \ldots & x_n \\
y_1 & \ldots & y_k & va_1 & \ldots & va_k & y_{2k+1} & \ldots & y_n \\
\end{bmatrix}.
\]

If \( i \geq 3 \) there exists a maximal prefix code with at least two inner leaves, of the form \( \{ ra_1, \ldots, ra_k, sa_1, \ldots, sa_k, z_{2k+1}, \ldots, z_n \} \).

We can insert this prefix code as a row into the table of \( \varphi \), yielding

\[
\begin{bmatrix}
ua_1 & \ldots & ua_k & x_{k+1} & \ldots & x_{2k} & x_{2k+1} & \ldots & x_n \\
r a_1 & \ldots & ra_k & sa_1 & \ldots & sa_k & z_{2k+1} & \ldots & z_n \\
y_1 & \ldots & y_k & va_1 & \ldots & va_k & y_{2k+1} & \ldots & y_n \\
\end{bmatrix}.
\]

This three-row table corresponds to a factorization \( \varphi = \varphi_2 \circ \varphi_1 \) where

\[
\varphi_1 = \begin{bmatrix}
ua_1 & \ldots & ua_k & x_{k+1} & \ldots & x_{2k} & x_{2k+1} & \ldots & x_n \\
r a_1 & \ldots & ra_k & sa_1 & \ldots & sa_k & z_{2k+1} & \ldots & z_n \\
\end{bmatrix},
\]

\[
\varphi_2 = \begin{bmatrix}
r a_1 & \ldots & ra_k & sa_1 & \ldots & sa_k & z_{2k+1} & \ldots & z_n \\
y_1 & \ldots & y_k & va_1 & \ldots & va_k & y_{2k+1} & \ldots & y_n \\
\end{bmatrix}.
\]

Then we also have the factorization \( \varphi = \psi_2 \circ \psi_1 \) where

\[
\psi_1 = \begin{bmatrix}
u & x_{k+1} & \ldots & x_{2k} & x_{2k+1} & \ldots & x_n \\
r & sa_1 & \ldots & sa_k & z_{2k+1} & \ldots & z_n \\
\end{bmatrix},
\]

\[
\psi_2 = \begin{bmatrix}
r a_1 & \ldots & ra_k & s & z_{2k+1} & \ldots & z_n \\
y_1 & \ldots & y_k & v & y_{2k+1} & \ldots & y_n \\
\end{bmatrix}.
\]

**Case 2:** The positions of \( \{ ua_1, \ldots, ua_k \} \) and \( \{ va_1, \ldots, va_k \} \) in the table of \( \varphi \) overlap.
Then the table of $\phi$ has the form
\[
\begin{bmatrix}
ua_1 & \ldots & \ldots & ua_k & \ldots & \ldots & \ldots & \ldots \\
\ldots & ua_{i_1} & \ldots & \ldots & va_{i_k} & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & va_{i_1} & \ldots & \ldots & va_{i_k} & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\end{bmatrix},
\]
where $ua_i$ is in column $i$ and row 1, and $va_{ij}$ is in column $i_j$ and row 2.

If $i \geq 4$ then a little calculation shows that for all $k \geq 2$: $n = 1 + (k - 1)i \geq 3k - 1$. The fact that $n \geq 3k - 1$ means that there are at least $k$ columns in the table, in addition to the $\leq 2k - 1$ columns occupied by $\{ua_1, \ldots, ua_k\}$ and $\{va_1, \ldots, va_k\}$. So we can insert two new rows, each corresponding to a prefix code with two inner leaves, as follows:
\[
\begin{bmatrix}
ua_1 & \ldots & \ldots & ua_k & \ldots & \ldots & \ldots & \ldots \\
ra_1 & \ldots & \ldots & ra_k & \ldots & \ldots & sa_1 & sa_k \\
\ldots & ra_{i_1} & \ldots & \ldots & ra_{i_k} & \ldots & sa_1 & sa_k \\
\ldots & va_{i_1} & \ldots & \ldots & va_{i_k} & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\end{bmatrix}.
\]

This four-row table corresponds to a factorization $\phi = \phi'_3 \circ \phi'_2 \circ \phi'_1$ where
\[
\phi'_1 = \begin{bmatrix}
ua_1 & \ldots & \ldots & ua_k & \ldots & \ldots & \ldots & \ldots \\
ra_1 & \ldots & \ldots & ra_k & \ldots & \ldots & sa_1 & sa_k \\
\ldots & ra_{i_1} & \ldots & \ldots & ra_{i_k} & \ldots & sa_1 & sa_k \\
\ldots & va_{i_1} & \ldots & \ldots & va_{i_k} & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\end{bmatrix},
\]
\[
\phi'_2 = \begin{bmatrix}
ra_1 & \ldots & \ldots & ra_k & \ldots & \ldots & sa_1 & sa_k \\
\ldots & ra_{i_1} & \ldots & \ldots & ra_{i_k} & \ldots & sa_1 & sa_k \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\end{bmatrix},
\]
\[
\phi'_3 = \begin{bmatrix}
\ldots & ra_{i_1} & \ldots & ra_{i_k} & \ldots & sa_1 & sa_k \\
\ldots & va_{i_1} & \ldots & va_{i_k} & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\end{bmatrix}.
\]

Then we also have the factorization $\phi = \psi'_3 \circ \psi'_2 \circ \psi'_1$ where
\[
\psi'_1 = \begin{bmatrix}
\ldots & \ldots & \ldots & \ldots & \ldots & sa_1 & sa_k \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & sa_1 & sa_k \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\end{bmatrix},
\]
\[
\psi'_2 = \begin{bmatrix}
r & \ldots & \ldots & sa_1 & sa_k \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
ra_{i_1} & \ldots & \ldots & ra_{i_k} & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\end{bmatrix},
\]
\[
\psi'_3 = \begin{bmatrix}
\ldots & \ldots & sa_1 & sa_k \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & v & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\end{bmatrix}.
\]

In both cases 1 and 2 the factors $\psi_1, \psi_2, \psi'_1, \psi'_2$ and $\psi'_3$ of $\phi$ have tables that have fewer columns than the table of $\phi$. We conclude, by induction, that every element $\phi \in riAut(k)$ can be written as a composition of elements of table-size $< 1 + 4(k - 1)$. Hence the table-size of these elements will be $\leq 1 + 3(k - 1)$ since a maximal prefix code has a size of the form $1 + i(k - 1)$.

There are only finitely many elements in $riAut(k)$ with table-size $\leq 1 + 3(k - 1)$, so $riAut(k)$ is finitely generated. This proves Theorem 3.1 for $riAut(k)$.  

\textbf{Proof that $riAut_{dict}(k)$ is finitely generated:} The following Lemma provides a finite generating set.

\textbf{Lemma 3.3} The monoid $riAut_{dict}(k)$ is generated by the set of elements of $riAut_{dict}(k)$ whose domain codes have prefix trees with $\leq k + 1$ inner vertices, i.e., whose table size is $\leq k^2$. 
The proof is similar to the proof of Lemma 3.2, with the added constraint that all factors must preserve the dictionary order. To ensure that all elements of $\text{riAut}(k)$ considered here preserve the dictionary order, we will write every maximal prefix code as a sequence, according to strictly increasing dictionary order. Since the alphabet $A$ is ordered (by $a_1 < \ldots < a_k$) the prefix tree of a prefix code is now an oriented tree, i.e., the set of children of every vertex is ordered. An element $\varphi \in \text{riAut}_{\text{dict}}(k)$ has a table $\begin{bmatrix} x_1 & \ldots & x_n \\ y_1 & \ldots & y_n \end{bmatrix}$ where $x_1 <_{\text{dict}} \ldots <_{\text{dict}} x_n$ and $y_1 <_{\text{dict}} \ldots <_{\text{dict}} y_n$. When we insert one or two rows into the table of $\varphi$, as we did in the proof of Lemma 3.2, the new rows must also be in increasing dictionary order.

In the proof of Lemma 3.2 we used the fact that for all $i \geq 3$ there exists a maximal prefix code with at least two inner leaves. For $\text{riAut}_{\text{dict}}(k)$ we need some control over the position of these inner leaves (according to the dictionary order of leaves of the prefix tree):

**Lemma 3.4** Let $P$ be a maximal prefix code, let $z$ be a leaf of the inner tree of $P$, let $\ell$ be the number of leaves of $P$ that are strictly to the left of $z$, and let $r$ be the number of leaves of $P$ that are strictly to the right of $z$. In other words, $|P| = \ell + k + r$ and $P$ is of the form

$$P = (x_1, \ldots, x_i, za_1, \ldots, za_k, x_{i+k+1}, \ldots, x_{i+k+r}).$$

Then if $|P| > 1 + (k-1)(k+1)$ ($= k^2$), there exists a maximal prefix code $Q$ such that:

- $|Q| = |P| = (\ell + k + r)$;
- $Q$ has an inner leaf $Z$ such that $Q$ has $\ell$ leaves strictly to the left of $Z$ and $r$ leaves strictly to the right of $Z$;
- $Q$ has an additional inner leaf $Z'$ ($\neq Z$).

**Proof.** If $P$ has two inner leaves we can take $Q$ to be $P$ itself. Let us assume now that $P$ has only one inner leaf, i.e., the inner tree of $P$ is just a path; let $z$ be the label of this path.

For reasons that will be clear below (Case 3) we assume that $z$ has length $|z| \geq k + 1$. This is always the case if the number of inner vertices of $P$ is at least $k+2$ (since the inner tree is a path), i.e., if $|P| \geq 1 + (k-1)(k+2)$. Equivalently (since $P$ is a maximal prefix code), $|P| > 1 + (k-1)(k+1)$.

The maximal prefix code $Q$ (with inner leaves $Z$, $Z'$, etc.) is constructed from the maximal prefix code $P$ by removing one edge from the inner path $z$, reconnecting, and possibly shifting, so as to make a new path $Z$ of length $|Z| = |z| - 1$. Next, an additional inner leaf is attached at an appropriate place on the side of the inner path $Z$. The details are given next. Note that $|z| \geq k + 1$ implies $|z| \geq 3$.

**Case 1:** $z$ contains $a_1$ and an additional letter $a_j \neq a_k$.

We have $z = ua_1v$ for some $u, v \in A^*$. To construct $Q$ from $P$ we remove an edge with label $a_1$ from the path $z$ and reconnect. The new path is $Z = uv$; also, $Z = Xa_jY$ with $j < k$, for some $X, Y \in A^*$. Since a vertex of the form $ua_1$ has no left-siblings, the replacement of $z$ by $Z$ does not change $\ell$; but the number of inner vertices has been decreased by 1. To preserve $|P|$ we attach an additional child to vertex $X$ on the right of $Xa_j$, i.e., we create a new inner vertex $Z' = Xa_{j+1}$ in $Q$.

**Case 2:** $z$ contains $a_k$ and an additional letter $a_i \neq a_1$.

This case is left-right symmetric to case 1, since preserving $|P|$ and $r$ is equivalent to preserving $|P|$ and $\ell$.

**Case 3:** $z$ contains no occurrences of $a_1$ nor $a_k$.

Then $z$ has the form $a_ja_{i_1} \ldots a_{i_{j-1}}w$ with $2 \leq j$, $i_1$, $\ldots$, $i_{j-1} \leq k-1$, and $w \in A^*$; recall that $|z| \geq k + 1$. We remove $a_j$ from $z$. This removes one vertex from the inner tree (since the inner tree is a path), and decreases $\ell$ by the amount $j - 1$. In order to preserve $\ell$ we let $Z = a_{i_1+1} \ldots a_{i_{j-1}+1}w$. In order to preserve the total number of inner vertices, and in order to create an additional inner leaf $Z'$ we add one inner vertex, namely $Z' = a_k$. 

8
Let us verify that his completes the construction of $Q$, i.e., that cases 1, 2, and 3 exhaust all possibilities. If case 3 does not hold, $z$ contains $a_1$ or $a_k$. If $z$ contains $a_1$ but case 1 does not hold, $z$ consists of $\geq k+1$ copies of $a_k$; then case 2 holds. If $z$ contains $a_k$ but case 2 does not hold, $z$ consists of $\geq k+1$ copies of $a_1$; then case 1 holds. \hfill$\Box$

**Proof of Lemma 3.3** Just as in the proof of Lemma 5.2 we can factor any element $\varphi \in \text{riAut}_{\text{dict}}(k)$ into a product of elements of $\text{riAut}_{\text{dict}}(k)$ with smaller tables, whenever the table of $\varphi$ has size $\geq 1 + (k-1)(k+1) = k^2$. \hfill$\Box$

Open problem: Are $\text{riAut}(k)$ and $\text{riAut}_{\text{dict}}(k)$ finitely presented?

### 4 The suffix expansion

For any monoid $M$ let $\mathcal{P}_{\text{fin}}(M)$ denote the set of finite subsets of $M$; the union operation makes $\mathcal{P}_{\text{fin}}(M)$ a semilattice. We define the left semidirect product $M \ltimes (\mathcal{P}_{\text{fin}}(M), \cup)$ with multiplication

$$(y, T) \cdot (x, S) = (yx, Tx \cup S),$$

where $Tx = \{tx : t \in T\}$. The subset $\{(x, S) \in M \ltimes \mathcal{P}_{\text{fin}}(M) : \{x, 1\} \subseteq S\}$ of $M \ltimes \mathcal{P}_{\text{fin}}(M)$ is closed under multiplication. Let $\Gamma$ be a generating set of $M$. By definition, the $\Gamma$-*generated suffix expansion* of $M$, denoted by $(M^\Sigma)_\Gamma$, is the submonoid of $M \ltimes \mathcal{P}_{\text{fin}}(M)$ generated by the subset $\{(\gamma, \{\gamma, 1\}) : \gamma \in \Gamma\}$. When $\Gamma$ is $M$ itself, $(M^\Sigma)_\Gamma$ is simply denoted by $M^\Sigma$. The monoid $(M^\Sigma)_\Gamma$ maps homomorphically onto $M$ by the projection $(x, S) \mapsto x$.

The transformation from $M$ to $M^\Sigma$ can also be applied to monoid homomorphisms, and thus becomes a functor. For details, see [3] and [5], where the suffix expansion was introduced and where many properties were proved. For example, for any group $G$ the inverse monoid $(G^\Sigma)_\Gamma$ is finite-$J$-above, hence it is a projective limit of finite inverse monoids [6]. The idea of semigroup expansions is due to John Rhodes (see [19]).

Dually (switching left and right) one defines the *prefix expansion* $(M^\Pi)_\Gamma$, as the submonoid generated by $\{(1, \gamma), \gamma \in \Gamma\}$ in the right semidirect product $(\mathcal{P}_{\text{fin}}(M), \cup) \rtimes M$. For any group $G$, $(G^\Pi)_\Gamma$ and $(G^\Pi)_\Gamma$ are isomorphic [5]; in this paper we will only work with the suffix expansion. Also [16], for a group the underlying set of $G^\Sigma$ is all of $\{(g, S) : g \in G, S \in \mathcal{P}_{\text{fin}}(G), \{g, 1\} \subseteq S\}$, and similarly for $G^\Pi$. Szendrei [16] proved that $(\cdot)^{\sim \Pi}$ is a functor from the category of groups to the category of F-inverse monoids, and that it is the left-adjoint of the maximum-group-image functor (i.e., the functor which maps an F-inverse semigroup to its maximum group homomorphic image).

The main result of this section is that for certain generating sets $\Gamma$ of $G_{k,1}$, the suffix expansion $(G_{k,1}^\Sigma)_\Gamma$ maps onto $\text{riAut}(k)$; similarly, $(F_{k,1}^\Sigma)_\Gamma$ maps onto $\text{riAut}(k)_{\text{dict}}$. We need some preliminary results.

**Lemma 4.1** Let $f_1 : X_1 \to X_2$, $f_2 : X_2 \to X_3$ be any partial functions. Then $\text{Dom}(f_2 \circ f_1) = \text{Dom}(f_1) \cap f_1^{-1}(\text{Dom}(f_2))$.

**Proof.** We have $x \in \text{Dom}(f_2 \circ f_1)$ iff $x \in \text{Dom}(f_1)$ and $f_1(x) \in \text{Dom}(f_2)$. The latter is equivalent to $x \in f_1^{-1}(\text{Dom}(f_2))$. \hfill$\Box$

We first give an embedding of $\text{riAut}(k)$ into a semidirect product of the Thompson-Higman group $G_{k,1}$ and a semilattice. Here each element of $G_{k,1}$ is represented by a maximally extended element of $\text{riAut}(k)$.

Let $I_\Sigma$ be the set of finitely generated essential right ideals of $A^*$. Each such ideal is of the form $PA^*$ where $P$ is a finite maximal prefix code. One can prove that the intersection of two essential right ideals is an essential right ideal ([4], Lemma A.2, p. 608), and that this intersection is finitely

---

Note: The above text is a transcription of the content visible in the image, formatted into a more readable and structured manner. It covers topics related to monoids, semigroups, and their expansions, including proofs and lemmas. The text is designed to be accessible to readers familiar with the basic concepts of algebra and category theory.
We consider the semidirect product $G$ generated (\[4\], Lemma 3.3, p. 579). Thus, $\mathcal{I}_R$ is closed under intersection, so $(\mathcal{I}_R, \cap)$ is a semilattice. We consider the semidirect product $G_{k,1} \rtimes (\mathcal{I}_R, \cap)$ with multiplication

$$(g_2, P_{2A^*}) \ast (g_1, P_{1A^*}) = (g_2 g_1, g_1^{-1}(P_{2A^*}) \cap P_{1A^*}).$$

It is easy to prove that this multiplication is associative. This semidirect product projects homomorphically onto $G_{k,1}$. Similarly, for the group $F_{k,1}$ we consider the submonoid $F_{k,1} \rtimes (\mathcal{I}_R, \cap)$ of $G_{k,1} \rtimes (\mathcal{I}_R, \cap)$.

Recall that $\eta$ denotes the surmorphism $\mathfrak{ri}(k) \to G_{k,1}$, or its restriction $\mathfrak{ri}(\mathfrak{dict}) \to F_{k,1}$.

**Proposition 4.2** The monoid $\mathfrak{ri}(k)$ is a retract of $G_{k,1} \rtimes \mathcal{I}_R$ by the maps $e : \varphi \in \mathfrak{ri}(k) \leftrightarrow (\eta(\varphi), \text{Dom}(\varphi)) \in G_{k,1} \rtimes \mathcal{I}_R$ (embedding), and $e' : (g, PA^*) \in G_{k,1} \rtimes \mathcal{I}_R \rightarrow g_{PA^*} \in \mathfrak{ri}(k)$, where $g_{PA^*}$ denotes the restriction of $g$ to $PA^*$. So $e(\mathfrak{ri}(k))$ is isomorphic to $\mathfrak{ri}(k)$.

A similar result holds for $F_{k,1}$, namely, $\mathfrak{ri}(\mathfrak{dict})$ is a retract of $F_{k,1} \rtimes \mathcal{I}_R$, and $e(\mathfrak{ri}(\mathfrak{dict}))$ is isomorphic to $\mathfrak{ri}(\mathfrak{dict})$. This is obtained by restricting $e$ to $\mathfrak{ri}(\mathfrak{dict}) \to F_{k,1} \rtimes \mathcal{I}_R$ and restricting $e'$ to $F_{k,1} \rtimes \mathcal{I}_R \to \mathfrak{ri}(\mathfrak{dict})$.

**Proof.** By the definition of the elements of $\mathfrak{ri}(k)$ the map $e$ is total and injective. That $e$ is a homomorphism follows from Lemma 4.1 and the fact that $\varphi(x) = (\eta(\varphi))(x)$ when $x \in \text{Dom}(\varphi)$. The restriction map $e' : (g, PA^*) \mapsto g_{PA^*} \in \mathfrak{ri}(k)$ is clearly surjective. It is a homomorphism by Lemma 4.1. The retraction property obviously holds, namely, $(e(\varphi))_{\text{Dom}(\varphi)} = \varphi$, and $e'$ is injective on $e(\mathfrak{ri}(k))$. $\square$

The map $e : \mathfrak{ri}(k) \to G_{k,1} \rtimes \mathcal{I}_R$ and its restriction $\mathfrak{ri}(\mathfrak{dict}) \to F_{k,1} \rtimes \mathcal{I}_R$ are not surjective; the respective images are

$$e(\mathfrak{ri}(k)) = \{(g, PA^*) \in G_{k,1} \rtimes \mathcal{I}_R : PA^* \subseteq \text{Dom}(g)\} \subseteq G_{k,1} \rtimes \mathcal{I}_R,$$

$$e(\mathfrak{ri}(\mathfrak{dict})) = \{(g, PA^*) \in F_{k,1} \rtimes \mathcal{I}_R : PA^* \subseteq \text{Dom}(g)\} \subseteq F_{k,1} \rtimes \mathcal{I}_R.$$

We now prove that the $\Gamma$-generated suffix expansions of the Thompson-Higman groups $G_{k,1}$ and $F_{k,1}$ map homomorphically onto $\mathfrak{ri}(k)$, respectively $\mathfrak{ri}(\mathfrak{dict})$. In the case of $G_{k,1}$ and $F_{k,1}$ (i.e. when $\Gamma = G_{k,1}$ respectively $F_{k,1}$), the “into”-part of Theorem 4.3 follows from Szendrei’s Corollary 3 in [10].

**Theorem 4.3**

1. For any generating set $\Gamma$ of the Thompson-Higman group $G_{k,1}$ the suffix expansion $(G_{k,1})_{\Gamma}$ maps homomorphically into $\mathfrak{ri}(k)$ by the map

$$\rho : (g, S) \in (G_{k,1})_{\Gamma} \mapsto (g, \bigcap_{h \in S} \text{Dom}(h)) \in e(\mathfrak{ri}(k)) \ (\simeq \mathfrak{ri}(k)).$$

Let us assume in addition that $\Gamma$ satisfies the following surjectiveness condition: There is a generating set $\Delta$ of $\mathfrak{ri}(k)$ such that

$$(\forall \delta \in \Delta)(\exists \gamma \in \Gamma) : \text{Dom}(\delta) = \text{Dom}(\gamma).$$

Then the homomorphism $\rho$ is onto $e(\mathfrak{ri}(k))$, and $e' \circ \rho$ is onto $\mathfrak{ri}(k)$.

2. Similarly, if $\Gamma$ is a generating set of the Thompson group $F_{k,1}$ then the suffix expansion $(F_{k,1})_{\Gamma}$ maps homomorphically into $\mathfrak{ri}(\mathfrak{dict})$, by restricting the map $e' \circ \rho$ to $(F_{k,1})_{\Gamma}$. This map is onto $\mathfrak{ri}(\mathfrak{dict})$ if $\Gamma$ satisfies the condition that there is a generating set $\Delta$ of $\mathfrak{ri}(\mathfrak{dict})$ such that $$(\forall \delta \in \Delta)(\exists \gamma \in \Gamma) : \text{Dom}(\delta) = \text{Dom}(\gamma).$$

10
Proof. (a) \( \rho : (G_{k,1}^-) \to G_{k,1} \times I_R \) is a homomorphism (for any generating set \( \Gamma \) of \( G_{k,1} \)):

For \((g_2, S_2), (g_1, S_1) \in (G_{k,1}^-)\), multiplication is defined by \((g_2, S_2) \cdot (g_1, S_1) = (g_2 g_1, S_2 g_1 \cup S_1)\), thus
\[
\rho((g_2, S_2) \cdot (g_1, S_1)) = (g_2 g_1, \cap_{h \in S_2 g_1 \cup S_1} \text{Dom}(h)).
\]
Moreover,
\[
\cap_{h \in S_2 g_1 \cup S_1} \text{Dom}(h) = \cap_{k \in S_2 g_1} \text{Dom}(k) \cap \cap_{h_1 \in S_1} \text{Dom}(h_1)
\]
\[
= \cap_{h_2 \in S_2} \text{Dom}(h_2) \cap \cap_{h_1 \in S_1} \text{Dom}(h_1);
\]
the last equality holds since \(\text{Dom}(h_2 g_1) = g_1^{-1}(\text{Dom}(h_2)) \cap \text{Dom}(g_1)\) (by Lemma 4.1). Also, since \(g_1 \in S_1\) we have \(\text{Dom}(g_1) \cap \cap_{h_1 \in S_1} \text{Dom}(h_1) = \cap_{h_1 \in S_1} \text{Dom}(h_1)\). Thus we have
\[
\rho((g_2, S_2) \cdot (g_1, S_1)) = (g_2 g_1, g_1^{-1}(\cap_{h_2 \in S_2} \text{Dom}(h_2)) \cap \cap_{h_1 \in S_1} \text{Dom}(h_1)).
\]
A straightforward multiplication in \(G_{k,1} \times I_R\) shows that the latter is also equal to the product \(\rho((g_2, S_2)) \ast \rho((g_1, S_1))\).

(b) \( \rho \) maps \((G_{k,1}^-)\) into \(e(\text{riAut}(k))\) (for any generating set \( \Gamma \) of \( G_{k,1} \)):

We want to show that for every \((g, S) \in (G_{k,1}^-)\), \(\rho((g, S)) = (g, \cap_{h \in S} \text{Dom}(h))\) is equal to \((g, PA^*)\) for some finite maximal prefix code \(P \subset A^*\) such that \(PA^* \subseteq \text{Dom}(g)\). We saw that the intersection of finitely many finitely generated essential right ideals is a finitely generated essential right ideal, so \(\cap_{h \in S} \text{Dom}(h) = PA^*\) for some finite maximal prefix code \(P\). Moreover, \(g \in S\) for every \((g, S) \in (G_{k,1}^-)\), hence \((PA^*) = \cap_{h \in S} \text{Dom}(h) \subseteq \text{Dom}(g)\).

(c) \( \rho \) maps \((G_{k,1}^-)\) onto \(e(\text{riAut}(k))\) (if \( \Gamma \) satisfies the surjectiveness condition):

Let \( \Gamma \) be a generating set of \( G_{k,1} \) satisfying the condition of the Theorem, and let \( \Delta \) be a corresponding generating set of \( \text{riAut}(k) \). To show that \( \rho \) maps onto \( e(\text{riAut}(k)) \) it is sufficient to show that \( e(\Delta) \) is in the image of \( \rho \).

By the definition of \( e \) (in Prop. 12), for any \( \delta \in \Delta \), \( e(\delta) \) is of the form \( e(\delta) = (g, PA^*) \), where \( g = \eta(\delta) \in G_{k,1} \) and \( P = \text{domC}(\delta) \), with \( PA^* \subseteq \text{Dom}(g)\). By the condition of the Theorem there exists \( \gamma \in \Gamma \) such that \( \text{domC}(\gamma) = \text{domC}(\delta) = P \). Then \( \gamma^{-1} \circ \gamma = \text{id}_{PA^*} \), so \( \delta = g \circ \gamma^{-1} \circ \gamma \) (product in \( \text{riAut}(k) \)). Then, by multiplying in \( (G_{k,1}^-) \) we obtain
\[
\rho((g, \{g, 1\}) \cdot (\gamma^{-1}, \{\gamma^{-1}, 1\}) \cdot (\gamma, \{\gamma, 1\})) = \rho((g, \{g, 1\}) \cdot (1, \{\gamma^{-1}, 1\}) \gamma \cup \{\gamma, 1\}))
\]
\[
= \rho((g, \{g, 1\}) \cdot (1, \{\gamma, 1\})) = (g, \text{Dom}(g)) \cdot (1, PA^*) = (g, 1^{-1}(\text{Dom}(g)) \cap PA^*)
\]
\[
= (g, PA^*) \text{, since } PA^* \subseteq \text{Dom}(g).
\]
Thus, \((g, PA^*) = e(\delta) = \rho((g, \{g, 1\}) \cdot (\gamma^{-1}, \{\gamma^{-1}, 1\}) \cdot (\gamma, \{\gamma, 1\})) \in \rho((G_{k,1}^-))\). So \(e(\delta)\) is in \(\rho((G_{k,1}^-))\) for every \(\delta \in \Delta\).

(d) The same proof applies to \((F_{k,1}^-) \to \text{riAut}_{\text{dict}}(k)\). □

We will prove next that the surjectiveness condition in Theorem 4.3 holds for some, but not all generating sets \( \Gamma \), and that it is necessary. We first need a Lemma.

**Lemma 4.4** For every finite maximal prefix code \(P \subset A^*\) there is an element \(\varphi \in F_{k,1} \subset G_{k,1}\) such that \(P = \text{domC}(\varphi)\) (when \(\varphi\) is in maximally extended form).

**Proof.** Let \(|P| = 1 + i (k - 1)\) where \(i\) is the number of inner vertices of the prefix tree of \(P\). Consider the maximal prefix code \(Q\) whose inner tree consists of the path \(a_1^{i-2}a_2\). Hence the set of inner vertices of \(Q\) is \(\text{pref}(a_1^{i-2}a_2)\), and \(Q\) has only one inner leaf. Also, \(Q\) has \(i\) inner vertices, so \(|Q| = |P|\).

If \(Q \neq P\) then \(P\) does not have \(a_1^{i-2}a_2\) as an inner leaf. Indeed, if the inner tree of \(P\) is not a path, it will not contain any path of length \(i - 1\); and if \(P\) is a path but \(P \neq Q\), this path is different from...
Proof. (1) Let $\Delta$ be any generating set of $\text{riAut}(k)$ there exists a generating set $\Gamma$ of $G_{k,1}$ that satisfies the surjectiveness condition of Theorem 4.3 (namely, for every $\delta \in \Delta$ there exists $\gamma \in \Gamma$ with $\text{Dom}(\delta) = \text{Dom}(\gamma)$).

If $\Delta$ is finite then $\Gamma$ is finite and $|\Gamma| \leq 2 \cdot |\Delta|$.

The generating set $\Gamma = G_{k,1}$ also satisfies the surjectiveness condition.

(2) The condition on $\Gamma$ in Theorem 4.3 is necessary for the surjectiveness of $\rho$, in general.

(3) Not every generating set $\Gamma$ of $G_{k,1}$ satisfies the surjectiveness condition. More strongly, for some generating set $\Gamma$ of $G_{2,1}$ there is no surjective homomorphism from $(G_{k,1}^{-L})_e$ onto $\text{riAut}(k)$.

Proposition 4.5

1. For every generating set $\Delta$ of $\text{riAut}(k)$ there exists a generating set $\Gamma$ of $G_{k,1}$ that satisfies the surjectiveness condition of Theorem 4.3 (namely, for every $\delta \in \Delta$ there exists $\gamma \in \Gamma$ with $\text{Dom}(\delta) = \text{Dom}(\gamma)$).

If $\Delta$ is finite then $\Gamma$ is finite and $|\Gamma| \leq 2 \cdot |\Delta|$.

The generating set $\Gamma = G_{k,1}$ also satisfies the surjectiveness condition.

2. The condition on $\Gamma$ in Theorem 4.3 is necessary for the surjectiveness of $\rho$, in general.

3. Not every generating set $\Gamma$ of $G_{k,1}$ satisfies the surjectiveness condition. More strongly, for some generating set $\Gamma$ of $G_{2,1}$ there is no surjective homomorphism from $(G_{k,1}^{-L})_e$ onto $\text{riAut}(k)$.

Proof. (1) Let $\Delta$ be any generating set of $\text{riAut}(k)$. By Lemma 4.4, for each $\delta \in \Delta$ there exists $\varphi_\delta \in F_{k,1}$ with $\text{domC}(\varphi_\delta) = \text{domC}(\delta)$. Let $\Gamma = \eta(\Delta) \cup \{\varphi_\delta : \delta \in \Delta\}$. Then $\Gamma$ has the claimed properties. When $\Delta$ is finite we have $|\Gamma| \leq |\eta(\Delta)| + |\{\varphi_\delta : \delta \in \Delta\}| \leq 2 \cdot |\Delta|$. In Section 3 we proved that $\text{riAut}(k)$ has a finite generating set.

For $\Gamma = G_{k,1}$ and $\Delta = \text{riAut}(k)$, every finite maximal prefix code $P$ occurs as a domain code of an element of $G_{k,1}$ and as the domain code of an element of $\text{riAut}(k)$; so the surjectiveness condition of Theorem 4.3 applies to $\Gamma$.

(2) For any finite generating set $\Gamma$ of $G_{k,1}$ the corresponding generating set of $(G_{k,1}^{-L})_e$ is $\tilde{\Gamma} = \{\gamma, \{\gamma, 1\} : \gamma \in \Gamma\}$. If Theorem 4.3 holds for $\Gamma$, i.e., $\Gamma$ is such that $\rho : (G_{k,1}^{-L})_e \rightarrow e(\text{riAut}(k))$ is surjective, then $\rho(\tilde{\Gamma}) = \{\gamma, \text{Dom}(\gamma) : \gamma \in \Gamma\}$ is a generating set of $e(\text{riAut}(k))$. Hence $\Gamma = \eta(\Delta)$ for some generating set $\Delta$ of $\text{riAut}(k)$.

Moreover, $\rho(\Delta) = \rho(\tilde{\Gamma}) = \{\gamma, \text{Dom}(\gamma) : \gamma \in \Gamma\}$, so for every for every $\delta \in \Delta$, $\rho(\delta)$ is of the form $(\gamma_\delta, \text{Dom}(\gamma_\delta))$ for some $\gamma_\delta \in \Gamma$; so, $\text{Dom}(\delta) = \text{Dom}(\gamma_\delta)$. So for every $\delta \in \Delta$ there exists $\gamma_\delta \in \Gamma$ such that $\text{Dom}(\delta) = \text{Dom}(\gamma_\delta)$. Thus, if $\Gamma$ is such that the map $\rho$ in Theorem 4.3 is surjective, then there exists a generating set $\Delta$ as required by the surjectiveness condition of 4.3.

(3) An example is the four-element generating set of $G_{2,1}$ given in [7] (pp. 240-241); let us call this generating set $\Gamma_{\text{CFP}}$. The elements of $\Gamma_{\text{CFP}}$ all have domain codes of cardinality 3 or 4. But any generating set of $\text{riAut}(2)$ needs to contain an element with domain code of cardinality 2, since composition cannot make domain codes smaller.

It follows that the elements of $\Gamma_{\text{CFP}}$ do not have all the domain codes of any generating set of $\text{riAut}(2)$, so $\Gamma_{\text{CFP}}$ does not satisfy the surjectiveness condition of Theorem 4.3.

It follows also that if $\Delta$ is a generating set of $\text{riAut}(k)$, then $\eta(\Delta) \neq \Gamma_{\text{CFP}}$. Indeed, $\Delta$ contains elements of table-size 2 (as we just saw), so $\eta(\Delta)$ also has elements of table-size $\leq 2$ (since application of $\eta$ means taking the maximum essential extension, hence the table-size cannot increase). But $\Gamma_{\text{CFP}}$ has no element of table-size $\leq 2$.

More strongly, let $\theta$ be any surjective homomorphism $\theta : (G_{k,1}^{-L})_e \rightarrow \text{riAut}(k)$. Then $\Delta = \theta(\tilde{\Gamma})$ is a generating set of $\text{riAut}(k)$, hence $\eta(\Delta)$ is a generating set of $G_{2,1}$. This rules out $\Gamma_{\text{CFP}}$, since $\eta(\Delta)$ cannot be equal to $\Gamma_{\text{CFP}}$. □
Proposition 4.6

(1) For every generating set \( \Delta \) of \( \text{riAut}_{\text{dict}}(k) \) there exists a generating set \( \Gamma \) of \( F_{k,1} \) that satisfies the surjectiveness condition of Theorem 4.3 (namely, \( \eta(\Delta) \subseteq \Gamma \), and for every \( \delta \in \Delta \) there exists \( \gamma \in \Gamma \) with \( \text{Dom}(\delta) = \text{Dom}(\gamma) \)).

If \( \Delta \) is finite then \( \Gamma \) is finite, and \( |\Delta| \leq 2 \cdot |\Gamma| \).

The generating set \( \Gamma = F_{k,1} \) satisfies the surjectiveness condition.

(2) The condition on \( \Gamma \) in Theorem 4.3 are necessary for the surjectiveness, in general.

(3) Not every generating set \( \Gamma \) of \( F_{k,1} \) satisfies the surjectiveness condition. More strongly, for some generating set \( \Gamma \) of \( F_{2,1} \) there is no surjective homomorphism from \( (F_{k,1})^{*} \) onto \( \text{riAut}_{\text{dict}}(k) \).

Proof. For (1) and (2) the proof is the same as for Proposition 4.5.

(3) An example is the two-element generating set \( \{B, B^{-1}A\} \) of \( F_{2,1} \) derived from the generating set \( \{A, B\} \) given in [7] (pp. 222 and 224). The elements have domain codes of size 4 (for \( B \)) or 5 (for \( B^{-1}A \)). But any generating set \( \Delta \) of \( \text{riAut}_{\text{dict}}(\{a_1, a_2\}^{*}) \) needs to contain an element with domain code of size 3, since composition cannot make domain codes smaller. It follows that the generating set \( \{B, B^{-1}A\} \) does not contain \( \eta(\Delta) \) for any generating set \( \Delta \) of \( \text{riAut}(\{a_1, a_2\}^{*}) \). The rest of the proof is as for Proposition 4.5 \( \square \)

Corollary 4.7

- The suffix expansion \( G_{k,1}^{\sim} \) maps onto \( \text{riAut}(k) \) and \( F_{k,1}^{\sim} \) maps onto \( \text{riAut}_{\text{dict}}(k) \).
- For every finite generating set \( \Delta \) of \( \text{riAut}(k) \) (or of \( \text{riAut}_{\text{dict}}(k) \)) there exists a finite generating set \( \Gamma \) of \( G_{k,1} \) (respectively \( F_{k,1} \)) with \( |\Gamma| \leq 2 \cdot |\Delta| \), such that the \( \Gamma \)-generated suffix expansion \( (G_{k,1}^{\sim})^{\Gamma} \) maps onto \( \text{riAut}(k) \) (respectively \( (F_{k,1}^{\sim})^{\Gamma} \) maps onto \( \text{riAut}_{\text{dict}}(k) \)).
- There also exist finite generating sets \( \Gamma \) of \( G_{k,1} \) such that \( (G_{k,1}^{\sim})^{\Gamma} \) admits no surjective homomorphism onto \( \text{riAut}(k) \). Similarly, there exist finite generating sets \( \Gamma \) of \( F_{k,1} \) such that \( (F_{k,1}^{\sim})^{\Gamma} \) has no surjective homomorphism onto \( \text{riAut}_{\text{dict}}(k) \).

Proof. This follows from Theorem 4.3 and Propositions 4.5, 4.6 \( \square \)

Remark. The fact that \( \text{riAut}(k) \) is a homomorphic image of \( (G_{k,1}^{\sim})^{\Gamma} \) for some finite generating set \( \Gamma \) of \( G_{k,1} \) (Theorem 4.3 and Proposition 4.5) implies that \( \text{riAut}(k) \) is finitely generated (and similarly for \( \text{riAut}_{\text{dict}}(k) \), using Proposition 4.6). However, at this point this does not provide a new proof that \( \text{riAut}(k) \) and \( \text{riAut}_{\text{dict}}(k) \) are finitely generated, because we used finite generation in the proofs of Propositions 4.5 and 4.6.

Remark. The results in Theorem 4.3 and Propositions 4.5, 4.6 show that different finite generating sets of \( G_{k,1} \) or \( F_{k,1} \) can have very different properties, and the characterization of these finite generating sets is non-trivial.

5 Miscellaneou

5.1 The map \( (G_{k,1}^{\sim})^{\Gamma} \rightarrow \text{riAut}(k) \) is finite-to-one

We give a property of the map \( \rho : (G_{k,1}^{\sim})^{\Gamma} \rightarrow \text{riAut}(k) \) showing that \( (G_{k,1}^{\sim})^{\Gamma} \) and \( \text{riAut}(k) \) are very close.

Proposition 5.1 Let \( \Gamma \) be any generating set of \( G_{k,1} \) (possibly infinite). The map \( \rho \) is finite-to-one, i.e., \( \rho^{-1}(\varphi) \) is finite for every \( \varphi \in \text{riAut}(k) \). It follows that \( (F_{k,1}^{\sim})^{\Gamma} \rightarrow \text{riAut}_{\text{dict}}(k) \) is also finite-to-one.
Proof. For any \( \varphi \in \riAut(k) \) let \((g, S) \in (G_{k,1})_{\Gamma} \) be such that \( \rho(g, S) = \varphi \). Then \( g = \max(\varphi) \), so \( g \) is uniquely determined by \( \varphi \). Moreover, for every \( h \in S \) we have \( \Dom(\varphi) \subseteq \Dom(h) \), hence, \( \domC(h) \subseteq \text{pref}(\domC(\varphi)) \). Therefore there are only finitely many choices for \( \domC(h) \). Hence, since \( |\text{imC}(h)| = |\domC(h)| \) and since there are only finitely many maximal prefix codes of a given cardinality (over a given alphabet), there are only finitely many choices for \( \text{imC}(h) \). Finally, since there are only finitely many bijections \( \domC(h) \rightarrow \text{imC}(h) \), there are only finitely many choices for \( h \). \( \square \)

5.2 The word problem for the suffix expansion of a group, and for \( \riAut(k) \)

We will see that the word problem for the suffix expansion of a monoid is closely related to the following problem. Let \( M \) be a monoid and let \( \Gamma \) be a generating set of \( M \). The set word problem of \( M \) over \( \Gamma \) is specified as follows:

Input: Two finite subsets \( U = \{u_1, \ldots, u_m\} \) and \( V = \{v_1, \ldots, v_n\} \) of \( \Gamma^* \).

Question: Is \( U = V \) when all strings \( u_i, v_j \) are evaluated in \( M \) ?

Lemma 5.2 The set word problem of the monoid \( M \) with generating set \( \Gamma \) can be reduced to the word problem of \( M \) over \( \Gamma \) by a polynomial-time AND-of-OR’s truth-table reduction.

Proof. We have \( U = V \) iff \( U \subseteq V \) and \( V \subseteq U \). And we have \( U \subseteq V \) iff the following boolean formula is true:

\[
\bigwedge_{u_i \in U} \bigvee_{v_j \in V} (u_i =_M v_j).
\]

This formula involves \( n \times m \) calls to the word problem of \( M \). \( \square \)

Corollary 5.3 Let \( M \) be a monoid with generating set \( \Gamma \). The word problem of the suffix expansion \((M^L)_{\Gamma}\) over \( \Gamma \) can be reduced to the word problem of \( M \) over \( \Gamma \) by a polynomial-time AND-of-OR’s truth-table reduction.

Proof. Let \( \langle x = y \rangle \) be an input for the word problem of \((M^L)_{\Gamma}\), where \( x = x_m \ldots x_1, y = y_n \ldots y_1 \), with \( x_i, y_j \in \Gamma \). Let us denote the value of a string \( w \in \Gamma^* \) in \( M \) by \( (w)_M \). Then the value of \( x_m \ldots x_1 \) in \((M^L)_{\Gamma}\) is

\[
\{(x_m \ldots x_1)_M, \{(x_m \ldots x_1)_M, \ldots, (x_2 x_1)_M, (x_1)_M, 1\}\},
\]

and similarly for \( y_n \ldots y_1 \). Thus, the word problem of \((M^L)_{\Gamma}\) reduces to the conjunction of the word problem of \( M \) and the set word problem of \( M \). Lemma 5.2 then yields the result. \( \square \)

Corollary 5.4 The word problem of the suffix expansion \((G_{\sim \ell})_{\Gamma}\) of the Thompson-Higman group \( G_{k,1} \) over a finite generating set \( \Gamma \) is in \( \mathcal{P} \).

Proof. This follows from Corollary 5.3 and the fact that the word problem of \( G_{k,1} \) over a finite generating set is in \( \mathcal{P} \) (proved in [4], and strengthened to co-context-free in [13]). \( \square \)

Proposition 5.5 The word problem of \( \riAut(k) \) over any finite generating set is in \( \mathcal{P} \).

Proof. Let \( \Delta \) be a finite generating set of \( \riAut(k) \). Given a string \( x_n \ldots x_1 \in \Delta^* \), the table for the value of \( x_n \ldots x_1 \) in \( \riAut(k) \) can be computed by simple composition. It was proved in [4] (Theorem 4.1) that this takes polynomial time; in fact it also belongs to the parallel complexity class \( \mathcal{AC}_1 \), which is a subclass of \( \mathcal{P} \). \( \square \)
6 Appendix: Monoids of right ideal homomorphisms

Composing two right-ideal homomorphisms of \( A^* \) yields again a right-ideal homomorphism. By \( \text{riHom}(k) \) we denote the monoid of all right-ideal homomorphisms between finitely generated right ideals of \( A^* \) (where \( |A| = k \)), with function composition as multiplication.

**Lemma 6.1** For every \( \varphi \in \text{riHom}(k) \), the image \( \text{Im}(\varphi) \) is a finitely generated right ideal, but there exists \( \varphi \in \text{riHom}(k) \) such that \( \varphi(\text{domC}(\varphi)) \) is not a prefix code.

**Proof.** Let \( P = \text{domC}(\varphi) \) (a finite prefix code) and \( \text{Dom}(\varphi) = PA^* \). Then \( \text{Im}(\varphi) = \varphi(\text{domC}(\varphi)) \), hence \( \text{Im}(\varphi) \) is a finitely generated right ideal.

It is easy to find examples where \( \varphi(P) \) is not a prefix code. E.g., when \( P = \{a, b\} \) and \( \varphi \) is defined by the table \( \{(a, a), (b, aa)\} \), then \( \varphi(P) = \{a, aa\} \). \( \square \)

In [1] (section 3.1) it was proved that \( \varphi(\text{domC}(\varphi)) \) is a prefix code iff the partition determined by \( \varphi \) on \( \text{Dom}(\varphi) \) is a prefix congruence. This inspires the following.

**Definition 6.2** Within the monoid \( \text{riHom}(k) \) we define the submonoid
\[
\text{riHom}_{pc}(k) = \{ \varphi \in \text{riHom}(k) : \varphi(\text{domC}(\varphi)) \text{ is a prefix code} \}.
\]
The elements of \( \text{riHom}_{pc}(k) \) are said to be prefix code preserving.

The subscript “pc” stands for “prefix code”. It is easy to check that \( \text{riHom}_{pc}(k) \) is indeed a monoid. The reason for calling the elements of \( \text{riHom}_{pc}(k) \) “prefix code preserving” is the following.

**Proposition 6.3** For every \( \varphi \in \text{riHom}(k) \) we have: \( \varphi(\text{domC}(\varphi)) \) is a prefix code iff for every prefix code \( P \subset A^* \), \( \varphi(P) \) is a prefix code.

**Proof.** The right-to-left implication is trivial. To prove the left-to-right implication, let \( x_1, x_2 \in \text{Dom}(\varphi) \) be prefix incomparable, but assume by contradiction that \( \varphi(x_2) = \varphi(x_1)w \), for some non-empty \( w \in A^* \). Since \( x_1, x_2 \in \text{Dom}(\varphi) \), there are \( p_1, p_2 \in \text{domC}(\varphi) \) such that \( x_1 = p_1u_1, x_2 = p_2u_2 \) (for some \( u_1, u_2 \in A^\ast \)). Then \( \varphi(x_2) = \varphi(x_1)w \) implies \( \varphi(p_2)u_2 = \varphi(p_1)u_1w \). This implies that \( \varphi(p_2) \) and \( \varphi(p_1) \) are prefix comparable, which contradicts the assumption that \( \varphi(\text{domC}(\varphi)) \) is a prefix code. \( \square \)

The following further demonstrates the importance of the monoid \( \text{riHom}_{pc}(k) \).

**Proposition 6.4** Every \( \varphi \in \text{riHom}(k) \) has an essential restriction to some element of \( \text{riHom}_{pc}(k) \).

**Proof.** It is straightforward to restrict \( \varphi \) to some element \( \Phi \) whose image code is \( \text{imC}(\Phi) = A^\ell \), where \( \ell \) is the length of a longest string in \( \varphi(\text{domC}(\varphi)) \). Obviously, \( A^\ell \) is a prefix code. \( \square \)

The Thompson-Higman monoid \( M_{k,1} \) (introduced in [2]) is a homomorphic image of \( \text{riHom}(k) \) and of \( \text{riHom}_{pc}(k) \). Indeed, an element of \( M_{k,1} \) is an equivalence class of elements of \( \text{riHom}(k) \) or of \( \text{riHom}_{pc}(k) \) where two elements \( \varphi_1 \) and \( \varphi_2 \) are considered equivalent iff they can be obtained from each other by a finite number of essentially equal restrictions and essentially equal extensions.

As a generalization of the monoid \( \text{riAut}(k) \) that we introduced earlier, we consider the monoid \( \text{riIso}(k) \) consisting of all right-ideal isomorphisms between finitely generated ideals (not necessarily essential) of \( A^* \). For \( \text{riIso}(k) \) and in particular, for \( \text{riAut}(k) \), we have:

---

1 A right-congruence \( \equiv \) on a right ideal \( R \subseteq A^* \) is called a prefix congruence iff there is a finite prefix code \( P \) and a partition \( \equiv_{P} \) on \( P \) such that for all \( x_1, x_2 \in R \): \( x_1 \equiv x_2 \iff (\exists w \in A^*) (\exists p_1, p_2 \in P) [p_1 \equiv_P p_2, x_1 = p_1w, p_2 = x_2w] \).
Proposition 6.5  Every element \( \varphi \in \text{riIso}(k) \) is prefix-code preserving.

Proof.  For \( \varphi \in \text{riIso}(k) \) let \( P = \text{domC}(\varphi) \) (a finite prefix code) and let \( Q = \varphi(P) \). If \( Q \) is not a prefix code then there exist \( q_1 \neq q_2 \in Q \) with \( q_2 = q_1 v \) for some \( v \in A^*, v \neq \varepsilon \). Since \( \varphi \) is an injective homomorphism there exist \( p_1 \neq p_2 \in P \) such that \( q_1 = \varphi(p_1) \neq \varphi(p_2) = q_2 = \varphi(p_1 v) \). By injectiveness, \( p_2 = p_1 v \), which contradicts the fact that \( P \) is a prefix code. \( \square \)

As a consequence, \( \text{riIso}(k) \) consists of all right-ideal isomorphisms \( \varphi \) such that \( \text{domC}(\varphi) \) and \( \varphi(\text{domC}(\varphi)) = \text{imC}(\varphi) \) are prefix codes (not necessarily maximal). And \( \text{riAut}(k) \) consists of all right-ideal isomorphisms \( \varphi \) such that \( \text{domC}(\varphi) \) and \( \varphi(\text{domC}(\varphi)) = \text{imC}(\varphi) \) are maximal prefix codes. The notation \( \text{riAut} \), where “Aut” stands for automorphism, is motivated by the fact that \( \text{riAut}(k) \) maps onto the group \( G_{k,1} \).

Note that \( \text{riIso}(k) \) does not map onto \( G_{k,1} \). Indeed, \( \text{riIso}(k) \) has a zero (the empty map), the only group that \( \text{riIso}(k) \) maps onto is the one-element group.

References

[1] J.C. Birget, “The \( \mathcal{R} \)- and \( \mathcal{L} \)-orders of the Thompson-Higman monoid \( M_{k,1} \) and their complexity”, International J. of Algebra and Computation, 20.4 (June 2010) 489-524.

[2] J.C. Birget, “Monoid generalizations of the Richard Thompson groups”, J. of Pure and Applied Algebra, 215(2) (Feb. 2009) 264-278.

[3] J.C. Birget, “Circuits, coNP-completeness, and the groups of Richard Thompson”, International J. of Algebra and Computation 16(1) (Feb. 2006) 35-90.

[4] J.C. Birget, “The groups of Richard Thompson and complexity”, International J. of Algebra and Computation 14(5,6) (Dec. 2004) 569-626. (Preprint: Mathematics ArXiv [math.GR/0204292] Apr. 2002).

[5] J.C. Birget, J. Rhodes, “Almost finite expansions of arbitrary semigroups”, J. of Pure and Applied Algebra 32 (1984) 239-287.

[6] J.C. Birget, J. Rhodes, “Group theory via global semigroup theory”, J. of Algebra 120 (1989) 284-300.

[7] J. W. Cannon, W. J. Floyd, W. R. Parry, “Introductory notes on Richard Thompson’s groups”, L’Enseignement Mathématique 42 (1996) 215-256.

[8] A.H. Clifford, G.B. Preston, The Algebraic Theory of Semigroups, Vol. 1 (Mathematical Survey, No 7 (I)) American Mathematical Society, Providence (1961).

[9] S. Eilenberg, Automata, Languages, and Machines, Vol. B, Academic Press (1976).

[10] P.A. Grillet, Semigroups, An Introduction to the Structure Theory, Marcel Dekker, New York (1995).

[11] G. Higman, “Finitely presented infinite simple groups”, Notes on Pure Mathematics 8, The Australian National University, Canberra (1974).

[12] M.V. Lawson, Inverse Semigroups, World Scientific (1998).

[13] J. Lehnert, P. Schweitzer, “Context-Freeness of Higman-Thompson group’s co-word problem”, Bulletin of the London Mathematical Society 39(2) (2007) 235-241.

[14] R. McKenzie, R.J. Thompson, “An elementary construction of unsolvable word problems in group theory”, in Word Problems, (W. W. Boone, F. B. Cannonito, R. C. Lyndon, editors), North-Holland (1973) pp. 457-478.

[15] E.A. Scott, “A construction which can be used to produce finitely presented infinite simple groups”, J. of Algebra 90 (1984) 294-322.
[16] M.B. Szendrei, “A note on Birget-Rhodes expansion of groups”, J. of Pure and Applied Algebra 58(1) (1989) 93-99.

[17] Richard J. Thompson, Manuscript (1960s).

[18] Richard J. Thompson, “Embeddings into finitely generated simple groups which preserve the word problem”, in Word Problems II, (S. Adian, W. Boone, G. Higman, editors), North-Holland (1980) pp. 401-441.

[19] B. Tilson, “Complexity of semigroups and morphisms”, Chapter XII in [9].

Jean-Camille Birget
Dept. of Computer Science
Rutgers University at Camden
Camden, NJ 08102, USA
birget@camden.rutgers.edu