Monoid generalizations of the Richard Thompson groups

Jean-Camille Birget *

May 13, 2014

Abstract

The groups $G_{k,1}$ of Richard Thompson and Graham Higman can be generalized in a natural way to monoids, that we call $M_{k,1}$, and to inverse monoids, called $Inv_{k,1}$; this is done by simply generalizing bijections to partial functions or partial injective functions. The monoids $M_{k,1}$ have connections with circuit complexity (studied in another paper). Here we prove that $M_{k,1}$ and $Inv_{k,1}$ are congruence-simple for all k. Their Green relations J and D are characterized: $M_{k,1}$ and $Inv_{k,1}$ are J-0-simple, and they have $k-1$ non-zero D-classes. They are submonoids of the multiplicative part of the Cuntz algebra $\mathcal{O}_k$. They are finitely generated, and their word problem over any finite generating set is in P. Their word problem is coNP-complete over certain infinite generating sets.

1 Thompson-Higman monoids

Since their introduction by Richard J. Thompson in the mid 1960s [25, 22, 26], the Thompson groups have had a great impact on infinite group theory. Graham Higman generalized the Thompson groups to an infinite family [17]. These groups and some of their subgroups have appeared in many contexts and have been widely studied; see for example [9, 5, 12, 7, 14, 15, 6, 8, 20].

The definition of the Thompson-Higman groups lends itself easily to generalizations to inverse monoids and to more general monoids. These monoids are also generalizations of the finite symmetric monoids (of all functions on a set), and this leads to connections with circuit complexity; more details on this appear in [1, 2, 4].

By definition the Thompson-Higman group $G_{k,1}$ consists of all maximally extended isomorphisms between finitely generated essential right ideals of A^*, where A is an alphabet of cardinality k. The multiplication is defined to be composition followed by maximal extension: for any $\varphi, \psi \in G_{k,1}$, we have $\varphi \cdot \psi = \max(\varphi \circ \psi)$. Every element $\varphi \in G_{k,1}$ can also be given by a bijection $\varphi : P \to Q$ where $P, Q \subset A^*$ are two finite maximal prefix codes over A; this bijection can be described concretely by a finite function *table*. For a detailed definition according to this approach, see [3] (which is also similar to [24], but with a different terminology); moreover, Subsection 1.1 gives all the needed definitions.

It is natural to generalize the maximally extended *isomorphisms* between finitely generated essential right ideals of A^* to *homomorphisms*, and to drop the requirement that the right ideals be essential. It will turn out that this generalization leads to interesting monoids, or inverse monoids, which we call Thompson-Higman monoids. Our generalization of the Thompson-Higman groups to monoids will also generalize the embedding of these groups into the Cuntz algebras [3, 23], which provides an additional motivation for our definition. Moreover, since these homomorphisms are close to being arbitrary finite string transformations, there is a connection between these monoids and combinational boolean circuits; the study of the connection between Thompson-Higman groups and circuits was started in [4, 2] and will be developed more generally for monoids in [1]; the present paper lays some of the foundations for [1].

*Supported by NSF grant CCR-0310793.

1.1 Definition of the Thompson-Higman groups and monoids

Before defining the Thompson-Higman monoids we need some basic definitions, that are similar to the introductory material that is needed for defining the Thompson-Higman groups $G_{k,1}$; we follow [3] (which is similar to [24]). We use an alphabet A of cardinality $|A| = k$, and we list its elements as $A = \{a_1, \ldots, a_k\}$. Let A^* denote the set of all finite *words* over A (i.e., all finite sequences of elements of A); this includes the *empty word* ε. The *length* of $w \in A^*$ is denoted by $|w|$; let A^n denote the set of words of length n. For two words $u, v \in A^*$ we denote their *concatenation* by uv or by $u \cdot v$; for sets $B, C \subseteq A^*$ the concatenation is $BC = \{uv : u \in B, v \in C\}$. A *right ideal* of A^* is a subset $R \subseteq A^*$ such that $RA^* \subseteq R$. A generating set of a right ideal R is a set C such that R is the intersection of all right ideals that contain C; equivalently, $R = CA^*$. A right ideal R is called *essential* iff R has a non-empty intersections with every right ideal of A^*. For words $u, v \in A^*$, we say that u is a *prefix* of v iff there exists $z \in A^*$ such that $uz = v$. A *prefix code* is a subset $C \subseteq A^*$ such that no element of C is a prefix of another element of C. A prefix code is *maximal* iff it is not a strict subset of another prefix code. 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; this prefix code is maximal iff R is an essential right ideal.

For right ideals $R' \subseteq R \subseteq A^*$ we say that R' is *essential in* R iff R' intersects all right subideals of R in a non-empty way.

Tree interpretation: The free monoid A^* can be pictured by its right Cayley graph, which is the rooted infinite regular k-ary tree with vertex set A^* and edge set $\{(v, va) : v \in A^*, a \in A\}$. We simply call this the *tree of* A^*. It is a directed tree, with all paths moving away from the root ε (the empty word); by "path" we will always mean a directed path. A word v is a prefix of a word w iff v is is an ancestor of w in the tree. A set P is a prefix code iff no two elements of P are on the same path. A set R is a right ideal iff any path that starts in R has all its vertices in R. The prefix code that generates R consists of the elements of R that are maximal (within R) in the prefix order, i.e., closest to the root ε. A finitely generated right ideal R is essential iff every infinite path of the tree eventually reaches R (and then stays in it from there on). Similarly, a finite prefix code P is maximal iff any infinite path starting at the root eventually intersects P. For two finitely generated right ideals $R' \subset R$, R' is essential in R iff any infinite path starting in R eventually reaches R' (and then stays in R' from there on). In other words for right ideals $R' \subseteq R$, R' is essential in R iff R' and R have the same *ends*.

For the prefix tree of A^* we can consider also the "boundary" A^ω (i.e., all infinite words). In Thompson's original definition [25, 26], $G_{2,1}$ was given by a total action on $\{0,1\}^\omega$. In [3] this total action was extended to a partial action on $A^* \cup A^\omega$; the partial action on $A^* \cup A^\omega$ is uniquely determined by the total action on A^ω; it is also uniquely determined by the partial action on A^*. Here, as in [3], we only use the partial action on A^*.

Definition 1.1 *A* right ideal homomorphism *of A^* is a total function $\varphi : R_1 \to A^*$ such that R_1 is a right ideal of A^*, and for all $x_1 \in R_1$ and all $w \in A^*$: $\varphi(x_1 w) = \varphi(x_1)\, w$.*

For any partial function $f : A^* \to A^*$, let $\mathrm{Dom}(f)$ denote the domain and let $\mathrm{Im}(f)$ denote the image (range) of f. For a right ideal homomorphism $\varphi : R_1 \to A^*$ it is easy to see that the image $\mathrm{Im}(\varphi)$ is also right ideal of A^*, which is finitely generated (as a right ideal) if the domain $R_1 = \mathrm{Dom}(\varphi)$ is finitely generated.

A right ideal homomorphism $\varphi : R_1 \to R_2$, where $R_1 = \mathrm{Dom}(\varphi)$ and $R_2 = \mathrm{Im}(\varphi)$, can be described by a function $P_1 \to S_2$, with $P_1, S_2 \subset A^*$; here P_1 is the prefix code (not necessarily maximal) that generates R_1 as a right ideal, and S_2 is a set (not necessarily a prefix code) that generates R_2 as a right ideal; so $R_1 = P_1 A^*$ and $R_2 = S_2 A^*$. The function $P_1 \to S_2$ corresponding to $\varphi : R_1 \to R_2$ is called the *table* of φ. The prefix code P_1 is called the *domain code* of φ and we write $P_1 = \mathrm{domC}(\varphi)$. When S_2 is a prefix code we call S_2 the *image code* of φ and we write $S_2 = \mathrm{imC}(\varphi)$.

Definition 1.2 *An injective right ideal homomorphism is called a right ideal* isomorphism. *A right ideal homomorphism $\varphi : R_1 \to R_2$ is called* total *iff the domain right ideal R_1 is essential. And φ is called* surjective *iff the image right ideal R_2 is essential.*

The table $P_1 \to P_2$ of a right ideal isomorphism φ is a bijection between prefix codes (that are not necessarily maximal). The table $P_1 \to S_2$ of a *total* right ideal homomorphism is a function from a *maximal* prefix code to a set, and the table $P_1 \to S_2$ of a surjective right ideal homomorphism is a function from a prefix code to a set that generates an essential right ideal. The word "total" is justified by the fact that if a homomorphism φ is total (and if $\mathrm{domC}(\varphi)$ is finite) then $\varphi(w)$ is defined for every word that is long enough (e.g., when $|w|$ is longer than the longest word in the domain code P_1); equivalently, φ is defined from some point onward on every infinite path in the tree of A^* starting at the root.

Definition 1.3 *An* essential restriction *of a right ideal homomorphism $\varphi : R_1 \to A^*$ is a right ideal homomorphism $\Phi : R_1' \to A^*$ such that R_1' is essential in R_1, and such that for all $x_1' \in R_1'$: $\varphi(x_1') = \Phi(x_1')$.*

We say that φ is an essential extension *of Φ iff Φ is an essential restriction of φ.*

Note that if Φ is an essential restriction of φ then $R_2' = \mathrm{Im}(\Phi)$ will automatically be essential in $R_2 = \mathrm{Im}(\varphi)$. Indeed, if I is any non-empty right subideal of R_1 then $I \cap R_1' \neq \varnothing$, hence $\varnothing \neq \Phi(I \cap R_1') \subseteq \Phi(I) \cap \Phi(R_1') = \Phi(I) \cap R_2'$; moreover, any right subideal J of R_2 is of the form $J = \Phi(I)$ where $I = \Phi^{-1}(J)$ is a right subideal of R_1; hence, for any right subideal J of R_2, $\varnothing \neq J \cap R_2'$.

Proposition 1.4 (1) *Let φ, Φ be homomorphisms between* finitely generated *right ideals of A^*, where $A = \{a_1, \ldots, a_k\}$. Then Φ is an essential restriction of φ iff Φ can be obtained from φ by starting from the table of φ and applying a finite number of* restriction steps *of the following form: Replace (x, y) in a table by $\{(xa_1, ya_1), \ldots, (xa_k, ya_k)\}$.*
(2) *Every homomorphism between finitely generated right ideals of A^* has a* unique maximal essential *extension.*

Proof. (1) Consider a homomorphism between finitely generated right ideals $\varphi : R_1 \to R_2$, let P_1 be the finite prefix code that generates the right ideal R_1, and let $S_2 = \varphi(P_1)$, so S_2 generates the right ideal R_2.

If $x \in P_1$ and $y = \varphi(x) \in S_2$ then (since φ is a right ideal homomorphism), $ya_i = \varphi(xa_i)$ for $i = 1, \ldots, k$. Then $R_1 - \{x\}$ is a right ideal which is essential in R_1, and $R_1 - \{x\}$ is generated by $(P_1 - \{x\}) \cup \{xa_1, \ldots, xa_k\}$. Indeed, in the tree of A^* every downward directed path starting at vertex x goes through one of the vertices xa_i. Thus, removing (x, y) from the graph of φ is an essential restriction; for the table of φ, the effect is to replace the entry (x, y) by the set of entires $\{(xa_1, ya_1), \ldots, (xa_k, ya_k)\}$. If finitely many restriction steps of the above type are carried out, the result is again an essential restriction of φ.

Conversely, let us show that if Φ is an essential restriction of φ then Φ can be obtained by a finite number of replacement steps of the form "replace (x, y) by $\{(xa_1, ya_1), \ldots, (xa_k, ya_k)\}$ in the table".

Using the tree of A^* we have: If R and R' are right ideals of A^* generated by the finite prefix codes P, respectively P', and if R' is essential in R then every infinite path from P intersects P'. It follows from this characterization of essentiality and from the finiteness of P_1 and P_1' that $R_1 - R_1'$ is finite.

Hence φ and Φ differ only in finitely many places, i.e., one can transform φ into Φ in a finite number of restriction steps.

So, the restriction Φ of φ is obtained by removing a finite number of pairs (x, y) from φ; however, not every such removal leads to a right ideal homomorphism or an essential restriction of φ. If (x_0, y_0) is removed from φ then x_0 is removed from R_1 (since φ is a function). Also, since R_1' is a right ideal, when x_0 is removed then all prefixes of x_0 (equivalently, all ancestor vertices of x_0 in the tree of A^*) have to be removed. So we have the following removal rule (still assuming that domain and image right ideals are finitely generated):

If Φ is an essential restriction of φ then φ can be transformed into Φ by removing a finite set of strings from R_1, with the following restriction: If a string x_0 is removed then all prefixes of x_0 are also removed from R_1; moreover, x_0 is removed from R_1 iff $(x_0, \varphi(x_0))$ is removed from φ.

As a converse of this rule, we claim that if the transformation from φ to Φ is done according to this rule, then Φ is an essential restriction of φ. Indeed, Φ will be a right ideal homomorphism: if $\Phi(x_1)$ is defined then $\Phi(x_1 z)$ will also be defined (if it were not, the prefix x_1 of $x_1 z$ would have been removed), and $\Phi(x_1 z) = \varphi(x_1 z) = \varphi(x_1)\ z = \Phi(x_1)\ z$. Moreover, $\mathrm{Dom}(\Phi) = R_1'$ will be essential in R_1: every directed path starting at R_1 eventually meets R_1' because only finitely many words were removed from R_1 to form R_1'. Hence by the tree characterization of essentiality, R_1' is essential in R_1.

In summary, if Φ is an essential restriction of φ then Φ is obtained from φ by a finite sequence of steps, each of wich removes one pair $(x, \varphi(x))$. In $\mathrm{Dom}(\varphi)$ the string x is removed. The domain code becomes $(P_1 - \{x\}) \cup \{xa_1, \ldots, xa_k\}$, since $\{xa_1, \ldots, xa_k\}$ is the set of children of x in the tree of A^*. This means that in the table of φ, the pair $(x, \varphi(x))$ is replaced by $\{(xa_1, \varphi(x)\, a_1), \ldots, (xa_k, \varphi(x)\, a_k)\}$.

(2) Uniqueness of the maximal essential extension: By (1) above, essential extensions are obtained by the set of rewrite rules of the form $\{(xa_1, ya_1), \ldots, (xa_k, ya_k)\} \to (x, y)$, applied to tables. This rewriting system is *locally confluent* (because different rules have non-overlapping left sides) and *terminating* (because they decrease the length); hence maximal essential extensions exist and are unique. $\square$

Proposition 1.4 yields another tree interpretation of essential restriction: Assume first that a total order $a_1 < a_2 < \ldots < a_k$ has been chosen for the alphabet A; this means that the tree of A^* is now an *oriented* rooted tree, i.e., the children of each vertex v have a total order (namely, $va_1 < va_2 < \ldots < va_k$). The rule "replace (x, y) in the table by $\{(xa_1, ya_1), \ldots, (xa_k, ya_k)\}$" has the following tree interpretation: Replace x and $y = \varphi(x)$ by the children of x, respectively of y, matched according to the order of the children.

Important remark:
As we saw, every right ideal homomorphism can be described by a table $P \to S$ where P is a prefix code and S is a set. But we also have: Every right ideal homomorphism φ has an essential restriction φ' whose table $P' \to Q'$ is such that *both P' and Q' are prefix codes*; moreover, Q' can be chosen to be a subset of A^n for some $n \le \max\{|s| : s \in S\}$. Example (with alphabet $A = \{a, b\}$):
$\left(\begin{array}{c|c} a & b \\ a & aa \end{array}\right)$ has an essential restriction $\left(\begin{array}{c|c|c} aa & ab & b \\ aa & ab & aa \end{array}\right)$.

Definition 1.5 *The Thompson-Higman* partial function monoid $M_{k,1}$ *consists of all maximal essential extensions of homomorphisms between finitely generated right ideals of A^*. The multiplication is composition followed by maximal essential extension.*

In order to prove *associativity* of the multiplication of $M_{k,1}$ we define the following and we prove a few Lemmas.

Definition 1.6 *By RI_k we denote the monoid of all right ideal homomorphisms between finitely generated right ideals of A^*, with function composition as multiplication. We consider the equivalence relation $\equiv$ defined for $\varphi_1, \varphi_2 \in RI_k$ by: $\varphi_1 \equiv \varphi_2$ iff $\max(\varphi_1) = \max(\varphi_2)$.*

It is easy to prove that RI_k is closed under composition. Moreover, by existence and uniquess of the maximal essential extension (Prop. 1.4(2)) each $\equiv$-equivalence class contains exactly one element of $M_{k,1}$. We want to prove:

Proposition 1.7 *The equivalence relation $\equiv$ is a monoid congruence on RI_k, and $M_{k,1}$ is isomorphic (as a monoid) to $RI_k/\equiv$. Hence, $M_{k,1}$ is associative.*

First some Lemmas.

Lemma 1.8 *If $R'_i \subseteq R_i$ $(i = 1, 2)$ are finitely generated right ideals with R'_i essential in R_i, then $R'_1 \cap R'_2$ is essential in $R_1 \cap R_2$.*

Proof. We use the tree characterization of essentiality. Any infinite path p in $R_1 \cap R_2$ is also in R_i $(i = 1, 2)$, hence p eventually enters into R'_i. Thus p eventually meets R'_1 and R'_2, i.e., p meets $R'_1 \cap R'_2$. $\Box$

Lemma 1.9 *All $\varphi_1, \varphi_2 \in RI_k$ have restrictions $\Phi_1, \Phi_2 \in RI_k$ (not necessarily essential restrictions) such that:*

- $\Phi_2 \circ \Phi_1 = \varphi_2 \circ \varphi_1$, *and*
- $\mathrm{Dom}(\Phi_2) = \mathrm{Im}(\Phi_1) = \mathrm{Dom}(\varphi_2) \cap \mathrm{Im}(\varphi_1)$.

Proof. Let $R = \mathrm{Dom}(\varphi_2) \cap \mathrm{Im}(\varphi_1)$. This is a right ideal which is finitely generated since $\mathrm{Dom}(\varphi_2)$ and $\mathrm{Im}(\varphi_1)$ are finitely generated (see Lemma 3.3 of [3]). Now we restrict φ_1 to Φ_1 in such a way that $\mathrm{Im}(\Phi_1) = R$ and $\mathrm{Dom}(\Phi_1) = \varphi_1^{-1}(R)$, and we restrict φ_2 to Φ_2 in such a way that $\mathrm{Dom}(\Phi_2) = R$ and $\mathrm{Im}(\Phi_2) = \varphi_2(R)$. Then $\Phi_2 \circ \Phi_1(.)$ and $\varphi_2 \circ \varphi_1(.)$ agree on $\varphi_1^{-1}(R)$; moreover, $\mathrm{Dom}(\Phi_2 \circ \Phi_1) = \varphi_1^{-1}(R)$. Since $\varphi_2 \circ \varphi_1(x)$ is only defined when $\varphi_1(x) \in R$, we have $\Phi_2 \circ \Phi_1 = \varphi_2 \circ \varphi_1$. Also, by the definition of R we have $\mathrm{Dom}(\Phi_2) = \mathrm{Im}(\Phi_1)$. $\Box$

Lemma 1.10 *For all $\varphi_1, \varphi_2 \in RI_k$ we have:*

$$\max(\varphi_2 \circ \varphi_1) = \max(\max(\varphi_2) \circ \varphi_1) = \max(\varphi_2 \circ \max(\varphi_1)).$$

Proof. We only prove the first equality; the proof of the second one is similar. By Lemma 1.9 we can restrict φ_1 and φ_2 to φ'_1, respectively φ'_2, so that $\varphi'_2 \circ \varphi'_1 = \varphi_2 \circ \varphi_1$, and $\mathrm{Dom}(\varphi'_2) = \mathrm{Im}(\varphi'_1) = \mathrm{Dom}(\varphi_2) \cap \mathrm{Im}(\varphi_1)$; let $R' = \mathrm{Dom}(\varphi_2) \cap \mathrm{Im}(\varphi_1)$.

Similarly we can restrict φ_1 and $\max(\varphi_2)$ to φ''_1, respectively φ''_2, so that $\varphi''_2 \circ \varphi''_1 = \max(\varphi_2) \circ \varphi_1$, and $\mathrm{Dom}(\varphi''_2) = \mathrm{Im}(\varphi''_1) = \mathrm{Dom}(\max(\varphi_2)) \cap \mathrm{Im}(\varphi_1)$; let $R'' = \mathrm{Dom}(\max(\varphi_2)) \cap \mathrm{Im}(\varphi_1)$.

Obviously, $R' \subseteq R''$ (since φ_2 is a restriction of $\max(\varphi_2)$). Moreover, R' is essential in R'', by Lemma 1.8; indeed, $\mathrm{Dom}(\varphi_2)$ is essential in $\mathrm{Dom}(\max(\varphi_2))$ since $\max(\varphi_2)$ is an essential extension of φ_2. Since R' is essential in R'', $\varphi_2 \circ \varphi_1$ is an essential restriction of $\max(\varphi_2) \circ \varphi_1$. Hence by uniqueness of the maximal essential extension, $\max(\max(\varphi_2) \circ \varphi_1) = \max(\varphi_2 \circ \max(\varphi_1))$. $\Box$

Proof of Prop. 1.7: If $\varphi_2 \equiv \psi_2$ then, by definition, $\max(\varphi_2) = \max(\psi_2)$, hence by Lemma 1.10:

$$\max(\varphi_2 \circ \varphi) = \max(\max(\varphi_2) \circ \varphi) = \max(\max(\psi_2) \circ \varphi) = \max(\psi_2 \circ \varphi),$$

for all $\varphi \in RI_k$. Thus (by the definition of $\equiv$), $\varphi_2 \circ \varphi \equiv \psi_2 \circ \varphi$, so $\equiv$ is a right congruence. Similarly one proves that $\equiv$ is a left congruence. Thus, $RI_k/\equiv$ is a monoid.

Since every $\equiv$-equivalence class contains exactly one element of $M_{k,1}$ there is a one-to-one correspondence between $RI_k/\equiv$ and $M_{k,1}$. Moreover, the map $\varphi \in RI_k \longmapsto \max(\varphi) \in M_{k,1}$ is a homomorphism, by Lemma 1.10 and by the definition of multiplication in $M_{k,1}$. Hence $RI_k/\equiv$ is isomorphic to $M_{k,1}$. $\Box$

1.2 Other Thompson-Higman monoids

We now introduce a few more families of Thompson-Higman monoids, whose definition comes about naturally in analogy with $M_{k,1}$.

Definition 1.11 *The Thompson-Higman* total *function monoid* $totM_{k,1}$ *and the Thompson-Higman* surjective *function monoid* $surM_{k,1}$ *consist of maximal essential extensions of homomorphisms between finitely generated right ideals of* A^* *where the domain, respectively, the image ideal, is an* essential *right ideal.*

The Thompson-Higman inverse *monoid* $Inv_{k,1}$ *consists of all maximal essential extensions of isomorphisms between finitely generated (not necessarily essential) right ideals of* A^**.*

Every element $\varphi \in totM_{k,1}$ can be described by a function $P \to Q$, called the *table* of φ, where $P, Q \subset A^*$ with P a finite *maximal* prefix code over A. A similar description applies to $surM_{k,1}$ but now with Q a finite maximal prefix code. Every $\varphi \in Inv_{k,1}$ can be described by a bijection $P \to Q$ where $P, Q \subset A^*$ are two finite prefix codes (not necessarily maximal).

It is easy to prove that essential extension and restriction of right ideal homomorphisms, as well as composition of such homomorphisms, preserve injectiveness, totality, and surjectiveness. Thus $totM_{k,1}$, $surM_{k,1}$, and $Inv_{k,1}$ are submonoids of $M_{k,1}$.

We also consider the intersection $totM_{k,1} \cap surM_{k,1}$, i.e., the monoid of all maximal essential extensions of homomorphisms between finitely generated essential right ideals of A^*; we denote this monoid by $totsurM_{k,1}$. The monoids $M_{k,1}$, $totM_{k,1}$, $surM_{k,1}$, and $totsurM_{k,1}$ are *regular* monoids. (A monoid M is regular iff for every $m \in M$ there exists $x \in M$ such that $mxm = m$.) The monoid $Inv_{k,1}$ is an inverse monoid. (A monoid M is inverse iff for every $m \in M$ there exists one and only one $x \in M$ such that $mxm = m$ and $x = xmx$.)

We consider the submonoids $totInv_{k,1}$ and $surInv_{k,1}$ of $Inv_{k,1}$, described by bijections $P \to Q$ where $P, Q \subset A^*$ are two finite prefix codes with P, respectively Q maximal. The (unique) inverses of elements in $totInv_{k,1}$ are in $surInv_{k,1}$, and vice versa, so these submonoids of $Inv_{k,1}$ are not regular monoids. We have $totInv_{k,1} \cap surInv_{k,1} = G_{k,1}$ (the Thompson-Higman group).

It is easy to see that for all $n > 0$, $M_{k,1}$ contains the symmetric monoids PF_{k^n} of all partial functions on k^n elements, represented by all elements of $M_{k,1}$ with a table $P \to Q$ where $P, Q \subseteq A^n$. Hence $M_{k,1}$ contains all finite monoids. Similarly, $totM_{k,1}$ contains the symmetric monoids F_{k^n} of all total functions on k^n elements. And $Inv_{k,1}$ contains $\mathcal{I}_{k^n}$ (the finite symmetric inverse monoid of all injective partial functions on A^n).

1.3 Cuntz algebras and Thompson-Higman monoids

All the monoids, inverse monoids, and groups, defined above, are submonoids of the multiplicative part of the Cuntz algebra $\mathcal{O}_k$.

The Cuntz algebra $\mathcal{O}_k$, introduced by Dixmier [13] (for $k = 2$) and Cuntz [11], is a k-generated star-algebra (over the field of complex numbers) with identity element $\mathbf{1}$ and zero $\mathbf{0}$, given by the following finite presentation. The generating set is $A = \{a_1, \ldots, a_k\}$. Since this is defined as a star-algebra, we automatically have the star-inverses $\{\overline{a}_1, \ldots, \overline{a}_k\}$; for clarity we use overlines rather than stars.

Relations of the presentation:

$\overline{a}_i a_i = \mathbf{1}$, for $i = 1, \ldots, k$;

$\overline{a}_i a_j = \mathbf{0}$, when $i \neq j$, $1 \le i, j \le k$;

$a_1 \overline{a}_1 + \ldots + a_k \overline{a}_k = \mathbf{1}$.

It is easy to verify that this defines a star-algebra. The Cuntz algebras are actually C*-algebras with many remarkable properties (proved in [11]), but here we only need them as star-algebras, without their norm and Cauchy completion.

In [3] and independently in [23] it was proved that the Thompson-Higman group $G_{k,1}$ is the subgroup of $\mathcal{O}_k$ consisting of the elements that have an expression of the form $\sum_{x \in P} f(x)\ \overline{x}$ where we require the following: P and Q range over all finite maximal prefix codes over the alphabet $\{a_1, \ldots, a_k\}$, and f is any bijection $P \to Q$. Another proof is given in [19]. More generally we also have:

Theorem 1.12 *The Thompson-Higman monoid $M_{k,1}$ is a submonoids of the multiplicative part of the Cuntz algebra $\mathcal{O}_k$.*

Proof outline. The Thompson-Higman partial function monoid $M_{k,1}$ is the set of all elements of $\mathcal{O}_k$ that have an expression of the form $\sum_{x \in P} f(x)\ \overline{x}$ where $P \subset A^*$ ranges over all finite prefix codes, and f ranges over functions $P \to A^*$.

The details of the proof are very similar to the proofs in [3, 23]; the definition of *essential* restriction (and extension) and Proposition 1.4 insure that the same proof goes through. $\Box$

The embeddability into the Cuntz algebra is a further justification of the definitional choices that we made for the Higman-Thompson monoid $M_{k,1}$.

2 Structure and simplicity of the Thompson-Higman monoids

We give some structural properties of the Thompson-Higman monoids; in particular, we show that $M_{k,1}$ and $Inv_{k,1}$ are simple for all k.

2.1 Group of units, J-relation, simplicity

By definition, the group of units of a monoid M is the set of invertible elements (i.e., the elements $u \in M$ for which there exists $x \in M$ such that $xu = ux = \mathbf{1}$, where $\mathbf{1}$ is the identity element of M).

Proposition 2.1 *The Thompson-Higman group $G_{k,1}$ is the* group of units *of the monoids $M_{k,1}$, $totM_{k,1}$, $surM_{k,1}$, $totsurM_{k,1}$, and $Inv_{k,1}$.*

Proof. It is obvious that the groups of units of the above monoids contain $G_{k,1}$. Conversely, we want to show that that if $\varphi \in M_{k,1}$ (and in particular, if φ is in one of the other monoids) and if φ has a left inverse and a right inverse, then $\varphi \in G_{k,1}$.

First, it follows that φ is injective, i.e., $\varphi \in Inv_{k,1}$. Indeed, existence of a left inverse implies that for some $\alpha \in M_{k,1}$ we have $\alpha\ \varphi = \mathbf{1}$; hence, if $\varphi(x_1) = \varphi(x_2)$ then $x_1 = \alpha\ \varphi(x_1) = \alpha\ \varphi(x_2) = x_2$.

Next, we show that $\mathrm{domC}(\varphi)$ is a *maximal* prefix code, hence $\varphi \in totInv_{k,1}$. Indeed, we can again consider $\alpha \in M_{k,1}$ such that $\alpha\ \varphi = \mathbf{1}$. For any essential restriction of $\mathbf{1}$ the domain code is a maximal prefix code, hence $\mathrm{domC}(\alpha \circ \varphi)$ is maximal (where $\circ$ denotes functional composition). Moreover, $\mathrm{domC}(\alpha \circ \varphi)$ is also contained in the domain code of some restriction of φ, since $\varphi(x)$ must be defined when $\alpha \circ \varphi(x)$ is defined. Hence $\mathrm{domC}(\varphi')$, for some restriction φ' of φ, is a maximal prefix code; it follows that $\mathrm{domC}(\varphi)$ is a maximal prefix code.

If we apply the reasoning of the previous paragraph to φ^{-1} (which exists since we saw that φ is injective), we conclude that $\mathrm{domC}(\varphi^{-1}) = \mathrm{imC}(\varphi)$ is a maximal prefix code. Thus, $\varphi \in surInv_{k,1}$.

We proved that if φ has a left inverse and a right inverse then $\varphi \in totInv_{k,1} \cap surInv_{k,1}$. Since $totInv_{k,1} \cap surInv_{k,1} = G_{k,1}$ we conclude that $\varphi \in G_{k,1}$. $\Box$

We now characterize some of the Green relations of $M_{k,1}$ and of $Inv_{k,1}$, and we prove simplicity.

By definition, two elements x, y of a monoid M are *J-related* (denoted $x \equiv_J y$) iff x and y belong to exactly the same ideals of M. More generally, the *J-preorder* of M is defined as follows: $x \leq_J y$ iff x belongs to every ideal that y belongs to. It is easy to see that $x \equiv_J y$ iff $x \leq_J y$ and $y \leq_J x$; moreover, $x \leq_J y$ iff there exist $\alpha, \beta \in M$ such that $x = \alpha y \beta$. A monoid M is called *J-simple* iff M has only one J-class (or equivalently, M has only one ideal, namely M itself). A monoid M is called *0-J-simple* iff M has exactly two J-classes, one of which consist of just a zero element (equivalently, M has only two ideals, one of which is a zero element, and the other is M itself). See [10, 16] for more information on the J-relation. Cuntz [11] proved that the multiplicative part of the C^*-algebra $\mathcal{O}_k$ is a 0-J-simple monoid, and that as an algebra $\mathcal{O}_k$ is simple. We will now prove similar results for the Thompson-Higman monoids.

Proposition 2.2 *The inverse monoid $Inv_{k,1}$ and the monoid $M_{k,1}$ are 0-J-simple. The monoid $totM_{k,1}$ is J-simple.*

Proof. Let $\varphi \in M_{k,1}$ (or $\in Inv_{k,1}$). When φ is not the empty map there are $x_0, y_0 \in A^*$ such that $y_0 = \varphi(x_0)$. Let us define $\alpha, \beta \in Inv_{k,1}$ by the tables $\alpha = \{(\varepsilon \mapsto x_0)\}$ and $\beta = \{(y_0 \mapsto \varepsilon)\}$. Recall that ε denotes the empty word. Then $\beta\,\varphi\,\alpha(.) = \{(\varepsilon \mapsto \varepsilon)\} = \mathbf{1}$. So, every non-zero element of $M_{k,1}$ (and of $Inv_{k,1}$) is in the same J-class as the identity element.

In the case of $totM_{k,1}$ we can take $\alpha = \{(\varepsilon \mapsto x_0)\}$ as before (since the domain code of α is $\{\varepsilon\}$, which is a maximal prefix code), and we take $\beta' : Q \mapsto \{\varepsilon\}$ (i.e., the map that sends every element of Q to ε), where Q is any finite maximal prefix code containing y_0. Then again, $\beta'\,\varphi\,\alpha(.) = \{(\varepsilon \mapsto \varepsilon)\} = \mathbf{1}$. $\Box$

Thompson proved that V $(= G_{2,1})$ is a simple group; Higman proved more generally that when k is even then $G_{k,1}$ is simple, and when k is odd then $G_{k,1}$ contains a simple normal subgroup of index 2. We will show next that in the monoid case we have *simplicity for all k* (not only when k is even). For a monoid M, "simple", or more precisely, *"congruence-simple"* is defined to mean that the only congruences on M are the trivial congruences (i.e., the equality relation, and the congruence that lumps all elements of M into one congruence class).

Theorem 2.3 *The Thompson-Higman monoids $Inv_{k,1}$ and $M_{k,1}$ are congruence-simple for all k.*

Proof. Let $\equiv$ be any congruence that is not the equality relation. We will show that then the whole monoid is congruent to the empty map $\mathbf{0}$. We make use of 0-J-simplicity, proved in Proposition 2.2.

If we have $\Phi \equiv \mathbf{0}$ for some element $\Phi \neq \mathbf{0}$ of $Inv_{k,1}$ or $M_{k,1}$ then for all $\alpha, \beta \in Inv_{k,1}$ or $\in M_{k,1}$ we have obviously $\alpha\,\Phi\,\beta \equiv \mathbf{0}$. moreover, by 0-$J$-simplicity of $M_{k,1}$ we have $M_{k,1} = \{\alpha\,\Phi\,\beta : \alpha, \beta \in M_{k,1}\}$ for any $\Phi \in M_{k,1}$ with $\Phi \neq 0$. Hence, all elements of $M_{k,1}$ are $\equiv \mathbf{0}$. Similarly, by 0-J-simplicity of $Inv_{k,1}$ we have $Inv_{k,1} = \{\alpha\,\Phi\,\beta : \alpha, \beta \in Inv_{k,1}\}$ for any $\Phi \in Inv_{k,1}$ $\Phi \neq 0$. Hence, all elements of $Inv_{k,1}$ are $\equiv \mathbf{0}$.

If we have $\varphi \equiv \psi$ and $\varphi \neq \psi$, for any elements φ, ψ of $Inv_{k,1} - \{\mathbf{0}\}$ or of $M_{k,1} - \{\mathbf{0}\}$, then there exist $x_0, y_0, y_1 \in A^*$ such that $\varphi(x_0) = y_0 \neq y_1 = \psi(x_0)$. Consider $\alpha, \beta \in Inv_{k,1} \subseteq M_{k,1}$, defined by the tables $\alpha = \{(y_0 \mapsto y_0)\}$, and $\beta = \{(x_0 \mapsto x_0)\}$. Then $\alpha\,\varphi\,\beta(.) = \{(x_0 \mapsto y_0)\}$, and $\alpha\,\psi\,\beta(.) = \mathbf{0}$. So, $\alpha\,\varphi\,\beta \equiv \alpha\,\psi\,\beta$, $\alpha\,\varphi\,\beta \neq \mathbf{0}$, but $\alpha\,\psi\,\beta = \mathbf{0}$. Hence the previous paragraph, applied to $\Phi = \alpha\,\varphi\,\beta$, implies that the entire monoid is $\equiv \mathbf{0}$. $\Box$

2.2 D-relation

Besides the J-relation and the J-preorder, based on ideals, there are the R- and L relations and preorders, based on right (or left) ideals. Two elements $x, y \in M$ are *R-related* (denoted $x \equiv_R y$) iff x and y belong to exactly the same right ideals of M. The *R-preorder* is defined as follows: $x \leq_R y$ iff x belongs to every right ideal that y belongs to. It is easy to see that $x \equiv_R$ iff $x \leq_R y$ and $y \leq_R x$; also, $x \leq_R y$ iff there exists $\alpha \in M$ such that $x = y\alpha$. In a similar way one defines $\equiv_L$ and $\leq_L$. Finally, there is the *D-relation* of M, which is defined as follows: $x \equiv_D y$ iff there exists $s \in M$ such that $x \equiv_R s \equiv_L y$; this is easily seen to be equivalent to saying that there exists $t \in M$ such that $x \equiv_L t \equiv_R y$. For more information on these definitions see for example [10, 16].

The D-relation of $M_{k,1}$ and $Inv_{k,1}$ has an interesting characterization, as we shall prove next. We will represent all elements of $M_{k,1}$ by tables of the from $\varphi : P \to Q$, where both P and Q are finite prefix codes over A (with $|A| = k$). For such a table we also write $P = \text{domC}(\varphi)$ (the domain code of φ) and $Q = \text{imC}(\varphi)$ (the image code of φ). In general, tables of elements of $M_{k,1}$ have the form $P \to S$, where P is a finite prefix code and S is a finite set; but by using essential restrictions, if necessary, every element of $M_{k,1}$ can be given a table $P \to Q$, where both P and Q are finite prefix codes.

Note the following invariants with respect to essential restrictions:

Proposition 2.4 *Let $\varphi_1 : P_1 \to Q_1$ be a table for an element of $M_{k,1}$, where $P_1, Q_1 \subset A^*$ are finite prefix codes. Let $\varphi_2 : P_2 \to Q_2$ be another finite table for the* same *element of $M_{k,1}$, obtained from the table φ_1 by an essential restriction. Then $P_2, Q_2 \subset A^*$ are finite prefix codes and we have*

$$|P_1| \equiv |P_2| \mod (k-1) \quad \textit{and}$$
$$|Q_1| \equiv |Q_2| \mod (k-1).$$

These modular congruences also hold for essential extensions, provided that in we only extend to tables in which the image is a prefix code.

Proof. An essential restriction consists of a finite sequence of essential restriction steps; an essential restriction step consists of replacing a table entry (x, y) of φ_1 by $\{(xa_1, ya_1), \ldots, (xa_k, ya_k)\}$ (according to Proposition 1.4). For a finite prefix code $Q \subset A^*$, and $q \in Q$, the finite set $(Q - \{q\}) \cup \{qa_1, \ldots, qa_k\}$ is also a prefix code, as is easy to prove. In this process, the cardinalities change as follows: $|P_1|$ becomes $|P_1| - 1 + k$ and $|Q_1|$ becomes $|Q_1| - 1 + k$. Indeed (looking at Q_1 for example), first an element y is removed from Q_1, then the k elements $\{ya_1, \ldots, ya_k\}$ are added. The elements ya_i that are added are all different from the elements that are already present in $Q_1 - \{y\}$; in fact, more strongly, ya_i and the elements of $Q_1 - \{y\}$ are not prefixes of each other. $\Box$

As a consequence of Prop. 2.4 it makes sense, for any $\varphi \in M_{k,1}$, to talk about $|\text{domC}(\varphi)|$ and $|\text{imC}(\varphi)|$ as elements of $\mathbb{Z}_k - 1$, indenpendently of the representation of φ by a right-ideal homomorphism.

Theorem 2.5 *For any non-zero elements φ, ψ of $M_{k,1}$ (or of $Inv_{k,1}$) the D-relation is characterized as follows:*

$$\varphi \equiv_D \psi \quad \textit{iff} \quad |\text{imC}(\varphi)| \equiv |\text{imC}(\psi)| \mod (k-1).$$

Hence, $M_{k,1}$ and $Inv_{k,1}$ have $k-1$ non-zero D-classes. In particular, $M_{2,1}$ and $Inv_{2,1}$ are 0-D-simple (also called 0-bisimple*).*

The proof of Theorem 2.5 uses several Lemmas.

Lemma 2.6 ([4] Lemma 9.9). *For every finite alphabet A and every integer $i \geq 0$ there exists a maximal prefix code (over A) of cardinality $1 + (|A| - 1)\,i$. And every finite maximal prefix code over the alphabet A has cardinality $1 + (|A| - 1)\,i$, for some integer $i \geq 0$.*

It follows that when $|A| = 2$, there are finite prefix codes over A of every finite cardinality. $\square$

As a consequence of this Lemma we have for all $\varphi \in G_{k,1}$: $\|\varphi\| \equiv 1 \bmod (k-1)$. Thus, except for the Thompson group V (when $k = 2$), there is a constraint on the table size of the elements of the group.

In the following we use the notation id_Q for the element of $Inv_{k,1}$ given by the table $\{(x \mapsto x) : x \in Q\}$ where $Q \subset A^*$ is any finite prefix code.

Lemma 2.7 **(1)** *For any $\varphi \in M_{k,1}$ (or $\in Inv_{k,1}$) with table $P \to Q$ (where P, Q are finite prefix codes) we have: $\varphi \equiv_R \mathrm{id}_Q$.*
(2) *If S, T are finite prefix codes with $|S| = |T|$ then $\mathrm{id}_S \equiv_D \mathrm{id}_T$.*
(3) *If $\varphi_1 : P_1 \to Q_1$ and $\varphi_2 : P_2 \to Q_2$ are such that $|Q_1| = |Q_2|$ then $\varphi_1 \equiv_D \varphi_2$.*

Proof. **(1)** Let $P' \subseteq P$ be a set of representatives modulo φ (i.e., we form P' by choosing one element in every set $\varphi^{-1}\varphi(x)$ as x ranges over P). So, $|P'| = |Q|$. Let $\alpha \in Inv_{k,1}$ be given by a table $Q \to P'$; the exact map does not matter, as long as α is bijective. Then $\varphi \circ \alpha(.)$ is a permutation of Q, and $\varphi \circ \alpha \equiv_R \varphi \circ \alpha \circ (\varphi \circ \alpha)^{-1} = \mathrm{id}_Q$.

Now, $\varphi \geq_R \varphi \circ \alpha \geq_R \varphi \circ \alpha \circ (\varphi \circ \alpha)^{-1} \circ \varphi = \mathrm{id}_Q \circ \varphi = \varphi$, hence $\varphi \equiv_R \varphi \circ \alpha$ $(\equiv_R \mathrm{id}_Q)$.

(2) Let $\alpha : S \to T$ be a bijection (which exists since $|S| = |T|$); so α represents an element of $Inv_{k,1}$. Then $\alpha = \alpha \circ \mathrm{id}_S(.)$ and $\mathrm{id}_S = \alpha^{-1} \circ \alpha(.)$; hence, $\alpha \equiv_L \mathrm{id}_S$.

Also, $\alpha = \mathrm{id}_T \circ \alpha(.)$ and $\mathrm{id}_T = \alpha \circ \alpha^{-1}(.)$; hence, $\alpha \equiv_R \mathrm{id}_T$. Thus, $\mathrm{id}_S \equiv_L \alpha \equiv_R \mathrm{id}_T$.

(3) If $|Q_1| = |Q_2|$ then $\mathrm{id}_{Q_1} \equiv_D \mathrm{id}_{Q_2}$ by (2). Moreover, $\varphi_1 \equiv_D \mathrm{id}_{Q_1}$ and $\varphi_2 \equiv_D \mathrm{id}_{Q_2}$ by (1). The result follows by transitivity of $\equiv_D$. $\square$

Lemma 2.8 **(1)** *For any $m \geq k$ let i be the residue of m modulo $k-1$ in the range $2 \leq i \leq k$, and let us write $m = i + (k-1)j$, for some $j \geq 0$. Then there exists a prefix code $Q_{i,j}$ of cardinality $|Q_{i,j}| = m$, such that $\mathrm{id}_{Q_{i,j}}$ is an essential restriction of $\mathrm{id}_{\{a_1,\ldots,a_i\}}$. Hence, $\mathrm{id}_{Q_{i,j}} = \mathrm{id}_{\{a_1,\ldots,a_i\}}$ as elements of $Inv_{k,1}$.*
(2) *In $M_{k,1}$ and in $Inv_{k,1}$ we have $\mathrm{id}_{\{a_1\}} \equiv_D \mathrm{id}_{\{a_1,\ldots,a_k\}} = \mathbf{1}$.*

Proof. **(1)** For any $m \geq k$ there exist $i, j \geq 0$ such that $1 \leq i \leq k$ and $m = i + (k-1)j$. We consider the prefix code

$$Q_{i,j} \;=\; \{a_2, \ldots, a_i\} \;\cup\; \bigcup_{r=1}^{j-1} a_1^r (A - \{a_1\}) \;\cup\; a_1^j A.$$

It is easy to see that $Q_{i,j}$ is a prefix code, which is maximal iff $i = k$; see Fig. 1 below. Clearly, $|Q_{i,j}| = i + (k-1)j$. Since $Q_{i,j}$ contains $a_1^j A$, we can perform an essential extension of $\mathrm{id}_{Q_{i,j}}$ by replacing the table entries $\{(a_1^j a_1, a_1^j a_1), (a_1^j a_2, a_1^j a_2), \ldots, (a_1^j a_k, a_1^j a_k)\}$ by (a_1^j, a_1^j). This replaces $Q_{i,j}$ by $Q_{i,j-1}$. So, $\mathrm{id}_{Q_{i,j}}$ can be essentially extended to $\mathrm{id}_{Q_{i,j-1}}$. By repeating this we find that $\mathrm{id}_{Q_{i,j}}$ is the same element (in $M_{k,1}$ and in $Inv_{k,1}$) as $\mathrm{id}_{Q_{i,0}} = \mathrm{id}_{\{a_1,\ldots,a_i\}}$.

(2) By essential restriction, $\mathrm{id}_{\{a_1\}} = \mathrm{id}_{\{a_1a_1, a_1a_2, \ldots, a_1a_k\}}$, in $M_{k,1}$ and in $Inv_{k,1}$. And by Lemma 2.7(2), $\mathrm{id}_{\{a_1a_1, a_1a_2, \ldots, a_1a_k\}} \equiv_D \mathrm{id}_{\{a_1,\ldots,a_k\}}$; the latter, by essential extension, is $\mathbf{1}$. $\square$

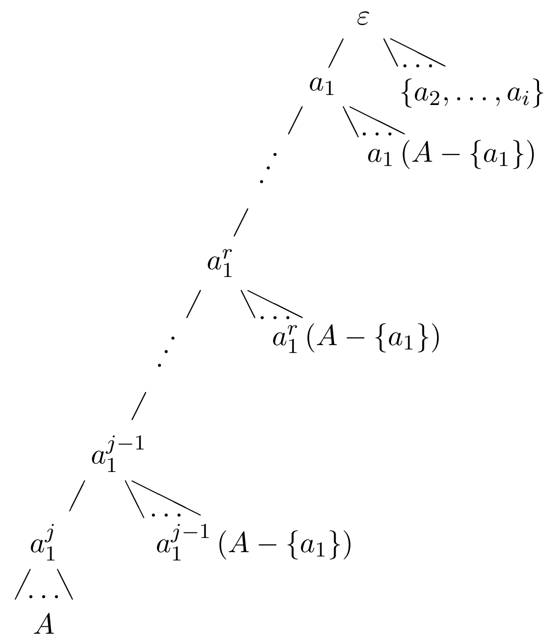

Fig. 1: The prefix tree of $Q_{i,j}$.

Lemma 2.9 *For all $\varphi, \psi \in Inv_{k,1}$: If $\varphi \geq_{L(M_{k,1})} \psi$, where $\geq_{L(M_{k,1})}$ is the L-preorder of $M_{k,1}$, then $\varphi \geq_{L(I_{k,1})} \psi$, where $\geq_{L(I_{k,1})}$ is the L-preorder of $Inv_{k,1}$.*

The same holds with $\geq_L$ replaced by $\equiv_L$, $\geq_R$, $\equiv_R$, $\equiv_D$, $\geq_J$ and $\equiv_J$.

Proof. If $\psi = \alpha\,\varphi$ for some $\alpha \in M_{k,1}$ then let us define α' by $\alpha' = \alpha\ \mathrm{id}_{\mathrm{Im}(\varphi)}$. Then we have: $\psi\ \varphi^{-1} = \alpha\ \varphi\ \varphi^{-1} = \alpha\ \mathrm{id}_{\mathrm{Im}(\varphi)} = \alpha'$, hence $\alpha' \in Inv_{k,1}$ (since $\varphi, \psi \in Inv_{k,1}$). Moreover, $\alpha'\,\varphi = \alpha\ \mathrm{id}_{\mathrm{Im}(\varphi)}\ \varphi = \alpha\,\varphi = \psi$. $\Box$

So far our Lemmas imply that in $M_{k,1}$ and in $Inv_{k,1}$, every non-zero element is $\equiv_D$ to one of the $k-1$ elements $\mathrm{id}_{\{a_1,\ldots,a_i\}}$, for $i = 1, \ldots, k-1$. Moreover the Lemmas show that if two elements of $M_{k,1}$ (or of $Inv_{k,1}$) are given by tables $\varphi_1 : P_1 \to Q_1$ and $\varphi_2 : P_2 \to Q_2$, where P_1, Q_1, P_2 and Q are finite prefix codes, then we have: If $|Q_1| \equiv |Q_2| \bmod (k-1)$ then $\varphi_1 \equiv_D \varphi_2$.

We still need to prove the converse of this. It is sufficient to prove the converse for $Inv_{k,1}$, by Lemma 2.9 and because every element of $M_{k,1}$ is $\equiv_D$ to an element of $Inv_{k,1}$ (namely $\mathrm{id}_{\{a_1,\ldots,a_i\}}$).

Lemma 2.10 *Let $\varphi, \psi \in Inv_{k,1}$. If $\varphi \equiv_D \psi$ in $Inv_{k,1}$, then $\|\varphi\| \equiv \|\psi\| \bmod (k-1)$.*

Proof. (1) We first prove that if $\varphi \equiv_L \psi$ then $|\mathrm{domC}(\varphi)| \equiv |\mathrm{domC}(\psi)| \bmod (k-1)$.

By definition, $\varphi \equiv_L \psi$ iff $\varphi = \beta\,\psi$ and $\psi = \alpha\,\varphi$ for some $\alpha, \beta \in Inv_{k,1}$. By Lemma 1.9 there are restrictions β' and ψ' of β, respectively ψ, and an essential restriction Φ of φ such that:

$\Phi = \beta' \circ \psi'$, and $\mathrm{Dom}(\beta') = \mathrm{Im}(\psi')$.

It follows that $\mathrm{Dom}(\Phi) \subseteq \mathrm{Dom}(\psi')$, since if $\psi'(x)$ is not defined then $\Phi(x) = \beta' \circ \psi'(x)$ is not defined either. Similarly, there is an essential restriction Ψ of ψ and a restriction φ' of φ and such that $\mathrm{Dom}(\Psi) \subseteq \mathrm{Dom}(\varphi')$.

Thus, the restriction of both φ and ψ to the intersection $\mathrm{Dom}(\Phi) \cap \mathrm{Dom}(\Psi)$ yields restrictions φ'', respectively ψ'' such that $\mathrm{Dom}(\varphi'') = \mathrm{Dom}(\psi'')$.

We claim: φ'' and ψ'' are essential restrictions of φ, respectively ψ.

Indeed, every right ideal R of A^* that intersects $\mathrm{Dom}(\psi)$ also intersects $\mathrm{Dom}(\Psi)$ (since Ψ is an essential restriction of ψ). Since $\mathrm{Dom}(\Psi) \subseteq \mathrm{Dom}(\varphi') \subseteq \mathrm{Dom}(\varphi)$, it follows that R also intersects $\mathrm{Dom}(\varphi)$. Moreover, since Φ is an essential restriction of φ, R also intersects $\mathrm{Dom}(\Phi)$. Thus, $\mathrm{Dom}(\Phi)$ is essential in $\mathrm{Dom}(\psi)$. Since $\mathrm{Dom}(\Psi)$ is also essential in $\mathrm{Dom}(\psi)$, it follows that $\mathrm{Dom}(\Phi) \cap \mathrm{Dom}(\Psi)$ is essential in $\mathrm{Dom}(\psi)$; indeed, in general, the intersection of two right ideals R_1, R_2 that are essential in a right ideal R_3, is essential in R_3 (this is a special case of Lemma 1.8). This means that ψ'' is an essential restriction of ψ. Similarly, one proves that φ'' is an essential restriction of φ.

So, φ'' and ψ'' are essential restrictions such that $\mathrm{Dom}(\varphi'') = \mathrm{Dom}(\psi'')$. Hence, $\mathrm{domC}(\varphi'') = \mathrm{domC}(\psi'')$; Proposition 2.4 then implies that $|\mathrm{domC}(\varphi)| \equiv |\mathrm{domC}(\varphi'')| = |\mathrm{domC}(\psi'')| \equiv |\mathrm{domC}(\psi)| \mod (k-1)$.

(2) Next, let us prove that if $\varphi \equiv_R \psi$ then $|\mathrm{imC}(\varphi)| \equiv |\mathrm{imC}(\psi)| \mod (k-1)$.

In $Inv_{k,1}$ we have $\varphi \equiv_R \psi$ iff $\varphi^{-1} \equiv_L \psi^{-1}$. Also, $\mathrm{imC}(\varphi) = \mathrm{domC}(\varphi^{-1})$. Hence, (2) follows from (1).

The Lemma now follows from (1) and (2), since for elements of $Inv_{k,1}$, $|\mathrm{imC}(\varphi)| = |\mathrm{domC}(\varphi)| = \|\varphi\|$, and since the D-relation is the composite of the L-relation and the R-relation. □

Proof of Theorem 2.5. We saw already (in the observations before Lemma 2.10 and in the preceding Lemmas) that for $\varphi_1 : P_1 \to Q_1$ and $\varphi_2 : P_2 \to Q_2$ (where P_1, Q_1, P_2 and Q are non-empty finite prefix codes we have: If $|Q_1| \equiv |Q_2| \mod (k-1)$ then $\varphi_1 \equiv_D \varphi_2$. In particular, when $|Q_1| \equiv i \mod (k-1)$ then $\varphi_1 \equiv_D \mathrm{id}_{\{a_1,\ldots,a_i\}}$.

It follows from Lemma 2.10 that the elements $\mathrm{id}_{\{a_1,\ldots,a_i\}}$ (for $i = 1, \ldots, k-1$) are all in different D-classes. □

So far we have characterized the D- and J-relations of $M_{k,1}$ and $Inv_{k,1}$. We leave the general study of the Green relations of $M_{k,1}$, $Inv_{k,1}$, and the other Thompson-Higman monoids for future work. The main result of this paper, to be proved next, is that the Thompson-Higman monoids $M_{k,1}$ and $Inv_{k,1}$ are finitely generated and that their word problem over any finite generating set is in P.

3 Finite generating sets

We will show that $Inv_{k,1}$ and $M_{k,1}$ are finitely generated. An application of the latter fact is that a finite generating set of $M_{k,1}$ can be used to build combinational circuits for finite boolean functions that do not have fixed-length inputs or outputs. In engineering, non-fixed length inputs or outputs make sense, for example, if the inputs or outputs are handled sequentially, and if the possible input strings form a prefix code.

First we need some more definitions about prefix codes. The *prefix tree* of a prefix code $P \subset A^*$ is, by definition, a tree whose vertex set is the set of all the prefixes of the elements of P, and whose edge set is $\{(x, xa) : a \in A,\ xa \text{ is a prefix of some element of } P\}$. The tree is rooted, with root ε (the empty word). Thus, the prefix tree of P is a subtree of the tree of A^*. The set of leaves of the prefix tree of P is P itself. The vertices that are not leaves are called *internal vertices*. We will say more briefly an "internal vertex of P" instead of internal vertex of the prefix tree of P. An internal vertex has between 1 and k children; an internal vertex is called *saturated* iff it has k children.

One can prove easily that a prefix code P is maximal iff every internal vertex of the prefix tree of P is saturated. Hence, every prefix code P can be embedded in a maximal prefix code (which is finite when P is finite), obtained by saturating the prefix tree of P. Moreover we have:

Lemma 3.1 *For any two finite non-maximal prefix codes $P_1, P_2 \subset A^*$ there are finite maximal prefix codes $P_1', P_2' \subset A^*$ such that $P_1 \subset P_1'$, $P_2 \subset P_2'$, and $|P_1'| = |P_2'|$.*

Proof. First we saturate P_1 and P_2 to obtain two maximal prefix codes P_1'' and P_2'' such that $P_1 \subset P_1''$, and $P_2 \subset P_2''$. If $|P_1''| \neq |P_2''|$ (e.g., if $|P_1''| < |P_2''|$) then $|P_1''|$ and $|P_2''|$ differ by a multiple of $k-1$ (by Prop. 2.4). So, in order to make $|P_1''|$ equal to $|P_2''|$ we repeat the following (until $|P_1''| = |P_2''|$): consider a leaf of the prefix tree of P_1'' that does not belong to P_1, and attach k children at that leaf; now this leaf is no longer a leaf, and the net increase in the number of leaves is $k-1$. $\square$

Lemma 3.2 *Let P and Q be finite prefix codes of A^* with $|P| = |Q|$. If P and Q are both maximal prefix codes, or if both are non-maximal, then there is an element of $G_{k,1}$ that maps P onto Q. On the other hand, if one of P and Q is maximal and the other one is not maximal, then there is no element of $G_{k,1}$ that maps P onto Q.*

Proof. When P and Q are both maximal then any one-to-one correspondence between P and Q is an element of $G_{k,1}$.

When P and Q are both non-maximal, we use Lemma 3.1 above to find two maximal prefix codes P' and Q' such that $P \subset P'$, $Q \subset Q'$, and $|P'| = |Q'|$. Consider now any bijection from P' onto Q' that is also a bijection from P onto Q. This is an element of $G_{k,1}$.

When P is maximal and Q is non-maximal, then every element $\varphi \in M_{k,1}$ that maps P onto Q will satisfy $\mathrm{domC}(\varphi) = P$; since φ is onto Q, we have $\mathrm{imC}(\varphi) = Q$. Hence, $\varphi \notin G_{k,1}$ since $\mathrm{imC}(\varphi)$ is a non-maximal prefix code. A similar reasoning shows that no element of $G_{k,1}$ maps P onto Q if P is non-maximal and Q is maximal. $\square$

Notation: For $u, v \in A^*$, the element of $Inv_{k,1}$ with one-element domain code $\{u\}$ and one-element image code $\{v\}$ is denoted by $(u \mapsto v)$. When $(u \mapsto v)$ is composed with itself j times the resulting element of $Inv_{k,1}$ is denoted by $(u \mapsto v)^j$.

Lemma 3.3 **(1)** *For all $j > 0$:* $(a_1 \mapsto a_1a_1)^j \ = \ (a_1 \mapsto a_1^{j+1})$.
(2) *Let $S = \{a_1^ja_1, a_1^ja_2, \ldots, a_1^ja_i\}$, for some $1 \le i \le k-1$, $0 \le j$. Then id_S is generated by the $k+1$ elements* $\{(a_1 \mapsto a_1a_1),\ (a_1a_1 \mapsto a_1)\} \cup \{\mathrm{id}_{\{a_1a_1,\ a_1a_2,\ \ldots,\ a_1a_i\}} : 1 \le i \le k-1\}$.
(3) *For all $j \ge 2$:* $(\varepsilon \mapsto a_1^j)(.) \ = \ (a_1 \mapsto a_1a_1)^{j-1} \cdot (\varepsilon \mapsto a_1)(.)$.

Proof. **(1)** We prove by induction that $(a_1 \mapsto a_1a_1)^j = (a_1 \mapsto a_1a_1^j)$ for all $j \ge 1$.
Indeed, $(a_1 \mapsto a_1a_1)^{j+1}(.) = (a_1 \mapsto a_1a_1) \cdot (a_1 \mapsto a_1a_1^j)(.)$, and by essential restriction this is

$$= \begin{pmatrix} a_1a_1^j & a_1w \quad (w \in A^j - \{a_1^j\}) \\ a_1a_1a_1^j & a_1a_1w \end{pmatrix} \cdot (a_1 \mapsto a_1a_1^j)(.) \ = \ (a_1 \mapsto a_1a_1a_1^j)(.).$$

(2) For $S = \{a_1^ja_1, a_1^ja_2, \ldots, a_1^ja_i\}$ we have

$$\mathrm{id}_S \ = \ \begin{pmatrix} a_1a_1 & a_1a_2 & \cdots & a_1a_i \\ a_1^ja_1 & a_1^ja_2 & \cdots & a_1^ja_i \end{pmatrix} \cdot \begin{pmatrix} a_1^ja_1 & a_1^ja_2 & \cdots & a_1^ja_i \\ a_1a_1 & a_1a_2 & \cdots & a_1a_i \end{pmatrix} (.)$$

and

$$\begin{pmatrix} a_1a_1 & a_1a_2 & \cdots & a_1a_i \\ a_1^ja_1 & a_1^ja_2 & \cdots & a_1^ja_i \end{pmatrix} =$$

$$\begin{pmatrix} a_1a_1 & a_1a_2 & \cdots & a_1a_i & a_1a_{i+1} & \cdots & a_1a_k \\ a_1^ja_1 & a_1^ja_2 & \cdots & a_1^ja_i & a_1^ja_{i+1} & \cdots & a_1^ja_k \end{pmatrix} \cdot \mathrm{id}_{\{a_1a_1,\ a_1a_2,\ \ldots,\ a_1a_i\}}(.)$$

$$= \ (a_1 \mapsto a_1^j) \cdot \mathrm{id}_{\{a_1a_1,\ a_1a_2,\ \ldots,\ a_1a_i\}} \ = \ (a_1 \mapsto a_1a_1)^{j-1} \cdot \mathrm{id}_{\{a_1a_1,\ a_1a_2,\ \ldots,\ a_1a_i\}}.$$

The map $\mathrm{id}_{\{a_1a_1\}}$ is redundant as a generator since $(a_1a_1 \mapsto a_1a_1) = (a_1a_1 \mapsto a_1)\ (a_1 \mapsto a_1a_1)(.)$.

(3) By (1) we have $(\varepsilon \mapsto a_1^j) = (a_1 \mapsto a_1^j) \cdot (\varepsilon \mapsto a_1)(.)$, and $(a_1 \mapsto a_1^j) = (a_1 \mapsto a_1a_1)^{j-1}$. $\square$

Theorem 3.4 *The inverse monoid $Inv_{k,1}$ is finitely generated.*

Proof. Our strategy for finding a finite generating set for $Inv_{k,1}$ is as follows: We will use the fact that the Thompson-Higman group $G_{k,1}$ is finitely generated. Hence, if $\varphi \in Inv_{k,1}$, $g_1, g_2 \in G_{k,1}$, and if $g_2\varphi g_1$ can be expressed as a product p over a fixed finite set of elements of $Inv_{k,1}$, then it follows that $\varphi = g_2^{-1} p\, g_1^{-1}$ can also be expressed as a product over a fixed finite set of elements of $Inv_{k,1}$. We assume that a finite generating set for $G_{k,1}$ has been chosen.

For any element $\varphi \in Inv_{k,1}$ with domain code $\mathrm{domC}(\varphi) = P$ and image code $\mathrm{imC}(\varphi) = Q$, we distinguish four cases, depending on the maximality or non-maximality of P and Q.

(1) If P and Q are both maximal prefix codes then $\varphi \in G_{k,1}$, and we can express φ over a finite fixed generating set of $G_{k,1}$.

(2) Assume P and Q are both non-maximal prefix codes. By Lemma 3.1 there are finite maximal prefix codes P', Q' such that $P \subset P'$, $Q \subset Q'$, and $|P'| = |Q'|$; and by Lemma 2.6, $|P'| = |Q'| = 1 + (k-1)N$ for some $N \geq 0$. Consider the following maximal prefix code C, of cardinality $|P'| = |Q'| = 1+(k-1)N$:

$$C \ = \ \bigcup_{r=0}^{N-2} a_1^r(A - \{a_1\}) \ \cup \ a_1^{N-1}A.$$

The maximal prefix code C is none other than the code $Q_{i,j}$ when $i = k$ and $j = N-1$ (introduced in the proof of Lemma 2.8, Fig. 1). The elements $g_1 : C \to P'$ and $g_2 : Q' \to C$ of $G_{k,1}$ can be chosen so that $\psi = g_2\varphi g_1(.)$ is a partial identity with $\mathrm{domC}(\psi) = \mathrm{imC}(\psi) \subset C$ consisting of the $|P|$ first elements of C in the dictionary order. So, ψ is the identity map restricted to these $|P|$ first elements of C, and ψ is undefined on the rest of C. To describe $\mathrm{domC}(\psi) = \mathrm{imC}(\psi)$ in more detail, let us write $|P| = i + (k-1)\,\ell$, for some i, ℓ with $1 \leq i < k$ and $0 \leq \ell \leq N-1$. Then

$$\mathrm{domC}(\psi) = \mathrm{imC}(\psi) \ = \ a_1^{N-1}A \ \cup \ \bigcup_{r=j+1}^{N-2} a_1^r(A - \{a_1\}) \ \cup \ a_1^j\, \{a_2, \ldots, a_i\}.$$

where $j = N - 1 - \ell$. Since $\psi = \mathrm{id}_{\mathrm{domC}(\psi)}$, we claim:

By essential maximal extension

$$\psi \ = \ \mathrm{id}_S \ \text{ (as elements of } Inv_{k,1}), \quad \text{where } \ S = \{a_1^j a_1, a_1^j a_2, \ldots, a_1^j a_i\},$$

with i, j as in the description of $\mathrm{domC}(\psi) = \mathrm{imC}(\psi)$ above, i.e., $1 < i < k$, $N-1 \geq j = N-1-\ell \geq 0$, and $|P| = i + (k-1)\,\ell$.

Indeed, if $|P| < k$ then S is just $\mathrm{domC}(\psi)$, with $i = |P|$, and $\ell = 0$ (hence $j = N-1$). If $|P| \geq k$ then the maximum essential extension of ψ will replace the $1 + (k-1)\,\ell$ elements $a_1^{N-1}A \ \cup \bigcup_{r=N-j+1}^{N-2} a_1^r(A - \{a_1\})$ by the single element $a_1^{N-\ell+1} = a_1^{j+1}$. What remains is the set

$$S \ = \ \{a_1^{j+1}\} \ \cup \ a_1^j\, \{a_2, \ldots, a_i\}.$$

Finally, by Lemma 3.3, id_S (where $S = \{a_1^j a_1, a_1^j a_2, \ldots, a_1^j a_i\}$) can be generated by the $k+1$ elements $\{(a_1 \mapsto a_1a_1),\ (a_1a_1 \mapsto a_1)\} \cup \{\mathrm{id}_{\{a_1a_1,\ a_1a_2,\ \ldots,\ a_1a_i\}} : 1 \leq i \leq k-1\}$.

(3) Assume P is a maximal prefix code and Q is non-maximal. Let Q' be the finite maximal prefix code obtained by saturating the prefix tree of Q. Then $Q \subset Q'$, $|Q'| = 1+(k-1)N'$, and $|P| = 1+(k-1)N$ for some $N' > N \geq 0$. We consider the maximal prefix codes C and C' as defined in the proof of (2), using N' for defining C'. We can choose $g_1 : C \to P$ and $g_2 : Q' \to C'$ in $G_{k,1}$ so that $\psi = g_2\varphi g_1(.)$ is the dictionary-order preserving map that maps C to the first $|C|$ elements of C'. So we have

$\mathrm{domC}(\psi) = C$, and

$\mathrm{imC}(\psi) = S_0$, where $S_0 \subset C'$ consist of the $|C|$ first elements of C', in dictionary order.

Since $|C| = 1 + (k-1)\,N$, we can describe S_0 in more detail by

$$S_0 \;=\; \bigcup_{r=N'-N}^{N'-2} a_1^r(A - \{a_1\}) \;\;\cup\;\; a_1^{N'-1}A.$$

Next, by essential maximal extension we now obtain $\psi \;=\; (\varepsilon \mapsto a_1^{N'-N})$.

Indeed, we saw that $|P| = 1 + (k-1)\,N$. If $|P| = 1$ then $P = \{\varepsilon\}$, and $\psi \;=\; (\varepsilon \mapsto a_1^{N'})$. If $|P| \geq k$ then maximum essential extension of ψ will replace all the elements of C by the single element ε, and it will replace all the elements of S_0 by the single element $a_1^{N'-N}$.

Finally, by Lemma 3.3, $(\varepsilon \mapsto a_1^{N'-N})$ is generated by the two elements $(\varepsilon \mapsto a_1)$ and $(a_1 \mapsto a_1a_1)$.

(4) The case where P is a non-maximal maximal prefix code and Q is maximal can be derived from case (3) by taking the inverses of the elements from case (3). $\square$

Theorem 3.5 *The monoid $M_{k,1}$ is finitely generated.*

Proof. Let $\varphi : P \to Q$ be the table of any element of $M_{k,1}$, mapping P onto Q, where $P, Q \subset A^*$ are finite prefix codes. The map described by the table is total and surjective, so if $|P| = |Q|$ (and in particular, if φ is the empty map) then $\varphi \in Inv_{k,1}$, hence φ can be expressed over the finite generating set of $Inv_{k,1}$. In the rest of the proof we assume $|P| > |Q|$. The main observation is the following.

Claim. φ can be written as the composition of finitely many elements $\varphi_i \in M_{k,1}$ with tables $P_i \to Q_i$ such that $0 \leq |P_i| - |Q_i| \leq 1$.

Proof of the Claim: We use induction on $|P| - |Q|$. There is nothing to prove when $|P| - |Q| \leq 1$, so we assume now that $|P| - |Q| \geq 2$.

If $\varphi(x_1) = \varphi(x_2) = \varphi(x_3) = y_1$ for some $x_1, x_2, x_3 \in P$ (all three being different) and $y_1 \in Q$, then we can write φ as a composition $\varphi(.) = \psi_2 \circ \psi_1(.)$, as follows. The map $\psi_1 : P \longrightarrow P - \{x_1\}$ is defined by $\psi_1(x_1) = \psi_1(x_2) = x_2$, and acts as the identity everywhere else on P. The map $\psi_2 : P - \{x_1\} \longrightarrow Q$ is defined by $\psi_2(x_2) = \psi_2(x_3) = y_1$, and acts in the same way as φ everywhere else on $P - \{x_1\}$. Then for ψ_1 we have $|P| - |P - \{x_1\}| \;<\; |P| - |Q|$, and for ψ_2 we have $|P - \{x_1\}| - |Q| \;<\; |P| - |Q|$.

If $\varphi(x_1) = \varphi(x_2) = y_1$ and $\varphi(x_3) = \varphi(x_4) = y_2$ for some $x_1, x_2, x_3, x_4 \in P$ (all four being different) and $y_1, y_2 \in Q$ ($y_1 \neq y_2$), then we can write φ as a composition $\varphi(.) = \psi_2 \circ \psi_1(.)$, as follows. First the map $\psi_1 : P \longrightarrow P - \{x_1\}$ is defined by $\psi_1(x_1) = \psi_1(x_2) = x_2$, and acts as the identity everywhere else on P. Second, the map $\psi_2 : P - \{x_1\} \longrightarrow Q$ is defined by $\psi_2(x_2) = y_1$ and $\psi_2(x_3) = \psi_2(x_4) = y_2$, and acts like φ everywhere else on $P - \{x_1\}$. Again, for ψ_1 we have $|P| - |P - \{x_1\}| \;<\; |P| - |Q|$ and for ψ_2 we have $|P - \{x_1\}| - |Q| \;<\; |P| - |Q|$. [End, proof of the Claim.]

Because of the Claim we now only need to consider elements $\varphi \in M_{k,1}$ with tables $P \to Q$ such that the prefix codes P, Q satisfy $|P| = |Q| + 1$. We denote $P = \{p_1, \ldots, p_n\}$ and $Q = \{q_1, \ldots, q_{n-1}\}$, with $\varphi(p_j) = q_j$ for $1 \leq j \leq n-1$, and $\varphi(p_{n-1}) = \varphi(p_n) = q_{n-1}$. We define the following prefix code C with $|C| = |P|$:

if $|P| = i \leq k$ then $C \;=\; \{a_1, \ldots, a_i\}$; note that $i \geq 2$, since $|P| > |Q| > 0$;

if $|P| > k$ then $C \;=\; \{a_2, \ldots, a_i\} \cup \bigcup_{r=1}^{j-1} a_1^r(A - \{a_1\}) \;\;\cup\;\; a_1^jA$,

where i, j are such that $|P| = i + (k-1)j$, $2 \leq i \leq k$, and $1 \leq j$ (see Fig. 1). Let us write C in increasing dictionary order as $C = \{c_1, \ldots, c_n\}$. The last element of C in the dictionary order is thus $c_n = a_i$.

We now write $\varphi(.) = \psi_3\,\psi_2\,\psi_1(.)$ where ψ_1, ψ_2, ψ_3 are as follows:

- $\psi_1 : P \longrightarrow C$ is bijective and is defined by $p_j \mapsto c_j$ for $1 \leq j \leq n$;
- $\psi_2 : C \longrightarrow C - \{a_i\}$ is the identity map on $\{c_1, \ldots, c_{n-1}\}$, and $\psi_2(c_n) = c_{n-1}$.
- $\psi_3 : C - \{a_i\} \longrightarrow Q$ is bijective and is defined by $c_j \mapsto q_j$ for $1 \leq j \leq n-1$.

It follows that ψ_1 and ψ_3 can be expressed over the finite generating set of $Inv_{k,1}$. On the other hand, ψ_2 has a maximum essential extension, as follows.

- If $2 \le |P| = i \le k$ then

$$\psi_2 = \begin{pmatrix} a_1 & \dots & a_{i-2} & a_{i-1} & a_i \\ a_1 & \dots & a_{i-2} & a_{i-1} & a_{i-1} \end{pmatrix} = \begin{pmatrix} \mathrm{id}_{\{a_1,\ \dots,\ a_{i-1}\}} & a_i \\ & a_{i-1} \end{pmatrix}.$$

- If $|P| = i + (k-1)j > k$ and if $i > 2$ then, after maximal essential extension, ψ_2 also becomes

$$\max(\psi_2) = \begin{pmatrix} \mathrm{id}_{\{a_1,\ \dots,\ a_{i-1}\}} & a_i \\ & a_{i-1} \end{pmatrix}.$$

- If $|P| = i + (k-1)j > k$ and if $i = 2$ then, after essential extensions,

$$\max(\psi_2) = \begin{pmatrix} a_1a_1 & \dots & a_1a_{k-2} & a_1a_{k-1} & a_1a_k & a_2 \\ a_1a_1 & \dots & a_1a_{k-2} & a_1a_{k-1} & a_1a_k & a_1a_k \end{pmatrix} = \begin{pmatrix} \mathrm{id}_{a_1A} & a_2 \\ & a_1a_k \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_1 & a_1a_k \end{pmatrix}.$$

In summary, we have factored φ over a finite set of generators of $Inv_{k,1}$ and k additional generators in $M_{k,1}$. $\square$

Factorization algorithm: The proofs of Theorems 3.4 and 3.5 are constructive; they provide algorithms that, given $\varphi \in Inv_{k,1}$ or $\in M_{k,1}$, output a factorization of φ over the finite generating set of $Inv_{k,1}$, respectively $M_{k,1}$.

In [17] (p. 49) Higman introduces a four-element generating set for $G_{2,1}$; a special property of these generators is that their domain codes and their image codes only contain words of length ≤ 2, and that $\big|\,|\gamma(x)| - |x|\,\big| \le 1$ for every generator γ and every $x \in \mathrm{domC}(\gamma)$. The generators in the finite generating set of $M_{k,1}$ that we introduced above also have those properties. Thus we obtain:

Corollary 3.6 *The monoid $M_{2,1}$ has a finite generating set such that all the generators have the following property: The domain codes and the image codes only contain words of length ≤ 2, and $\big|\,|\gamma(x)| - |x|\,\big| \le 1$ for every generator γ and every $x \in \mathrm{domC}(\gamma)$.* $\square$

For reference we list an explicit *finite generating set for $M_{2,1}$*. It consists, first, of the Higman generators of $G_{2,1}$ ([17] p. 49):

$$\textsc{Not} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad (01 \leftrightarrow 1) = \begin{pmatrix} 00 & 01 & 1 \\ 00 & 1 & 01 \end{pmatrix}, \quad (0 \leftrightarrow 10) = \begin{pmatrix} 00 & 01 & 1 \\ 00 & 1 & 01 \end{pmatrix}, \quad \text{and}$$

$$\tau_{1,2} = \begin{pmatrix} 00 & 01 & 10 & 11 \\ 00 & 10 & 01 & 11 \end{pmatrix};$$

the additional generators for $Inv_{2,1}$:

$$(\varepsilon \to 0), \quad (0 \to \varepsilon), \quad (0 \to 00), \quad (00 \to 0);$$

the additional generators for $M_{2,1}$:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ 0 & 01 \end{pmatrix} = \begin{pmatrix} 00 & 01 & 1 \\ 00 & 01 & 01 \end{pmatrix}.$$

Observe that Higman's generators of $G_{k,1}$ (in [17] p. 27) have domain and image codes with at most 3 internal vertices. We observe that the additional generators that we introduced for $Inv_{k,1}$ and $M_{k,1}$ have domain and image codes have at most 2 internal vertices.

The following problem remains open: Are $Inv_{k,1}$ and $M_{k,1}$ finitely **presented**?

4 The word problem of the Thompson-Higman monoids

We saw that the Thompson-Higman monoid $M_{k,1}$ is finitely generated. We want to show now that the word problem of $M_{k,1}$ over any finite generating set can be decided in deterministic polynomial time, i.e., belongs to the complexity class P. It follows immediately that all finitely generated submonoids of $M_{k,1}$ have their word problem (over any finite generating set) in P.

In [3] it was shown that the word problem of the Thompson-Higman group $G_{k,1}$ over any finite generating set is in P (in fact, in the parallel complexity class AC_1). In [4] it was shown that the word problem of the Thompson-Higman group $G_{k,1}$ over the infinite generating set $\Gamma_{k,1} \cup \{\tau_{i,i+1} : i > 0\}$ is coNP-complete, where $\Gamma_{k,1}$ is any finite generating set of $G_{k,1}$; the position transposition $\tau_{i,i+1} \in G_{k,1}$ has $\mathrm{domC}(\tau_{i,i+1}) = \mathrm{imC}(\tau_{i,i+1}) = A^{i+1}$, and is defined by $u\alpha\beta \mapsto u\beta\alpha$ for all letters $\alpha, \beta \in A$ and all words $u \in A^{i-1}$. The word problem of $M_{k,1}$ over $\Gamma_{k,1} \cup \{\tau_{i,i+1} : i > 0\}$ is in coNP (as we shall see below), where $\Gamma_{k,1}$is any finite generating set of $M_{k,1}$; it follows that the word problem of $M_{k,1}$ over $\Gamma_{k,1} \cup \{\tau_{i,i+1} : i > 0\}$ is coNP-complete.

4.1 The image code formula

Our proof (in [3]) that the word problem of $G_{k,1}$ (over any finite generating set) is in P was based on the following fact (the *table size formula*):

$\forall \varphi, \psi \in G_{k,1}$: $\quad \|\psi \circ \varphi\| \le \|\psi\| + \|\varphi\|$.

Here $\|\varphi\|$ denotes the table size of φ, or equivalently, the cardinality of $\mathrm{domC}(\varphi)$. See Proposition 3.5, Theorem 3.8, and Proposition 4.2 in [3]. In $M_{k,1}$ the above formula does not hold in general, as the following example shows.

Proposition 4.1 *For every $n > 0$ there exist $\varphi_n, \Phi_n \in M_{2,1}$ with $\Phi_n = \varphi_n \circ \ldots \circ \varphi_1$, with the following properties:*
(1) *The table sizes are $\|\Phi_n\| = 2^n$, and $\|\varphi_n\| = 2$. So, $\|\Phi_n\| = \|\varphi_n \circ \ldots \circ \varphi_1\|$ is exponentially larger than $\sum_{i=1}^{n} \|\varphi_i\|$, and hence the table size formula does not hold in $M_{2,1}$.*
(2) *The word lengths of φ_n and Φ_n (over the finite generating set of $M_{2,1}$ from the previous Section) satisfy $|\varphi_n| \le n$, and $|\Phi_n| < n^2$. So the table size of Φ_n is exponentially larger than its word length: $\|\Phi_n\| > 2^{\sqrt{|\Phi_n|}}$.*

Proof. Consider the elements $\varphi_i \in M_{2,1}$ given by the tables $\varphi_i = \{(0^i \mapsto 0),\ (0^{i-1}1 \mapsto 0)\}$, for $i \ge 1$. So each φ_i has table size $\|\varphi_i\| = 2$. However, one verifies easily that $\Phi_n = \varphi_n \circ \ldots \circ \varphi_2 \circ \varphi_1(.)$ has a table that sends every bitstring of length n to the word 0^n; its domain code is $\{0,1\}^n$, its image code is $\{0\}$, and it is its maximum essential extension. Thus, $\|\varphi_n \circ \ldots \circ \varphi_2 \circ \varphi_1\| = 2^n$, whereas $\sum_{i=1}^{n} \|\varphi_i\| = 2 \cdot n$. Hence the table size formula "$\|\psi \circ \varphi\| \le \|\psi\| + \|\varphi\|$" does not hold in general in $M_{2,1}$.

It is straightforward to verify that $\varphi_n(.) = (0 \mapsto 0, 1 \mapsto 0) \cdot (0 \mapsto \varepsilon) \cdot (00 \mapsto 0)^{n-2}(.)$. Hence $|\varphi_n| \le n$ and $|\Phi_n| \le n(n+1)/2$. $\square$

Definition 4.2 *The* table size *of the right-ideal homomorphism $\theta : PA^* \to QA^*$ where $P, Q \subset A^*$ are prefix codes, is by definition $\|\theta\| = |P|$.*

The length of the longest word in the table $P \to Q$ of θ is denoted by $\ell(\theta)$; formally, $\ell(\theta) = \max\{|s| : s \in \mathrm{domC}(\theta) \cup \mathrm{imC}(\theta)\}$.

For any finite prefix code $Q \subseteq A^*$ we also denote the length of the longest word in Q by $\ell(Q)$.

We will use the following facts that are easy to prove. If $R \subset A^*$ is a right ideal and φ is a right-ideal homomorphism then $\varphi(R)$ and $\varphi^{-1}(R)$ are right ideals. We also need the following result (Lemma 3.3 of [3]): *If $P, Q, S \subseteq A^*$ are such that $PA^* \cap QA^* = SA^*$, and if S is a prefix code then $S \subseteq P \cup Q$.*

Before proving Theorem 4.5 that generalizes the table size formula to the monoid case we need two Lemmas.

Lemma 4.3 *Assume $\theta : PA^* \to QA^*$ is a right-ideal homomorphism, and assume $SA^* \subseteq PA^*$, where $P, Q, S \subset A^*$ are finite prefix codes. Then there is a finite prefix code $R \subset A^*$ such that $\theta(SA^*) = RA^*$ and $R \subseteq \theta(S)$.*

Proof. Since θ is a right-ideal homomorphism we have $\theta(SA^*) = \theta(S)\ A^*$. Since $\theta(S)$ might not be a prefix code we take $R = \{r \in \theta(S) : r$ is minimal (shortest) in the prefix order within $\theta(S)\}$. Then R is a prefix code that has the required properties. □

Lemma 4.4 *Let θ be a right-ideal homomorphism with image $\mathrm{Im}(\theta) = QA^*$ such that $Q \subset A^*$ is a prefix code. Then $\theta^{-1}(Q)$ is a prefix code, and $\mathrm{domC}(\theta) = \theta^{-1}(Q)$.*

Proof. First, $\theta^{-1}(Q)$ is a prefix code. Indeed, if we had $x_1 = x_2 u$ for some $x_1, x_2 \in \theta^{-1}(Q)$ with u non-empty, then $\theta(x_1) = \theta(x_2)\ u$, with $\theta(x_1), \theta(x_2) \in Q$. This would contradict the assumption that Q is a prefix code.

Second, $\theta^{-1}(Q)\ A^* = \theta^{-1}(QA^*)$. Indeed, for all $\theta^{-1}(Q) \subset \theta^{-1}(QA^*)$, hence $\theta^{-1}(Q)\ A^* \subseteq \theta^{-1}(QA^*)$. Moreover, if $y \in QA^*$ then any element of $\theta^{-1}(y)$ has the form rw for some $r \in \theta^{-1}(QA^*)$ such that no prefix of r is in $\theta^{-1}(QA^*)$. Since we just saw that $\theta^{-1}(Q)$ is a prefix code, it follows that $r \in \theta^{-1}(Q)$; hence, $\theta^{-1}(QA^*) \subseteq \theta^{-1}(Q)\ A^*$.

Finally, since $\theta^{-1}(Q)\ A^* = \theta^{-1}(QA^*)$, and since $\theta^{-1}(Q)$ is a prefix code, it follows that $\mathrm{domC}(\theta) = \theta^{-1}(Q)$. □

The next Theorem is a useful generalization of the "table size formula" of $G_{k,1}$ to the monoid $M_{k,1}$.

Theorem 4.5 (Image code formula). *Let $\varphi_1 : P_1A^* \to Q_1A^*$ and $\varphi_2 : P_2A^* \to Q_2A^*$ be right-ideal homomorphisms, where $P_1, P_2, Q_1, Q_2 \subset A^*$ are finite prefix codes. Then*

(1) $\quad \big|\mathrm{imC}(\varphi_2 \circ \varphi_1)\big| \ \le\ \big|\mathrm{imC}(\varphi_2)\big| \ +\ \big|\mathrm{imC}(\varphi_1)\big|$,

(2) $\quad \ell(\varphi_2 \circ \varphi_1) \le \ell(\varphi_2) + \ell(\varphi_1)$.

Proof. **(1)** The proof is similar to the proof of Proposition 3.5 in [3]. We have $\mathrm{Dom}(\varphi_2 \circ \varphi_1) = \varphi_1^{-1}(Q_1A^* \cap P_2A^*)$ and $\mathrm{Im}(\varphi_2 \circ \varphi_1) = \varphi_2(Q_1A^* \cap P_2A^*)$. So the following maps are total and onto, on the indicated sets:

$$\varphi_1^{-1}(Q_1A^* \cap P_2A^*) \ \xrightarrow{\varphi_1}\ Q_1A^* \cap P_2A^* \xrightarrow{\varphi_2}\ \varphi_2(Q_1A^* \cap P_2A^*).$$

By Lemma 3.3 of [3] (quoted above) we have $Q_1A^* \cap P_2A^* = SA^*$ for some finite prefix code S with $S \subseteq Q_1 \cup P_2$. Moreover, by Lemma 4.3 we have $\varphi_2(SA^*) = R_2A^*$ for some finite prefix code R_2 such that $R_2 \subseteq \varphi_2(S)$. Now, since $S \subseteq Q_1 \cup P_2$ we have $R_2 \subseteq \varphi_2(S) \subseteq \varphi_2(Q_1) \cup \varphi_2(P_2) = \varphi_2(Q_1) \cup Q_2$. Thus, $|\mathrm{imC}(\varphi_2 \circ \varphi_1)| = |R_2| \le |\varphi_2(Q_1)| + |Q_2| \le |Q_1| + |Q_2|$.

(2) We want to bound the length of words in $\mathrm{imC}(\varphi_2 \circ \varphi_1)$ and in $\mathrm{domC}(\varphi_2 \circ \varphi_1)$.

(2.a) Let us first look at $\mathrm{imC}(\varphi_2 \circ \varphi_1)$. We saw above that $\mathrm{imC}(\varphi_2 \circ \varphi_1) = R_2 \subseteq \varphi_2(Q_1) \cup Q_2$. The longest words in Q_2 are of length $\le \ell(\varphi_2)$ ($\le \ell(\varphi_2) + \ell(\varphi_1)$).

On the other hand, for a longest word y in $\varphi_2(Q_1)$ we have the following: $y = \varphi_2(q_1)$ for some $q_1 \in Q_1 \cap P_2A^*$ (we have $q_1 \in P_2A^*$ since φ_2 is defined on q_1). Thus, $q_1 = p_2w$ for some $p_2 \in P_2, w \in A^*$, hence $|w| \le |q_1|$. Now $y = \varphi_2(q_1w) = \varphi_2(q_1)\, w$, hence $|y| = |\varphi_2(q_1)| + |w| \le \ell(\varphi_2) + |q_1| \le \ell(\varphi_2) + \ell(\varphi_1)$.

(2.b) Let us now look at $\text{domC}(\varphi_2 \circ \varphi_1)$. We saw above that $\text{Dom}(\varphi_2 \circ \varphi_1) = \varphi_1^{-1}(SA^*)$, where $S \subseteq Q_1 \cup P_2$. By Lemma 4.4, $\text{domC}(\varphi_2 \circ \varphi_1) = \varphi_1^{-1}(S)$. Hence, $\varphi_1^{-1}(S) \subseteq \varphi_1^{-1}(Q_1) \cup \varphi_1^{-1}(P_2)$, hence $\text{domC}(\varphi_2 \circ \varphi_1) = \varphi_1^{-1}(S) \subseteq P_1 \cup \varphi_1^{-1}(P_2)$.

For $x \in P_1$ we obviously have $|x| \le \ell(\varphi_1)$ ($\le \ell(\varphi_2) + \ell(\varphi_1)$).

On the other hand, consider a longest word x in $\varphi_1^{-1}(P_2)$. We have $x \in P_1A^*$ since φ_1 is defined on x. Therefore, $x = p_1w$ for some $p_1 \in P_1$, $w \in A^*$. Since $\varphi_1(x) = \varphi_1(p_1)\, w$ we have $|w| \le |\varphi_1(x)|$; since $\varphi_1(x) \in P_2$ we have $|w| \le \ell(\varphi_2)$. Thus, $|x| = |p_1| + |w| \le \ell(\varphi_1) + \ell(\varphi_2)$. $\square$

For elements of $Inv_{k,1}$ the image code has the same size as the domain code, which is also the table size. Thus Theorem 4.5 implies:

Corollary 4.6 *For all $\varphi, \psi \in Inv_{k,1}$:* $\|\psi \circ \varphi\| \le \|\psi\| + \|\varphi\|$. $\square$

In other words, the table size formula holds for $Inv_{k,1}$. Another immediate consequence of Theorem 4.5 is the following.

Corollary 4.7 *Let $\varphi_i : P_iA^* \to Q_iA^*$ be right-ideal homomorphisms for $i = 1, \ldots, n$, where $P_i, Q_i \subset A^*$ are finite prefix codes. Let c_1, c_2 be positive constants.*

(1) *If $|Q_i| \le c_1$ for all i then* $|\text{imC}(\varphi_n \circ \ldots \circ \varphi_1)| \le c_1\, n$.

(2) *If $\ell(\varphi_i) \le c_2$ for all i then* $\ell(\varphi_n \circ \ldots \circ \varphi_1)| \le c_2\, n$.

So, if $|Q_i| \le c_1$ and $\ell(\varphi_i) \le c_2$ for all i then $\text{imC}(\varphi_n \circ \ldots \circ \varphi_1)$ *consists of a linearly bounded number ($\le c_1\, n$) of words, each of linearly bounded length ($\le c_2\, n$).* $\square$

The position transposition $\tau_{i,j}$ (with $0 < i < j$) is, by definition, the partial permutation of A^* which transposes the letters positions i and j; $\tau_{i,j}$ is undefined on words of length $< j$. More precisely, we have $\text{domC}(\tau_{i,j}) = \text{imC}(\tau_{i,j}) = A^j$, and $u\alpha v\beta \mapsto u\beta v\alpha$ for all letters $\alpha, \beta \in A$ and all words $u \in A^{i-1}$ and $v \in A^{j-i-1}$. In this form, $\tau_{i,j}$ is equal to its maximum essential extension.

Corollary 4.8 *The word-length of $\tau_{i,j}$ over any finite generating set of $M_{k,1}$ is exponential.*

Proof. We have $|\text{imC}(\tau_{i,j})| = k^j$. The Corollary follows then from Corollary 4.7(1). $\square$

4.2 Some algorithmic problems about right-ideal homomorphisms

We consider several problems about right-ideal homomorphisms of A^* and show that they have deterministic polynomial-time algorithms. We also show that the word problem of $M_{k,1}$ over $\Gamma_{k,1} \cup \{\tau_{i,i+1} : 0 < i\}$ is coNP-complete, where $\Gamma_{k,1}$ is any finite generating set of $M_{k,1}$. This will help us with the complexity analysis of the word problem of the Thompson-Higman monoids $M_{k,1}$, and provide other corollaries of independent interest.

Notation: We denote the unique prefix code that generates a right ideal $R \subseteq A^*$ by $\text{prefC}(R)$. We observe that if $\varphi_1 : P_1A^* \to Q_1A^*$ and $\varphi_2 : P_2A^* \to Q_2A^*$ are right-ideal homomorphisms, where $P_1, Q_1, P_2, Q_2 \subset A^*$ are finite prefix codes, then $\text{imC}(\varphi_2 \circ \varphi_1(.)) = \text{prefC}(\varphi_2(Q_1A^*))$.

Lemma 4.9 *The following input-output problem is in* P*.*
• Input: *A finite prefix code* $Q_0 \subset A^*$ *(given explicitly by a list of words), and* n *right-ideal homomorphisms* $\varphi_i : P_iA^* \to Q_iA^*$ *for* $i = 1, \ldots, n$ *(given explicitly by finite tables);* $P_i, Q_i \subset A^*$ *are finite prefix codes.*
• Output: *The finite prefix code* $\mathrm{prefC}(\varphi_n \circ \ldots \circ \varphi_1(Q_0A^*))$*, described explicitly by a list of words.*

Proof. By Theorem 4.5 applied to $\varphi_n, \ \ldots, \ \varphi_1, \ \mathrm{id}_{Q_0}$ we have for all j $(1 \le j \le n)$:

$$\big|\mathrm{imC}(\varphi_j \circ \ldots \circ \varphi_1(Q_0A^*))\big| \ \le \ |Q_0| \ + \ \textstyle\sum_{i=1}^{j} |\mathrm{imC}(\varphi_i)|, \quad \text{and}$$

$$\ell(\mathrm{prefC}(\varphi_j \circ \ldots \circ \varphi_1(Q_0A^*))) \ \le \ \ell(Q_0) \ + \ \textstyle\sum_{i=1}^{j} \ell(\varphi_i).$$

So in terms of the input size, the cardinality of $\mathrm{prefC}(\varphi_j \circ \ldots \circ \varphi_1(Q_0A^*))$ is linearly bounded and its words have linearly bounded length. Let us denote the alphabet by $A = \{a_1, \ldots, a_k\}$, with the elements listed in increasing dictionary order. The following algorithm computes $\mathrm{prefC}(\varphi_n \circ \ldots \circ \varphi_1(Q_0A^*))$; note that in this algorithm, the set Q_0 that appears in the condition of the for-loop can change during execution of the body of the loop.

```
// 1. Compute the set φn ∘ ... ∘ φ1(Q0 A*)
S := ∅;
for x ∈ Q0 in increasing dictionary order do
      if φn ∘ ... ∘ φ1(x) is defined
         then put φn ∘ ... ∘ φ1(x) into S;
         else replace Q0 by (Q0 − {x}) ∪ xA;
              // in the else case, the successor of x in the updated set Q0 is x a1
// Now S is φn ∘ ... ∘ φ1(Q0 A*)

// 2. Turn S into a prefix code
for x1 ∈ S in increasing dictionary order do
    for x2 ∈ S in increasing dictionary order starting with the successor of x1 in S do
         if x1 is a prefix of x2
              then remove x2 from S;
// Now S is prefC(φn ∘ ... ∘ φ1(Q0 A*))
```

Running time of the algorithm: In part 1, computing $\varphi_n \circ \ldots \circ \varphi_1(x)$ when it is defined, or checking whether it is not defined, can be done by successive application of $\varphi_1(.)$, then $\varphi_2(.)$, $\varphi_3(.)$, etc. This takes polynomial time; indeed, by Theorem 4.5 all intermediate results $\varphi_i \circ \ldots \circ \varphi_1(x)$ (including the final result $\varphi_n \circ \ldots \circ \varphi_1(x)$) have linearly bounded length.

As we saw, there is a linearly bounded number of words in $\mathrm{prefC}(\varphi_n \circ \ldots \circ \varphi_1(Q_0A^*))$, all of linearly bounded length. Part 2 of the algorithm examines words of $\mathrm{prefC}(\varphi_n \circ \ldots \circ \varphi_1(Q_0A^*))$ and some of their prefixes; each word is examined just once. Moreover, a finite prefix code P of size $|P|$ with words of length $\le \ell$ has $\le (\ell + 1) \ |P|$ prefixes. Hence, the algorithm above runs in polynomial time. □

Corollary 4.10 *The following input-output problem has a deterministic polynomial-time algorithm.*
• Input: *Right-ideal homomorphisms* $\varphi_j : P_jA^* \to Q_jA^*$ *(for* $j = 1, \ldots, n$*), where* $P_j, Q_j \subset A^*$ *are finite prefix codes; each* φ_j *is explicitly given by its table.*
• Output: *The set* $\mathrm{imC}(\varphi_n \circ \ldots \circ \varphi_1)$*, given explicitly by a list of words.*

Proof. This is a special case of Lemma 4.9 with $Q_0 = \{\varepsilon\}$. □

When we consider the word problem of $M_{k,1}$ over a finite generating set, we measure the input size by the length of input word (with each generator having length 1). But for the word problem of $M_{k,1}$ over the infinite generating set $\Gamma_{k,1} \cup \{\tau_{i-1,i} : i > 1\}$ we count the length of the position transpositions $\tau_{i-1,i}$ as i, in the definition of the input size of the word problem. Indeed, at least $\log_2 i$ bits are needed to describe the subscript i of $\tau_{i-1,i}$. Moreover, in the connection between $M_{k,1}$ (over $\Gamma_{k,1} \cup \{\tau_{i-1,i} : i > 1\}$) and circuits $\tau_{i-1,i}$ is interpreted as the wire-crossing operation of wire number i and wire number $i-1$; this suggests that viewing the size of $\tau_{i-1,i}$ as i is more natural. In any case, we will see next that the word problem of $M_{k,1}$ over $\Gamma_{k,1} \cup \{\tau_{i-1,i} : i > 1\}$ is coNP-complete, even if the size of $\tau_{i-1,i}$ is more generously measured as i; this is a stronger result than if $\log_2 i$ were used.

Theorem 4.11 (coNP-complete word problem). *The word problem of $M_{k,1}$ over the infinite generating set $\Gamma_{k,1} \cup \{\tau_{i-1,i} : i > 1\}$ is coNP-complete, where $\Gamma_{k,1}$ is any finite generating set of $M_{k,1}$.*

Proof. In [4] (see also [2]) it was shown that the word problem of the Thompson-Higman group $G_{k,1}$ over $\Gamma_{G_{k,1}} \cup \{\tau_{i-1,i} : i > 1\}$ is coNP-complete, where $\Gamma_{G_{k,1}}$ is any finite generating set of $G_{k,1}$. Hence, since the elements of the finite set $\Gamma_{G_{k,1}}$ can be expressed by a finite set of words over $\Gamma_{k,1}$, it follows that the word problem of $M_{k,1}$ over $\Gamma_{k,1} \cup \{\tau_{i-1,i} : i > 1\}$ is also coNP-hard.

We will prove now that the word problem of $M_{k,1}$ over $\Gamma_{k,1} \cup \{\tau_{i-1,i} : i > 1\}$ is in coNP. The *input* of the problem consists of two words $(\rho_m, \ldots, \rho_1)$ and $(\sigma_n, \ldots, \sigma_1)$ over $\Gamma_{k,1} \cup \{\tau_{i-1,i} : i > 1\}$. The *input size* is the length $\sum_{h=1}^{m} |\rho_h| + \sum_{j=1}^{n} |\sigma_j|$, where each generator in $\Gamma_{k,1}$ has length 1, and each generator of the form $\tau_{i-1,i}$ has length i.

Since $\Gamma_{k,1}$ is finite there is a constant $c > 0$ such that $c \geq \ell(\gamma)$ for all $\gamma \in \Gamma_{k,1}$; also, for each $\tau_{i-1,i}$ that occurs in $\{\rho_m, \ldots, \rho_1\} \cup \{\sigma_n, \ldots, \sigma_1\}$ we have $\ell(\tau_{i-1,i}) = i = |\tau_{i-1,i}|$. By Theorem 4.5 (2), the table of $\sigma_n \circ \ldots \circ \sigma_1$ (and more generally, the table of $\sigma_j \circ \ldots \circ \sigma_1$ for any j with $n \geq j \geq 1$) only contains words of length $\leq \sum_{j=1}^{n} \ell(\sigma_j)$, and similarly for $\rho_m \circ \ldots \circ \rho_1$ (and for $\rho_i \circ \ldots \circ \rho_1$, $m \geq i \geq 1$). So all the words in the tables for any $\sigma_j \circ \ldots \circ \sigma_1$ and any $\rho_i \circ \ldots \circ \rho_1$ have lengths that are linearly bounded by the size of the input $\big((\rho_m, \ldots, \rho_1), (\sigma_n, \ldots, \sigma_1)\big)$.

Claim. Let $N = \max\{\sum_{i=1}^{m} \ell(\rho_i),\ \sum_{j=1}^{n} \ell(\sigma_j)\}$. Then $\rho_m \cdot \ldots \cdot \rho_1 \neq \sigma_n \cdot \ldots \cdot \sigma_1$ as elements of $M_{k,1}$ iff there exists $x \in A^N$ such that $\rho_m \circ \ldots \circ \rho_1(x) \neq \sigma_n \circ \ldots \circ \sigma_1(x)$.

Proof of the Claim: As we saw above, the tables of $\rho_m \circ \ldots \circ \rho_1$ and $\sigma_n \circ \ldots \circ \sigma_1$ only contain words of length $\leq N$. Thus, restricting $\rho_m \circ \ldots \circ \rho_1$ and $\sigma_n \circ \ldots \circ \sigma_1$ to $A^N A^*$ is an essential restriction, and the resulting tables have domain codes in A^N. Therefore, $\rho_m \cdot \ldots \cdot \rho_1$ and $\sigma_n \cdot \ldots \cdot \sigma_1$ are equal (as elements of $M_{k,1}$) iff $\rho_m \circ \ldots \circ \rho_1$ and $\sigma_n \circ \ldots \circ \sigma_1$ are equal on A^N. [End, Proof of Claim]

Based on the Claim, we obtain a nondeterministic polynomial-time algorithm which decides (nondeterministically) whether there exists $x \in A^N$ such that $\rho_m \circ \ldots \circ \rho_1(x) \neq \sigma_n \circ \ldots \circ \sigma_1(x)$, as follows:

The algorithm guesses $x \in A^N$, computes $\rho_m \circ \ldots \circ \rho_1(x)$ and $\sigma_n \circ \ldots \circ \sigma_1(x)$, and checks that they are different words ($\in A^*$) or that one is undefined and the other is a word. Applying Theorem 4.5 (2) to $\rho_m \circ \ldots \circ \rho_1 \circ \mathrm{id}_{A^N}$ and to $\sigma_n \circ \ldots \circ \sigma_1 \circ \mathrm{id}_{A^N}$ shows that $|\rho_m \circ \ldots \circ \rho_1(x)| \leq 2N$ and $|\sigma_n \circ \ldots \circ \sigma_1(x)| \leq 2N$. Also by Theorem 4.5 (2), all intermediate results (as we successively apply ρ_i for $i = 1, \ldots, m$, or σ_j for $j = 1, \ldots, n$) are words of length $\leq 2N$. These successive words are computed by applying the table of ρ_i or σ_j (when ρ_i or σ_j belong to $\Gamma_{k,1}$), or by directly applying the position permutation $\tau_{h,h-1}$ (if ρ_i or σ_j is $\tau_{h,h-1}$). Thus, the output $\rho_m \circ \ldots \circ \rho_1(x)$ (and similarly for $\sigma_n \circ \ldots \circ \sigma_1(x)$) can be computed in polynomial time.

The above is a nondeterministic polynomial-time algorithm for the negated word problem. Hence the word problem of $M_{k,1}$ over $\Gamma_{k,1} \cup \{\tau_{i-1,i} : i > 1\}$ is in coNP. $\Box$

4.3 The word problem of $M_{k,1}$ is in P

We now move ahead with the the proof of our main result.

Theorem 4.12 (Word problem in P). *The word problem of the Thompson-Higman monoids $M_{k,1}$, over any finite generating set, can be decided in deterministic polynomial time.*

We assume that a fixed finite generating set $\Gamma_{k,1}$ of $M_{k,1}$ has been chosen. The input consists of two sequences $(\rho_m, \ldots, \rho_1)$ and $(\sigma_n, \ldots, \sigma_1)$ over $\Gamma_{k,1}$, and the input size is $m + n$. We want to decide in deterministic polynomial time whether, as elements of $M_{k,1}$, the products $\rho_m \cdot \ldots \cdot \rho_1$ and $\sigma_n \cdot \ldots \cdot \sigma_1$ are the same.

Overview of the proof:

- We compute the finite sets $\mathrm{imC}(\rho_m \circ \ldots \circ \rho_1)$, $\mathrm{imC}(\sigma_n \circ \ldots \circ \sigma_1) \subset A^*$, explicitly described by lists of words. By Corollary 4.10 we can do this in polynomial time, and these sets have polynomial size. (Note however that by Proposition 4.1, the table sizes of $\rho_m \circ \ldots \circ \rho_1$ or $\sigma_n \circ \ldots \circ \sigma_1$ could be exponential in m or n.)
- We check whether $\mathrm{Im}(\rho_m \circ \ldots \circ \rho_1) \cap \mathrm{Im}(\sigma_n \circ \ldots \circ \sigma_1)$ is essential in $\mathrm{Im}(\rho_m \circ \ldots \circ \rho_1)$ and in $\mathrm{Im}(\sigma_n \circ \ldots \circ \sigma_1)$. By Lemma 4.13 (Question 2) this can be done in polynomial time. If the answer is "no" then $\rho_m \cdot \ldots \cdot \rho_1 \neq \sigma_n \cdot \ldots \cdot \sigma_1$, since they don't have a common maximum essential extension. If "yes", we continue.
- We compute the finite prefix code $\Pi \subset A^*$ such that $\Pi A^* = \mathrm{Im}(\rho_m \circ \ldots \circ \rho_1) \cap \mathrm{Im}(\sigma_n \circ \ldots \circ \sigma_1)$. By Lemma 4.13 (Output 1) this can be done in polynomial time, and Π has polynomial size.
- For every $r \in \Pi$ we compute a deterministic finite automaton (DFA) accepting the finite set $(\rho_m \circ \ldots \circ \rho_1)^{-1}(r) \subset A^*$, and a DFA accepting the finite set $(\sigma_n \circ \ldots \circ \sigma_1)^{-1}(r) \subset A^*$. By Corollary 4.15 this can be done in polynomial time, and the DFAs have polynomial size. (Note that the finite sets themselves could have exponential size in m or n.)
- For every $r \in \Pi$ we check whether the DFAs for $(\rho_m \circ \ldots \circ \rho_1)^{-1}(r)$, respectively $(\sigma_n \circ \ldots \circ \sigma_1)^{-1}(r)$, are equivalent. By classical automata theory, this can be done in polynomial time.

These DFAs are equivalent for all $r \in \Pi$ iff $(\rho_m \circ \ldots \circ \rho_1)^{-1}(r) = (\sigma_n \circ \ldots \circ \sigma_1)^{-1}(r)$ for all $r \in \Pi$, i.e., iff $\rho_m \circ \ldots \circ \rho_1$ and $\sigma_n \circ \ldots \circ \sigma_1$ agree on Π. Since ΠA^* is essential in $\mathrm{Im}(\rho_m \circ \ldots \circ \rho_1)$ and in $\mathrm{Im}(\sigma_n \circ \ldots \circ \sigma_1)$, this is iff $\rho_m \cdot \ldots \cdot \rho_1 = \sigma_n \cdot \ldots \cdot \sigma_1$ (in $M_{k,1}$). [End of Overview.]

Lemma 4.13 *There are deterministic polynomial time algorithms for the following problems.*
Input: *Two finite prefix codes $P_1, P_2 \subset A^*$, given explicitly by lists of words;*
Output 1: *The finite prefix code $\Pi \subset A^*$ such that $\Pi A^* = P_1 A^* \cap P_2 A^*$; the output Π should be produced explicitly as a list of words.*
Question 2: *Is $P_1 A^* \cap P_2 A^*$ essential in $P_1 A^*$ (or in $P_2 A^*$, or in both)?*

Proof. We saw already that Π exists. Indeed, the intersection of right ideals is a right ideal, and every right ideal is generated by a maximal prefix code, and this prefix code is unique (this is not hard to prove – see Lemma A.1 of [3]). Moreover Π is finite (since $\Pi \subseteq P_1 \cup P_2$, by Lemma 3.3 of [3]).

Algorithm for Output 1:

Since we know that $\Pi \subseteq P_1 \cup P_2$, we just need to search for the elements of Π within $P_1 \cup P_2$. For each $x \in P_1$ we check whether x also belongs to $P_2 A^*$ (by checking whether any element of P_2 is a prefix of x). Since P_1 and P_2 are explicitly given as lists, this takes polynomial time. Similarly, for each $x \in P_2$ we check whether x also belongs to $P_2 A^*$. Thus, we have computed the set $\Pi_1 = (P_1 \cap P_2 A^*) \cup (P_2 \cap P_1 A^*)$. Now, Π is obtained from Π_1 by eliminating every word that has another word of Π_1 as a prefix. Since Π is explicitly listed, this takes just polynomial time.

Algorithm for Question 2:

We first compute Π by the previous algorithm. Next, we check whether every $p_1 \in P_1$ and every $p_2 \in P_2$ is a prefix of some $r \in \Pi$; since P_1, P_2, and Π are explicitly listed, this takes just polynomial time. $\Box$

Notation and terminology: In the following, DFA stands for *deterministic finite automaton.* The language accepted by a DFA $\mathcal{A}$ is denoted by $\mathcal{L}(\mathcal{A})$. A DFA is a structure (S, A, δ, s_0, F) where S is the set of states, A is the input alphabet, $s_0 \in S$ is the start state, $F \subseteq S$ is the set of accept states, and $\delta : S \times A \to S$ is the next-state function; in general, δ is a partial function. We extend the definition of δ to a function $S \times A^* \to S$ by defining $\delta(s, w)$ to be the state that the DFA reaches from s after reading w (for any $w \in A^*$ and $s \in S$). See [18, 21] for background on finite automata. A DFA is called *acyclic* iff its underlying directed graph has no directed cycle. It is easy to prove that a language $L \subseteq A^*$ is finite iff L is accepted by an acyclic DFA. Moreover, L is a finite prefix code iff L is accepted by an acyclic DFA that has a single accept state (take the prefix tree of the prefix code, with the leaves as accept states, then glue all the leaves together into a single accept state). By the *size* of a DFA $\mathcal{A}$ we mean the number of states, $|S|$, of the DFA; we denote this by $\mathsf{size}(\mathcal{A})$. By the *min-depth* of a DFA $\mathcal{A}$ with single accept state we mean the length of the *shortest* path from the start state to the accept state; we denote this by $\mathsf{mindepth}(\mathcal{A})$. (We use the term "min-depth" to avoid confusion with the usual concept of "depth" of an acyclic graph, which refers to the length of the longest path from a source vertex to a sink vertex.) For a finite prefix code $P \subseteq A^*$ we denote the length of the longest word in P by $\ell(P)$, and we define the *total length* of P by $\|P\| = \sum_{x \in P} |x|$.

For a language $L \subseteq A^*$ and a partial function $\Phi : A^* \to A^*$, we define the inverse image of L under Φ by $\Phi^{-1}(L) = \{x \in A^* : \Phi(x) \in L\}$.

For $L \subseteq A^*$ we denote the set of all *strict* prefixes of the words in L by $\mathsf{spref}(L)$.

The reason why we use acyclic DFAs to describe finite sets is that a finite set can be exponentially larger than the number of states of a DFA that accepts it; e.g., A^n is accepted by an acyclic DFA with $n+1$ states. This conciseness plays a crucial role in our polynomial-time algorithm for the word problem of $M_{k,1}$.

Lemma 4.14 *Let $\mathcal{A}$ be an acyclic DFA with a single accept state. Let $\varphi : PA^* \to QA^*$ be a right-ideal homomorphism, where $P, Q \subset A^*$ are finite prefix codes. We assume that $\ell(Q) \le \mathsf{mindepth}(\mathcal{A})$, and that $\varphi^{-1}(\mathcal{L}(\mathcal{A})) \neq \varnothing$.*

Then $\varphi^{-1}(\mathcal{L}(\mathcal{A}))$ is accepted by a one-accept-state acyclic DFA whose size is $< \mathsf{size}(\mathcal{A}) + \|P\|$, and whose min-depth is $\ge \mathsf{mindepth}(\mathcal{A}) - \ell(Q)$. Moreover, the transition table of this DFA can be constructed deterministically in polynomial time, based on the transition table of $\mathcal{A}$ and the table of φ.

Proof. Let $\mathcal{A} = (S, A, \delta, s_0, \{s_A\})$ where s_A is the single accept state; s_A has no out-going edges. For any set $X \subseteq A^*$ and any state $s \in S$ we denote $\{\delta(s, x) : x \in X\}$ by $\delta(s, X)$. Recall that $\mathsf{spref}(Q)$ denotes the set of all strict prefixes of the words in Q. Since $\mathcal{A}$ is acyclic, its state set S can be partioned into the following two sets: $\delta(s_0, \mathsf{spref}(Q))$, and $\delta(s_0, QA^*)$. The block $\delta(s_0, \mathsf{spref}(Q))$ is non-empty since it contains s_0; the block $\delta(s_0, QA^*)$ is non-empty because of the assumption $\varphi^{-1}(\mathcal{L}(\mathcal{A})) \neq \varnothing$.

Since $\mathcal{L}(\mathcal{A})$ is a prefix code and φ is a right-ideal homomorphism, $\varphi^{-1}(\mathcal{L}(\mathcal{A}))$ is a prefix code. To accept $\varphi^{-1}(\mathcal{L}(\mathcal{A}))$ we introduce an acyclic DFA with single accept state, called $\varphi^{-1}(\mathcal{A})$, constructed as follows:

- State set of $\varphi^{-1}(\mathcal{A})$: $\mathsf{spref}(P) \ \cup \ \delta(s_0, QA^*)$.
  The start state is ε, i.e., the root of the prefix tree of P.
  The accept state is the accept state s_A of $\mathcal{A}$.
- State-transition function δ_1 of $\varphi^{-1}(\mathcal{A})$:

For every $r \in \mathsf{spref}(P)$ and $a \in A$ such that $ra \in \mathsf{spref}(P)$: $\delta_1(r, a) = ra$.
For every $r \in \mathsf{spref}(P)$ and $a \in A$ such that $ra \in P$: $\delta_1(r, a) = \delta(s_0, \varphi(ra))$.
For every $s \in \delta(s_0, QA^*)$: $\delta_1(s, a) = \delta(s, a)$.

It follows immediately from this definition we have for all $p \in P$: $\delta_1(\varepsilon, p) = \delta(s_0, \varphi(p))$.

The DFA $\varphi^{-1}(\mathcal{A})$ can be pictured as being constructed as follows: The DFA has two parts. The first part is the prefix tree of P, but with the leaves left out (and with the leaf edges dangling). The second part is the DFA $\mathcal{A}$ restricted to the state subset $\delta(s_0, QA^*)$. The two parts are connected together by gluing each (hypothetical) leaf $p \in P$ to the state $\delta(s_0, \varphi(p)) \in \delta(s_0, QA^*)$.

The description of $\varphi^{-1}(\mathcal{A})$ constitutes a deterministic polynomial time algorithm for constructing the transition table of $\varphi^{-1}(\mathcal{A})$, based on the transition table of $\mathcal{A}$ and on the table of φ.

We will prove now that the DFA $\varphi^{-1}(\mathcal{A})$ accepts exactly $\varphi^{-1}(\mathcal{L}(\mathcal{A}))$; i.e., $\varphi^{-1}(\mathcal{L}(\mathcal{A})) = \mathcal{L}(\varphi^{-1}(\mathcal{A}))$.

[$\subseteq$] Consider any $y \in \mathcal{L}(\mathcal{A})$ such that $\varphi^{-1}(y) \neq \varnothing$. We want to show that $\varphi^{-1}(\mathcal{A})$ accepts all the words in $\varphi^{-1}(y)$. Since $\varphi^{-1}(y) \neq \varnothing$ we have $y = qw$ for some strings $q \in Q = \mathrm{imC}(\varphi)$ and $w \in A^*$. Since Q is a prefix code, q and w are uniquely determined by y. Moreover, since $y \in \mathcal{L}(\mathcal{A})$ it follows that $y = qw$ has an accepting path in $\mathcal{A}$ of the form

$$s_0 \xrightarrow{q} \delta(s_0, q) \xrightarrow{w} s_A.$$

Then for every $x \in \varphi^{-1}(y)$ we have $x = pv$ for some strings $p \in P$ and $v \in A^*$, so $\varphi(x) = \varphi(p)\ v$; we also have $\varphi(x) = qw$, hence $\varphi(p)$ and q are prefix-comparable. Therefore, $\varphi(p) = q$, since Q is a prefix code, and hence $v = w$. Thus every $x \in \varphi^{-1}(qw)$ has the form pw for some string $p \in \varphi^{-1}(q)$. Now in $\varphi^{-1}(\mathcal{A})$ there is the following accepting path on input $x = pw \in \varphi^{-1}(qw) = \varphi^{-1}(q)\ w$:

$$\varepsilon \xrightarrow{p} \delta_1(\varepsilon, p) = \delta(s_0, \varphi(p)) \xrightarrow{w} s_A.$$

Thus $\varphi^{-1}(\mathcal{A})$ accepts $x = pw$.

[$\supseteq$] Suppose $\varphi^{-1}(\mathcal{A})$ accepts x. Then, because of the prefix tree of P at the beginning of $\varphi^{-1}(\mathcal{A})$, x must have the form $x = pw$ for some strings $p \in P$ and $w \in A^*$. The accepting path in $\varphi^{-1}(\mathcal{A})$ on input pw has the form

$$s_0 \xrightarrow{p} \delta_1(\varepsilon, p) = \delta(s_0, \varphi(p)) \xrightarrow{w} s_A.$$

Also, $\varphi(x) = qw$ where $q = \varphi(p) \in Q$. Hence $\mathcal{A}$ has the following accepting path on input qw:

$$s_0 \xrightarrow{q} \delta(s_0, q) = \delta(s_0, \varphi(p)) \xrightarrow{w} s_A.$$

So, $qw \in \mathcal{L}(\mathcal{A})$. Hence, $x \in \varphi^{-1}(qw) \subseteq \varphi^{-1}(\mathcal{L}(\mathcal{A}))$. Thus $\mathcal{L}(\varphi^{-1}(\mathcal{A})) \subseteq \varphi^{-1}(\mathcal{L}(\mathcal{A}))$. $\Box$

Corollary 4.15 *Let $\mathcal{A}$ be an acyclic DFA with a single accept state. For $i = 1, \ldots, n$, let $P_i, Q_i \subset A^*$ be finite prefix codes, and let $\varphi_i : P_iA^* \to Q_iA^*$ be a right-ideal homomorphism. We assume that $\sum_{i=1}^n \ell(Q_i) \leq \mathsf{mindepth}(\mathcal{A})$, and that $(\varphi_n \circ \ldots \circ \varphi_1)^{-1}(\mathcal{L}(\mathcal{A})) \neq \varnothing$,*

Then $(\varphi_n \circ \ldots \circ \varphi_1)^{-1}(\mathcal{L}(\mathcal{A}))$ is accepted by a one-accept-state acyclic DFA whose size is $<$ $\mathsf{size}(\mathcal{A}) + \sum_{i=1}^n \|P_i\|$, and whose min-depth is $\geq \mathsf{mindepth}(\mathcal{A}) - \sum_{i=1}^n \ell(Q_i)$.

Moreover, the transition table of this DFA can be constructed deterministically in polynomial time, based on the transition table of $\mathcal{A}$ and the tables of φ_i ($i = 1, \ldots, n$).

Proof. We use induction on n. For $n = 1$ the Corollary is just Lemma 4.14.

Let $n \geq 0$, assume the Corollary holds for n homomorphisms, and consider one more right-ideal homomorphism $\varphi_0 : P_0A^* \to Q_0A^*$, where $P_0, Q_0 \subset A^*$ are finite prefix codes. Assume $\sum_{i=0}^n \ell(Q_i) \leq$ $\mathsf{mindepth}(\mathcal{A})$, and assume $(\varphi_n \circ \ldots \circ \varphi_1 \circ \varphi_0)^{-1}(\mathcal{L}(\mathcal{A})) \neq \varnothing$.

Since $(\varphi_n \circ \ldots \circ \varphi_1 \circ \varphi_0)^{-1}(\mathcal{L}(\mathcal{A})) = \varphi_0^{-1} \circ (\varphi_n \circ \ldots \circ \varphi_1)^{-1}(\mathcal{L}(\mathcal{A}))$, let us apply Lemma 4.14 to φ_0 and the DFA $(\varphi_n \circ \ldots \circ \varphi_1)^{-1}(\mathcal{A})$. The hypothesis that $\ell(Q_0)$ is at most equal to the min-depth of this DFA holds; indeed, $\sum_{i=0}^{n} \ell(Q_i) \le \mathsf{mindepth}(\mathcal{A})$ implies $\ell(Q_0) \le \mathsf{mindepth}(\mathcal{A}) - \sum_{i=1}^{n} \ell(Q_i) \le \mathsf{mindepth}((\varphi_n \circ \ldots \circ \varphi_1 \circ \varphi_0)^{-1}(\mathcal{A}))$.

The conclusion of Lemma 4.14 is then that $(\varphi_n \circ \ldots \circ \varphi_1 \circ \varphi_0)^{-1}(\mathcal{L}(\mathcal{A}))$ is accepted by a DFA whose size is $< \mathsf{size}((\varphi_n \circ \ldots \circ \varphi_1)^{-1}(\mathcal{A})) + \ell(P_0) < \mathsf{size}(\mathcal{A}) + \sum_{i=1}^{n} \|P_i\| + \ell(P_0)$. And the min-depth of this DFA is $\ge \mathsf{mindepth}((\varphi_n \circ \ldots \circ \varphi_1)^{-1}(\mathcal{A})) - \ell(Q_0) \ge \mathsf{mindepth}(\mathcal{A}) - \sum_{i=1}^{n} \ell(Q_i) - \ell(Q_0)$. $\Box$

Proof of Theorem 4.12:

Let $(\rho_m, \ldots, \rho_1)$ and $(\sigma_n, \ldots, \sigma_1)$ be two sequences of generators from the finite generating set $\Gamma_{k,1}$. We want to decide in deterministic polynomial time whether the products $\rho_m \cdot \ldots \cdot \rho_1$ and $\sigma_n \cdot \ldots \cdot \sigma_1$ are the same (as elements of $M_{k,1}$).

First, by Corollary 4.10, we can compute the sets $\mathrm{imC}(\rho_m \circ \ldots \circ \rho_1)$ and $\mathrm{imC}(\sigma_n \circ \ldots \circ \sigma_1)$, explicitly described by lists of words, in polynomial time. By Lemma 4.13 we can check in polynomial time whether the right ideal $\mathrm{Im}(\rho_m \circ \ldots \circ \rho_1) \cap \mathrm{Im}(\sigma_n \circ \ldots \circ \sigma_1)$ is essential in $\mathrm{Im}(\rho_m \circ \ldots \circ \rho_1)$ and in $\mathrm{Im}(\sigma_n \circ \ldots \circ \sigma_1)$. If not, we immediately conclude that $\rho_m \cdot \ldots \cdot \rho_1 \ne \sigma_n \cdot \ldots \cdot \sigma_1$. Otherwise, Lemma 4.13 lets us compute a generating set Π for the right ideal $\mathrm{Im}(\rho_m \circ \ldots \circ \rho_1) \cap \mathrm{Im}(\sigma_n \circ \ldots \circ \sigma_1)$, in deterministic polynomial time; this generating set Π will be a finite prefix code, given explicitly by a list of words. By Corollary 4.7 and because $\Pi \subseteq \mathrm{imC}(\rho_m \circ \ldots \circ \rho_1) \cup \mathrm{imC}(\sigma_n \circ \ldots \circ \sigma_1)$, Π has linearly bounded cardinality and the length of the longest words in Π is linearly bounded.

To find out whether $\rho_m \cdot \ldots \cdot \rho_1 = \sigma_n \cdot \ldots \cdot \sigma_1$, it is sufficient to check whether $(\rho_m \circ \ldots \circ \rho_1)^{-1}(r) = (\sigma_n \circ \ldots \circ \sigma_1)^{-1}(r)$ for every $r \in \Pi$, since ΠA^* is essential in both $\mathrm{Im}(\rho_m \circ \ldots \circ \rho_1)$ and $\mathrm{Im}(\sigma_n \circ \ldots \circ \sigma_1)$.

Let $\lambda = \max\{\sum_{i=1}^{m} \ell(\mathrm{imC}(\rho_i)),\ \sum_{j=1}^{n} \ell(\mathrm{imC}(\sigma_j))\}$. For every $r \in \Pi$ we have $(\rho_m \circ \ldots \circ \rho_1)^{-1}(r) \ne \varnothing$ and $(\sigma_n \circ \ldots \circ \sigma_1)^{-1}(r) \ne \varnothing$, because $\Pi \subset \mathrm{Im}(\rho_m \circ \ldots \circ \rho_1) \cap \mathrm{Im}(\sigma_n \circ \ldots \circ \sigma_1)$.

If $|r| \ge \lambda$ then Corollary 4.15 implies that $(\rho_m \circ \ldots \circ \rho_1)^{-1}(r)$ is accepted by an acyclic one-accept-state DFA $\mathcal{A}_\rho$, which can be constructed deterministically in polynomial time; similarly, we can be construct an acyclic one-accept-state DFA $\mathcal{A}_\sigma$ which accepts $(\sigma_n \circ \ldots \circ \sigma_1)^{-1}(r)$.

If $|r| < \lambda$, we replace r by $r\, A^{\lambda - |r|}$. It is easy to see that $r\, A^{\lambda-|r|}$ is accepted by an acyclic single-accept-state DFA with $\lambda+1$ states. By Corollary 4.15, $(\rho_m \circ \ldots \circ \rho_1)^{-1}(r\, A^{\lambda-|r|})$ is accepted by an acyclic one-accept-state DFA $\mathcal{A}_\rho$, which can be constructed deterministically in polynomial time. Similarly, we can be construct an acyclic one-accept-state DFA $\mathcal{A}_\sigma$ which accepts $(\sigma_n \circ \ldots \circ \sigma_1)^{-1}(r\, A^{\lambda-|r|})$.

Obviously, $(\rho_m \circ \ldots \circ \rho_1)^{-1}(r\, A^{\lambda-|r|}) = (\sigma_n \circ \ldots \circ \sigma_1)^{-1}(r\, A^{\lambda-|r|})$ (or, in case $|r| \ge \lambda$, $(\rho_m \circ \ldots \circ \rho_1)^{-1}(r) = (\sigma_n \circ \ldots \circ \sigma_1)^{-1}(r)$) if and only if $\mathcal{A}_\rho$ and $\mathcal{A}_\sigma$ accept the same language, i.e., they are equivalent DFAs. It is well known (see e.g., [18], or [21] pp. 103-104) that the equivalence problem for DFAs that are given explicitly by transition tables, is decidable deterministically in polynomial time. This proves Theorem 4.12. $\Box$

Acknowledgement. I would like to thank John Meakin for many discussions over the years concerning the Thompson groups and generalizations to inverse monoids.

References

[1] J.C. Birget, "One-way permutations, computational asymmetry and distortion", Mathematics ArXiv, 2007.

[2] J.C. Birget, "Factorizations of the Thompson-Higman groups, and circuit complexity", Mathematics ArXiv: math.GR/0607349, July 2006.

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

[4] J.C. Birget, "Circuits, coNP-completeness, and the groups of Richard Thompson", *International J. of Algebra and Computation*, 16(1) (Feb. 2006) 35-90 (Mathematics ArXiv: http://arXiv.org/abs/math.GR/0310335, Oct. 2003).

[5] M. Brin, C. Squier, "Groups of piecewise linear homeomorphisms of the real line", *Inventiones Mathematicae* 79 (1985) 485-498.

[6] M. Brin, "The Chameleon Groups of Richard J. Thompson: Automorphisms and Dynamics", *Publications Math. de l'IHES* 84 (1997) 5-33.

[7] K. Brown, R. Geoghegan, "An infinite-dimensional torsion-free FP_∞ group", *Inventiones Mathematicae* 77 (1984) 367-381.

[8] J. Burillo, S. Cleary, M. Stein, J. Taback, "Combinatorial and metric properties of Thompson's group T", Mathematics ArXiv math.GR/0503670; to appear in *Transactions of the AMS*.

[9] J. W. Cannon, W. J. Floyd, W. R. Parry, "Introductory notes on Richard Thompson's groups", *L'Enseignement Mathématique* 42 (1996) 215-256.

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

[11] J. Cuntz, "Simple C*-algebras", *Communications in Mathematical Physics* 57 (1977) 173-185.

[12] P. Dehornoy, "Geometric presentations for Thompson's groups", *J. of Pure and Applied Algebra* 203 (2005) 1-44.

[13] J. Dixmier, "Traces sur les C*-algèbres II", *Bulletin des Sciences Mathématiques* 88 (1964) 39-57.

[14] E. Ghys, V. Sergiescu, "Sur un groupe remarquable de difféomorphismes du cercle", *Commentarii Mathematici Helvetici* 62(2) (1987) 185-239.

[15] V. Guba, M.V. Sapir, "Diagram groups", *Memoirs American Math. Soc.*, 130 no. 620 (1997), viii+117 pages.

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

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

[18] J. Hopcroft, J. Ullman, *Introduction to Automata Theory, Languages, and Computation*, Addison-Wesley (1979).

[19] B. Hughes, "Trees, Ultrametrics, and Noncommutative Geometry" ,(revised March 2006), 60 pages; PDF `http://www.math.vanderbilt.edu/~hughescb`

[20] M.V. Lawson, "Orthogonal completions of the polycyclic monoids", *Communications in Algebra*, to appear.

[21] H. Lewis, Ch. Papadimitriou, *Elements of the Theory of Computation*, 2nd ed., Prentice Hall (1998).

[22] 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.

[23] V.V. Nekrashevych, "Cuntz-Pimsner algebras of group actions", *J. Operator Theory* 52(2) (2004) 223-249.

[24] Elizabeth A. Scott, "A construction which can be used to produce finitely presented infinite simple groups", *J. of Algebra* 90 (1984) 294-322.

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

[26] 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.

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