Newcastle University ePrints

Barker N, Duncan AJ, Robertson DM. The power conjugacy problem in Higman-Thompson groups. *International Journal of Algebra and Computation* 2016, 26(2), 309-374.

Copyright:

© 2016 World Scientific Publishing Company. Published with Open Access.

DOI link to article:

http://dx.doi.org/10.1142/S0218196716500144

Date deposited:

26/05/2016

This work is licensed under a Creative Commons Attribution 4.0 International License

Newcastle University ePrints - eprint.ncl.ac.uk

International Journal of Algebra and Computation
Vol. 26, No. 2 (2016) 309–374
© World Scientific Publishing Company
DOI: 10.1142/S0218196716500144

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

The power conjugacy problem in Higman–Thompson groups

Nathan Barker
Department for Pure Mathematics and Mathematical Statistics
Cambridge University, CB3 OWB, UK
nb443@cam.ac.uk

Andrew J. Duncan* and David M. Robertson†
School of Mathematics and Statistics, Newcastle University
Newcastle upon Tyne, NE1 7RU, UK
**andrew.duncan@ncl.ac.uk*
†*d.m.robertson@newcastle.ac.uk*

Received 2 March 2015
Accepted 18 January 2016
Published 9 March 2016

Communicated by M. Sapir

An introduction to the universal algebra approach to Higman–Thompson groups (including Thompson's group V) is given, following a series of lectures by Graham Higman in 1973. In these talks, Higman outlined an algorithm for the conjugacy problem; which although essentially correct fails in certain cases, as we show here. A revised and complete version of the algorithm is written out explicitly. From this, we construct an algorithm for the power conjugacy problem in these groups. Python implementations of these algorithms can be found in [26].

Keywords: Higman–Thompson; conjugacy problem; power conjugacy.

Mathematics Subject Classification: 20E32, 20F10, 20F29

1. Introduction

In 1965, Thompson introduced the group now called "Thompson's group V" and its subgroups $F < T$. In doing so he gave the first examples (namely V and T) of finitely presented, infinite simple groups (see [11, 28]). McKenzie and Thompson [23] later used V to construct finitely presented groups with unsolvable word problem. Subsequently, Galvin and Thompson (unpublished) identified V with the automorphism group of an algebra $V_{2,1}$, studied by Jónsson and Tarski [18]. Higman [17] generalized this construction, defining $G_{n,r}$ as the automorphism group of a generalization $V_{n,r}$ of $V_{2,1}$, for $n \geq 2$ and $r \geq 1$. Moreover, Higman showed that the commutator subgroup of $G_{n,r}$ is a finitely generated, infinite, simple group, for all

$n \geq 2$. ($G_{n,r}$ is perfect when n is even, and its commutator subgroup has index 2 when n is odd.)

The groups $G_{n,r}$ are the "Higman–Thompson" groups of the title. There are many isomorphic groups in this set: in fact the algebras $V_{n,r}$ and $V_{n',r'}$ are isomorphic if and only if $n = n'$ and $r \equiv r' \bmod n-1$; so $G_{n,r} \cong G_{n',r'}$ if $n = n'$ and $r \equiv r' \bmod n-1$. Higman [17] showed that there are infinitely many non-isomorphic groups $G_{n,r}$ and gave necessary conditions for such groups to be isomorphic. Recently Pardo [24] completed the isomorphism classification, showing that Higman's necessary conditions are also sufficient: that is $G_{n,r} \cong G_{n',r'}$ if and only if $n = n'$ and $\gcd(n-1, r) = \gcd(n'-1, r')$. Higman–Thompson groups have been much studied and further generalized: we refer to [11, 8, 6, 22, 15, 10] for example.

In this paper, we consider the conjugacy and power conjugacy problems in Higman–Thompson groups. We use Higman's method, describing the groups $G_{n,r}$ in terms of universal algebra. This allows us to give a detailed description of the algorithm for the conjugacy problem; and to uncover a gap in the original algorithm proposed by Higman. To be precise, [17, Lemma 9.6] is false, and consequently the "orbit sharing" algorithm in [17] does not always detect elements in the same orbit of an automorphism. The orbit sharing algorithm is crucial to the algorithm for conjugacy given in [17], which may fail to recognize that a pair of elements of $G_{n,r}$ is conjugate. Fortunately it is not difficult to complete the algorithm. We then extend these results to construct an algorithm for the power conjugacy problem: that is, given elements g, h in a group G decide whether or not there exist nonzero integers a and b such that g^a is conjugate to h^b.

The power conjugacy problem though less well known than the conjugacy problem, already occurs as one of the problems in the hierarchy of decision problems studied by Lipschutz and Miller [20]. The problem has been shown to be decidable in, for example, certain HNN-extensions and free products with cyclic amalgamation [1, 14], in certain one-relator groups [25], in Artin groups of extra large type [5], in groups with small cancellation conditions C(3) and T(6) [4] and in free-by-cyclic groups [7]. Cryptographic protocols based on the power conjugacy search problem have been proposed, see for example [19], although these may be susceptible to attack by quantum computer [16].

The third author has implemented the algorithms described in this paper in Python [26]. In fact it was the process of testing this implementation which uncovered the existence of an orbit unrecognized in [17]; and it became evident that the algorithms of [17] were incomplete.

Note that other approaches to algorithmic problems in $G_{n,r}$ have been developed. For example [27] proposes an algorithm for the conjugacy problem in $G_{2,1}$ based on the revealing tree pairs of Brin [8]. In [6] the same methods are used to study the centralizers of elements of $G_{n,1}$ for $n \geq 2$. Again Belk and Matucci [3] gave a solution to the conjugacy problem in $G_{2,1}$ based on strand diagrams. In another direction, Higman's methods were used by Brown [9] to show that all the Higman–Thompson groups are of type FP_∞. This discussion of finiteness properties

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

has been extended to generalizations of Higman–Thompson groups, by Martinez-Perez and Nucinkis [22].

In detail the contents of the paper are as follows. In order to make this account self-contained, we begin with an introduction to universal algebra. Sec. 2, outlines the universal algebra required, following Cohn's account [13]. In Sec. 2.1, we introduce Ω-algebras; that is universal algebras with signature Ω. Sections 2.2 and 2.3 cover quotients of Ω-algebras, varieties of Ω-algebras and free Ω-algebras. We use this machinery in Sec. 3 to define the algebras $V_{n,r}$ and establish their basic properties, following the exposition of [17].

The groups $G_{n,r}$ are defined in Sec. 4 as the automorphism groups of $V_{n,r}$. We represent elements of $G_{n,r}$ as bijections between carefully chosen generating sets of the algebras $V_{n,r}$. This is done in two stages, beginning with the semi-normal forms of Sec. 4.1. There are many ways of representing a given automorphism in *semi-normal* form, but in Sec. 4.2 it is shown that this representation may be refined to a unique *quasi-normal* form. Furthermore, an algorithm is given which takes an automorphism and produces a quasi-normal form representation.

The solution to the conjugacy problem is based on an analysis of certain orbits of automorphisms in quasi-normal form, and we give a full account of this analysis in Secs. 4.1 and 4.2. Here we follow [17] except that, as pointed out above, there exist orbits of types not recognized there, which give automorphisms in quasi-normal form a richer structure, as described here.

Section 5 contains the algorithm for the conjugacy problem. This involves breaking an automorphism down into well-behaved parts. It is shown that every element of $G_{n,r}$ decomposes into factors which are called *periodic* and *regular infinite* parts. The conjugacy problem for periodic and regular infinite components is solved separately and then the results recombined. The decomposition into these parts is the subject of Sec. 5.1 and here we give the main algorithm for the conjugacy problem, Algorithm 5.6. This algorithm depends on algorithms for periodic and regular infinite automorphisms: namely Algorithm 5.13 in Sec. 5.3 and Algorithm 5.27 in Sec. 5.4.

In Sec. 6, we turn to the power conjugacy problem. In the version considered here the problem is, given $g, h \in G_{n,r}$ to find all pairs of nonzero integers (a, b) such that g^a is conjugate to h^b. Again the problem splits into the periodic and regular infinite parts. The periodic part is straightforward, and reduces to the conjugacy problem; see Sec. 6.1. The algorithm for power conjugacy of regular infinite elements is Algorithm 6.13, in Sec. 6.3 and gives the main result of the paper Theorem 6.14: that the power conjugacy problem is solvable. On input $g, h \in G_{n,r}$ the algorithm returns a (possibly empty) set S consisting of all pairs of integers (a, b) such that g^a and h^b are conjugate; as well as a conjugator, for each pair.

In outline, the main steps of the algorithm for the (power-)conjugacy problem are:

- Lemma 4.28 which computes the quasi-normal basis of a given automorphism.
- Lemma 4.30, the "component-sharing test", as in Higman's original algorithm.

- Lemma 4.34, the "orbit-sharing test", which recognizes and combines components which belong to a single orbit.
- Algorithm 5.6 which is Higman's solution to the conjugacy problem.
- Algorithm 6.13 which determines if two automorphisms are power conjugate.

The examples given throughout the text are used as examples in [26], from where these and other examples may be run through the third author's implementations of the algorithms. To find Example $x.y$ in [26], follow the instructions in the documentation to install the program; then run

```
>>> from thompson import *
>>> f = load_example('example_x_y')
```

in a Python session. The automorphism will then be available as the Python object `f`.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

2. Universal Algebra

2.1. Ω-*algebras*

In this section, we review enough universal algebra to underpin the construction of the Higman–Thompson groups in later sections. We follow [13].

Definition 2.1. An *operator domain* consists of a set Ω and a mapping $a : \Omega \to \mathbb{N}_0$. The elements of Ω are called *operators*. If $\omega \in \Omega$, then $a(\omega)$ is called the *arity* of ω. We shall write $\Omega(n) = \{\omega \in \Omega \mid a(\omega) = n\}$, and refer to the members of $\Omega(n)$ as *n-ary operations*.

An *algebra* with *operator domain* (or *signature*) Ω consists of a set S, called the *carrier* of the algebra, and a family of maps $\{\varphi_\omega\}_{\omega\in\Omega}$ indexed by Ω, such that for $\omega \in \Omega(n)$, φ_ω is a map from S^n to S.

Following [13] we suppress all mention of the maps φ_ω, identifying φ_ω with ω, and referring to any algebra with carrier S and operator domain Ω as an Ω-*algebra*, which we denote by (S, Ω). For example, a group $(G, \cdot, ^{-1}, 1)$ is a Ω-algebra with operator domain $\{\cdot, ^{-1}, 1\}$ and carrier G, where $\cdot$ is binary, $^{-1}$ is unary and 1 is a constant. For this to describe a group, certain laws must hold between these operations, i.e. the group axioms.

Given an Ω-algebra (S, Ω) and $f \in \Omega(n)$, we write $s_1 \cdots s_n f$ for the image of the n-tuple $(s_1, \ldots, s_n) \in S^n$ under f. We say that a subset $T \subseteq S$ is *closed under the operations of* Ω (or that T is Ω-*closed*) if, for all $n \geq 0$, for all f in $\Omega(n)$ and for all $s_1, \ldots, s_n \in T$ the element $s_1 \cdots s_n f$ is also an element of T. Indeed, if T is a subset of S then T is Ω-closed if and only if (T, Ω) is an Ω-algebra: which brings us to the next definition.

Definition 2.2. Given an Ω-algebra (S, Ω), an Ω-*subalgebra* is an Ω-algebra (T, Ω) whose carrier T is a subset of S.

The intersection of any family of subalgebras is again a subalgebra. Hence, for any subset X of the set S we may define the subalgebra $\langle X \rangle$ *generated* by X to

be the intersection of all subalgebras containing X. The subalgebra $\langle X\rangle$ may also be defined recursively: that is $\langle X\rangle$ is the subset of S such that (i) $X \subseteq \langle X\rangle$, (ii) if $y_1, \ldots, y_n \in \langle X\rangle$ then $y_1 \cdots y_n f \in \langle X\rangle$, for all $f \in \Omega(n)$ and (iii) if s does not satisfy (i) or (ii) then s does not belong to $\langle X\rangle$. Loosely speaking we might say that $\langle X\rangle$ is obtained from X by applying a finite sequence of operations of Ω. If the subalgebra generated by X is the whole of S, then X is called a *generating set* for (S, Ω).

A mapping $g : \mathcal{A} \to \mathcal{B}$ between two Ω-algebras $\mathcal{A} = (S, \Omega), \mathcal{B} = (S', \Omega)$ is said to be *compatible* with $f \in \Omega(n)$ if, for all $s_1, \ldots, s_n \in S$,

$$(s_1 g) \cdots (s_n g) f = (s_1 \cdots s_n f) g.$$

If g is compatible with each $f \in \Omega$, it is called a *homomorphism* from $\mathcal{A} = (S, \Omega)$ to $\mathcal{B} = (S', \Omega)$. If a homomorphism g from $\mathcal{A}$ to $\mathcal{B}$ has an inverse g^{-1} which is again a homomorphism, g is called an *isomorphism* and then the Ω-algebras $\mathcal{A} = (S, \Omega), \mathcal{B} = (S', \Omega)$ are said to be *isomorphic*. An isomorphism of an algebra $\mathcal{A} = (S, \Omega)$ with itself is called an *automorphism* and a homomorphism of an algebra into itself is called an endomorphism. A homomorphism is determined once the images of a generating set are fixed.

Proposition 2.3 ([13, Proposition 1.1]). *Let $g, h : \mathcal{A} \to \mathcal{B}$ be two homomorphisms between Ω-algebras $\mathcal{A} = (S, \Omega), \mathcal{B} = (S', \Omega)$. If g and h agree on a generating set for $\mathcal{A}$, then they are equal.*

From a family $\{\mathcal{A}_i\}_{i=1}^m$ ($\mathcal{A}_i = (S_i, \Omega)$) of Ω-algebras we can form the *direct product* $P = \prod_{i=1}^m \mathcal{A}_i$ of Ω-algebras. Its set is the Cartesian product S of the S_i, and the operations are carried out component wise. Thus, if $\pi_i : S \to S_i$ are the projections from the product to the factors then any $f \in \Omega$ of arity n is defined on S^n by the equation

$$(p_1 \cdots p_n f)\pi_i = (p_1 \pi_i) \cdots (p_n \pi_i) f,$$

where $p_i \in S$.

Let $\mathcal{C}$ be a class of Ω-algebras, whose elements we will call $\mathcal{C}$-algebras. By a *free $\mathcal{C}$-algebra* on a set X we mean a $\mathcal{C}$-algebra F with the following universal property.

> There is a mapping $\mu : X \to F$ such that every mapping $f : X \to \mathcal{A}$ into a $\mathcal{C}$-algebra $\mathcal{A}$ can be factored uniquely by μ to give a homomorphism from F to $\mathcal{A}$, i.e. there exists a unique homomorphism $f' : F \to \mathcal{A}$ such that $\mu f' = f$.

In this case we say that X is a *free generating set* or a *basis* for F. If X is a subset of F then we shall always assume that μ is the inclusion map. Not every class has free algebras, but they do exist in the class under consideration here (see Proposition 2.16).

A *free product* is defined similarly, replacing the set X by a collection of $\mathcal{C}$ algebras. Given an indexing set I and for each $i \in I$ an Ω algebra A_i from $\mathcal{C}$ the

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

free product $\mathcal{A}$ of $\{A_i\}_{i\in I}$, written $\mathcal{A} = *_{i\in I}\mathcal{A}_i$, is an Ω-algebra in $\mathcal{C}$ satisfying the following property.

> There exist homomorphisms $\mu_i : A_i \to \mathcal{A}$, for all $i \in I$, such that for any Ω-algebra $\mathcal{B}$ and homomorphisms $f_i : A_i \to \mathcal{B}$, for all $i \in I$, there exists a unique homomorphism $f' : \mathcal{A} \to \mathcal{B}$ such that $\mu_i f' = f_i$, for all i.

Given collections $\{\mathcal{A}_i\}_{i\in I}$ and $\{\mathcal{B}_i\}_{i\in I}$ of Ω-algebras such that there exist free products $\mathcal{A} = *_{i\in I}\mathcal{A}_i$ and $\mathcal{B} = *_{i\in I}\mathcal{B}_i$, then, by definition, there exist homomorphisms $\mu_i : \mathcal{A}_i \to \mathcal{A}$ and $\mu'_i : \mathcal{B}_i \to \mathcal{B}$, for all $i \in I$. In this case, given homomorphisms $f_i : \mathcal{A}_i \to \mathcal{B}_i$, for all $i \in I$, the composition $f_i\mu'_i$ is a homomorphism from $\mathcal{A}_i$ to $\mathcal{B}$, so there exists a unique homomorphism $f' : \mathcal{A} \to \mathcal{B}$, with $\mu_i f' = f_i\mu'_i$, for all $i \in I$. We denote f' by $*_{i\in I} f_i$.

2.2. *Congruence on an Ω-algebra*

A *relation* between two sets S and R is defined to be a subset of the Cartesian product $S \times R$. A *mapping* $f : S \to R$ is a relation $\Gamma_f \subset S \times R$ with the properties that for each $s \in S$ there exists $r \in R$ such that $(s, r) \in \Gamma_f$ (everywhere defined) and if $(s, r), (s, r') \in \Gamma_f$ then $r = r'$ (single valued). A relation $\Gamma \subset S \times R$ has an *inverse* Γ^{-1}, defined by

$$\Gamma^{-1} = \{(r, s) \in R \times S \mid (s, r) \in \Gamma\};$$

and if $\Delta \subset R \times T$ is a relation then the composition $\Gamma \circ \Delta$ of Γ and Δ is defined by

$$\Gamma \circ \Delta = \{(s, t) \in S \times T \mid (s, x) \in \Gamma \text{ and } (x, t) \in \Delta \text{ for some } x \in R\}.$$

If $\Gamma \subset S \times R$ and $S' \subset S$ we define

$$S'\Gamma = \{r \in R \mid (s, r) \in \Gamma \text{ for some } s \in S'\}.$$

Given a set S the *identity relation* $1_S = \{(s, s) \mid s \in S\}$ and the *universal relation* $S^2 = \{(s, s') \mid s, s' \in S\}$ always exist.

An *equivalence* on a set S is a subset Γ of S^2 with the properties $\Gamma \circ \Gamma \subset \Gamma$ (transitivity): $\Gamma^{-1} = \Gamma$ (symmetry) and $1_S \subseteq \Gamma$ (reflexivity). The *equivalence class* of $s \in S$ is $\{s' \in S \mid (s, s') \in \Gamma\} = \{s\}\Gamma$. Given any subset U of $S \times S$, the *equivalence generated* by U is

$$E = \bigcap\{V \subseteq S \times S \mid V \text{ is an equivalence and } U \subseteq V\};$$

that is, the smallest equivalence E on S containing U. It follows that E is

$$\{(a, b) \in S \times S \mid \text{there exists } a_0, \ldots, a_n \text{ such that } a_0 = a,\ a_n = b \text{ and } (a_i, a_{i+1}) \in U\}.$$

Of particular interest in the study of Ω-algebras are relations which are also subalgebras. Firstly, if $\mathcal{A} = (S, \Omega)$ and $\mathcal{B} = (R, \Omega)$ are Ω-algebras and $\Gamma \subset S \times R$ is a relation which is closed under the operations of Ω, as defined in $\mathcal{A} \times \mathcal{B}$, then (Γ, Ω) is a subalgebra of $\mathcal{A} \times \mathcal{B}$. In this case we abuse notation and say Γ is a subalgebra of $\mathcal{A} \times \mathcal{B}$.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Lemma 2.4 ([13, Lemma 2.1, Chap. 1]). *Let $\mathcal{A}, \mathcal{B}, \mathcal{C}$ be Ω-algebras and let Γ, Δ be subalgebras of $\mathcal{A} \times \mathcal{B}, \mathcal{B} \times \mathcal{C}$ respectively. Then Γ^{-1} is a subalgebra of $\mathcal{B} \times \mathcal{A}, \Gamma \circ \Delta$ is a subalgebra of $\mathcal{A} \times \mathcal{C}$ and if $\mathcal{A}'$ is a subalgebra of $\mathcal{A}$, with carrier $S' \subseteq S$, then $(S'\Gamma, \Omega)$ is a subalgebra of $\mathcal{B}$.*

Let S and T be sets and $f : S \to T$ a mapping between them. The *image* of f is defined as $S\Gamma_f$, and the *kernel* of f is defined as

$$\ker f = \{(x, y) \in S^2 \mid xf = yf\}.$$

The latter is an equivalence on S; the equivalence classes are the inverse images of elements in the image (sometimes called the fibers of f).

Example 2.5 (Groups). Given a group homomorphism $f : G \to H$, the (group-theoretic) kernel of f is a normal subgroup N; and the different cosets of N in G are the fibers of f. So, the equivalence classes of $\ker f$, in the definition above, are the cosets of N in G.

A *congruence* on an Ω-algebra $\mathcal{A} = (S, \Omega)$ is an equivalence on S which is also a subalgebra of $\mathcal{A}^2$ i.e. an equivalence $\Gamma \subset S \times S$ which is Ω-closed. From the above, $1_{\mathcal{A}}$ and $\mathcal{A}^2$ are congruences on $\mathcal{A}$. Given any subset $U \subseteq S \times S$ the *congruence generated by* U is

$$C = \bigcap \{V \subseteq S \times S \mid V \text{ is a congruence and } U \subseteq V\}.$$

It follows that C is the smallest congruence on $\mathcal{A}$ containing U.

Let $\mathcal{A}$ be an Ω-algebra. By definition a congruence is an equivalence which admits the operations ω ($\omega \in \Omega$). Now each n-ary operator ω defines an n-ary operation on $\mathcal{A}$:

$$(a_1, \ldots, a_n) \mapsto a_1 \cdots a_n \omega \text{ for } a_1, \ldots, a_n \in \mathcal{A}. \tag{2.1}$$

By giving fixed values in $\mathcal{A}$ to some of the arguments, we obtain r-ary operations for $r \leq n$. In particular, if we fix all the a_j except one, say the ith, we obtain, for any $n-1$ fixed elements $a_1, \ldots, a_{n-1} \in \mathcal{A}$, a unary operation

$$x \mapsto a_1 \cdots a_{i-1} x a_i \cdots a_{n-1} \omega; \tag{2.2}$$

and this applies for all $i \in \{1, \ldots, n\}$. We say that the operation (2.2) is an *elementary translation* (derived from Ω by specialization in $\mathcal{A}$). Given a finite sequence $\tau_1, \ldots, \tau_n$ of elementary transformations the composition $\tau = \tau_1 \circ \cdots \circ \tau_n$ is also a unary operation on $\mathcal{A}$, which we call a *translation*. (In particular we allow $n = 0$ in this definition, so the identity map on $\mathcal{A}$ is a translation.)

Proposition 2.6 ([12, Proposition 6.1, Chap. 6]). *An equivalence $\mathfrak{q}$ on an Ω-algebra $\mathcal{A}$ is a congruence if and only if it is closed under all translations. More precisely, a congruence is closed under all translations, while any equivalence which is closed under all elementary translations is a congruence.*

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Remark 2.7. If $U \subseteq S \times S$, then the congruence generated by U can be seen to consist of pairs $(a, b) \in S \times S$ such that there exist $m \geq 0$, $a_0, \ldots, a_m \in S$, and a translation τ with

- $a_0 = a$, $a_m = b$ and
- $(a_i, a_{i+1}) = (u_i\tau, u_{i+1}\tau)$,

where either $(u_i, u_{i+1}) \in U$, $(u_{i+1}, u_i) \in U$ or $u_i = u_{i+1}$. That is, there exist $s_1, \ldots, s_{n-1} \in S$, $u_0, \ldots, u_m \in S$, and $\omega \in \Omega(n)$ such that $(u_i, u_{i+1}) \in U \cup U^{-1} \cup 1_S$ and setting

$$a_i = (s_1, \ldots, s_{j-1}, u_i, s_j, \ldots, s_{n-1})\omega,$$

for $0 \leq i \leq m$, we have $a = a_0$ and $b = a_m$.

The next two theorems explain the significance of congruences for Ω-algebras and will be used in the following section on free algebras and varieties.

Theorem 2.8 ([13, Theorem 2.2, Chap. 1]). *Let $g : \mathcal{A} \to \mathcal{B}$ be a homomorphism of Ω-algebras. Then the image of g is a subalgebra of $\mathcal{B}$ and the kernel of g is a congruence on $\mathcal{A}$.*

Theorem 2.9 ([13, Theorem 2.3, Chap. 1]). *Let $\mathcal{A}$ be an Ω-algebra and $\mathfrak{q}$ a congruence on $\mathcal{A}$. Then, there exists a unique Ω-algebra, denoted $\mathcal{A}/\mathfrak{q}$, with carrier the set of all $\mathfrak{q}$-classes such that the natural mapping $\nu : \mathcal{A} \to \mathcal{A}/\mathfrak{q}$ is a homomorphism.*

The homomorphism ν in the previous theorem, which maps an element s of the carrier of $\mathcal{A}$ to its $\mathfrak{q}$-equivalence class, is called the *natural homomorphism* from $\mathcal{A}$ to $\mathcal{A}/\mathfrak{q}$. The algebra $\mathcal{A}/\mathfrak{q}$ is called the *quotient algebra* of $\mathcal{A}$ by $\mathfrak{q}$.

Example 2.10. Given a group G and a normal subgroup N of G, the natural mapping $G \to G/N$ is a homomorphism.

2.3. *Free algebras and varieties*

Let $X = \{x_1, x_2, \ldots\}$ be a non-empty, finite or countably enumerable set, called an *alphabet*, and Ω an operator domain, with $\Omega \cap X = \emptyset$. We define an Ω-algebra as follows. An Ω-*row* in X is a finite sequence of elements of $\Omega \cup X$. The set of all Ω-rows in X is denoted as $W(\Omega; X)$. The *length* of the Ω-row $w = w_1 \cdots w_m$ (where $w_i \in \Omega \cup X$) is defined to be m and is written as $|w|$. The carrier of our Ω-algebra is $W(\Omega; X)$, the set of Ω-rows.

We define the action of elements Ω on $W(\Omega; X)$ by concatenation. First observe that if u and v are Ω-rows then the concatenation uv of u with v is also an Ω-row, and this may be extended to the concatenation of arbitrarily many Ω-rows in the obvious way. For $f \in \Omega(n)$ and $u_1, \ldots, u_n \in W(\Omega; X)$, we define the image of the

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

n-tuple $(u_1, \ldots, u_n) \in W(\Omega, X)^n$ under the operation f to be the Ω-row $u_1 \cdots u_n f$. By abuse of notation we will refer to $W(\Omega; X)$ as an Ω-algebra.

The alphabet $X \subset W(\Omega; X)$ and we call the subalgebra generated by X the Ω-*word algebra* on X, denoted $W_\Omega(X)$. Its elements are called Ω-*words* in the alphabet X. There is a clear distinction between Ω-rows that are Ω-words and those that are not. For example, if f is a binary operation then

$$x_1 x_2 x_3 f x_4 f f = (x_1, ((x_2, x_3)f, x_4)f)f$$

is a Ω-row which is also an Ω-word, whereas $x_1 f f x_2 f x_3$ is an Ω-row which is not an Ω-word.

Definition 2.11 ([13, Chap. 1]). We define the *valency* of an Ω-row $w = w_1 \cdots w_m$ $(w_i \in \Omega \cup X)$ as $v(w) = \sum_{i=1}^m v(w_i)$ where

$$v(w_i) = \begin{cases} 1, & \text{if } w_i \in X, \\ 1 - \text{arity}(w_i), & \text{if } w_i \in \Omega. \end{cases}$$

Proposition 2.12 ([13, Proposition 3.1, Chap. 1]). *An Ω-row $w = w_1 \cdots w_m$ in $W(\Omega; X)$ is an Ω-word if and only if every left-hand factor $u_i = w_1 \cdots w_i$ of w satisfies*

$$v(u_i) > 0 \text{ for } i = 1, \ldots, m \quad \text{and} \quad v(w) = 1.$$

Moreover, each Ω-word can be obtained in precisely one way by applying a finite sequence of operations of Ω to elements of X.

Let $\mathcal{A}$ be an Ω-algebra. If in an element w of $W_\Omega(X)$ we replace each element of X by an element of $\mathcal{A}$ we obtain a unique element of $\mathcal{A}$. For $|w| = 1$, this is clear, so assume $|w| > 1$ and we will use induction on the length of w. We have $w = u_1 \cdots u_n f$ $(f \in \Omega(n),\ u_i \in W_\Omega(X))$, where, by Proposition 2.12, the u_i are uniquely determined once w is given. By induction each u_i becomes a unique element $a_i \in \mathcal{A}$, when we replace the elements of X by elements of $\mathcal{A}$. Hence w becomes $a_1 \cdots a_n f$; a uniquely determined element of $\mathcal{A}$.

This establishes the next theorem.

Theorem 2.13 ([13, Theorem 3.2, Chap. 1]). *Let $\mathcal{A}$ be an Ω-algebra and let X be a set. Then any injective mapping $\theta : X \to \mathcal{A}$ extends, in just one way, to a homomorphism $\bar{\theta} : W_\Omega(X) \to \mathcal{A}$. That is, $W_\Omega(X)$ is a free Ω-algebra, freely generated by X.*

Corollary 2.14 ([13, Corollary 3.3, Chap. 1]). *Any Ω-algebra $\mathcal{A}$ can be expressed as a homomorphic image of an Ω-word algebra $W_\Omega(X)$ for a suitable set X. Here X can be taken to be any set mapping onto a generating set of $\mathcal{A}$.*

By an *identity* or *law* over Ω in X we mean a pair $(u, v) \in W_\Omega(X) \times W_\Omega(X)$ or an equation $u = v$ formed from such a pair. We say that the law (u, v) *holds* in the Ω-algebra $\mathcal{A}$ or that $\mathcal{A}$ *satisfies* the equation $u = v$ if every homomorphism $W_\Omega(X) \to \mathcal{A}$ maps u and v to the same element of $\mathcal{A}$. This correspondence between

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

sets of laws and classes of algebras establishes a pair of maps, with the following definitions.

- Given a set Σ of laws over Ω in X, form $\mathcal{V}_\Omega(\Sigma)$, the class of all Ω-algebras satisfying all the laws in Σ. This class $\mathcal{V}_\Omega(\Sigma)$ is called the *variety* generated by Σ.
- Given a class $\mathcal{C}$ of Ω-algebras we can form the set $\mathfrak{q} = \mathfrak{q}(\mathcal{C})$ of all laws over Ω in X which hold in all algebras of $\mathcal{C}$.

Thus we have a pair of maps $\mathcal{V}_\Omega$ and $\mathfrak{q}$; relating each variety of Ω-algebras to a relation $\mathfrak{q}$ on $W_\Omega(X)$ and vice-versa. We shall see below that $\mathfrak{q}(\mathcal{C})$ is a congruence, but first we make a further definition.

A subalgebra of an Ω-algebra $\mathcal{A}$ is called *fully invariant* if it is mapped into itself by all endomorphisms of $\mathcal{A}$. A congruence Γ on $\mathcal{A}$ is said to be *fully invariant* if $(u, v) \in \Gamma$ implies $(u\theta, v\theta) \in \Gamma$, for all endomorphisms θ of $\mathcal{A}$. The *fully invariant congruence generated by* Γ is

$$\mathcal{I} = \bigcap \{V \mid V \text{ is a fully invariant congruence and } \Gamma \subseteq V\}.$$

It follows that $\mathcal{I}$ is the smallest invariant congruence on $\mathcal{A}$ generated by Γ.

We claim that if $\mathcal{C}$ is a class of Ω-algebras then $\mathfrak{q}(\mathcal{C})$ is a fully invariant congruence on $W_\Omega(X)$. To see that $\mathfrak{q}(\mathcal{C})$ is a congruence, note that in every class $\mathcal{C}$ of Ω-algebras we have the following: $u = u$ for all $u \in W_\Omega(X)$; if $u = v$ holds then so does $v = u$; and if $u = v$ and $v = w$ then also $u = w$. Further, if $u_i = v_i$ for $i = 1, \ldots, n$ are laws holding in $\mathcal{A}$ and if $\omega \in \Omega(n)$, then $u_1 \cdots u_n\omega = v_1 \cdots v_n\omega$ holds in $\mathcal{A}$. Hence $\mathfrak{q}(\mathcal{C})$ is indeed a congruence.

To see that $\mathfrak{q}(\mathcal{C})$ is a fully invariant congruence, let $(u, v) \in \mathfrak{q}(\mathcal{C})$ and let θ be any endomorphism of $W_\Omega(X)$. If $\mathcal{A} \in \mathcal{C}$ and $\alpha : W_\Omega(X) \to \mathcal{A}$ is any homomorphism, then so is $\theta\alpha$, hence $u\theta\alpha = v\theta\alpha$. Thus the law $u\theta = v\theta$ holds in $\mathcal{A}$, so $(u\theta, v\theta) \in \mathfrak{q}(\mathcal{C})$ and thus $\mathfrak{q}(\mathcal{C})$ is a fully invariant congruence. Cohn shows in addition that the map $\mathcal{V}_\Omega$ is a bijection with inverse $\mathfrak{q}$, and deduces the following theorem.

Given sets S and T and a relation Γ from S to T, we may use Γ to define a system of subsets of S, T, as follows. For any subset X of S we define a subset X^* of T by

$$X^* = \{y \in T \mid (x, y) \in \Gamma \text{ for all } x \in X\} = \bigcap_{x \in X} \{x\}\Gamma,$$

and similarly, for any subset Y of T we define a subset Y^* of S by

$$Y^* = \{x \in S \mid (x, y) \in \Gamma \text{ for all } y \in Y\} = \bigcap_{y \in Y} \{y\}\Gamma^{-1}.$$

We thus have mappings $X \mapsto X^*$ and $Y \mapsto Y^*$ of the power sets of S and T with the following properties:

$$X_1 \subseteq X_2 \Rightarrow X_1^* \supseteq X_2^*, \quad Y_1 \subseteq Y_2 \Rightarrow Y_1^* \supseteq Y_2^*, \tag{2.3}$$

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

$$X \subseteq X^{**}, \quad Y \subseteq Y^{**}, \tag{2.4}$$

$$X^{***} = X^*, \quad Y^{***} = Y^*. \tag{2.5}$$

A pair of maps $X \mapsto X^*$, from the power set 2^S of S to the power set 2^T of T, and $Y \mapsto Y^*$, from 2^T to 2^S, satisfying (2.3)–(2.5) is called a *Galois connection.*

Theorem 2.15 ([13, Theorem 3.5, Chap. 1]). *Let $W = W_\Omega(X)$ be the Ω-word algebra on the alphabet X. The pair of maps $\Sigma \mapsto \mathcal{V}_\Omega(\Sigma)$ and $\mathcal{C} \mapsto \mathfrak{q}(\mathcal{C})$ forms a Galois connection giving a bijection between varieties of Ω-algebras and fully invariant congruences $\mathfrak{q}$ on $W_\Omega(X)$.*

Proposition 2.16 ([13, Proposition 3.6, Chap. 1]). *Let $\mathcal{V}$ be a variety of Ω-algebras and $\mathfrak{q}$ the congruence on $W_\Omega(X)$ (the Ω-word algebra generated by X) consisting of all the laws on $\mathcal{V}$* i.e. *the fully invariant congruence $\mathfrak{q}(\mathcal{V})$. Then $W_\Omega(X)/\mathfrak{q}$ is the free $\mathcal{V}$-algebra on X.*

Suppose Σ is a set of laws over Ω in X and let $\mathcal{V} = \mathcal{V}_\Omega(\Sigma)$ and $\mathfrak{q} = \mathfrak{q}(\mathcal{V})$. Then $\Sigma \subseteq \mathfrak{q}$ and, from Proposition 2.16, $\mathfrak{q}$ is a fully invariant congruence and $W_\Omega(X)/\mathfrak{q}$ is the free $\mathcal{V}$-algebra.

Now let $\mathfrak{p}$ be the fully invariant congruence generated by Σ. Then, as $\Sigma \subseteq \mathfrak{q}$ and $\mathfrak{q}$ is a fully invariant congruence, we have $\mathfrak{p} \subseteq \mathfrak{q}$. Let $\mathcal{A} = W_\Omega(X)/\mathfrak{p}$. Then $\mathcal{A}$ is an Ω-algebra, in which every law of Σ holds (as $\Sigma \subseteq \mathfrak{p}$). Thus $\mathcal{A}$ is a $\mathcal{V}$-algebra. Then, from Proposition 2.16, the natural map $X \to \mathcal{A}$ extends to a homomorphism $W_\Omega(X)/\mathfrak{q} \to \mathcal{A}$. It follows that $\mathfrak{q} \subseteq \mathfrak{p}$. Therefore $\mathfrak{p} = \mathfrak{q} = \mathfrak{q}(\mathcal{V})$. We record this as a corollary which we shall use in Sec. 3 to construct Higman's algebras $V_{n,r}$.

Corollary 2.17. *Let Σ be a set of laws over Ω in X, let $\mathcal{V} = \mathcal{V}_\Omega(\Sigma)$ and $\mathfrak{q} = \mathfrak{q}(\mathcal{V})$. Then $\mathfrak{q}$ is the fully invariant congruence generated by Σ.*

3. The Higman Algebras $V_{n,r}$

In this section, we define the algebras which Higman called $V_{n,r}$. Let $n \geq 2$ be an integer and let $\mathcal{A}$ be an Ω-algebra, with carrier S and operator domain $\Omega = \{\lambda, \alpha_1, \ldots, \alpha_n\}$, such that $a(\alpha_i) = 1$, for $i = 1, \ldots, n$ and $a(\lambda) = n$. We call the n-ary operation $\lambda : S^n \to S$ a *contraction* and the unary operations $\alpha_i : S \to S$ *descending operations.* We define a map $\alpha : S \to S^n$, which we shall call an *expansion*, by

$$v\alpha = (v\alpha_1, \ldots, v\alpha_n),$$

for all $v \in S$. For any subset Y of S, a *simple expansion* of Y consists of substituting some element y of Y by the n elements of the tuple $y\alpha$. A sequence of d simple expansions of Y is called a *d-fold expansion of Y*. A set obtained from Y by a d-fold expansion, $d \geq 0$, is called an *expansion* of Y. For example, if $x \in S$ then $\{x\alpha_1, \ldots, x\alpha_n\}$ is the unique simple expansion of $\{x\}$ and the 2-fold expansions of $\{x\}$ are the sets $\{x\alpha_1, \ldots, x\alpha_{i-1}, x\alpha_i\alpha_1, \ldots, x\alpha_i\alpha_n, x\alpha_{i+1}, \ldots, x\alpha_n\}$, for $1 \leq i \leq n$. Every d-fold expansion of Y has $|Y| + (n-1)d$ elements. Similarly, a

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

simple contraction of Y consists of substituting n distinct elements $\{y_1, \ldots, y_n\} \in Y$ by the single element $(y_1, \ldots, y_n)\lambda$. A set obtained from Y by applying a finite number of simple contractions is called a *contraction* of Y.

From now on in this paper, Ω is fixed as above. Let $\mathbf{x}$ be a non-empty set and recall that the Ω-word algebra $W_\Omega(\mathbf{x})$ is the free Ω-algebra on $\mathbf{x}$.

Definition 3.1. Let Σ_n be the set of laws over Ω in $\mathbf{x}$:

(1) for all $w \in W_\Omega(\mathbf{x})$, $w\alpha\lambda = w$, (or explicitly $w\alpha_1 \cdots w\alpha_n\lambda = w$),
(2) for all $(w_1, \ldots, w_n) \in W_\Omega(\mathbf{x})^n$ and $i \in \{1, \ldots, n\}$, $w_1 \cdots w_n\lambda\alpha_i = w_i$.

That is,

$$\Sigma_n = \{(w\alpha_1 \cdots w\alpha_n\lambda, w) \mid w \in W_\Omega(\mathbf{x})\} \cup \bigcup_{i=1}^{n} \{(w_1 \cdots w_n\lambda\alpha_i, w_i) \mid w_i \in W_\Omega(\mathbf{x})\}.$$

Let $\mathcal{V}_n = \mathcal{V}_\Omega(\Sigma_n)$ the variety of Ω-algebras which satisfy Σ_n and let $\mathfrak{q} = \mathfrak{q}(\mathcal{V}_n)$.

From Proposition 2.16 and Corollary 2.17, it follows that $\mathfrak{q}$ is the fully invariant congruence on $W_\Omega(\mathbf{x})$ generated by Σ_n and $W_\Omega(\mathbf{x})/\mathfrak{q}$ is the free $\mathcal{V}_n$-algebra on $\mathbf{x}$.

Definition 3.2. Let $\mathbf{x}$ be a non-empty, finite or countably enumerable set of cardinality r and $n \geq 2$ an integer. Then $V_{n,r}(\mathbf{x})$ is the free $\mathcal{V}_n$-algebra $W_\Omega(\mathbf{x})/\mathfrak{q}$, where $\mathfrak{q} = \mathfrak{q}(\mathcal{V}_n)$ and $\mathcal{V}_n = \mathcal{V}_\Omega(\Sigma_n)$.

When no ambiguity arises we refer to $V_{n,r}(\mathbf{x})$ as $V_{n,r}$.

Remark 3.3. In [17, Sec. 2] Higman defines a *standard form over* $\mathbf{x}$ to be one of the finite sequences of elements of $\mathbf{x} \cup \{\alpha_1, \ldots, \alpha_n, \lambda\}$ specified by the following rules.

(i) $x\alpha_{i_1} \cdots \alpha_{i_k}$ is a standard form whenever $k \geq 0$, $x \in \mathbf{x}$ and $1 \leq i_j \leq n$ for $j = 1, \ldots, k$.
(ii) If $w_1, \ldots, w_n$ are standard forms then so is $w_1 \cdots w_n\lambda$, unless there is a standard form u such that $w_i = u\alpha_i$ for $i = 1, \ldots, n$.
(iii) No sequence is a standard form unless this follows from (i) and (ii).

We define the descending operations $\alpha_1, \ldots, \alpha_n$ by the rules

$$(x\alpha_{i_1} \cdots \alpha_{i_k})\alpha_i = x\alpha_{i_1} \cdots \alpha_{i_k}\alpha_i,$$
$$(w_1 \cdots w_n\lambda)\alpha_i = w_i$$

for $i \in \{1, \ldots, n\}$. The contraction operation λ is defined by

$$(w_1, \ldots, w_n)\lambda = w_1 \cdots w_n\lambda,$$

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

unless there is a standard form u such that $w_i = u\alpha_i$ for $i = 1, \ldots, n$ in which case

$$(w_1, \ldots, w_n)\lambda = (u\alpha_1, \ldots, u\alpha_n)\lambda = u.$$

These operations turn the set of standard forms into an Ω-algebra. Higman then goes on to prove that this is a free $\mathcal{V}_n$-algebra, freely generated by $\mathbf{x}$ ([17, Lemma 2.1]). This follows in our case from the definition above, and the remarks following it, together with Lemma 3.4 below.

Lemma 3.4. *Let U be an equivalence class of the congruence $\mathfrak{q}$ on $W_\Omega(\mathbf{x})$. Then there exists a unique minimal length element u in U. The unique minimal length elements of equivalence classes are precisely the standard forms of Higman.*

To prove Lemma 3.4, one can use a standard argument which proves a statement of this form in an algebra of an appropriate type. Details may be found in [2, Lemma 2.4.5].

Let y be the minimal length representative of its equivalence class in $V_{n,r}$ i.e. let y be a standard form. Then the *length* of the equivalence class of y is the length of y, denoted $|y|$, and the λ-*length* of the equivalence class of y is the number of times the symbol λ occurs in y.

Now that we have a concrete description of the free algebra $V_{n,r}$ in the variety $\mathcal{V}_n$, we recall those results of [17, Sec. 2], required in the sequel.

Lemma 3.5 (cf. [17, Lemma 2.3]). *Let B be a basis of $V_{n,r}(\mathbf{x})$.*

(1) *Every expansion of B is a basis of $V_{n,r}(\mathbf{x})$.*
(2) *Every contraction of B is a basis of $V_{n,r}(\mathbf{x})$.*

Proof. (1) Let Y be a d-fold expansion of B, where $d \geq 0$. Arguing by induction, we assume that every d-fold expansion of B is a basis of $V_{n,r}$ and show that any simple expansion of Y is also a basis. Let $y \in Y$ and let Y' be the simple expansion

$$Y' = (Y \backslash \{y\}) \cup \{y\alpha_1, \ldots, y\alpha_n\}.$$

Since $y = y\alpha_1 \cdots y\alpha_n\lambda$, the set Y' generates $V_{n,r}$. It remains to show that Y' is a basis for $V_{n,r}$.

Given $\mathcal{A} \in \mathcal{V}_n$ and a map $\theta : Y' \to \mathcal{A}$, we shall show that there is a unique homomorphism $\bar{\theta} : V_{n,r} \to \mathcal{A}$ extending θ. First, define θ^* from Y to $\mathcal{A}$ by $y'\theta^* = y'\theta$, for $y' \in Y \backslash \{y\}$, and $y\theta^* = y\alpha_1\theta \cdots y\alpha_n\theta\lambda$. As Y is a basis, there is a unique homomorphism $\bar{\theta}^*$ from $V_{n,r}$ to $\mathcal{A}$ extending θ^*. Now

$$(y\alpha_i)\bar{\theta}^* = (y\bar{\theta}^*)\alpha_i = (y\theta^*)\alpha_i = (y\alpha_1\theta \cdots y\alpha_n\theta\lambda)\alpha_i = y\alpha_i\theta.$$

Hence $\bar{\theta}^*$ also extends θ. Furthermore, any other homomorphism which extends θ must equal $\bar{\theta}^*$, since any such map must be defined on Y in the same way as θ^*.

(2) This is proved in the same way as (1). □

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

The final statement of Corollary 3.13 forms a partial converse to this lemma, for finite bases. Mostly we work with bases for $V_{n,r}(\mathbf{x})$ which are expansions of $\mathbf{x}$, so we make the following definition.

Definition 3.6. Let $A = \{\alpha_1, \ldots, \alpha_n\} \subset \Omega$. An *$A$-basis* of $V_{n,r}(\mathbf{x})$ is an expansion of $\mathbf{x}$.

If $\mathcal{A} = (S, \Omega)$ is an Ω-algebra with carrier S then we may form the A-algebra (S, A) and the $\{\lambda\}$-algebra $(S, \{\lambda\})$, where the elements of A and $\{\lambda\}$ have actions inherited from $\mathcal{A}$. We call these, respectively, the *A-algebra* and *$\{\lambda\}$-algebra of $\mathcal{A}$*. A subset U of $V_{n,r}$ is said to be *A-closed* if $u\alpha_i \in U$, for all $\alpha_i \in A$, and an A-closed subset is called an *A-subalgebra* of (the A-algebra of) $V_{n,r}$. Similarly $W \subseteq V_{n,r}$ is called a *$\{\lambda\}$-subalgebra* (of the $\{\lambda\}$-algebra of $V_{n,r}$) if it is *$\{\lambda\}$-closed*: that is if $w\lambda \in W$, for all $w \in W$.

Definition 3.7. Let Y be a subset of $V_{n,r}$. The A-subalgebra generated by Y is denoted $Y\langle A\rangle$. The $\{\lambda\}$-subalgebra generated by Y is denoted $Y\langle\lambda\rangle$.

The free monoid on a set L is denoted L^*. If Y is a subset of $V_{n,r}(\mathbf{x})$ then $YA^* = \{y\Gamma \mid y \in Y, \Gamma \in A^*\}$ is A-closed, and it follows that $Y\langle A\rangle = YA^*$. If in addition $Y \subseteq \mathbf{x}\langle A\rangle$, then $y\Gamma$ is a standard form for all $y \in Y$ and $\Gamma \in A^*$. In the sequel we write $Y\langle A\rangle\langle\lambda\rangle$ for $(Y\langle A\rangle)\langle\lambda\rangle$.

Lemma 3.8. *Let B be an A-basis and Y a finite basis for $V_{n,r}(X)$. If $B \subseteq Y\langle A\rangle$ then B is an expansion of Y.*

Proof. Since Y is finite, there exists an expansion of Y contained in $B\langle A\rangle$. Let d be minimal such that there is a d-fold expansion of Y contained in $B\langle A\rangle$, and let W be such a d-fold expansion. Each $w \in W$ is of the form $w = b\Gamma$, for some $b \in B$ and $\Gamma \in A^*$. As $B \subseteq Y\langle A\rangle$ we have $b = y\Delta$, for some $y \in Y$ and $\Delta \in A^*$; so $w = y\Delta\Gamma$. Also, as $w \in W$, there exists $y' \in Y$ such that $w = y'\Gamma'$, as part of an expansion of Y. As Y is a basis it follows that $y = y'$ and $\Delta\Gamma = \Gamma'$.

Suppose that $\Gamma \neq 1$, so that $\Gamma = \Gamma_0\alpha_j$, for some $\alpha_j \in A$ and $\Gamma_0 \in A^*$. As W is an expansion of Y it follows that $y\Delta\Gamma_0\alpha_i \in W$, for all $i \in \{1, \ldots, n\}$. Furthermore $y\Delta\Gamma_0 \in B\langle A\rangle$, so the union

$$W' = (W \backslash \{y\Delta\Gamma_0\alpha_i \mid 1 \leq i \leq n\}) \cup \{y\Delta\Gamma_0\}$$

is contained in $B\langle A\rangle$. Now W' is a simple contraction of W, so W' is a basis by Lemma 3.5. But W' is a $(d-1)$-fold expansion of Y, which contradicts the minimality of d. So $\Gamma = 1$ and $w \in B$, and hence $W \subseteq B$.

Conversely, if $b \in B$ then $b = y\Gamma$, for some $y \in Y$ and $\Gamma \in A^*$. So either $b\Delta = y\Gamma\Delta \in W$ for some $\Delta \in A^*$, or $y\Gamma_0 = w \in W$, where $\Gamma = \Gamma_0\Gamma_1$. In the first case, $b\Delta = w \in B$ implies $w = b$ and $\Delta = 1$. In the second case, $b = y\Gamma = y\Gamma_1\Gamma_0 = w\Gamma_0$, with $w \in B$, so again $w = b$ and $\Gamma_0 = 1$. Thus $B \subseteq W$. □

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

A word $\Gamma \in A^*$ is called *primitive* if it is not a proper power of another word. Explicitly, this means that if Γ is nontrivial and $\Gamma \in \{\Delta\}^*$, for some $\Delta \in A^*$, then $\Gamma = \Delta$.

Proposition 3.9 ([21, Proposition 1.3.1, Chap. 1]). *If $\Gamma^n = \Delta^m$ with $\Gamma, \Delta \in A^*$ and $n, m \geq 0$, there exists a word Λ such that $\Gamma, \Delta \in \{\Lambda\}^*$. In particular, for each word $\Gamma \in A^*$, there exists a unique primitive word Λ such that $\Gamma \in \{\Lambda\}^*$.*

Proposition 3.10 ([21, Proposition 1.3.2, Chap. 1]). *Two words $\Gamma, \Delta \in A^*$ commute if and only if they are powers of the same word. More precisely, the set of words commuting with a word $\Gamma \in A^*$ is a monoid generated by a single primitive word.*

Lemma 3.11 ([17, Sec. 2, Lemma 2.2]). *Let Y be a subset of $V_{n,r}$ and let W be the Ω-subalgebra of $V_{n,r}$ generated by Y. Then*

(1) *$W = Y\langle A\rangle\langle\lambda\rangle$ and*
(2) *for all $w \in W$, the set $w\langle A\rangle \backslash Y\langle A\rangle$ is finite.*

Proof. (1) Let $w \in W$. Then there exists a finite subset Y_0 of Y such that w belongs to the Ω-subalgebra W_0 of $V_{n,r}$ generated by Y_0. Let Z be an expansion of $\mathbf{x}$ such that $|Z| \geq |Y_0|$. Choose a surjection β of Z onto Y_0. As $V_{n,r}$ is freely generated by Z we may extend β to a homomorphism from $V_{n,r}$ to W_0. Let w_0 be the preimage of w under this homomorphism and let l be the λ-length of the standard form of w_0 over Z. By a straightforward induction on l it is apparent that $w_0 \in Z\langle A\rangle\langle\lambda\rangle$. Hence the image w of w_0 in W_0 belongs to $Y_0\langle A\rangle\langle\lambda\rangle \subseteq Y\langle A\rangle\langle\lambda\rangle$, as required.

(2) As in the previous part of the proof, we may assume that W is freely generated by Y. Let $w \in W$ and let l be the λ-length of the standard form of w over Y. Then $w\alpha_{i_1} \cdots \alpha_{i_r} \in Y\langle A\rangle$, whenever $r \geq l$. Hence, the only elements of the set difference $w\langle A\rangle \backslash Y\langle A\rangle$ are those of the form $w\alpha_{i_1} \cdots \alpha_{i_r}$ with $r < l$, and there are only finitely many of these since we only have n choices for each α_{i_j}. □

Lemma 3.12 ([17, Sec. 2, Lemma 2.4]). *Let $\mathbf{x}$ be a set of size $r \geq 1$ and let $X \subseteq V_{n,r}(\mathbf{x})$ be an expansion of $\mathbf{x}$. If U is a subset of $V_{n,r}(\mathbf{x})$ contained in $X\langle A\rangle$, then the following are equivalent.*

(1) *$U = X\langle A\rangle \cap Y\langle A\rangle$, for some generating set Y of $V_{n,r}$.*
(2) *U is A-closed and $X\langle A\rangle \backslash U$ is finite.*
(3) *$U = Z\langle A\rangle$ for some expansion Z of X.*

Moreover, if Y in statement (1) *is a finite basis for $V_{n,r}(\mathbf{x})$ then Z in statement* (3) *is an expansion of Y.*

Proof. First, let $U = X\langle A\rangle \cap Y\langle A\rangle$. Since U is the intersection of A-closed sets, it is also A-closed. By Lemma 3.11, $X\langle A\rangle \backslash Y\langle A\rangle$ is finite and therefore $X\langle A\rangle \backslash U$ is finite. So (1) implies (2).

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Second, assume that U is A-closed and $X\langle A\rangle\backslash U$ is finite. We will prove statement (3) by induction on the size of $|X\langle A\rangle\backslash U|$. If $|X\langle A\rangle\backslash U| = 0$, then statement (3) holds with $Z = X$. Otherwise, $|X\langle A\rangle\backslash U| > 0$ and we choose an element $w \in X\langle A\rangle\backslash U$ whose length $|w|$ is maximal. Then the set $U^* = U \cup \{w\}$ is A-closed and $|X\langle A\rangle\backslash U^*| = |X\langle A\rangle\backslash U| - 1$.

By induction, there is an expansion Z^* of X such that $U^* = Z^*\langle A\rangle$. The element w belongs to Z^*, otherwise w would have the form $w = z\alpha_{i_1}\cdots\alpha_{i_t}$, where $z \in Z^*$ and $t > 0$, and hence $z \in U^*\backslash\{w\} = U$. However, U is A-closed and so this would imply that $w \in U$, a contradiction. If we take

$$Z = (Z^*\backslash\{w\}) \cup \{w\alpha_i \mid 1 \le i \le n\},$$

then this is again an expansion of X and by the choice of w we have $w\alpha_i \in U$, for all i. Therefore $U = Z\langle A\rangle$ and (2) implies (3).

For the last implication: if $U = Z\langle A\rangle$ for some expansion Z of X, then $U = X\langle A\rangle \cap Y\langle A\rangle$, with $Y = Z$, and so (3) implies (1).

Finally, let $U = X\langle A\rangle \cap Y\langle A\rangle$ as in statement (1), so that $U = Z\langle A\rangle$ by statement (3). In particular this means that $Z \subseteq Y\langle A\rangle$. As Z is an expansion of X, it is also an expansion of $\mathbf{x}$; then Lemma 3.8 tells us that Z is a basis of $V_{n,r}(\mathbf{x})$. Now suppose that Y is a finite basis. Apply Lemma 3.8 to see that Z is an expansion of Y. □

Corollary 3.13 (cf. [17, Corollary 1, p. 12]). *Let B and C be finite bases of $V_{n,r}(\mathbf{x})$. Then B and C have a common expansion Z, which may be chosen such that $Z\langle A\rangle = B\langle A\rangle \cap C\langle A\rangle$. In particular, every finite basis of $V_{n,r}(\mathbf{x})$ may be obtained from $\mathbf{x}$ by an expansion followed by a contraction.*

Proof. Let f be the homomorphism from $V_{n,r}(\mathbf{x})$ to $V_{n,|B|}(B)$ defined by mapping $b \in B \subseteq V_{n,r}(\mathbf{x})$ to $b \in V_{n,|B|}(B)$, for all $b \in B$. As this is a bijection between bases, f is an isomorphism. Let $C' = Cf$, so C' is a basis for $V_{n,|B|}(B)$. From Lemma 3.12, B and C' have a common expansion Z' such that $B\langle A\rangle \cap C'\langle A\rangle = Z'\langle A\rangle$. Then B and C have common expansion $Z = Z'f^{-1}$, and the remainder of the first statement of the lemma follows. The final statement follows on taking B to be an arbitrary finite free generating set and $C = \mathbf{x}$. □

Corollary 3.14 ([17, Corollary 2, p. 12]). *$V_{n,r} \cong V_{n,s}$ if and only if $r \equiv s \bmod n-1$.*

Proof. If $r \equiv s \bmod n-1$ then it follows from Lemma 3.5 that $V_{n,r} \cong V_{n,s}$. Conversely, let θ be an isomorphism from $V_{n,r}(X)$ to $V_{n,s}(Y)$, where X and Y are sets of size r and s, respectively. Then $X\theta$ is a basis of $V_{n,s}(Y)$ of size r. From Corollary 3.13, there is a common expansion Z of $X\theta$ and Y. If Z is a d-fold expansion of $X\theta$ and an e-fold expansion of Y then $r+(n-1)d = |Z| = s+(n-1)e$, so $r \equiv s \bmod (n-1)$, as claimed. □

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

We could henceforth restrict to $V_{n,r}$, where $1 \leq r \leq n-1$. However, we do not need to do this for what follows here, and it is convenient to allow arbitrary positive values of r, and multiple instances of the same algebra.

Definition 3.15. Let u, v be elements of $V_{n,r}$. Then, u is said to be a *proper initial segment* of v if $v = u\Gamma$ for some nontrivial $\Gamma \in A^*$. If $u = v$ or u is a proper initial segment of v then u is called an *initial segment* of v .

Lemma 3.16 ([17, Sec. 2, Lemma 2.5(i)–(iii)]). *Let B be an A-basis of $V_{n,r}$ and V a subset of $B\langle A\rangle$.*

(1) *If B and V are finite, then V is contained in an expansion of B if and only if the following condition is satisfied:*

$$\textit{no element of } V \textit{ is a proper initial segment of another.} \qquad (\dagger)$$

(2) *If B and V are finite, then V is an expansion of B if and only if $(\dagger)$ is satisfied and for each $u \in B\langle A\rangle$ there exists $v \in V$ such that one of u, v is an initial segment of the other.*

(3) *V is a set of free generators for the Ω-subalgebra it generates if and only if $(\dagger)$ is satisfied.*

Proof. (1) If V is contained in an expansion of B then, using Lemma 3.5(1), $(\dagger)$ is satisfied.

Suppose V satisfies $(\dagger)$ and write

$$U = B\langle A\rangle \backslash \{\text{proper initial segments of elements of } V\}.$$

Then $(\dagger)$ implies that $V \subseteq U$. Also, U is A-closed and $B\langle A\rangle \backslash U$ consists of initial segments of the elements of the finite set V, so it is finite. Thus, by Lemma 3.12, there is an expansion Z of B such that $U = Z\langle A\rangle$. Therefore, $U \subseteq Z\langle A\rangle$, and this implies that $V \subseteq Z$ (for an element of $Z\langle A\rangle \backslash Z$ has a proper initial segment in $Z \subseteq U$ so it cannot be in V by the definition of U). Hence, V is contained in an expansion of B.

(2) If V is an expansion of B then $(\dagger)$ is satisfied and for each $u \in B\langle A\rangle$ there exists $v \in V$ such that one of u, v is an initial segment of the other.

Suppose V satisfies $(\dagger)$ and for each $u \in B\langle A\rangle$ there exists $v \in V$ such that one of u, v is an initial segment of the other. By part (1), V is contained in an expansion Z of B. If $V \neq Z$ then there is an element $z \in Z \backslash V$ and hence by the hypothesis there exists $v \in V$ such that one of v or z is an initial segment of the other. But no element of Z can be an initial segment of another, so this is a contradiction and hence $V = Z$.

(3) If V is a set of free generators for the Ω-subalgebra it generates then $(\dagger)$ is satisfied.

Suppose $(\dagger)$ is satisfied. If V is not a free generating set then the same is true of some finite subset V_0 and clearly $(\dagger)$ is also satisfied with V replaced by V_0. Then

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

$V_0 \subseteq B_0\langle A\rangle$ for some finite subset B_0 of B. As (†) holds, it follows from part (1) that V_0 is a subset of an expansion Z_0 of B_0. However, this means that V_0 is a subset of a basis of $V_{n,r}$, a contradiction. □

Corollary 3.17. *Let Y_i be a finite basis for $V_{n,r}$, for $i = 1, \ldots, m$. Then there is a unique minimal common expansion Z of all the Y_i, and Z satisfies $Z\langle A\rangle = \bigcap_{i=1}^{m}(Y_i\langle A\rangle)$.*

Proof. For $m = 2$, from Corollary 3.13 we have a common expansion Z of Y_1 and Y_2 such that $Z\langle A\rangle = Y_1\langle A\rangle \cap Y_2\langle A\rangle$. Furthermore, if W is a common expansion of Y_1 and Y_2 then, from Lemma 3.16, $W \subseteq Z\langle A\rangle$, which implies that W is an expansion of Z.

For $m > 2$, let $Z\langle A\rangle = \bigcap_{i=1}^{m-1}(Y_i\langle A\rangle)$ and $V = Z\langle A\rangle \cap Y_m\langle A\rangle$, where we assume inductively that Z is the unique minimal expansion of $Y_1, \ldots, Y_{m-1}$. From the previous paragraph there exists a unique minimal expansion W of Z and Y_m such that $W\langle A\rangle = V$. It follows that the result holds for $Y_1, \ldots, Y_m$ and hence by induction for all m. □

Corollary 3.18. *Let Y be a finite basis and let B be an A-basis of $V_{n,r}(\mathbf{x})$. If $Y \subseteq B\langle A\rangle$ then Y is an expansion of B : i.e. Y is an A-basis.*

Proof. As $Y \subseteq B\langle A\rangle$ and Y is a basis, Y satisfies (†) from Lemma 3.16(3). If $u \in B\langle A\rangle$ then $u \in Y\langle A\rangle\langle\lambda\rangle$, so for some $\Gamma, \Delta \in A^*$ and $y \in Y$ we have $u\Gamma = y\Delta$. As $u \in B\langle A\rangle$ and $y \in Y \subseteq B\langle A\rangle$ there exist $b, b' \in B$ and $\Lambda, \Lambda' \in A^*$ such that $u = b\Lambda$ and $y = b'\Lambda'$, so $b\Lambda\Gamma = b'\Lambda'\Delta$, and therefore $b = b'$. Thus $b\Lambda\Gamma = b\Lambda'\Delta$, so either $u = b\Lambda$ is an initial segment of $y = b\Lambda'$, or vice-versa. Hence, from Lemma 3.16(2), Y is an expansion of B. □

Lemma 3.19 ([17, Sec. 2, Lemma 2.5(iv)]). *Let B be an A-basis of $V_{n,r}$. Let Y and Z be d-fold expansions of B, for $d \geq 1$. If $Y \neq Z$ then some element of Y is a proper initial segment of an element of Z.*

Proof. If no element of Y is a proper initial segment of an element of Z then, from Corollary 3.13, $Y \subseteq Z\langle A\rangle$. Then Lemma 3.16 implies that Y is an expansion of Z. However, Y and Z are both d-fold expansions of B and thus $Y = Z$. This completes the proof. □

Lemma 3.20. *Let $u \in V_{n,r}$ and let d be a non-negative integer.*

(1) *If $v \in V_{n,r}$ then $u = v$ if and only if $u\Gamma = v\Gamma$, for all $\Gamma \in A^*$ of length d.*
(2) *If S is an Ω-subalgebra of $V_{n,r}$ then $u \in S$ if and only if $u\Gamma \in S$, for all $\Gamma \in A^*$ of length d.*

Proof. (1) If $u = v$ then $u\Gamma = v\Gamma$ for all $\Gamma \in A^*$ of length d.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

We shall show that given $d \geq 0$ we have

$$u, v \in V_{n,r} \text{ satisfy } u\Gamma = v\Gamma \text{ for all } \Gamma \in A^* \text{ of length } d \quad \Longrightarrow \quad u = v. \qquad (*)$$

If $d = 0$ this holds trivially; to proceed we use induction on d. Our hypothesis is that for all d' such that $0 \leq d' < d$, the implication $(*)$ holds with d' instead of d. Suppose then that $u, v \in V_{n,r}$ and $u\Gamma = v\Gamma$ for all Γ of length d. We may uniquely write $\Gamma = \Delta\alpha_i$, where $1 \leq i \leq n$ and $\Delta \in A^*$ has length $d-1$. Write $u\Delta$ as a contraction $u\Delta = u\Delta\alpha_1 \ldots u\Delta\alpha_n\lambda$. Each string $\Delta\alpha_j$ has length d, so $u\Delta\alpha_j = v\Delta\alpha_j$ for each j. Then the contraction above is equal to $v\Delta\alpha_1 \ldots v\Delta\alpha_n\lambda = v\Delta$, and so $u\Delta = v\Delta$.

Now apply this argument to all strings Γ of length d. In doing so we will use every length $d-1$ string Δ (n times), and so $u\Delta = v\Delta$ for every Δ of length $d-1$. By the inductive hypothesis we conclude $u = v$.

(2) The proof is similar to that of part (1). □

4. The Higman–Thompson Groups $G_{n,r}$

In this section we define the groups which form the object of study in this paper. Throughout the remainder of the paper, we assume that $n \geq 2$, and that $V_{n,r} = V_{n,r}(\mathbf{x}) = W_\Omega(\mathbf{x})/\mathfrak{q}$, where $\mathbf{x} = \{x_1, \ldots, x_r\}$. When $r = 1$ we let $\mathbf{x} = \{x\}$.

When we discuss automorphisms of $V_{n,r}$ we assume that they are given by listing the images of a (finite) basis of $V_{n,r}$. For instance, let $\psi \in V_{n,r}$ be defined by the bijection $\psi : Y \to Z$, where Y and Z are bases of $V_{n,r}$. If we expand $y \in Y$ to form $Y' = Y \backslash \{y\} \cup \{y\alpha_1, \ldots, y\alpha_n\}$, the result Y' is also a basis by Lemma 3.8. As $y\alpha_i\psi = y\psi\alpha_i = z\alpha_i$ for $i = 1, \ldots, n$, we see that the automorphism ψ induces an expansion Z' of Z such that $Y'\psi = Z'$. Thus, if Y and Z are not expansions of $\mathbf{x}$, we can find Y' and $Z' = Y'\psi$ contained in $\mathbf{x}\langle A\rangle$ and redefine ψ in terms of Y' and Z'. In other words, we may always describe an automorphism by a bijection between A-bases.

As bijections between bases are not particularly easy to read, we represent automorphisms using pairs of rooted forests. An *n-ary rooted tree* is a tree with a single distinguished *root* vertex of degree n, such that all other vertices have degree $n+1$ or 1. If a vertex v is at distance $d \geq 1$ from the root then the n vertices incident to v and not on the path to the root are its *children*. Vertices of degree 1 are called *leaves*. An n-ary rooted tree is said to be *A-labeled* if the edges joining a vertex v to its n children are labeled with the elements $\alpha_i \in A$, so that two edges joining v to different children are labeled differently. An A-labeled, r-rooted, n-ary forest is a disjoint union of r rooted, A-labeled, n-ary trees.

Let T be such a forest consisting of trees $T_1, \ldots, T_r$. For each $1 \leq i \leq r$, we identify the root of T_i with the generator $x_i \in \mathbf{x}$ of $V_{n,r}(\mathbf{x})$. We proceed by recursively identifying vertices of T_i with elements of $\{x_i\}\langle A\rangle \subseteq V_{n,r}$. Suppose that $v \in T_i$ is not a leaf, and that v has been identified with $x_i\Gamma$ for some $\Gamma \in A^*$. Then v has n children $c_1, \ldots, c_n$, where c_j is the child connected to v by an edge

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

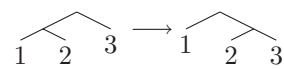
labeled a_j. For each $1 \leq j \leq n$ we identify c_j with $x_i \Gamma \alpha_j$; this identifies each vertex of T with a uniquely determined element of $\mathbf{x}\langle A\rangle$. Furthermore, by construction, the leaves of T correspond to an expansion of $\mathbf{x}$. We use such trees to represent automorphisms, as in the following example.

Example 4.1. Let $n = 2$, $r = 1$, $\mathbf{x} = \{x\}$ and let ψ be the element of $G_{2,1}$ corresponding to the bijective map between A-bases $Y = \{x\alpha_1^2, x\alpha_1\alpha_2, x\alpha_2\}$ and $Z = Y\psi = \{x\alpha_1, x\alpha_2\alpha_1, x\alpha_2^2\}$ given by

$$x\alpha_1^2\psi = x\alpha_1,\ x\alpha_1\alpha_2\psi = x\alpha_2\alpha_1,\ x\alpha_2\psi = x\alpha_2^2.$$

The A-labeled binary trees corresponding to these bases are shown below. The labeling of edges is not shown, but edges from a vertex to its children are always ordered from left to right in the order $\alpha_1, \ldots, \alpha_n$. Thus the leaves of the left-hand tree correspond to Y and the leaves of the right-hand tree to Z. The numbering below the leaves determines the mapping ψ; by taking leaf labeled j on the left to leaf labeled j on the right.

ψ :



Definition 4.2 ([17]). The *Higman–Thompson group* $G_{n,r}$ is the group of Ω-algebra automorphisms of $V_{n,r}$.

Note that the largest Thompson group V is isomorphic to $G_{2,1}$, because the A-labeled trees we have described are exactly the tree-pair diagrams used to represent elements of V.

Lemma 4.3 ([17, Lemma 4.1]). *If $\{\psi_1, \ldots, \psi_k\}$ is a finite subset of $G_{n,r}$ and X is an A-basis of $V_{n,r}$, then there is a unique minimal expansion Y of X such that $Y\psi_i \subseteq X\langle A\rangle$, for $i = 1, \ldots, k$. That is, any other expansion of X with this property is an expansion of Y.*

Proof. For each i, $X\psi_i^{-1}$ is a generating set for $V_{n,r}$, but may not be a subset of $X\langle A\rangle$. Let $U_i = X\langle A\rangle \cap X\psi_i^{-1}\langle A\rangle$. Then, by Lemma 3.12, U_i is A-closed and there exists an expansion Y_i of X such that $U_i = Y_i\langle A\rangle$. Now, Corollary 3.17 gives a unique minimal common expansion Y, of the Y_i's, and $Y\langle A\rangle = \bigcap_{i=1}^k (Y_i\langle A\rangle)$. Then, for all i, $Y \subseteq Y_i\langle A\rangle = U_i \subseteq X\psi_i^{-1}\langle A\rangle$, so $Y\psi_i \subseteq X\langle A\rangle$.

Let Z be an expansion of X. If $Z\psi_i \subseteq X\langle A\rangle$, for all i, then (by the definition of U_i) $Z \subseteq U_i = Y_i\langle A\rangle$, so $Z \subseteq \bigcap_{i=1}^k (Y_i\langle A\rangle) = Y\langle A\rangle$. Hence, from Lemma 3.12, Z is an expansion of Y. □

Definition 4.4. Let $\{\psi_1, \ldots, \psi_k\}$ be a finite subset of $G_{n,r}$ and let X be an A-basis of $V_{n,r}$. The expansion Y of X given by Lemma 4.3 is called the *minimal expansion of X associated to $\{\psi_1, \ldots, \psi_k\}$*.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

4.1. *Semi-normal forms*

Let $\psi \in G_{n,r}$, let X be an A-basis of $V_{n,r}$, and $y \in V_{n,r}$. The *ψ-orbit* of y is the set $\mathcal{O}_y = \{y\psi^n \mid n \in \mathbb{Z}\}$. We consider how ψ-orbits intersect the A-subalgebra $X\langle A\rangle$. To this end an *X-component* of the ψ-orbit of y is a maximal subsequence $\mathcal{C}$ of the sequence $(y\psi^i)_{i=-\infty}^{i=\infty}$ such that all elements of $\mathcal{C}$ are in $X\langle A\rangle$. More precisely, $\mathcal{C}$ must satisfy

(1) if $y\psi^p$ and $y\psi^q$ belong to $\mathcal{C}$, where $p < q$ then $y\psi^k$ belongs to $X\langle A\rangle$, for all k such that $p \le k \le q$; and
(2) $\mathcal{C}$ is a maximal subset of the ψ-orbit of y for which statement (1) holds.

Note: Higman [17, Sec. 9] refers to X-components as "orbits in $X\langle A\rangle$".

First we distinguish the five possible types of X-component of ψ by giving them names.

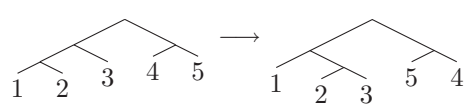
(1) *Complete infinite X-components.* For any y in such an X-component, $y\psi^i$ belongs to $X\langle A\rangle$ for all $i \in \mathbb{Z}$, and the elements $y\psi^i$ are all different.
(2) *Complete finite X-components.* For any y in such an X-component, $y\psi^i = y$ for some positive integer i, and $y, y\psi, \ldots, y\psi^{i-1}$ all belong to $X\langle A\rangle$.
(3) *Right semi-infinite X-components.* For some y in the X-component, $y\psi^i$ belongs to $X\langle A\rangle$ for all $i \ge 0$, but $y\psi^{-1}$ does not. The elements $y\psi^i$, $i \ge 0$, are then necessarily all different.
(4) *Left semi-infinite X-components.* For some y in the X-component, $y\psi^{-i}$ belongs to $X\langle A\rangle$ for all $i \ge 0$, but $y\psi$ does not. The elements $y\psi^{-i}$, $i \ge 0$, are then necessarily all different.
(5) *Incomplete finite X-components.* For some y in the X-component and some non-negative integer i we have $y, y\psi, \ldots, y\psi^i$ belonging to $X\langle A\rangle$ but $y\psi^{-1}$ and $y\psi^{i+1}$ do not.

Example 4.5. Let $n = 2$, $r = 1$, $\mathbf{x} = \{x\}$. Let our bases be

$$Y = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\} \quad \text{and}$$
$$Z = \{x\alpha_1^2, x\alpha_1\alpha_2\alpha_1, x\alpha_1\alpha_2^2, x\alpha_2^2, x\alpha_2\alpha_1\}.$$

Define the automorphism ψ by $Y\psi = Z$, with the ordering given above.

ψ :



Then Y is the minimal expansion of $\mathbf{x}$ associated to ψ. Take the basis X to be just $X = \mathbf{x}$. The X-component of $x\alpha_1^3$ is left semi-infinite

$$\cdots \mapsto x\alpha_1^4 \mapsto x\alpha_1^3 \mapsto x\alpha_1^2,$$

and the X-component of $x\alpha_1\alpha_2$ is right semi-infinite:

$$x\alpha_1\alpha_2 \mapsto x\alpha_1\alpha_2^2 \mapsto x\alpha_1\alpha_2^3 \mapsto \cdots.$$

The X-component of $x\alpha_1^2\alpha_2$ is complete infinite

$$\cdots \mapsto x\alpha_1^4\alpha_2 \mapsto x\alpha_1^3\alpha_2 \mapsto x\alpha_1^2\alpha_2 \mapsto x\alpha_1\alpha_2\alpha_1 \mapsto x\alpha_1\alpha_2^2\alpha_1 \mapsto \cdots,$$

and $(x\alpha_2\alpha_1, x\alpha_2^2)$ is a complete finite X-component. We have $x\alpha_2 = x\alpha_2\alpha_1 x a_2^2\lambda$, so $x\alpha_2\psi = x a_2^2 x\alpha_2\alpha_1\lambda$ and $x\alpha_2\psi^2 = x\alpha_2$; therefore $(x\alpha_2)$ is an incomplete finite X-component.

Let $\psi \in G_{n,r}$, let X be an A-basis of $V_{n,r}$, let Y be the minimal expansion of $X\langle A\rangle$ associated to ψ and let $Z = Y\psi$. Then, as discussed above, Y and Z are both expansions of X. From Lemma 3.12, both $X\langle A\rangle\backslash Z\langle A\rangle$ and $X\langle A\rangle\backslash Y\langle A\rangle$ are finite. Furthermore, as $|Y| = |Z|$, both X and Y are d-fold expansions, for some d, so $|X\langle A\rangle\backslash Z\langle A\rangle| = |X\langle A\rangle\backslash Y\langle A\rangle|$.

By definition $Y\langle A\rangle = X\langle A\rangle \cap X\langle A\rangle\psi^{-1}$, and moreover ψ maps no proper contraction of Y into $X\langle A\rangle$. Hence

$$Z\langle A\rangle = Y\langle A\rangle\psi = X\langle A\rangle\psi \cap X\langle A\rangle.$$

Thus, if $u \in X\langle A\rangle\backslash Z\langle A\rangle$ then $u \notin X\langle A\rangle\psi$, so $u\psi^{-1} \notin X\langle A\rangle$ and hence u is an initial element either of an incomplete finite X-component or of a right semi-infinite X-component i.e. in an X-component of type (3) or (5). Similarly, if $v \in X\langle A\rangle\backslash Y\langle A\rangle$ then $v \notin X\langle A\rangle\psi^{-1}$, so $v\psi \notin X\langle A\rangle$ and hence v is a terminal element either of an incomplete finite X-component or of a left semi-infinite X-component i.e. in an X-component of type (4) or (5).

If $\mathcal{C}$ is an X-component of type (3) or (5), then by definition $\mathcal{C}$ has an initial element u: that is $u\psi^{-1} \notin X\langle A\rangle$. Then $u \notin X\langle A\rangle\psi$, and so $u \in X\langle A\rangle\backslash Z\langle A\rangle$. Similarly, if $\mathcal{C}$ is an X-component of type (4) or (5), then $\mathcal{C}$ has a terminal element v: that is $v\psi \notin X\langle A\rangle$. Again, $v \notin X\langle A\rangle\psi^{-1}$ and so $v \in X\langle A\rangle\backslash Y\langle A\rangle$.

Let u be an initial element of an incomplete finite X-component $\mathcal{C}$. By the above, $u \in X\langle A\rangle\backslash Z\langle A\rangle$ and by definition of an incomplete finite X-component, there is some non-negative integer k such that $u, u\psi, \ldots, u\psi^k$ all belong to $X\langle A\rangle$ but $u\psi^{k+1}$ does not. Since $u\psi^k$ is the terminal element of the incomplete finite X-component $\mathcal{C}$, we have $u\psi^k \in X\langle A\rangle\backslash Y\langle A\rangle$. Therefore, the initial elements of incomplete finite X-components in $X\langle A\rangle\backslash Z\langle A\rangle$ and terminal elements of incomplete finite X-components in $X\langle A\rangle\backslash Y\langle A\rangle$ pair up.

Given that the initial and terminal elements of the incomplete finite X-components must be in one-to-one correspondence, all other elements of $|X\langle A\rangle\backslash Z\langle A\rangle|$ (respectively, $|X\langle A\rangle\backslash Y\langle A\rangle|$) are initial (respectively, terminal) elements in right (respectively, left) semi-infinite X-components. Hence there are as many right semi-infinite X-components as left semi-infinite X-components.

The above is summarized in a lemma.

Lemma 4.6 ([17, Lemma 9.1]). *Let ψ be an element of $G_{n,r}$ and let X be an A-basis of $V_{n,r}$. There are only finitely many X-components of ψ of types* (3)–(5) *and there are as many of type* (3) *as of type* (4). *If Y is the minimal expansion of $X\langle A\rangle$ associated to ψ and $Z = Y\psi$ then*

- $Y\langle A\rangle = X\langle A\rangle \cap X\langle A\rangle\psi^{-1}$ *and* $Z\langle A\rangle = X\langle A\rangle\psi \cap X\langle A\rangle$;

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

- *$X\langle A\rangle\backslash Z\langle A\rangle$ is exactly the set of initial elements of X-components of types* (3) *or* (5); *and*
- *$X\langle A\rangle\backslash Y\langle A\rangle$ is exactly the set of terminal elements of X-components of types* (4) *or* (5).

Example 4.7. In Example 4.5, we have $X\langle A\rangle\backslash Z\langle A\rangle = \{x, x\alpha_1, x\alpha_1\alpha_2, x\alpha_2\}$ and $X\langle A\rangle\backslash Y\langle A\rangle = \{x, x\alpha_1, x\alpha_1^2, x\alpha_2\}$. The incomplete finite X-components are (x), $(x\alpha_1)$ and $(x\alpha_2)$, while $x\alpha_1\alpha_2$ is an initial element of a right semi-infinite X-component and $x\alpha_1^2$ is a terminal element of a left semi-infinite X-component. All other X-components of elements of $X\langle A\rangle$ are complete.

Definition 4.8 ([17, Sec. 9]). An element ψ of $G_{n,r}$ is in *semi-normal form* with respect to the A-basis X if no element of $X\langle A\rangle$ is in an incomplete finite X-component of ψ.

Lemma 4.9 ([17, Lemma 9.2]). *Let $\psi \in G_{n,r}$ and let X be an A-basis of $V_{n,r}$. There exists an expansion of X with respect to which ψ is in semi-normal form.*

Proof. Let $\psi \in G_{n,r}$. We prove the lemma by induction on the number of elements in $X\langle A\rangle$ which belong to an incomplete finite X-component. Note that Lemma 4.6 shows us that this number is finite. If there are no such elements then we are done.

Suppose then that there exists an element u in $X\langle A\rangle$ which belongs to an incomplete finite X-component. Thus, there exist $y \in X$ and $\Gamma \in A^*$ such that $u = y\Gamma$ and some minimal $m, k \in \mathbb{N}_0$ such that $u\psi^{-(m+1)}, u\psi^{k+1} \notin X\langle A\rangle$. It follows that $y\psi^{-(m+1)}, y\psi^{k+1} \notin X\langle A\rangle$, so that y is also in an incomplete finite X-component. Let X' be the simple expansion $X' = X\backslash\{y\} \cup \{y\alpha_1, \ldots, y\alpha_n\}$. Then X' is a A-basis for $V_{n,r}$ and $X\langle A\rangle\backslash X'\langle A\rangle = \{y\}$. Thus the number of elements of $X''\langle A\rangle$ in an incomplete finite X''-component is one less than the number of elements of $X\langle A\rangle$ in an incomplete finite X-component. Hence, by induction, there exists an expansion of X with respect to which ψ is in semi-normal form. □

Remark 4.10. Continuing the discussion above Lemma 4.6, observe that if $u \in X\langle A\rangle$ and $u \notin Y\langle A\rangle \cup Z\langle A\rangle$ then u is both the initial and terminal element of an X-component of ψ; so (u) constitutes an incomplete finite X-component. Therefore, when implementing the argument of Lemma 4.9 to find a semi-normal form for ψ, we may pass immediately to a minimal expansion containing no elements of $X\langle A\rangle\backslash(Y\langle A\rangle \cup Z\langle A\rangle)$: that is an expansion minimal amongst those contained in $Y\langle A\rangle \cup Z\langle A\rangle$.

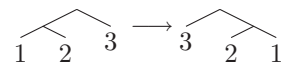
Example 4.11. Let $n = 2$, $r = 1$, $\mathbf{x} = \{x\}$ and let ψ be the automorphism of Example 4.1. Here $Y = \{x\alpha_1^2, x\alpha_1\alpha_2, x\alpha_2\}$ is the minimal expansion of $\mathbf{x}$ associated to ψ and $Z = Y\psi = \{x\alpha_1, x\alpha_2\alpha_1, x\alpha_2^2\}$. In this example, $\mathbf{x}\langle A\rangle\backslash(Y\langle A\rangle \cup Z\langle A\rangle) = \{x\}$ and the minimal expansion of $\mathbf{x}$ not containing x is $X = \{x\alpha_1, x\alpha_2\}$. Then Y remains the minimal expansion of X associated to ψ, $X\langle A\rangle\backslash Z\langle A\rangle = \{x\alpha_2\}$ and

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

$X\langle A\rangle \backslash Y\langle A\rangle = \{x, x\alpha_1\}$. As $x\alpha_1$ is the terminal element of a left semi-infinite X-component, while $x\alpha_2$ is the initial element of a right semi-infinite X-component it follows that ψ is in semi-normal form with respect to X.

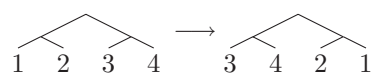
Example 4.12. Let $n = 2$, $r = 1$, $\mathbf{x} = \{x\}$ and let ψ be the element of $G_{2,1}$ corresponding to the bijective map:

$$x\alpha_1^2\psi = x\alpha_2^2, \quad x\alpha_1\alpha_2\psi = x\alpha_2\alpha_1, \quad x\alpha_2\psi = x\alpha_1.$$

ψ : 

Again, $Y = \{x\alpha_1^2, x\alpha_1\alpha_2, x\alpha_2\}$ is the minimal expansion of $\mathbf{x}$ associated to ψ and setting $Z = Y\psi = \{x\alpha_1, x\alpha_2\alpha_1, x\alpha_2^2\}$, the minimal expansion of $\mathbf{x}$ contained in $Y\langle A\rangle \cup Z\langle A\rangle$ is $X_1 = \{x\alpha_1, x\alpha_2\}$; and Y is still the minimal expansion of X_1 associated to ψ. However $(x\alpha_2, x\alpha_1)$ is an incomplete finite X_1-component, so ψ is not in semi-normal form with respect to X_1. As $x\alpha_1$ is in an incomplete finite X_1-component, we first take the simple expansion of X_1 at $x\alpha_1$, giving $X_2 = Y$. As $x\alpha_2\psi = x\alpha_1 \notin X_2\langle A\rangle$, $(x\alpha_2)$ is now an incomplete finite X_2-component, so ψ is not in semi-normal form with respect to X_2. We take a further simple expansion of X_2 at $x\alpha_2$, to obtain a new A-basis $X_3 = \{x\alpha_1^2, x\alpha_1\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\}$. Then ψ maps X_3 to itself:

$$x\alpha_1^2\psi = x\alpha_2^2, \quad x\alpha_1\alpha_2\psi = x\alpha_2\alpha_1, \quad x\alpha_2\alpha_1\psi = x\alpha_1^2, x\alpha_2^2 = x\alpha_1\alpha_2.$$

ψ : 

As all elements of X_3 are in the same complete finite X_3-component, ψ is in semi-normal form with respect to X_3. The minimal expansion of X_3 associated to ψ is just X_3.

Example 4.13. The automorphism ψ of Example 4.7 is not in semi-normal form with respect to X or $X_1 = \{x\alpha_1, x\alpha_2\}$, as both $x\alpha_1$ and $x\alpha_2$ are in incomplete finite X-components. However, ψ is in semi-normal form with respect to $X_2 = \{x\alpha_1^2, x\alpha_1\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\}$. The minimal expansion of X_2 associated to ψ is the A-basis Y of Example 4.5.

The following, which follows directly from the definitions, summarizes the possibilities for the intersection with $X\langle A\rangle$ of the orbit of an element under an automorphism in semi-normal form.

Corollary 4.14. *Let ψ be an element of $G_{n,r}$ in semi-normal form with respect to the A-basis X, let $v \in V_{n,r}$ and let $\mathcal{O}_v$ be the ψ-orbit of v. Then $\mathcal{O}_v$ has one of the following six types.*

(1) *$\mathcal{O}_v \cap X\langle A\rangle = \emptyset$.*
(2) *$\mathcal{O}_v$ is finite and $O_v \subseteq X\langle A\rangle$, so $\mathcal{O}_v$ is a complete finite X-component.*
(3) *$\mathcal{O}_v$ is infinite and $O_v \subseteq X\langle A\rangle$, so $\mathcal{O}_v$ is a complete infinite X-component.*

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

(4) $\mathcal{O}_v \cap X\langle A\rangle$ *consists of a unique left semi-infinite* X*-component.*
(5) $\mathcal{O}_v \cap X\langle A\rangle$ *consists of a unique right semi-infinite* X*-component.*
(6) $\mathcal{O}_v \cap X\langle A\rangle$ *is the disjoint union of a left semi-infinite* X*-component and a right semi-infinite* X*-component.*

Remark 4.15. As can be seen from Example 4.17 below, there are automorphisms for which orbits of the final type in this list exist. In fact we shall show in Example 4.31 that there exist automorphisms which have such orbits with respect to *every* semi-normal form. This means that [17, Lemma 9.6] is false. Consequently, the algorithms [17, Lemma 9.7] for determining if two elements of $V_{n,r}$ belong to a single orbit, and [17, Theorem 9.3] for conjugacy of automorphisms are incomplete.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

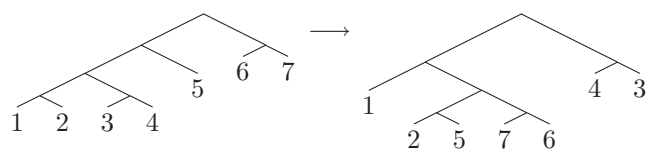
Definition 4.16. Let ψ be an element of $G_{n,r}$ in semi-normal form with respect to the A-basis X, and let $\mathcal{O}$ be a ψ-orbit of type (6), as given in Corollary 4.14. Then $\mathcal{O}$ is called a *pond orbit* with respect to X. The subsequence $P \subset \mathcal{O}$ of elements not in $X\langle A\rangle$ is called a *pond*. The *width of* P is one more than number of elements in P; this is the number of times we need to apply ψ to get from the endpoint of one semi-infinite X-component to the other.

Example 4.17. Let $n = 2$, $r = 1$ and $V_{2,1}$ be free on $\mathbf{x} = \{x\}$. Let

$$Y = \{x\alpha_1^4, x\alpha_1^3\alpha_2, x\alpha_1^2\alpha_2\alpha_1, x\alpha_1^2\alpha_2^2, x\alpha_1\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\},$$
$$Z = \{x\alpha_1^2, x\alpha_1\alpha_2\alpha_1^2, x\alpha_1\alpha_2\alpha_1\alpha_2, x\alpha_1\alpha_2^2\alpha_1, x\alpha_1\alpha_2^3, x\alpha_2\alpha_1, x\alpha_2^2\}$$

and let $\psi \in G_{2,1}$ be determined by the bijection $Y \to Z$ illustrated below.

ψ :



As usual, Y is the minimal expansion of $\mathbf{x}$ associated to ψ and $Z = Y\psi$. The minimal expansion of $\mathbf{x}$ contained in $Y\langle A\rangle \cup Z\langle A\rangle$ is $X = \{x\alpha_1^2, x\alpha_1\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\}$. Two of these elements are endpoints of semi-infinite X-components, whereas the other two belong to complete infinite X-components.

$$\cdots \mapsto x\alpha_1^4 \mapsto x\alpha_1^2, \tag{4.1}$$

$$x\alpha_1\alpha_2 \mapsto x(\alpha_1\alpha_2)^2 \mapsto \cdots, \tag{4.2}$$

$$\cdots \mapsto x\alpha_1^4\alpha_2^2 \mapsto x\alpha_1^2\alpha_2^2 \mapsto x\alpha_2\alpha_1 \mapsto x\alpha_1\alpha_2^3 \mapsto x(\alpha_1\alpha_2)^2\alpha_2^2 \mapsto \cdots, \tag{4.3}$$

$$\cdots \mapsto x\alpha_1^4\alpha_2\alpha_1 \mapsto x\alpha_1^2\alpha_2\alpha_1 \mapsto x\alpha_2^2 \mapsto x\alpha_1\alpha_2^2\alpha_1 \mapsto x(\alpha_1\alpha_2)^2\alpha_2\alpha_1 \mapsto \cdots. \tag{4.4}$$

Thus ψ is in semi-normal form with respect to X. Now let us compute the ψ-orbit of the element $x\alpha_1^2\alpha_2$.

$$\begin{aligned} &\cdots x\alpha_1^6\alpha_2 \mapsto x\alpha_1^4\alpha_2 \mapsto x\alpha_1^2 a_2 \mapsto x\alpha_2^2 x\alpha_2\alpha_1\lambda \\ &\mapsto x\alpha_1\alpha_2^2 \mapsto x(\alpha_1\alpha_2)^2\alpha_2 \mapsto \cdots. \end{aligned} \tag{4.5}$$

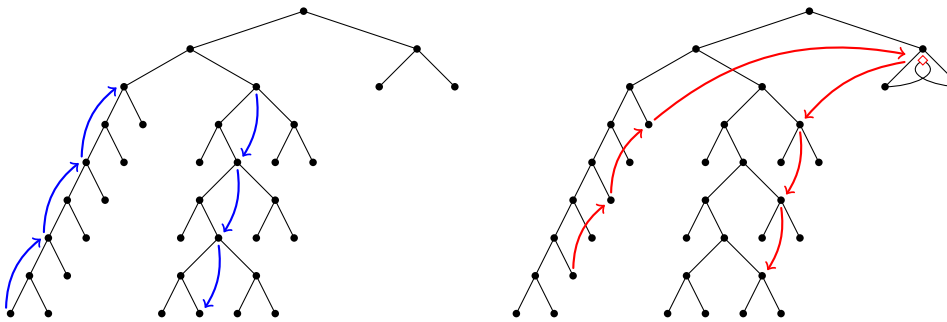


Fig. 1. The binary trees above represent a finite subset of $\mathbf{x}\langle A\rangle$, as described in the introduction to Sec. 4. On the left we have annotated this tree, highlighting the semi-infinite X-components (4.1) and (4.2). Below these components sit the pond orbit (4.5), which is shown on the right tree. Note that the element $w = x\alpha_2^2 x\alpha_2\alpha_1\lambda \notin \mathbf{x}\langle A\rangle$ does not correspond to a vertex of this tree; we have represented it as a "phantom" vertex $\diamond$ below $x\alpha_2$ whose left child is $x\alpha_2^2$ and whose right child is $x\alpha_2\alpha_1$ — a "twisted" version of $x\alpha_2$.

Figure 1 illustrates the orbit (4.5), which consists of two semi-infinite X-components and a single element $x\alpha_2^2 x\alpha_2\alpha_1\lambda$ (the pond) outside of $X\langle A\rangle$. In this case, the pond has width $1 + 1 = 2$.

Lemma 4.18 ([17, Lemma 9.3]). *Let ψ be an element of $G_{n,r}$ in semi-normal form with respect to the A-basis X. Suppose that x is an element of X. Exactly one of the following holds.*

(A) *There exists $\Gamma \in A^*$ such that $x\Gamma$ is in a complete finite X-component. In this case x itself belongs to a complete finite X-component, which consists of elements of X, and we say x is of type* (A).

(B) *There exist $\Gamma, \Delta \in A^*$, with $\Gamma \neq \Delta$, such that $x\Gamma$ and $x\Delta$ belong to the same X-component. In this case there exists $\Lambda \in A^*$ and $m \in \mathbb{Z}\backslash\{0\}$ with $|m|$ minimal, such that $x\psi^m = x\Lambda$; we say x is of type* (B). *If $m > 0$ then the X-component containing x is right semi-infinite; if $m < 0$ then the X-component containing x is left semi-infinite.*

(C) *x is not of type* (A) *or* (B) *above and there exists some $z \in X$ of type* (B) *and nontrivial $\Delta \in \langle A\rangle$ such that $x\psi^i = z\Delta$. In this case the X-component containing x is infinite; and we say x is of type* (C).

Proof. (A) If x belongs to an infinite X-component of ψ (of types (1), (3) or (4) that is), then so does $x\Gamma$, a contradiction. As ψ is in semi-normal form with respect to X it follows that x is in a complete finite X-component. Let d be the smallest positive integer such that $x\psi^d = x$. For each $1 \leq i \leq d-1$ write $x\psi^i = z\Delta$ for some $z \in X$ and $\Delta \in A^*$. Then z must also belong to a complete finite X-component, so we can write $z\psi^{d-i} = y\Gamma$ for some $y \in X$ and $\Gamma \in A^*$. Then $x = x\psi^d = z\Delta\psi^{d-i} = z\psi^{d-i}\Delta = y\Gamma\Delta$. From Lemma 3.16, we have $y = x$ and $\Gamma = \Delta = \varepsilon$, so $x\psi^i = z \in X$, as claimed.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

(B) If x belongs to a finite X-component then, from (A), the X-component of $x\Gamma$ consists of elements $z\Gamma$, where $z \in X$, contrary to the hypotheses of (B). Therefore x belongs to an infinite X-component of ψ. Without loss of generality we may assume that there is $i > 0$ such that $x\Gamma\psi^i = x\Delta$. Suppose first that $x\psi^k \in X\langle A\rangle$, for all $k \geq 0$. Then $x\psi^i = v\Lambda$, for some $v \in X$ and $\Lambda \in A^*$, and thus $x\Delta = x\Gamma\psi^i = v\Lambda\Gamma$; so $v = x$ and $\Delta = \Lambda\Gamma$, and we obtain $x\psi^i = x\Lambda$.

Similarly, if $x\psi^{-k} \in X\langle A\rangle$, for all $k \geq 0$, then $x\psi^{-i} = x\Lambda'$, for some $\Lambda' \in A^*$, with $\Gamma = \Lambda'\Delta$. Note that if $x\psi^k \in X\langle A\rangle$ for all k, then $x = x\Lambda\Lambda'$, which forces $\Lambda = \Lambda' = \varepsilon$, so $\Gamma = \Delta$, a contradiction. Hence the final statement of (B) holds.

(C) In this case x must belong to an infinite X-component, as (A) does not hold. As X is finite there is $z \in X$ such that $z\Gamma$ and $z\Delta$ belong to the X-component of x, for distinct Γ and Δ in A^*; and then z is of type (B), as required. □

Definition 4.19. Let $u \in V_{n,r}$ and $\psi \in G_{n,r}$. If $u\psi^d = u\Gamma$ for some $d \in \mathbb{Z}\backslash\{0\}$ and some $\Gamma \in A^*\backslash\{1\}$, then u is a *characteristic element* for ψ. If u is a characteristic element for ψ then the *characteristic* of u is the pair (m, Γ) such that $m \in \mathbb{Z}\backslash\{0\}$, $\Gamma \in A^*$ with

- $u\psi^m = u\Gamma$ and
- for all i such that $0 < |i| < |m|$, $u\psi^i \notin u\langle A\rangle$.

In this case Γ is called the *characteristic multiplier* and m is the *characteristic power* for u, with respect to ψ.

From the definition, if ψ is in semi-normal form with respect to X then an element $x \in X$ is of type (B) if and only if x is a characteristic element: in which case it follows from Lemma 4.24 below that the ψ-orbit of x is of type (4) or (5) in Corollary 4.14. On the other hand, if $x \in X$ has type (C) then the ψ-orbit of x may be of types (3), (4), (5) or (6) in Corollary 4.14.

Example 4.20. In Example 4.13, the automorphism ψ is in semi-normal form with respect to an A-basis X. The elements $x\alpha_2\alpha_1$ and $x\alpha_2^2$ of X are of type (A). The element $x\alpha_1^2 \in X$ is of type (B) with characteristic $(-1, \alpha_1)$, while $x\alpha_1\alpha_2 \in X$ is of type (B) with characteristic $(1, \alpha_2)$; and both of these elements are endpoints of their semi-infinite X-components.

In Example 4.17 the elements $x\alpha_2\alpha_1$ and $x\alpha_2^2$ of X are of type (C), are not characteristic and belong to complete infinite X-components. The elements $x\alpha_1^2\alpha_2$ and $x\alpha_1\alpha_2^2$ in the pond orbit (4.5) are also type (C) and non-characteristic, but belong to semi-infinite X-components.

Lemma 4.21. *If $u \in V_{n,r}$ is a characteristic element for $\psi \in G_{n,r}$ then*

(1) *the characteristic (m, Γ) is uniquely determined, and*
(2) *if v is in the same ψ-orbit as u then v is a characteristic element with the same characteristic as u.*

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Proof. To see part (1), suppose that u has characteristic (m, Γ). If $u\psi^{m'} = u\Delta$ and for all $0 < |k| < |m'|$ we have $u\psi^k \notin u\langle A\rangle$, then $|m'| \geq |m|$ by Definition 4.19, so $m = \pm m'$. If $u\psi^{-m} = u\Delta$ then $u = u\psi^m\Delta = u\Gamma\Delta$, which cannot happen as $\Gamma \neq 1$.

For part (2), let $u\psi^r = v$. For all k such that $u\psi^k = u\Delta$ with $\Delta \in A^*$, we have

$$v\psi^k = u\psi^r\psi^k = u\psi^k\psi^r = u\Delta\psi^r = u\psi^r\Delta = v\Delta.$$

Interchanging u and v we also see that whenever $v\psi^k = v\Delta$ then $u\psi^k = u\Delta$. □

From Lemma 4.21, if a ψ-orbit has a characteristic element, then every X-component of this ψ-orbit contains a characteristic element, and all these elements have the same characteristic. Bearing this in mind we make the following definition.

Definition 4.22. Let $\psi \in G_{n,r}$ have an X-component $\mathcal{C}$ containing a characteristic element u. Then we define the *characteristic* of $\mathcal{C}$ to be equal to the characteristic of u.

Theorem 4.23 ([17, Theorem 9.4]). *Let $\psi \in G_{n,r}$ be in semi-normal form with respect to X. Then ψ is of infinite order if and only if it has a characteristic element u. Moreover, if ψ is of infinite order then we may assume that $u \in X$.*

Proof. If u is a characteristic element for ψ with characteristic (m, Γ) then $u\psi^m = u\Gamma$, so $u\psi^{mq} = u\Gamma^q$. So for sufficiently large q, $u\psi^{mq} \in X\langle A\rangle$. Then $u\psi^{mq}$ also has characteristic (m, Γ) by Lemma 4.21. Write $u\psi^{mq} = x\Delta$, for some $x \in X$ and $\Delta \in A^*$. Now $x\Delta\Gamma = u\psi^{mq}\Gamma = u\psi^{m(q+1)} = x\Delta\psi^m$, so from Lemma 4.18, x has type (B). Thus we may assume $u \in X$. Now

$$\begin{aligned} u\psi^{mj} &= u\psi^m\psi^{m(j-1)} = u\Gamma\psi^{m(j-1)} = u\Gamma\psi^m\psi^{m(j-2)} \\ &= u\psi^m\Gamma\psi^{m(j-2)} = u\Gamma^2\psi^{m(j-2)} = \cdots = u\Gamma^j, \end{aligned}$$

for $j \in \mathbb{N}$. Since Γ is a characteristic multiplier, the elements $u\Gamma^j$ are all different for $j \in \mathbb{N}$, so ψ has infinite order.

Conversely, if ψ has no characteristic element, then certainly there are none in X, so X has no elements of type (B) nor type (C). Thus all elements of X are of type (A), as ψ is in semi-normal form; whence ψ is a permutation of X and has finite-order. □

Lemma 4.24. *Let ψ be in semi-normal form with respect to an A-basis X and let $u \in V_{n,r}$. If u has characteristic (m, Γ) then the ψ-orbit of u has precisely one X-component, which is semi-infinite (right semi-infinite if $m > 0$ and left semi-infinite if $m < 0$) and consists of elements of the form $x\Lambda$, where $x \in X$ is of type (B) and $\Lambda \in A^*$.*

Furthermore, if $x\Lambda$ belongs to the X-component of the ψ-orbit of u, where $x \in X$ and $\Lambda \in A^*$, then x has characteristic $(m, \Gamma_1\Gamma_0)$, where $\Gamma = \Gamma_0\Gamma_1, \Lambda = (\Gamma_1\Gamma_0)^p\Gamma_1 = \Gamma_1\Gamma^p, p \geq 0$, and Γ_0 is nontrivial.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Proof. As $u\psi^m = u\Gamma$ we have $u\psi^{mq} = u\Gamma^q$, for all integers $q \geq 0$, and choosing q sufficiently large $u\Gamma^q \in X\langle A\rangle$. Thus we may assume that $u \in X\langle A\rangle$. Let $\mathcal{C}$ denote the X-component containing u and write $u = x\Lambda$, where $x \in X$ and $\Lambda \in A^*$.

Assume first that $m > 0$. As u has characteristic (m, Γ), both $x\Lambda$ and $x\Lambda\Gamma$ belong to $\mathcal{C}$, so x is of type (B) by Lemma 4.18. Suppose there is an integer $K \geq 0$ such that $u\psi^{-k} \in X\langle A\rangle$, for all $k \geq K$. (That is, suppose that the ψ-orbit of u contains a left semi-infinite X-component.) Let $\Lambda = \Lambda_0\Gamma^t$, where Λ_0 has no terminal segment equal to Γ. Then, for j such that $m(j+1) \geq K$ and $j \geq t$, $u\psi^{-m(j+1)} \in X\langle A\rangle$, so $u\psi^{-m(j+1)} = z\Xi$ for some $z \in X$ and $\Xi \in A^*$. From Lemma 4.21 we see that $z\Xi$ has characteristic (m, Γ). Hence

$$z\Xi\Gamma^{j+1} = z\Xi\psi^{m(j+1)} = u = x\Lambda_0\Gamma^t,$$

which implies $z = x$ and $\Xi\Gamma^{j-t+1} = \Lambda_0$, a contradiction. As ψ is in semi-normal form with respect to X and $\mathcal{C}$ is not a complete X-component, the $\mathcal{C}$ must be right semi-infinite. We have just shown the ψ-orbit of u contains no left semi-infinite X-component, so $\mathcal{C}$ is the unique X-component of this ψ-orbit.

For the second part of the lemma, suppose x has characteristic (k, Ω). The X-component of x cannot be left semi-infinite, or else $x\Lambda\psi^{-i} \in X\langle A\rangle$ for all $i \geq 0$; this would mean that $\mathcal{C}$ is not right semi-infinite. Hence x is in a right semi-infinite X-component and $k > 0$. If $\Lambda = \Omega^j\Lambda_1$ then $x\Lambda_1\psi^{kj} = x\Omega^j\Lambda_1 = u$ and so $\mathcal{C}$ contains $x\Lambda_1$; and it suffices to prove the lemma under the assumption that Λ has no initial segment equal to Ω.

Suppose that $m = kp+r$, where $0 \leq r < k$. Then $x\Lambda\psi^{kp} = x\Omega^p\Lambda$ and $x\Omega^p\Lambda\psi^r = x\Lambda\psi^{kp+r} = x\Lambda\psi^m = x\Lambda\Gamma$. However, as x is in a right semi-infinite X-component, $x\psi^r = z\Xi$, for some $z \in X$ and $\Xi \in A^*$. Thus $x\Lambda\Gamma = x\Omega^p\Lambda\psi^r = x\psi^r\Omega^p\Lambda = z\Xi\Omega^p\Lambda$, which implies that $z = x$ and $\Lambda\Gamma = \Xi\Omega^p\Lambda$. Now, as $x\psi^r = x\Xi$, $0 \leq r < k$ and x has characteristic (k, Ω), it must be that $r = 0$, $m = kp$ and $\Xi = \varepsilon$. We have now $\Lambda\Gamma = \Omega^p\Lambda$, and as Λ has no initial segment equal to Ω it follows that $\Omega = \Lambda\Omega_1$. Now $u\psi^k = x\Lambda\psi^k = x\psi^k\Lambda = x\Omega\Lambda = x\Lambda\Omega_1\Lambda = u\Omega_1\Lambda$, so $k \geq m$, by definition of characteristic. Therefore $k = m$ and $\Gamma = \Omega_1\Lambda$, completing the proof in the case $m > 0$.

In the case when $m < 0$ the result follows from the above on replacing ψ by ψ^{-1}. □

An element w of the free monoid A^* is said to be *periodic with period* i if $w = a_1 \cdots a_n$, where $a_j \in A$, and $a_k = a_{k+i}$, for $1 \leq k \leq n-k$. In this sense, in Lemma 4.24 above, $\Lambda = (\Gamma_1\Gamma_0)^p\Gamma_1$ is periodic of period m.

Lemma 4.25. *Let $\psi \in G_{n,r}$ and $u \in V_{n,r}$ such that $u\psi^k = u\Delta$, where $\Delta \neq \varepsilon$. Then u has characteristic (m, Γ) with respect to ψ, where $k = mq$ and $\Delta = \Gamma^q$, for some positive integer q.*

Proof. Let ψ be in semi-normal form with respect to X, and let (m, Γ) be the characteristic of u. Suppose first that $k > 0$. As in the proof of Lemma 4.24, we may

assume that $u \in X\langle A\rangle$, the X-component of u is right semi-infinite and that there exist $x \in X$ and $\Gamma_1 \in A^*$ such that $u = x\Gamma_1$ and x has characteristic power m. Then $k \geq m$, say $k = mq + s$, where $0 \leq s < m$ and $q \geq 1$. Let $x\psi^s = y\Lambda'$, where $y \in X$ and $\Lambda' \in A^*$. Now $x\Gamma_1\Delta = u\Delta = u\psi^k = u\psi^{mq+s} = u\Gamma^q\psi^s = x\psi^s\Gamma_1\Gamma^q = y\Lambda'\Gamma_1\Gamma^q$. Hence $x = y$ and so $s = 0$ and $k = mq$. Moreover $x\Lambda\Delta = u\Delta = u\psi^k = u\psi^{mq} = u\Gamma^q = x\Lambda\Gamma^q$, so $\Lambda\Delta = \Lambda\Gamma^q$, from which $\Delta = \Gamma^q$, as required.

If $k < 0$, replace ψ with ψ^{-1} in the argument above. We have $u\psi^{-k} = u\Delta$, so from the previous part of the proof, u has characteristic (m, Γ), with respect to ψ, where $-k = mq$, $q > 0$, and $\Delta = \Gamma^q$. If follows that u has characteristic $(-m, \Gamma)$, with respect to ψ, and $-m = kq$, completing the proof. □

Corollary 4.26. *Let ψ be in semi-normal form with respect to an A-basis X and let $u \in V_{n,r}$. Then there exists an element $\Lambda \in A^*$ such that $u\Lambda$ belongs to a complete X-component of ψ.*

Proof. Multiplying by a sufficiently long element of A^* we may, as usual, assume that $u \in X\langle A\rangle$, so u belongs to either a complete or a semi-infinite X-component of ψ. There are finitely many semi-infinite X-components (Lemma 4.6). If S is a characteristic semi-infinite X-component with characteristic (m, Γ) then, from Lemma 4.24, elements of S have the form $x\Lambda$ where $x \in X$, $\Lambda \in A^*$ and, for all but finitely many elements of S, Λ is periodic of period m.

Let F_S be the finite subset of elements of A^* such that $\Lambda \in F_S$ only if $x\Lambda \in S$ and Λ is not periodic of period m. Let F_0 be the union of the F_S over all characteristic semi-infinite X-components. If S is non-characteristic then, from Lemma 4.18, S contains an element $z\Delta$, where $z \in X$ of type (B), with characteristic (m', Γ'), say. It follows, from Lemma 4.24 again, that all but finitely many elements of S have the form $x\Lambda\Delta$ where $x \in X$, $\Lambda \in A^*$ and Λ is periodic of period m'. This time, let F_S be the finite subset of elements of A^* such that $\Lambda\Delta \in F_S$ only if $x\Lambda\Delta \in S$ and Λ is not periodic of period m'. Let F_1 be the union of the F_S over all non-characteristic semi-infinite X-components.

Let M be the maximum of lengths of elements of $F_0 \cup F_1$ and assume $u = x\Gamma$, where $x \in X$, $\Gamma \in A^*$. Choose element Ξ of A^* such that $\Gamma\Xi$ has length greater than M, is not periodic and does not factor as $\Lambda\Delta$, where Λ is periodic and $\Delta \in F_1$. Then $u\Xi = x\Gamma\Xi$ cannot belong to a semi-infinite X-component, so must belong to a complete X-component. □

4.2. *Quasi-normal forms*

Quasi-normal forms are particular semi-normal forms which give representations of automorphisms minimizing the number of elements in pond orbits. In [17, Sec. 9] it is claimed that if an automorphism is given with respect to a quasi-normal form, then it has no pond orbits. In this section we shall see that this is not the case.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Definition 4.27 ([17, Sec. 9]). An element ψ of $G_{n,r}$ is in *quasi-normal* form with respect to the A-basis X if it is in semi-normal form with respect to X, but not with respect to any proper contraction of X.

It follows from Lemma 4.3 that for $\psi \in G_{n,r}$ there exists an A-basis X with respect to which ψ is in quasi-normal form. For instance, the automorphisms ψ in Examples 4.11, 4.13 and 4.17 are in quasi-normal form with respect to the bases X in those examples. Additionally, the automorphism ψ of Example 4.12 is in quasi-normal form with respect to the basis X_3.

Lemma 4.28 (cf. [17, Lemma 9.7]). *Given an element $\psi \in G_{n,r}$ there exists a unique A-basis, denoted X_ψ, with respect to which ψ is in quasi-normal form. Furthermore X_ψ may be effectively constructed.*

Proof. Assume ψ is given by listing the images of elements of X, where X is an A-basis of $V_{n,r}$. We modify X to find an A-basis X' with respect to which ψ is in semi-normal form. For each $y \in X$ we can list elements of the ψ-orbit of y.

$$\ldots, y\psi^{-3}, y\psi^{-2}, y\psi^{-1}, y, y\psi, y\psi^2, y\psi^3, \ldots.$$

We enumerate the forward sequence $(y\psi^m)_{m\geq 0}$, until we reach $m \geq 0$ such that

(1F) either $y\psi^m \in X\langle A\rangle$ with $y\psi^{m+1} \notin X\langle A\rangle$, or
(2F) for some $0 \leq l < m$, $\hat{y} \in X$ and $\Gamma, \Delta \in A^*$ we have $y\varphi^l = \hat{y}\Gamma$ and $y\varphi^m = \hat{y}\Delta$.

Similarly, we enumerate the backwards sequence $(y\psi^{-k})_{k\geq 0}$ until we reach $k \geq 0$ such that

(1B) either $y\psi^{-k} \in X\langle A\rangle$ with $y\psi^{-(k+1)} \notin X\langle A\rangle$ or,
(2B) for some $0 \leq l < k$, $\hat{y} \in X$ and $\Gamma, \Delta \in A^*$ we have $y\varphi^{-l} = \hat{y}\Gamma$ and $y\varphi^{-k} = \hat{y}\Delta$.

Given $y \in X$, the forward part of the process above produces a sequence of elements of $X\langle A\rangle$, until it halts. As X is finite, if it does not halt at step (1F) then it halts at step (2F); so always halts. Similarly, the backward part of the process always halts.

If some y satisfies **(1F)** and **(1B)**, then y is in an incomplete X-component, so ψ is not in semi-normal form with respect to X. In this case we take a simple expansion X' of X at the element y. Next, use the proof of Lemma 4.9 to find an expansion X'' of X' with respect to which ψ is in semi-normal form. We now replace X with X'' and return to the start of this proof. Repeating as necessary, eventually we shall find X such that no $y \in X$ satisfies both **(1F)** and **(1B)**. The repetition terminates because the number of elements $x'' \in X''$ belonging to incomplete X'' components is strictly smaller than the corresponding number for X.

At this stage, every $y \in X$ satisfies one of **(2F)** and **(2B)**, so ψ is in semi-normal form with respect to X by Lemma 4.18. We can now test all the contractions of the A-basis X to find an expansion of $\mathbf{x}$ with respect to which ψ is in a quasi-normal form.

For uniqueness, we will argue by contradiction. Let ψ be in quasi-normal form with respect to X_1 and X_2, with $X_1 \neq X_2$. Since X_1, X_2 are expansions of $\mathbf{x}$, (without loss of generality) there exists a simple contraction X_1' of X_1 which contains an element y of $X_2 \backslash X_1$. Then $X_1'\langle A\rangle = X_1\langle A\rangle \cup \{y\}\langle A\rangle$ and, as ψ is in semi-normal form with respect to X_2, it is also in semi-normal form with respect to X_1', contrary to the definition of quasi-normal form. □

Remark 4.29. Let $\psi \in G_{n,r}$ be in quasi-normal form with respect to X. The proof of this lemma illustrates that if ψ is in semi-normal form with respect to X', then X' is an expansion of X. The converse is false: it is not true in general that ψ is in semi-normal form with respect to all expansions of X.

Lemma 4.30. *Let $\psi \in G_{n,r}$ be in semi-normal form with respect to an A-basis X and let $u, v \in X\langle A\rangle$. Then we can effectively decide whether or not u, v are in the same X-component, and if so, find the integers m for which $u\psi^m = v$.*

Proof. As $u \in X\langle A\rangle$, we have $u = y\Lambda$ where $y \in X$ and $\Lambda \in A^*$. We now run the process of Lemma 4.28 on y. If the process halts with $y\psi^m = y$, for some m then we may list the elements $u\psi^i = y\psi^i\Lambda$, $i = 0, \ldots, m-1$, of the (complete finite) ψ-orbit of u. In this case v is in the same ψ-orbit as u if and only if it appears in the list, so we are done.

Otherwise the process halts at least one of the states (2F) and (2B). We obtain $\widetilde{y} \in X$ and integers $k \neq l$ such that $y\varphi^k = \widetilde{y}\Lambda_1$ and $y\varphi^l = \widetilde{y}\Lambda_2$, where Λ_1 and Λ_2 are distinct elements of A^*. It follows from Lemma 4.18 that $\widetilde{y}$ is of type (B). As u and $u\varphi^k = y\Lambda\varphi^k = \widetilde{y}\Lambda_1\Lambda$ are k steps apart in the same X-component, we may replace $u = y\Lambda$ with $\widetilde{u} = \widetilde{y}\Lambda_1\Lambda$. Therefore we now assume that $u = y\Lambda$, where y is of type (B).

Now, when we run the process of Lemma 4.28 on y it halts either at (2F) and (1B) or else at (1F) and (2B). Suppose first the forward part halts at (2F). Then y is in a right semi-infinite X-component and there is a minimal positive integer m such that $y\psi^m = y\Gamma$, with $\Gamma \neq 1$. That is y has characteristic (m, Γ), with $m > 0$. Set $u_0 = y\Lambda_0$. If $\Lambda = \Gamma^i\Lambda_0$ where Λ_0 has no initial segment Γ, then

$$u_0\psi^{mi} = y\Lambda_0\psi^{mi} = y\psi^{mi}\Lambda_0 = y\Gamma^i\Lambda_0 = y\Lambda = u,$$

so u_0 is mi steps away from u in the ψ-orbit of u. We may replace $u = y\Lambda$ by $u_0 = y\Lambda_0$. This allows us to assume from now on that Λ has no initial segment equal to the characteristic multiplier Γ of y.

Next we run the process of Lemma 4.28 on u instead of y. As y is in a right semi-infinite X-component the forward part of the process halts at (2F). We obtain a list of elements of the X-component of u of the form

$$z_r\Phi_r, \ldots, z_1\Phi_1, u = y\Lambda, y_1\Gamma_1'\Lambda, \ldots, y_{m-1}\Gamma_{m-1}'\Lambda, y\Gamma\Lambda, \tag{4.6}$$

where $y_j, z_j \in X$, $\Gamma_j', \Phi_j \in A^*$, $z_j\Phi_j = u\psi^{-j}$, for $1 \leq j \leq r$ and for some $r \geq 0$, and $y\psi^s = y_s\Gamma_s'$, for $0 < s < m$. (The y_i's must be distinct otherwise u would have

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

characteristic power less than m.) We proceed differently based on which state the backwards enumeration finishes in.

Case (1B). If the backward part of the process halts at (1B) then $z_r\Phi_r\psi^{-1} = u\psi^{-r-1} \notin X\langle A\rangle$. In this case, the entire X-component of u consists of the elements on this list together with elements

$$y_i\Gamma_i'\Gamma^q\Lambda, \quad \text{with } q > 0 \text{ and } 0 < i \leq m,$$

where we set $y_0 = y$, $\Gamma_0' = \Gamma$.

As $v \in X\langle A\rangle$ we also have $z \in X$ and Δ in A^* such that $v = z\Delta$. If z is in a finite X-component then v cannot belong to the same X-component as u, so we assume z is in an infinite X-component. As in the case of u, we may adjust v so that z is of type (B). As before we find a characteristic multiplier Φ for z and, replacing Δ with a shorter element if necessary, we may assume that Δ has no initial segment equal to Φ.

If $v = u\psi^d$, where $d \geq 0$, then $v = y_i\Gamma_i'\Gamma^q\Lambda$, for some $q \geq 0$ and i with $0 \leq i < m$. In this case, $z = y_i$ and by Lemma 4.24 and our assumption on v we have $q = 0$, so $v = y_i\Gamma_i'\Lambda$, which appears on list (4.6). Assume then that $v = u\psi^d$, where $d < 0$. As the backward part of the enumeration of the ψ-orbit of u halts at (1B), the X-component of u has initial element $z_r\Phi_r$, and v must appear on list (4.6).

Case (2B). On the other hand, if the backward part of the process stops at (2B) then u is in a complete infinite X-component and, for some s with $0 \leq s \leq r$, we have $z_r = z_s$ (and r is minimal with this property). It follows that z_s is of type (B) and in a left semi-infinite X-component. Again, we may assume that $v = z\Delta$, where $\Delta \in A^*$, $z \in X$ is of type (B) and has characteristic multiplier Φ, such that Δ has no initial segment equal to Φ. As before, if $v = u\psi^d$ with $d \geq 0$, then v appears on list (4.6). Assume then that $v = u\psi^d$, where $d < 0$. Repeating the argument above, using the left semi-infinite X-component of z_s instead of the right semi-infinite X-component of y, it follows again that v appears on list (4.6).

Therefore, in the case where y is in a right semi-infinite X-component we have v in the X-component of u if and only if v lies on the list (4.6); and we may compute m such that $u\psi^m = v$, if this is the case. Finally, if the enumeration of the X-component of y halts at steps (1F) and (2B) then the process is essentially the same, except that we deal with a left, rather than a right, semi-infinite X-component of y. □

This procedure allows us to decide if two given words in $X\langle A\rangle$ belong to the same X-component so, if there are no pond orbits, we may decide if two such words belong to the same ψ-orbit. On the other hand, as the enumeration of components always stops once we fall outside $X\langle A\rangle$, we cannot detect when a pair of elements lie in the same ψ-orbit but on opposite sides of a pond. We demonstrate below that there exist automorphisms for which every semi-normal form has a pond; thus we require a strategy to deal with ponds.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Lemma 4.31. *Let $\psi \in G_{n,r}$ be in semi-normal form with respect to X, and suppose that some ψ-orbit $\mathcal{O}$ contains a pond with respect to X. If ψ is in semi-normal form with respect to an expansion X' of X, then $\mathcal{O}$ is also a pond-orbit with respect to X'.*

Proof. Let us write $\mathcal{O}$ as

$$\mathcal{O}: \qquad \dots\, l\psi^{-t},\, \dots\, l\psi^{-1},\, l,\, p_1, \dots\, p_k,\, r,\, r\psi, \dots\, r\psi^s, \dots,$$

where $l, r \in X\langle A\rangle$ are endpoints of semi-infinite X-components and the $p_i \notin X\langle A\rangle$ form a pond of width $k+1$. To begin with we claim that, for sufficiently large $s \geq 0$, we have $r\psi^s \in X'\langle A\rangle$. Indeed, because r belongs to a semi-infinite X-component, Lemma 4.18 implies that there is some $s' \geq 0$ for which $r\psi^{s'} = r'\Delta$, where $\Delta \in A^*$ and $r' \in X$ has characteristic (m, Γ). Therefore, for all $q \geq 0$,

$$r\psi^{s'+mq} = r\psi^{s'}\psi^{mq} = r'\Delta\psi^{mq} = r'\psi^{mq}\Delta = r'\Gamma^q\Delta.$$

By taking q sufficiently large, we can ensure that $r\psi^{s'+mq} \in X'\langle A\rangle$. This works because the difference $X\langle A\rangle \backslash X'\langle A\rangle$ is finite. So we can find $s \geq 0$ such that $r\psi^s \in X'\langle A\rangle$. Similarly, there is some $t \geq 0$ for which $l\psi^{-t} \in X'\langle A\rangle$.

Since $X'\langle A\rangle \subset X\langle A\rangle$, it follows that each $p_i \notin X'\langle A\rangle$. Appealing to Corollary 4.14, the only possibility is that $\mathcal{O}$ is a pond-orbit with respect to X'. □

Notice that the pond width with respect to X' is at least the previous width $(k+1)$ with respect to X. Additionally, if ψ was in *quasi*-normal form with respect to X, this (with Remark 4.29) shows that every semi-normal form X' for ψ contains the pond given above. Example 4.17 shows that this possibility does occur.

Lemma 4.32. *Given an element $\psi \in G_{n,r}$ in semi-normal form with respect to an A-basis X we may effectively construct the set $P(\psi)$ of the triples (l, k, r) such that r (respectively, l) is the initial (respectively, terminal) word in a right (respectively, left) semi-infinite X-component, and k is the width of the pond between them.*

Proof. Let Y be the minimal expansion of X associated to ψ and let $Z = Y\psi$. Since there are no incomplete X-components, Lemma 4.6 tells us that the set of initial elements of right semi-infinite X-components is $R = X\langle A\rangle \backslash Z\langle A\rangle$. This is finite, so we may enumerate this effectively. The same is true for the set $L = X\langle A\rangle \backslash Z\langle A\rangle$ of terminal elements of left semi-infinite X-components. To enumerate $P(\psi)$, for each $(l, r) \in L \times R$ we need to solve the equation $r = l\psi^k$ for some k, or to determine that there is no solution. A solution exists if and only if $r\Gamma = l\Gamma\psi^k$, for all $\Gamma \in A^*$.

With this in mind, first find $\Gamma \in A^*$ such that $l\Gamma$ is in a complete infinite X-component. We do this by enumerating the words Γ of length $1, 2, \dots$ and applying the process of Lemma 4.28 to each element $l\Gamma$ in turn. We stop when we find Γ such that the process halts at (2F) and (2B). Now use Lemma 4.30 to determine whether $r\Gamma$ and $l\Gamma$ are in the same X-component. If not, then there cannot exist an element of the form $(l, k, r) \in P(\psi)$; that is l and r are not joined by a pond.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Assume then that $r\Gamma = l\Gamma\psi^k$, for some k. We can test to see if $r = l\psi^k$ directly, which holds if and only if $(l, k, r) \in P(\psi)$. If the equality were false, is it possible that $(l, k', r) \in P(\psi)$ for a different $k' \neq k$? This would mean that $r = l\psi^{k'}$, so $l\psi^k\Gamma = r\Gamma = l\Gamma\psi^{k'}$ and thus $l\Gamma\psi^{k-k'} = l\Gamma$. As $l\Gamma$ belongs to a complete infinite X-component, this means $k = k'$; so the answer to our previous question is "no". In this situation there are no elements of the form (l, k', r) in $P(\psi)$. □

In practice, when enumerating the sets L and R in the proof above, we need to consider only non-characteristic elements, as Lemma 4.24 implies that no characteristic element belongs to a pond orbit.

Example 4.33. Let ψ and X be the automorphism and basis described in Example 4.17; we noted above that ψ is in quasi-normal form with respect to X. We claim that this ψ-orbit is the only pond orbit with respect to X.

The endpoints of semi-infinite X-components are precisely

$$L = X\langle A\rangle \backslash Y\langle A\rangle = \{x\alpha_1^2, x\alpha_1^3, x\alpha_1^2\alpha_2\}$$
$$\text{and } R = X\langle A\rangle \backslash Z\langle A\rangle = \{x\alpha_1\alpha_2, x\alpha_1\alpha_2\alpha_1, x\alpha_1\alpha_2^2\}.$$

The four endpoints $x\alpha_1^2$, $x\alpha_1^3$, $x\alpha_1\alpha_2$ and $x\alpha_1\alpha_2\alpha_1$ have characteristics $(-1, \alpha_1^2)$, $(-1, \alpha_1^2)$, $(1, \alpha_1\alpha_2)$ and $(1, \alpha_2\alpha_1)$, respectively. Are the two remaining endpoints $l = x\alpha_1^2\alpha_2$ and $r = x\alpha_1\alpha_2^2$ separated by a pond? (We saw before in computation (4.5) that they are, but to illustrate Lemma 4.32 we will remain ignorant of this.)

Multiplying by $\Gamma = \alpha_1$ we obtain $l\Gamma = x\alpha_1^2\alpha_2\alpha_1$, which is in a complete infinite X-component. We also see that $r\Gamma = l\psi^2\Gamma = x\alpha_1\alpha_2^2\alpha_1$ is in this component, so we have a candidate pond width of $k = 2$. Fortunately we directly computed that $r = l\psi^2$ in (4.5), so $P(\psi) = \{(x\alpha_1^2 a_2, 2, x\alpha_1\alpha_2^2)\}$.

Lemma 4.34 (cf. [17, Lemma 9.7]). *Let $\psi \in G_{n,r}$ and $u, v \in V_{n,r}$. Then we can effectively decide whether or not u, v are in the same ψ-orbit, and if so, find the integers m for which $u\psi^m = v$.*

Proof. For a fixed integer $s \geq 0$ we have $u\psi^m = v$ if and only if $(u\Gamma)\psi^m = u\psi^m\Gamma = v\Gamma$ for all $\Gamma \in A^*$ of length s (using Lemma 3.20). Now, suppose that we have an algorithm $\mathcal{A}$ to decide whether $v' = u'\psi^m$ for some m, given elements u', v' of $X\langle A\rangle$ (and to return m, if so). Then if u, v are arbitrary elements of $V_{n,r}$ we may choose s such that $u\Gamma$ and $v\Gamma$ belong to $X\langle A\rangle$, for all $\Gamma \in A^*$ of length s, and input all these elements to the algorithm $\mathcal{A}$ in turn. In the light of the previous remark, this allows us to determine whether or not u and v belong to the same ψ-orbit (and to return appropriate m, if so). Hence we may assume $u, v \in X\langle A\rangle$.

By Corollary 4.14, u and v belong to the same ψ-orbit if and only if either they belong to the same X-component of a ψ-orbit, or they belong to different X-components of a single pond orbit. We may use Lemma 4.30 to decide whether or not u and v both belong to the same X-component. If so we are finished. If not, and

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

both belong to semi-infinite X-components, then for each triple (l, k, r) in $P(\psi)$ we check whether u belongs to the same component as l or r.

If u belongs to neither component then u is not in a pond orbit, and thus u and v do not share a ψ-orbit. Otherwise if u and l (respectively, r) share an X-component, we run the same check on v and r (respectively, l). If the check determines that v is not in the X-component in question, then u and v do not share a ψ-orbit. Else we have $l = u\psi^a$ and $v = r\psi^b$ for some a and b, so $v = u\psi^{a+k+b}$. □

Example 4.35. Let ψ be the automorphism of Examples 4.17 and 4.33, which is in quasi-normal form with respect to $X = \{q_1 = x\alpha_1^2, q_2 = x\alpha_1\alpha_2, q_3 = x\alpha_2\alpha_1, q_4 = x\alpha_2^2\}$. The elements q_1 and q_2 have characteristics $(-1, \alpha_1^2)$ and $(1, \alpha_1\alpha_2)$, respectively, whereas q_3 and q_4 belong to complete infinite X-components such that $q_3\psi = q_2\alpha_2^2$ and $q_4\psi^{-1} = q_1\alpha_2\alpha_1$.

(1) We wish to test if $u = x\alpha_1\alpha_2^2\alpha_1^2\alpha_2 = q_2\alpha_2\alpha_1^2\alpha_2$ and $v = x\alpha_2\alpha_1^2 = q_3\alpha_1$ belong to the same ψ-orbit. Because q_3 is not characteristic, Lemma 4.30 first replaces $v = q_3\alpha_1$ with $v' = v\psi = q_3\psi\alpha_1 = q_2\alpha_2^2\alpha_1$, which begins with the characteristic element q_2 of X. Enumerating the X-component containing u gives us a specific instance of list (4.6)

$$\begin{aligned} x\alpha_1^4\alpha_2\alpha_1^2\alpha_2 &\mapsto x\alpha_1^2\alpha_2\alpha_1^2\alpha_2 \mapsto x\alpha_2^2\alpha_1\alpha_2 \\ &\mapsto \underbrace{x\alpha_1\alpha_2^2\alpha_1^2\alpha_2}_{u} \mapsto x(\alpha_1\alpha_2)^2\alpha_2\alpha_1^2\alpha_2 \end{aligned} \tag{4.6$'$}$$

once the enumeration has halted at stages (2F) and (2B). Since v' does not lie on this list, we conclude that v' does not belong to the X-component of u, so neither does v.

We now need to check if u and v are separated by a pond. In Example 4.33, we showed that ψ has only one pond-orbit, and referring to the computation (4.5) we see that neither u nor v belong to this orbit. Hence u and v' do not share a ψ-orbit.

(2) Now let us test if u and $w = x\alpha_1^4\alpha_2\alpha_1^2\alpha_2 = q_1\alpha_1^2\alpha_2\alpha_1^2\alpha_2$ share a ψ-orbit. We remove the characteristic multiplier α_1^2 of q_1 from w, obtaining $w' = q_1\alpha_2\alpha_1^2\alpha_2$ where $w'\psi^{-1} = w$. From list (4.6$'$) we notice that $u\psi^{-2} = w'$, so $u\psi^{-3} = w$.

(3) Let $u = x\alpha_1^8\alpha_2$, $v = x\alpha_1^4\alpha_2\alpha_1$ and $w = x(\alpha_1\alpha_2)^3\alpha_2$. In terms of X, these are $u = q_1\alpha_1^6\alpha_2$, $v = q_1\alpha_1^2\alpha_2\alpha_1$, and $w = q_2(\alpha_1\alpha_2)^2\alpha_2$. Since q_1 and q_2 are characteristic, we remove copies of the characteristic multipliers. We obtain $u' = q_1\alpha_2 = u\psi^3$, $v' = q_1\alpha_2\alpha_1 = v'\psi$ and $w' = q_2\alpha_2 = w\psi^{-2}$. Enumerating the X-component of u' gives us

$$\ldots \mapsto x\alpha_1^4\alpha_2 \mapsto x\alpha_1^2\alpha_2 = u',$$

(halting at stages (1F) and (2B)) and we see that neither v' nor w' are in this list. However, u' is adjacent to a pond. Referring once again to Example 4.17,

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

we see that the corresponding endpoint is $\bar{u} = u'\psi^2 = x\alpha_1\alpha_2^2$. Its X-component begins

$$\bar{u} = x\alpha_1\alpha_2^2 \mapsto x(\alpha_1\alpha_2)^2\alpha_2 \mapsto \dots.$$

Since this list does not contain v', we conclude that u and v do not share a ψ-orbit. On the other hand, we note that $w' = \bar{u}$ belongs to the list. Hence u and w belong to the same ψ-orbit, and having kept track of the various powers, we calculate that

$$w\psi^{-2} = w' = \bar{u} = u'\psi^2 = u\psi^3\psi^2 \implies w = u\psi^7.$$

5. The Conjugacy Problem

For a group with presentation $G = \langle X \mid R\rangle$, the conjugacy problem is to determine, given words $g, h \in \mathbb{F}(X)$ whether or not g is conjugate to h in G; denoted $g \sim h$. The strong form, which we consider here, requires us to produce a conjugator $c \in \mathbb{F}(X)$ when g is conjugate to h, i.e. an element c such that $c^{-1}gc =_G h$. We say the conjugacy problem is *decidable* if there is an algorithm which for inputs g and h outputs "yes" if they are conjugate and "no" otherwise. The stronger form is decidable if there is an algorithm which produces a conjugator c in the "yes" case. Note that the word problem is the special case of the conjugacy problem where $h = 1$.

As pointed out at the beginning of Sec. 4, an element ψ of $G_{n,r}$ may be uniquely represented by the triple (Y, Z, ψ_0), where Y is the minimal expansion of ψ, $Z = Y\psi$ and ψ_0 is a bijection between Y and Z, namely $\psi_0 = \psi|_Y$. This triple is called a *symbol* for ψ. In [17, Sec. 4] a finite presentation of $G_{n,r}$ is given, with generators the symbols (Y, Z, ψ_0) such that Y is a d-fold expansion of $\mathbf{x}$, for $d \leq 3$. As we may effectively enumerate symbols and effectively construct the symbol for $\psi_1\psi_2$, from the symbols for ψ_1 and ψ_2, words in Higman's generators effectively determine symbols and vice-versa. Therefore when we consider algorithmic problems in $G_{n,r}$ we may work with symbols for automorphisms, and leave the presentation in the background. That is, we always assume that automorphisms are given as maps between bases of $V_{n,r}$ (from which a symbol may be computed). As minimal expansions are unique it follows immediately that the word problem is solvable in $G_{n,r}$. In this section, we give an algorithm for the conjugacy problem in $G_{n,r}$, based on (a complete version of) Higman's solution.

5.1. *Higman's ψ-invariant subalgebras*

Let ψ be an element of $G_{n,r}$. Higman defined two Ω-subalgebras of $V_{n,r}$ determined by ψ, namely

- the Ω-subalgebra $V_{P,\psi}$ generated by the set of elements of $V_{n,r}$ which belong to finite ψ-orbits.
- the Ω-subalgebra $V_{RI,\psi}$ generated by the set of characteristic elements for ψ.

Where there is no ambiguity, we will write V_P for $V_{P,\psi}$ and V_{RI} for $V_{RI,\psi}$.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

If $u \in V_{n,r}$ then the ψ-orbit of u is identical to the ψ-orbit of $u\psi$; so u is in a finite ψ-orbit if and only if $u\psi$ is in a finite ψ-orbit. From Lemma 4.21, an element u is a characteristic element for ψ if and only if $u\psi$ is a characteristic element for ψ. Therefore $V_{P,\psi}$ and $V_{RI,\psi}$ are ψ-invariant subalgebras of $V_{n,r}$. (A subalgebra S is *ψ-invariant* if $S\psi = S$.) Hence $\psi_P = \psi|_{V_{P,\psi}}$ is an automorphism of $V_{P,\psi}$ and $\psi_{RI} = \psi|_{V_{RI,\psi}}$ is an automorphism of $V_{RI,\psi}$.

If ψ and φ are conjugate elements of $G_{n,r}$ and $\rho^{-1}\psi\rho = \varphi$ for some conjugator $\rho \in G_{n,r}$, then for all $\Gamma \in A^*$ we have $u\varphi^m = u\Gamma$ if and only if $u\rho^{-1}\psi^m\rho = u\Gamma$ if and only if $(u\rho^{-1})\psi^m = (u\rho^{-1})\Gamma$. Thus u is in a finite φ-orbit if and only if $u\rho^{-1}$ is in a finite ψ-orbit (taking $\Gamma = \varepsilon$) and u is a characteristic element for φ if and only if $u\rho^{-1}$ is a characteristic element for ψ ($\Gamma \neq \varepsilon$). It follows that the restriction $\rho|_{V_{P,\psi}}$ of ρ to $V_{P,\psi}$ maps $V_{P,\psi}$ isomorphically to $V_{P,\varphi}$, and similarly $\rho|_{V_{RI,\psi}}$ is an isomorphism from $V_{RI,\psi}$ to $V_{RI,\varphi}$.

Now suppose that ψ is in semi-normal form with respect to an A-basis X. Partition X into

$$X_P = X_{P,\psi} = \{y \in X \mid y \text{ is of type (A)}\}$$
$$\text{and } X_{RI} = X_{RI,\psi} = \{y \in X \mid y \text{ is of type (B) or (C)}\}.$$

Theorem 5.1 ([17, Theorem 9.5]). *Let ψ be an element of $G_{n,r}$, in semi-normal form with respect to A-basis X. Then, with the notation above, the following statements hold.*

(1) *$V_{n,r} = V_P * V_{RI}$, the free product of the ψ-invariant subalgebras V_P and V_{RI}.*
(2) *$V_P = X_P\langle A\rangle\langle\lambda\rangle$ and $V_{RI} = X_{RI}\langle A\rangle\langle\lambda\rangle$; that is, V_P (V_{RI}) is generated by X_P (X_{RI}).*
(3) *Given $\psi, \varphi, \rho \in G_{n,r}$ define six restrictions as follows.*

$$\psi_P = \psi|_{V_{P,\psi}}, \quad \varphi_P = \varphi|_{V_{P,\varphi}}, \quad \rho_P = \rho|_{V_{P,\psi}},$$
$$\psi_{RI} = \psi|_{V_{RI,\psi}}, \quad \varphi_{RI} = \varphi|_{V_{RI,\varphi}}, \quad \rho_{RI} = \rho|_{V_{RI,\psi}}.$$

We have $\rho^{-1}\psi\rho = \varphi$ if and only if $\rho_P^{-1}\,\psi_P\,\rho_P = \varphi_P$ and $\rho_{RI}^{-1}\,\psi_{RI}\,\rho_{RI} = \varphi_{RI}$.

Proof. Write $W_P = X_P\langle A\rangle\langle\lambda\rangle$ and $W_{RI} = X_{RI}\langle A\rangle\langle\lambda\rangle$. As X is the disjoint union of X_P and X_{RI}, we have $V_{n,r} = W_P * W_{RI}$, using Lemma 3.11. We shall show that $V_P = W_P$ and $V_{RI} = W_{RI}$. By definition, $W_P \subseteq V_P$. If $x \in X_{RI}$ is of type (B) then $x \in V_{RI}$, by definition. If $x \in X_{RI}$ is of type (C) then there exists $z \in X_{RI}$, of type (B), and $\Delta \in A^*$, such that $x\psi^i = z\Delta$. As $z \in V_{RI}$, so is $z\Delta$, and as V_{RI} is ψ-invariant we have $x = z\Delta\psi^{-i} \in V_{RI}$. Hence $W_{RI} \subseteq V_{RI}$.

To see that $V_P \subseteq W_P$, let $u \in V_{n,r}$ have a finite ψ-orbit. Choose $d \in \mathbb{N}$ such that, $u\Gamma \in X\langle A\rangle$, for all $\Gamma \in A^*$ of length d. For each such Γ write $u\Gamma = x\Delta$, where $x \in X$ and $\Delta \in A^*$. As u is in a finite ψ-orbit so is $u\Gamma$, so $x \in X_P$ and thence $u\Gamma = x\Delta \in W_P$. As this holds for all Γ in A^* of length d, we have $u \in W_P$, by Lemma 3.11. Hence $V_P \subseteq W_P$.

To see that $V_{RI} \subseteq W_{RI}$, we first show that W_{RI} is ψ-invariant. Let Y be the minimal expansion of X associated to ψ and let $x \in X_{RI}$. Then choose d such that $x\Gamma \in Y\langle A\rangle$, for all $\Gamma \in A^*$ of length d. Given such a Γ, write $x\Gamma = y\Delta$ for $y \in Y$ and $\Delta \in A^*$. Then $x\Gamma\psi = y\psi\Delta \in X\langle A\rangle$, so $x\Gamma\psi = z\Lambda$, for some $z \in X$ and $\Lambda \in A^*$. Moreover, z must have type (B) or (C), as x does, so $x\Gamma\psi \in X_{RI}\langle A\rangle \subseteq W_{RI}$. This holds for all Γ of length d, so again $x\psi \in W_{RI}$. It follows that $W_{RI}\psi \subseteq W_{RI}$.

Repeating the same argument, using $Z = Y\psi$ instead of Y and ψ^{-1} instead of ψ gives $W_{RI}\psi^{-1} \subseteq W_{RI}$; so W_{RI} is ψ-invariant as claimed. Now let $u \in V_{n,r}$ be a characteristic element for ψ. Then, from Lemma 4.24, we have $u\psi^i = x\Lambda$, for some integer i, $x \in X_{RI}$ and $\Lambda \in A^*$. Thus $u = x\Lambda\psi^{-i} \in W_{RI}$, as W_{RI} is ψ-invariant; and we have $V_{RI} \subseteq W_{RI}$. This proves (1) and (2) of the theorem, and (3) then follows from the discussion preceding the statement of the theorem. □

Note that in the case that $\rho^{-1}\psi\rho = \varphi$ in the theorem above we have $\rho = \rho_P * \rho_{RI}$ an isomorphism from $V_{P,\psi} * V_{RI,\psi}$ to $V_{P,\varphi} * V_{RI,\varphi}$, both of which are isomorphic to $V_{n,r}$.

Example 5.2. Let ψ be as in Example 4.5. Then $X_P = \{x\alpha_2\alpha_1, x\alpha_2^2\}$ and $X_{RI} = \{x\alpha_1^2, x\alpha_1\alpha_2\}$. Thus ψ_P is the automorphism of $V_P = X_P\langle A\rangle\langle\lambda\rangle$ defined by

$$x\alpha_2\alpha_1 \mapsto x\alpha_2^2, \qquad x\alpha_2^2 \mapsto x\alpha_2\alpha_1.$$

Let $Y_{RI} = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2\}$ and $Z_{RI} = \{x\alpha_1^2, x\alpha_1\alpha_2\alpha_1, x\alpha_1\alpha_2^2\}$, both of which are expansions of X_{RI}. Then ψ_{RI} is the automorphism of $V_{RI} = X_{RI}\langle A\rangle\langle\lambda\rangle$ defined by

$$x\alpha_1^3 \mapsto x\alpha_1^2, \quad x\alpha_1^2\alpha_2 \mapsto x\alpha_1\alpha_2\alpha_1, \quad x\alpha_1\alpha_2 \mapsto x\alpha_1\alpha_2^2.$$

Theorem 5.1 allows us to decompose the conjugacy problem for (ψ, φ) into conjugacy problems for (ψ_P, φ_P) and $(\psi_{RI}, \varphi_{RI})$. Indeed, $V_P \cong V_{n,|X_P|}$ and $V_{RI} \cong V_{n,|X_{RI}|}$, and we regard ψ_P and ψ_{RI} as automorphisms of $V_{n,|X_P|}$ and $V_{n,|X_{RI}|}$, respectively. It turns out that ψ_P and ψ_{RI} are each of particularly simple types; so if we can solve the conjugacy problem for these simple types of automorphism, then we can solve it in general. In the remainder of this subsection we describe in detail how this decomposition works.

First consider a single automorphism $\psi \in G_{n,r}$, where ψ is in semi-normal form with respect to an A-basis X. As before, we take $V_{n,r}$ to be the free $\mathcal{V}_n$ algebra on a set $\mathbf{x}$ of size r, so that X is an expansion of $\mathbf{x}$. Let X_P and X_{RI} be defined as above, let Y be the minimal expansion of X associated to ψ and let $Z = Y\psi$. As Y is an expansion of X, for all $x \in X$ the set $Y_x = Y \cap \{x\}\langle A\rangle$ is an expansion of $\{x\}$, by Lemma 3.16. Therefore $Y_P = Y \cap X_P\langle A\rangle$ is an expansion of X_P, and $Y_{RI} = Y \cap X_{RI}\langle A\rangle$ is an expansion of X_{RI}. Similarly, $Z_P = Z \cap X_P\langle A\rangle$ and $Z_{RI} = Z \cap X_{RI}\langle A\rangle$ are expansions of X_P and X_{RI}, respectively. In fact, as ψ permutes the elements of X with type (A), ψ_P permutes the elements of X_P, so $X_P = Y_P = Z_P$. Therefore ψ_P is an automorphism of $V_P = X_P\langle A\rangle\langle\lambda\rangle$, which permutes the elements of X_P.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

For all $y \in Y_{RI}$ we have $y\psi = z \in Z$; moreover $z \in X_{RI}\langle A\rangle$ because V_{RI} is ψ-invariant, so $Y_{RI}\psi = Z_{RI}$. Now ψ_{RI} is an automorphism of V_{RI}, where V_{RI} is freely generated by X_{RI}, and Y_{RI} is the minimal expansion of X_{RI} associated to ψ_{RI} (as Y is the minimal expansion of X associated to ψ). Furthermore $Y_{RI}\psi_{RI} = Z_{RI}$ and if u is an element of $X_{RI}\langle A\rangle$ such that $u\psi \in X\langle A\rangle$ then $u\psi \in X\langle A\rangle \cap V_{RI} = X_{RI}\langle A\rangle$; so no element of $X_{RI}\langle A\rangle$ is in an incomplete finite X_{RI}-component of ψ_{RI}.

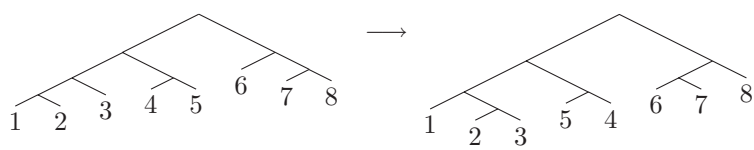
To summarize, let $|X_P| = a$, $|X_{RI}| = b$ and let $X_P = \{x_1, \ldots, x_a\}$ and $X_{RI} = \{x_{a+1}, \ldots, x_{a+b}\}$, where $x_i \in \mathbf{x}\langle A\rangle$. Then, regarding the x_i as new generators, we may view V_P as $V_{n,a}$, the free $\mathcal{V}_n$ algebra on $\{x_1, \ldots, x_a\}$, and V_{RI} as $V_{n,b}$, the free $\mathcal{V}_n$ algebra on $\{x_{a+1}, \ldots, x_{a+b}\}$. We regard ψ_P and ψ_{RI} as elements of $G_{n,a}$ and $G_{n,b}$, respectively. In this case, ψ_P (respectively, ψ_{RI}) is in quasi-normal form with respect to the A-basis X_P (respectively, ψ_{RI}). We write all elements of Y and Z in terms of the x_i, rather than as expansions of elements of $\mathbf{x}$.

Example 5.3. Let $n = 2$, $r = 1$ and $V_{2,1}$ be free on $\mathbf{x} = \{x\}$. Use bases Y and Z

$$Y = \{x\alpha_1^4, x\alpha_1^3\alpha_2, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2\alpha_1, x\alpha_1\alpha_2^2, x\alpha_2\alpha_1, x\alpha_2^2\alpha_1, x\alpha_2^3\},$$
$$Z = \{x\alpha_1^3, x\alpha_1^2\alpha_2\alpha_1, x\alpha_1^2\alpha_2^2, x\alpha_1\alpha_2\alpha_1, x\alpha_1\alpha_2^2, x\alpha_2\alpha_1^2, x\alpha_2\alpha_1\alpha_2, x\alpha_2^2\}$$

to define the element ψ of $G_{n,r}$ illustrated below.

ψ :



Then Y is the minimal expansion of $\mathbf{x}$ associated to ψ. The minimal expansion of $\mathbf{x}$ contained in $Y\langle A\rangle \cup Z\langle A\rangle$ is

$$X = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2\alpha_1, x\alpha_1\alpha_2^2, x\alpha_2\alpha_1, x\alpha_2^2\}.$$

Then $X\langle A\rangle \backslash (Y\langle A\rangle \cap Z\langle A\rangle) = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\}$. The X-components of these elements are

$$\cdots \mapsto x\alpha_1^4 \mapsto x\alpha_1^3, \qquad x\alpha_1^2\alpha_2 \mapsto x\alpha_1^2\alpha_2^2 \mapsto \cdots,$$
$$\cdots \mapsto x\alpha_2^3 \mapsto x\alpha_2^2, \qquad x\alpha_2\alpha_1 \mapsto x\alpha_2\alpha_1^2 \mapsto \cdots,$$

so ψ is in quasi-normal form with respect to X. Introduce new generators $x_1 = x\alpha_1^3$, $x_2 = x\alpha_1^2\alpha_2$, $x_3 = x\alpha_1\alpha_2\alpha_1$, $x_4 = x\alpha_1\alpha_2^2$, $x_5 = x\alpha_2\alpha_1$ and $x_6 = x\alpha_2^2$. Then $X_P = \{x_3, x_4\}$ and $X_{RI} = \{x_1, x_2, x_5, x_6\}$.

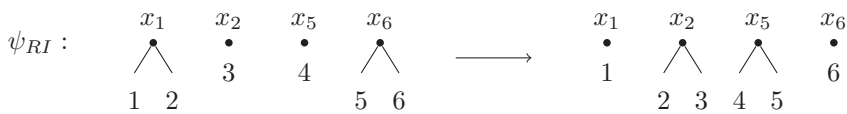
Let $V_{2,2}$ be free on $\{x_3, x_4\}$. Then, as an element of $G_{2,2}$ the map ψ_P is the map sending x_3 to x_4 and x_4 to x_3. Let $V_{2,4}$ be free on $\{x_1, x_2, x_5, x_6\}$. We have

$$\begin{aligned} Y_{RI} &= \{x\alpha_1^4, x\alpha_1^3\alpha_2, x\alpha_1^2\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\alpha_1, x\alpha_2^3\} \\ &= \{x_1\alpha_1, x_1\alpha_2, x_2, x_5, x_6\alpha_1, x_6\alpha_2\} \quad \text{and} \end{aligned}$$

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

$$\begin{aligned} Z_{RI} &= \{x\alpha_1^3, x\alpha_1^2\alpha_2\alpha_1, x\alpha_1^2\alpha_2^2, x\alpha_2\alpha_1^2, x\alpha_2\alpha_1\alpha_2, x\alpha_2^2\} \\ &= \{x_1, x_2\alpha_1, x_2\alpha_2, x_5\alpha_1, x_5\alpha_2, x_6\}, \end{aligned}$$

so as an element of $G_{2,4}$ the map ψ_{RI} is given by the following forest diagram.



Definition 5.4. Let ψ be an element of $G_{n,r}$. Then ψ is called *periodic* if $V_{RI} = \emptyset$ and ψ is called *regular infinite* if $V_P = \emptyset$.

Lemma 5.5. *Let ψ be an element of $G_{n,r}$ in semi-normal form with respect to an A-basis X.*

(1) *ψ is periodic if and only if ψ permutes the elements of X.*
(2) *ψ is regular infinite if and only if no element of X is of type* (A).

Proof. (1) If ψ permutes the elements of X then X contains no element of type (B) or (C); so $X = X_P$ and $V_{n,r} = V_P$, by Theorem 5.1. As $V_{n,r}$ is the free product of V_P and V_{RI} it follows that $V_{RI} = \emptyset$, so ψ is periodic.

If ψ is periodic then $X_{RI} \subseteq V_{RI} = \emptyset$, so $X = X_P$. Thus X consists of elements of type (A), which are permuted by ψ, by Lemma 4.18.

(2) If ψ is regular infinite then $V_P = \emptyset$, so $X_p = \emptyset$; i.e. no element of X is of type (A). If X contains no element of type (A) then $X_P = \emptyset$, and therefore $V_P = \emptyset$ by Theorem 5.1, so ψ is regular infinite. □

It follows that, in the notation established above Example 5.3, the automorphism $\psi_P \in G_{n,a}$ is periodic and $\psi_{RI} \in G_{n,b}$ is regular infinite. Thus, the decomposition of Theorem 5.1 may be viewed as factoring ψ into a product of a periodic and a regular infinite automorphism. It remains to see how to regard a pair of automorphisms in this way, simultaneously in the same algebra.

To this end suppose that $\psi_i \in G_{n,a_i}$ is in semi-normal form with respect to an A-basis X_i, where $|X_i| = a_i$, for $i = 1, 2$. If there exists an isomorphism $\rho : V_{n,a_1} \to V_{n,a_2}$ with the property that $\rho^{-1}\psi_1\rho = \psi_2$ then, from Corollary 3.14, $a_1 \equiv a_2 \bmod n-1$. Also, if $a_1 \equiv a_2 \bmod n-1$ then V_{n,a_i} is isomorphic to $V_{n,s}$ where $1 \le s \le n-1$ and $s \equiv a_i$. If this is the case then we may take an A-basis $\mathbf{x}_s$ of s elements of $V_{n,s}$ and choose expansions X_1' and X_2' of $\mathbf{x}_s$ of a_1 and a_2 elements, respectively. Now let f_i be the map taking X_i to X_i'. Then there exists an isomorphism $\rho : V_{n,a_1} \to V_{n,a_2}$ such that $\rho^{-1}\psi_1\rho = \psi_2$ if and only if $a_1 \equiv a_2 \bmod n-1$ and, setting $\widehat{\psi}_i = f_i^{-1}\psi_i f_i \in G_{n,s}$, we have $\rho^{-1}f_1\widehat{\psi}_1 f_1^{-1}\rho = f_2\widehat{\psi}_2 f_2^{-1}$: that is $\theta^{-1}\widehat{\psi}_1\theta = \widehat{\psi}_2$, where $\theta = f_1^{-1}\rho f_2 \in G_{n,s}$ (see Fig. 2).

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

$$\begin{tikzcd}
V_{n,a_1} \arrow[rrr, "\psi_1"] \arrow[dr, "f_1"] \arrow[ddd, "\rho"'] & & & V_{n,a_1} \arrow[dl, "f_1"'] \arrow[ddd, "\rho"] \\
& V_{n,s} \arrow[r, "\widehat{\psi}_1"] \arrow[d, "\theta"] & V_{n,s} \arrow[d, "\theta"] & \\
& V_{n,s} \arrow[r, "\widehat{\psi}_2"] & V_{n,s} & \\
V_{n,a_2} \arrow[rrr, "\psi_2"] \arrow[ur, "f_2"] & & & V_{n,a_2} \arrow[ul, "f_2"']
\end{tikzcd}$$

Fig. 2. Isomorphisms of V_{n,a_i} and $V_{n,s}$.

Combining this with Theorem 5.1(1) gives a decomposition of the conjugacy problem into the conjugacy problem for periodic and for regular infinite elements, separately. Let ψ and φ be elements of $G_{n,r}$, write $V_{n,a_1} = V_{RI,\psi}$, $\psi_1 = \psi_{RI}$, $V_{n,a_2} = V_{RI,\varphi}$ and $\psi_2 = \varphi_{RI}$. Using the procedure above, if ρ_{RI} exists (in the notation of Theorem 5.1) then we may regard ψ_i, $i = 1, 2$, as a regular infinite element of $G_{n,s}$, namely $\widehat{\psi}_i$, for appropriate s. Similarly, we may regard ψ_P and φ_P as periodic automorphisms of a single algebra.

We can now outline the algorithm for the conjugacy problem.

5.2. *The conjugacy algorithm*

Algorithm 5.6. Let ψ and φ be an elements of $G_{n,r}$.

Step 1: Find A-bases X_ψ and X_φ such that ψ and φ are in quasi-normal form with respect to X_ψ and X_φ, respectively, as in Lemma 4.28. The sets $X_{P,\psi}$, $X_{RI,\psi}$, $X_{P,\varphi}$ and $X_{RI,\varphi}$ are obtained as part of this process.

If $|X_{P,\psi}| \equiv |X_{P,\varphi}| \bmod n-1$ and $|X_{RI,\psi}| \equiv |X_{RI,\varphi}| \bmod n-1$; continue. Otherwise output "No" and stop.

Step 2: Find the minimal expansion Y_ψ of X_ψ associated to ψ and the minimal expansion Y_φ of X_φ associated to φ. (See Lemma 4.3.) Construct $Y_{RI,\psi}$ and $Y_{RI,\varphi}$; the sets elements of Y_ψ and Y_φ which are not in finite orbits (as in the discussion following Theorem 5.1). Construct $Z_{RI,\psi} = Y_{RI,\psi}\psi$ and $Z_{RI,\varphi} = Y_{RI,\varphi}\varphi$.

Step 3: For $T = P$ and for $T = RI$ carry out the following. Find the integer s_T such that $1 \le s_T \le n-1$ and $s_T \equiv |X_{T,\psi}|$. Let $\mathbf{x}_T$ be a set of s_T elements, let V_{n,s_T} be free on $\mathbf{x}_T$ and find expansions $W_{T,\psi}$ and $W_{T\varphi}$ of $\mathbf{x}_T$ of sizes $|X_{T,\psi}|$ and $|X_{T,\varphi}|$, respectively. Construct a map $f_{T,\psi}$ mapping $X_{T,\psi}$ bijectively to $W_{T,\psi}$ and $f_{T,\varphi}$ mapping $X_{T,\varphi}$ bijectively to $W_{T,\varphi}$. Write ψ_T and φ_T as elements of G_{n,s_T}, using these maps.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Step 4: Input ψ_P and φ_P into Algorithm 5.13 below for conjugacy of periodic elements of $G_{n,r}$. If ψ_P and φ_P are not conjugate, return "No" and stop. Otherwise obtain a conjugating element ρ_P.

Step 5: Input ψ_{RI} and φ_{RI} into Algorithm 5.27 below for conjugacy of regular infinite elements of $G_{n,s_{RI}}$. If ψ_{RI} and φ_{RI} are not conjugate, return "No" and stop. Otherwise obtain a conjugating element ρ_{RI}.

Step 6: Return the conjugating element $\rho_P * \rho_{RI}$.

Given this algorithm we have the following theorem.

Theorem 5.7 ([17, Theorem 9.3]). *The conjugacy problem is soluble in $G_{n,r}$.*

Proof. Apply Algorithm 5.6. □

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

5.3. *Conjugacy of periodic elements*

Let $\psi \in G_{n,r}$ be a periodic element. For $u \in V_{n,r}$ the *size* of the ψ-orbit of u is the least positive integer d such that $u\psi^d = u$.

Definition 5.8. Let ψ be a periodic element of $G_{n,r}$ in semi-normal form with respect to the A-basis X. The *cycle type* of ψ is the set

$$T_\psi(X) = \{d \in \mathbb{N} \,|\, \text{some } x \in \text{ has a } \psi\text{-orbit of size } d\}.$$

For $d \in \mathbb{N}$, define the *ψ-multiplicity* of d to be $m_\psi(d, X) = D/d$, where D is the number of elements of X which belong to a ψ-orbit of size d.

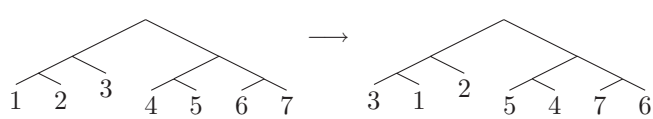
Note that, as ψ is periodic and in semi-normal form with respect to X, all X-components of ψ are (ordered) ψ-orbits and all ψ-orbits of elements of $X\langle A\rangle$ are X-components (once ordered appropriately). Also, $d \in T_\psi(X)$ if and only if $m_\psi(d, X) \neq 0$; the size of the set X is $|X| = \sum_{d \in T_\psi(X)} d m_\psi(d, X)$; if $d \in T_\psi(X)$ then X contains $m_\psi(d, X)$ disjoint ψ-orbits of size d; and ψ is a torsion element of order equal to the least common multiple of elements of $T_\psi(X)$.

Example 5.9. Let $n = 2$, $r = 1$ and $V_{2,1}$ be free on $\mathbf{x} = \{x\}$. Let

$$X = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2, x\alpha_2\alpha_1^2, x\alpha_2\alpha_1\alpha_2, x\alpha_2^2\alpha_1, x\alpha_2^3\}$$

and let ψ be the periodic element of $G_{2,1}$ defined by the tree pair diagram below.

ψ :



Then the cycle type of ψ is $\{2, 3\}$ with multiplicites $m_\psi(2, X) = 2$ and $m_\psi(3, X) = 1$.

Lemma 5.10. *Let ψ be a periodic element of $G_{n,r}$ in semi-normal form with respect to the A-basis X and the A-basis Z, where Z is a q-fold expansion of X. Then $T_\psi(X) = T_\psi(Z)$ and $m_\psi(d, X) \equiv m_\psi(d, Z) \bmod n - 1$, for all $d \in T_\psi(X)$.*

Proof. It suffices to prove the lemma in the case where Z is a *simple* expansion of X, because any expansion is obtained by a finite sequence of simple expansions. Suppose the expansion happens at $w \in X$, so that $Z = (X \backslash \{w\}) \cup \{w\alpha_1, \ldots, w\alpha_n\}$. To compute $T_\psi(Z)$ we need to break Z into a union of ψ-orbits.

Let d be the size of the ψ-orbit of w, so that $\mathcal{O}_w = \{w, w\psi, \ldots, w\psi^{d-1}\}$. For each $1 \leq i \leq n$ the orbit of $w\alpha_i$ is $\mathcal{O}_{w\alpha_i} = \{w\alpha_i, w\psi\alpha_i, \ldots, w\psi^{d-1}\alpha_i\}$, which is of size at most d. In fact its size is exactly d: if there are integers $0 \leq j < k < d$ for which $w\psi^j\alpha_i = w\psi^k\alpha_i$, we would have $w\psi^j = w\psi^k$, which cannot occur.

Thus, in moving from X to Z we have lost 1 and gained n ψ-orbits of size d; all other ψ-orbits inside Z are ψ-orbits inside X. Therefore $T_\psi(X) = T_\psi(Z)$. In terms of multiplicities this means $m_\psi(d, Z) = m_\psi(d, X) + n - 1$ and $m_\psi(e, Z) = m_\psi(e, X)$, for every positive integer $e \neq d$; whence the result. □

Note that it follows from this lemma that if ψ is in semi-normal form with respect to both X and X' then $T_\psi(X) = T_\psi(X')$, since we may take a common expansion of both X and X' and then expand this to an A-basis Z with respect to which ψ is in semi-normal form. So from now on, we refer to the cycle type T_ψ without reference to an A-basis X.

Proposition 5.11. *Let ψ and φ be periodic elements of $G_{n,r}$ in semi-normal form with respect to the A-bases X_ψ and X_φ, respectively. Then ψ is conjugate to φ if and only if*

(1) $T_\psi = T_\varphi$ *and*
(2) $m_\psi(d, X_\psi) \equiv m_\varphi(d, X_\varphi) \bmod n - 1$, *for all* $d \in \mathbb{N}$.

Proof. Assume that ψ and φ are conjugate and let $\rho \in G_{n,r}$ be such that $\rho^{-1}\psi\rho = \varphi$. Let ρ be in semi-normal form with respect to X_ρ, let Y be the minimal expansion of X_ρ associated to ρ and let $Z = Y\rho$. Let W be a common expansion of X_ψ and Y and let ψ be in semi-normal form with respect to an expansion X'_ψ of W. (Such an expansion of W exists, by Lemma 4.9.) As ψ is periodic and in semi-normal form it permutes the elements of X'_ψ, so for all $x \in X'_\psi$ we have $x' \in X'_\psi$ such that $x\rho\varphi = x\psi\rho = x'\rho \in X\rho$. Therefore φ permutes the elements of $X'_\psi\rho$, so φ is in semi-normal form with respect to $X'_\varphi = X'_\psi\rho$. As X'_ψ is an expansion of Y and $Z = Y\rho$ it follows that X'_φ is an expansion of Z.

Now if $x \in X'_\psi$ and $i \in \mathbb{Z}$ then $x\rho\varphi^i = x\psi^i\rho$, so we have $x\psi^d = x$ if and only if $x\rho\varphi^d = x\rho$; in other words, x and $x\rho$ have orbits of equal size. This applies to any x, so $T_\psi = T_\varphi$ and both X'_ψ and X'_φ have the same number of elements with an orbit of size d. Therefore $m_\psi(d, X'_\psi) = m_\varphi(d, X'_\varphi)$, for all $d \in T_\psi = T_\varphi$. Statement (2) follows, from Lemma 5.10 and the fact that X'_ψ and X'_φ are expansions of X_ψ and X_φ, respectively.

Conversely, suppose that statements (1) and (2) hold. Let $T_\psi = T_\varphi = \{d_1, \ldots, d_k\}$ and write $m_j = m_\psi(d_j, X_\psi)$ and $m'_j = m_\varphi(d_j, X_\varphi)$. Fix $j \in \{1, \ldots, k\}$. Assume first that $m_j > m'_j$. Then, by hypothesis, $m_j = m'_j + q_j(n-1)$ for some

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

positive integer q_j. Select an element $x \in X_\varphi$ whose φ-orbit $\mathcal{O}_x$ has size d_j. Let Y_x be a q_j-fold expansion of $\{x\}$ and set $E = \{\Gamma \in A^* \mid x\Gamma \in Y_x\}$, so that $Y_x = xE$. Then for each $0 \le i < d_j$, $x\varphi^i E$ is a q_j-fold expansion of $\{x\varphi^i\}$.

For every string $\Gamma \in E$, the set $\{x\Gamma, x\varphi\Gamma, \ldots, x\varphi^{d-1}\Gamma\}$ is a φ-orbit of size d. (We saw this in Lemma 5.10 for $\Gamma = \alpha_i$.) Hence the set $\mathcal{O}_x E = \{x\varphi^i\Gamma \mid \Gamma \in E, 0 \le i < d_j\}$ is a $q_j d_j$-fold expansion of $\mathcal{O}_x$; more precisely it is a disjoint union of $|E| = q_j(n-1)$ φ-orbits of size d_j. After $\mathcal{O}_x$ is expanded to $\mathcal{O}_x E$, the resulting expansion X_φ has exactly $m'_j + q_j(n-1) = m'_j$ size d_j φ-orbits.

For each j such that $m_j > m'_j$ apply this process to a single element of X_φ with φ-orbit size d_j. Dually, for each j such that $m'_j > m_j$ apply the process to an element of X_ψ with ψ-orbit size d_j, interchanging the roles of φ and ψ. The result is an expansion X'_ψ of X_ψ and an expansion X'_φ of X_φ such that $m_\varphi(d, X'_\varphi) = m_\psi(d, X'_\psi)$ for every positive integer d.

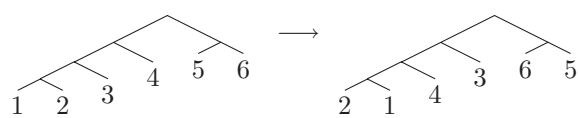
Now define $\rho : X'_\psi \to X'_\varphi$ by mapping orbits of size d to each other, preserving the order within each orbit. In detail, for each d set $m = m_\psi(d, X_\psi) = m_\varphi(d, X_\varphi)$. Let $\mathcal{O}_1, \ldots, \mathcal{O}_m$ be the size d ψ-orbits (in any order) in X'_ψ and let $\mathcal{O}'_1, \ldots, \mathcal{O}'_m$ be the size d φ-orbits in X'_φ (also in any order). Select a representative $o_i \in \mathcal{O}_i$ and $o'_i \in \mathcal{O}'_i$ for each of these $2m$ orbits. We define ρ by the rule $o_i\psi^j\rho = o'_i\varphi^j$. By construction we have $x\psi\rho = x\rho\varphi$, for all $x \in X'_\psi$. Hence $\rho^{-1}\psi\rho = \varphi$. □

Example 5.12. Let $n = 2$, $r = 1$ and $V_{2,1}$ be free on $\mathbf{x} = \{x\}$. Let

$$X = \{x\alpha_1^4, x\alpha_1^3\alpha_2, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\}$$

and let ψ be the periodic element of $G_{2,1}$ given by the tree pair diagram below.

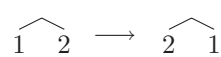
ψ :



Then ψ has cycle type $T_\psi = \{2\}$ and multiplicity $m_\psi(2, X) = 3$. The ψ-orbits of elements of X are $\mathcal{O}_1 = \{x\alpha_1^4, x\alpha_1^3\alpha_2\}$, $\mathcal{O}_2 = \{x\alpha_1^2\alpha_2, x\alpha_1\alpha_2\}$ and $\mathcal{O}_3 = \{x\alpha_2\alpha_1, x\alpha_2^2\}$.

Let $Y = \{x\alpha_1, x\alpha_2\}$ and let φ be the periodic element of $G_{2,1}$ which swaps the elements of Y.

φ :



Then φ has cycle type $T_\varphi = \{2\}$ and $m_\varphi(2, Y) = 1$. From Proposition 5.11, ψ is conjugate to φ. We can construct a conjugator by applying the process of the proof. We take the same 2-fold expansion of both $x\alpha_1$ and $x\alpha_2$ to give a 4-fold expansion

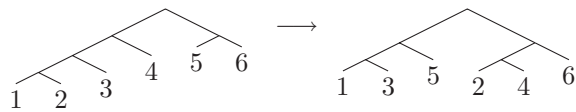
$$Y' = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2, x\alpha_2\alpha_1^2, x\alpha_2\alpha_1\alpha_2, x\alpha_2^2\}$$

of Y such that φ is in semi-normal form with respect to Y'. The φ-orbits of elements of Y' are $\mathcal{O}'_1 = \{x\alpha_1^3, x\alpha_2\alpha_1^2\}$, $\mathcal{O}'_2 = \{x\alpha_1^2\alpha_2, x\alpha_2\alpha_1\alpha_2\}$ and $\mathcal{O}'_3 = \{x\alpha_1\alpha_2, x\alpha_2^2\}$, so $m_\varphi(2, Y') = 3$. Take the representative of each orbit to be the first element listed in its description. The corresponding conjugator ρ is the element of $G_{2,1}$ which sends

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

$\mathcal{O}_i$ to $\mathcal{O}'_i$ via $x\alpha_1^4\rho = x\alpha_1^3$, $x\alpha_1^3\alpha_2\rho = x\alpha_2\alpha_1^2$, $x\alpha_1^2\alpha_2\rho = x\alpha_1^2\alpha_2$, $x\alpha_1\alpha_2\rho = x\alpha_2\alpha_1\alpha_2$, $x\alpha_2\alpha_1\rho = x\alpha_1\alpha_2$ and $x\alpha_2^2\rho = x\alpha_2^2$.

ρ :



Then $\rho^{-1}\psi\rho = \varphi$.

From the proof of Theorem 5.11 we extract the following algorithm for the conjugacy of periodic elements of $G_{n,r}$.

Algorithm 5.13. Let ψ and φ be periodic elements of $G_{n,r}$.

Step 1: Construct A-bases X_ψ and X_φ with respect to which ψ and φ are in semi-normal form (Lemma 4.9).
Step 2: Compute the cycle types T_ψ and T_φ. If $T_\psi \neq T_\varphi$, output "No" and stop.
Step 3: Compute $m_\psi(d, X_\psi)$ and $m_\varphi(d, X_\varphi)$, for all $d \in T_\psi$. If $m_\psi(d, X_\psi) \not\equiv m_\varphi(d, X_\varphi) \bmod n-1$, output "No" and stop.
Step 4: Construct A-bases X'_ψ and X'_φ as described in the proof of Theorem 5.11.
Step 5: Choose a map ρ sending ψ-orbits of elements of X'_ψ to φ-orbits of elements of X'_φ, as in the proof of the theorem, and output ρ.

5.4. *Conjugacy of regular infinite elements*

We begin with a necessary condition for two regular infinite elements to be conjugate. Let ψ be a regular infinite element of $G_{n,r}$ in semi-normal form with respect to X. By Lemma 4.6, ψ has finitely many semi-infinite X-components, each of which has a characteristic element u with some characteristic (m, Γ) (see Definition 4.22). If ψ is also in semi-normal form with respect to Y, the ψ-orbit of u has precisely one Y-component, which is again semi-infinite of characteristic (m, Γ). Therefore, the set of pairs (m, Γ) which are characteristics of semi-infinite X-components is independent of the choice of a basis for a semi-normal form. With this in mind, we make the following definition.

Definition 5.14. Let ψ be a regular infinite element of $G_{n,r}$ in semi-normal form with respect to X. Define

$$\mathcal{M}_\psi = \{(m, \Gamma) \mid (m, \Gamma) \text{ is the characteristic of a semi-infinite } X\text{-component of } \psi\}.$$

Example 5.15. We refer to the following example through the remainder of this section. Let $n = 2$, $r = 1$, $\mathbf{x} = \{x\}$ and $\varphi \in G_{2,1}$ be determined by the bijection from A-basis

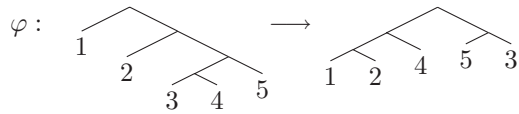
$$Y = \{x\alpha_1, x\alpha_2\alpha_1, x\alpha_2^2\alpha_1^2, x\alpha_2^2\alpha_1\alpha_2, x\alpha_2^3\}$$

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

to the A-basis

$$Z = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\}$$

as illustrated below.



Then Y is the minimal expansion of $\mathbf{x}$ associated to φ and $Z = Y\varphi$. The elements of $\mathbf{x}\langle A\rangle\backslash(Y\langle A\rangle \cup Z\langle A\rangle)$ are x and $x\alpha_2$, so we start the search for a quasi-normal form by taking the unique minimal expansion $X = \{x\alpha_1, x\alpha_2\alpha_1, x\alpha_2^2\}$ of $\mathbf{x}$ not containing either of these elements.

The X-component of $x\alpha_1$ is

$$x\alpha_1 \mapsto x\alpha_1^3 \mapsto x\alpha_1^5 \mapsto \cdots,$$

which is right semi-infinite of characteristic $(1, \alpha_1^2)$. Next, $x\alpha_2\alpha_1$ belongs to a complete infinite X-component:

$$\cdots x\alpha_2^5 \mapsto x\alpha_2^4 \mapsto x\alpha_2^3 \mapsto x\alpha_2\alpha_1 \mapsto x\alpha_1^2\alpha_2 \mapsto x\alpha_1^4\alpha_2 \mapsto x\alpha_1^6\alpha_2 \mapsto \cdots.$$

Finally, the X-component of $x\alpha_2^2$ is

$$\cdots \mapsto x\alpha_2^2\alpha_1^4 \mapsto x\alpha_2^2\alpha_1^2 \mapsto x\alpha_2^2,$$

which is left semi-infinite of characteristic $(-1, \alpha_1^2)$. Thus φ is in quasi-normal form with respect to X.

To determine $\mathcal{M}_\varphi$, we compute the sets $X\langle A\rangle\backslash Y\langle A\rangle = \{x\alpha_2^2, x\alpha_2^2\alpha_1\}$ and $X\langle A\rangle\backslash Z\langle A\rangle = \{x\alpha_1, x\alpha_1^2\}$. The X-components we have yet to calculate are those of $x\alpha_2^2\alpha_1$ and $x\alpha_1^2$; these are the sets $\{x\alpha_2^2\alpha_1^{2i-1} \mid i \geq 1\}$ and $\{x\alpha_1^{2i} \mid i \geq 1\}$ with characteristics $(1, \alpha_1^2)$ and $(-1, \alpha_1^2)$, respectively. Hence

$$\mathcal{M}_\varphi = \{(1, \alpha_1^2), (-1, \alpha_1^2)\}.$$

Lemma 5.16. *Let ψ and φ be regular infinite elements of $G_{n,r}$ in semi-normal form with respect to A-bases X and Y, respectively. Suppose that the elements are conjugate via $\rho \in G_{n,r}$ with $\rho^{-1}\psi\rho = \varphi$. Then the sets $\mathcal{M}_\psi$ and $\mathcal{M}_\varphi$ coincide. Moreover, ρ maps a semi-infinite X-component of ψ into a φ-orbit which contains a (unique) semi-infinite Y-component with the same characteristic.*

Proof. If u is an element of $X\langle A\rangle$ such that $u\psi^m = u\Gamma$, for some m and Γ, then

$$u\rho\varphi^m = u\psi^m\rho = u\Gamma\rho = u\rho\Gamma.$$

The same argument can be applied starting with an element $v \in Y\langle A\rangle$ and interchanging ψ and φ. Hence if u belongs to a ψ-orbit of characteristic (m, Γ) then $u\rho$ belongs to an φ-orbit of characteristic (m, Γ). Thus, from Lemma 4.24, a ψ-orbit that contains a semi-infinite X-component of characteristic (m, Γ) is

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

mapped by ρ to a φ-orbit which has a semi-infinite Y-component of the same characteristic. □

Definition 5.17. Let ψ be in semi-normal form with respect to X. The equivalence relation $\equiv$ on X, is that generated by the relation $x \equiv x'$, whenever $x\Gamma$ and $x'\Delta$ are in the same ψ-orbit, for some $\Gamma, \Delta \in A^*$.

Example 5.18. Let φ be as in Example 5.15. Then $x\alpha_2\alpha_1\varphi = (x\alpha_1)\alpha_1\alpha_2$, so $x\alpha_2\alpha_1 \equiv x\alpha_1$. Also, $x\alpha_2\alpha_1\varphi^{-1} = (x\alpha_2^2)\alpha_2$, so $x\alpha_2\alpha_1 \equiv x\alpha_2^2$. Therefore all elements of X are related by $\equiv$.

Proposition 5.19. *Let ψ be a regular infinite element in semi-normal form with respect to X. Let $X = \coprod_{i=1}^m \mathcal{X}_i$, where the $\mathcal{X}_i$ are the equivalence classes of $\equiv$ defined on X under the action of ψ. Then $V_{n,r}$ is the free product of the ψ-invariant Ω-subalgebras $V_1, \ldots, V_m$, where V_i is the Ω-subalgebra generated by $\mathcal{X}_i$.*

Proof. As ψ is regular infinite, the sets $\mathcal{X}_i$ partition X, so $V_{n,r}$ is the free product of the V_i's. To show that V_i is ψ-invariant it suffices to show that if $x \in \mathcal{X}_i$ then $x\psi$ and $x\psi^{-1}$ are in V_i. To this end, choose $d \geq 0$ such that $x\psi\Gamma$ and $x\psi^{-1}\Gamma$ belong to $X\langle A\rangle$, for all $\Gamma \in A^*$ of length d. Then for all such Γ we have $x\psi\Gamma = y\Delta$ and $x\psi^{-1}\Gamma = z\Lambda$, for some $y, z \in X$ and $\Delta, \Lambda \in A^*$. By definition then $y \equiv x \equiv z$, so $x, y, z \in \mathcal{X}_i$. This implies that $x\psi\Gamma = y\Delta \in V_i$ and $x\psi^{-1}\Gamma = z\Lambda \in V_i$. This holds for all Γ of length d, so from Lemma 3.20, $x\psi$ and $x\psi^{-1}$ belong to V_i, as required. Hence V_i is ψ-invariant. □

Lemma 5.20. *Let ψ be a regular infinite element in semi-normal form with respect to X and let $\mathcal{X}_i, i = 1, \ldots, m$, be the equivalence classes of $\equiv$ defined on X under the action of ψ. We may effectively construct the $\mathcal{X}_i$.*

Proof. From Lemmas 4.28 and 4.3, we may effectively construct X, the minimal expansion Y of ψ with respect to X, and the basis $Z = Y\psi$. For each $v \in X \cup Y \cup Z$ we may enumerate a finite subsequence C_v of the X-component of v using the procedure of Lemma 4.28. Let $\equiv_0$ be the equivalence relation on X generated by $y \equiv_0 z$ if $y\Gamma$ and $z\Delta$ belong to C_v, for some $v \in X \cup Y \cup Z$ and $\Gamma, \Delta \in A^*$. We claim that $\equiv_0 = \equiv$.

By definition, $\equiv_0 \subseteq \equiv$. To prove the opposite inclusion, we suppose that there exist $p \in \mathbb{Z}$, $x, y \in X$ and $\Delta, \Phi \in A^*$ such that $x\Phi = y\Delta\psi^p$ and x and y are not related under the relation $\equiv_0$. In this case we may assume, interchanging x and y if necessary, that $p > 0$. Let p be a minimal positive integer for which such x, y exist. As $y\Delta\psi^p = x\Phi$ it follows that $y\Delta\psi^{p'} \in X\langle A\rangle$, for $p' = 1, \ldots, p-1$. Let $y\Delta\psi = y'\Delta'$, so $y'\Delta'\psi^{p-1} = x\Phi$. By minimality of p we have $y' \equiv_0 x$.

Let Δ_0 be an initial subword of Δ of maximal length such that $y\Delta_0\psi \in X\langle A\rangle$, say $\Delta = \Delta_0\Delta_1$. Then $y\Delta_0 \in Y$ and $y\Delta_0\psi = y''\Delta_0''$, for some $y'' \in X$ and $\Delta_0'' \in A^*$. Now $y'\Delta' = y\Delta_0\Delta_1\psi = y''\Delta_0''\Delta_1$, so $y'' = y'$ and $\Delta' = \Delta_0''\Delta_1$. Thus $y\Delta_0\psi = y'\Delta_0''$

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

and, as $y\Delta_0 \in Y$, $y'\Delta_0'' \in Z$ we have $y \equiv_0 y'$. Therefore $y \equiv_0 x$, a contradiction. We conclude that no such p, x and y exist and so $\equiv \subseteq \equiv_0$, as required. Thus $\equiv_0 = \equiv$, and as we may effectively compute the sets C_v, it follows that we may compute the equivalence classes $\mathcal{X}_i$. □

Lemma 5.21. *Let ψ be a regular infinite element in semi-normal form with respect to X and let $\mathcal{X}_i, i = 1, \ldots, m$ be the equivalence classes of $\equiv$ defined on X under the action of ψ. Define*

$$x\theta_i = \begin{cases} x\psi & \text{if } x \in \mathcal{X}_i, \\ x & \text{if } x \in \mathcal{X}_j \text{ for } i \neq j, \end{cases}$$

for $i = 1, \ldots, m$. Then θ_i extends to an element of $G_{n,r}$ which commutes with ψ and with θ_j, for all $j = 1, \ldots, m$.

Proof. Let V_i be the Ω-subalgebra generated by $\mathcal{X}_i$, $i = 1, \ldots, m$. Since $V_{n,r} = V_1 * \cdots * V_m$ and the V_i are ψ invariant, we have $\psi = \psi_1 * \cdots * \psi_m$, where $\psi_i = \psi|_{V_i}$. Moreover ψ_i is an automorphism of V_i. By definition, $\psi_i|_{\mathcal{X}_i} = \psi|_{\mathcal{X}_i} = \theta_i|_{\mathcal{X}_i}$, so $\theta_i|_{\mathcal{X}_i}$ extends to the automorphism ψ_i of V_i. Thus (the extension to $V_{n,r}$ of) $\theta_i = 1_{V_1} * \cdots * \psi_i * \cdots * 1_{V_m}$ is an automorphism of $V_{n,r}$. For $i < j$ we have $\theta_i\theta_j = 1_{V_1} * \cdots * \psi_i * \cdots * \psi_j \cdots * 1_{V_m} = \theta_j\theta_i$, and it follows that θ_i commutes with ψ. □

Lemma 5.22. *Let ψ and φ be regular infinite elements of $G_{n,r}$, in semi-normal form with respect to the A-bases X and Y, respectively. Let $\mathcal{X}_1, \ldots, \mathcal{X}_m$ be the equivalence classes of $\equiv$ defined on X under the action of ψ. Choose a representative $x_i \in \mathcal{X}_i$ of type* (B) *for each i. If ψ and φ are conjugate, there exists a conjugator ρ such that $x_i\rho$ is a terminal or initial element in a semi-infinite Y-component of φ.*

Proof. Let $\rho' \in G_{n,r}$ be a conjugator with $\rho'^{-1}\psi\rho' = \varphi$. We will explain how to modify ρ' to form another conjugator ρ satisfying the requirements of the lemma. Lemma 5.16 asserts that $x_i\rho'$ belongs to a φ-orbit containing a semi-infinite Y-component, which has the same characteristic as x_i. Let $y_i \in Y\langle A\rangle$ be the initial or terminal element of this Y-component. Then there exists j_i such that $x_i\rho' = y_i\varphi^{j_i}$, meaning that

$$y_i = y_i\varphi^{j_i}\varphi^{-j_i} = x_i\rho'\varphi^{-j_i} = x_i\psi^{-j_i}\rho'.$$

For each equivalence class $\mathcal{X}_i$, define θ_i as in Lemma 5.21 and $\rho \in G_{n,r}$ by

$$\rho = \left(\prod_{i=1}^{n} \theta_i^{-j_i}\right)\rho'.$$

Then $\theta = \prod_{i=1}^{n} \theta_i^{-j_i}$ commutes with ψ, so $\rho^{-1}\psi\rho = \rho'^{-1}\theta^{-1}\psi\theta\rho' = \rho'^{-1}\psi\rho' = \varphi$; furthermore for each chosen $x_i \in \mathcal{X}_i$ we have

$$x_i\rho = x_i\left(\prod_{i=1}^{n} \theta_i^{-j_i}\right)\rho' = x_i\theta_i^{-j_i}\rho' = x_i\psi^{-j_i}\rho' = y_i.$$

Thus ρ is the required conjugator. □

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Definition 5.23. Let ψ and φ be regular infinite elements in semi-normal form with respect to X and Y and let $\mathcal{X}_1, \ldots, \mathcal{X}_m$, be the equivalence classes of $\equiv$ defined on X under the action of ψ. We define $\mathcal{R}_i(\psi, \varphi)$ to be the set of pairs (x, y), where $x \in \mathcal{X}_i$ is of type (B) and y is an initial or terminal element of a semi-infinite Y-component of φ with the same characteristic as x.

Given a choice of elements $(x_i, y_i) \in \mathcal{R}_i(\psi, \varphi)$ for each $1 \leq i \leq m$, let ρ_0 be the map from $\{x_1, \ldots, x_m\}$ to $\{y_1, \ldots, y_m\}$ given by $x_i\rho_0 = y_i$ for each i. We define $\mathcal{R}(\psi, \varphi)$ to be the set of all such maps ρ_0 constructed in this way.

The set $\mathcal{R}_i(\psi, \varphi)$ is finite since the number of elements of type (B) in X and the number of semi-infinite Y-components of φ is finite, so $\mathcal{R}(\psi, \varphi)$ is also finite.

Lemma 5.24. *Given $\rho_0 \in R(\psi, \varphi)$, there are finitely many ways of extending ρ_0 to an element ρ of $G_{n,r}$ such that $\varphi = \rho^{-1}\psi\rho$. Moreover the existence of such an extension ρ can be effectively determined, and if such ρ exists then the images $y\rho$ can be effectively determined, for all $y \in X$.*

Proof. Throughout the proof, when we say ρ exists we mean that an extension ρ of ρ_0 to an element of $G_{n,r}$ exists and satisfies $\varphi = \rho^{-1}\psi\rho$. From Lemma 5.20, we may effectively construct the equivalence classes $\mathcal{X}_i$, and so also the sets $R_i(\psi, \varphi)$. First consider a single equivalence class $\mathcal{X}_i$. We are given a representative element $x_i \in \mathcal{X}_i$ of type (B) and an element y_i such that $x_i\rho_0 = y_i$, where y_i is an initial or terminal element of a semi-infinite Y-component of φ with the same characteristic as x_i.

Let $x \in X$ of type (B). Then, by definition of $\equiv$, we have $x \in \mathcal{X}_i$ if and only if there exist elements $x_i = u_0, \ldots, u_t = x$ of X, elements $\Gamma_j, \Delta_j \in A^*$ and $k_j \in \mathbb{Z}$ with $u_{j+1}\Delta_{j+1} = u_j\Gamma_j\psi^{k_j}$, for $j = 0, \ldots, t-1$. Before going any further, we show that we may assume that u_j is of type (B), for all j. Suppose not, say u_j is of type (C). Then, by Lemma 4.18, there exist $k'_j \in \mathbb{Z}$, $\Gamma'_j \in A^*$ and $u'_j \in X$ of type (B) such that $u_j\psi^{k'_j} = u'_j\Gamma'_j$. Now

$$u_{j-1}\Gamma_{j-1}\psi^{k_{j-1}+k'_j} = u_j\Delta_j\psi^{k'_j} = u'_j\Gamma'_j\Delta_j$$

and

$$u'_j\Gamma'_j\Gamma_j\psi^{k_j-k'_j} = u'_j\Gamma'_j\psi^{-k'_j}\Gamma_j\psi^{k_j} = u_j\Gamma_j\psi^{k_j} = u_{j+1}\Delta_{j+1},$$

so we may replace u_j by u'_j. Continuing this way, eventually all u_j will be of type (B).

We show, by induction on t, that there are finitely many possible values of $x\rho$, for a conjugator $\rho \in G_{n,r}$ such that $x\varphi = x\rho^{-1}\psi\rho$ which extends ρ_0. (That is, where $x_i\rho = x_i\rho_0 = y_i$.) We also describe an effective procedure to enumerate the set of all such elements. Suppose first that $t = 1$, so $x = u_1$ and we have $\Gamma = \Gamma_0$, $\Delta = \Delta_1$ and $k = k_0$ such that $x_i\Gamma\psi^k = x\Delta$. Given that ρ exists, from Lemma 5.16, $x\rho$ belongs to a semi-infinite Y-component $\mathcal{C}$ of φ with the same characteristic as x. Therefore (if ρ exists) there exists an element $(x, w) \in R_i(\psi, \varphi)$ such that w is the

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

initial or terminal element of $\mathcal{C}$, as well as an integer l such that $w\varphi^l = x\rho$. This implies that

$$w\Delta\varphi^l = (x\Delta)\rho = x_i\Gamma\psi^k\rho = x_i\Gamma\rho\varphi^k = x_i\rho_0\varphi^k\Gamma,$$

so

$$w\Delta\varphi^{l-k} = x_i\rho_0\Gamma = y_i\Gamma. \tag{5.1}$$

Lemma 4.34 gives an effective procedure to determine whether an integer l satisfying (5.1) exists, and if so find it. Given ρ_0 and x, the integer k and the elements Γ and Δ are uniquely determined so, to decide whether an appropriate value $x\rho$ exists, we may check each pair (x, w) in the set $R_i(\psi, \varphi)$ to see if (5.1) holds for some l or not. For each such w there is at most one l such that (5.1) has a solution and, as $R_i(\psi, \varphi)$ is finite, we may effectively enumerate the values $w\Delta\varphi^{l-k}$ that could be assigned to $x\rho$. Hence the result holds if $t = 1$.

Now assume that $t > 1$ and the result holds for all x related to x_i by a chain of length at most $t - 1$. Then u_{t-1} is of type (B) and by assumption $u_{t-1}\rho$ may be given one of finitely many values, and we have a procedure to enumerate these values. Suppose then that $u_{t-1}\rho = v$. Now $x = u_m$ and we have $\Gamma_{t-1}, \Delta_t \in A^*$ and $k_{t-1} \in \mathbb{Z}$ such that $u_{t-1}\Gamma_{t-1}\psi^{k_{t-1}} = x\Delta_t$. Applying the argument of the case $m = 1$ with u_{t-1}, Γ_{t-1}, Δ_t and v in place of x_i, Γ, Δ and y, we see that a finite set of possible values for $x\rho$ may be effectively determined. Therefore, by induction, the result holds for all $x \in \mathcal{X}_i$ of type (B).

Finally, if $x \in \mathcal{X}_i$ is of type (C), then by Lemma 4.18 there is a $z\Sigma$ in the X-component of x, for some z of type (B) and $\Sigma \in A^*$, i.e. $x\psi^p = z\Sigma$ for some integer p. Since we have already determined the possible images of all the type (B) elements in $\mathcal{X}_i$, if ρ exists we have, for each choice of $z\rho$,

$$x\rho = z\Sigma\psi^{-p}\rho = z\rho\Sigma\varphi^{-p}$$

and this determines the image of the type (C) element under ρ (uniquely once we have made our initial choice for the image of $z\rho$).

We carry out this process on each equivalence class in turn. If the process results in at least one possible value for each element of X, we obtain a potential extension ρ of ρ_0. For such a ρ to be a genuine extension, we need to check if ρ defines an automorphism of $V_{n,r}$. This is the case if and only if the image $X\rho$ of the A-basis X is itself a basis for $V_{n,r}$, which we can effectively determine using Lemma 3.16. (Note that $X\rho$ need not be an A-basis — see Example 5.26 below.) □

We are now able to state the main result of this section.

Proposition 5.25. *Let ψ and φ be regular infinite elements of $G_{n,r}$ in quasi-normal form with respect to X and Y, respectively. Then ψ is conjugate to φ if and only if there exists a map $\rho_0 \in \mathcal{R}(\psi, \varphi)$ which extends to an element ρ of $G_{n,r}$ with $\rho^{-1}\psi\rho = \varphi$.*

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Proof. If ρ_0 extends to an element $\rho \in G_{n,r}$ with $\rho^{-1}\psi\rho = \varphi$, then ψ is certainly conjugate to φ.

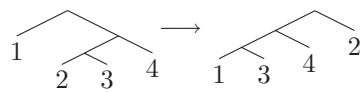
Assume that ψ is conjugate to φ. Lemma 5.22 tells us that there exists a conjugator ρ such that, for each equivalence class $\mathcal{X}_i$, there exists an element x_i of type (B) in $\mathcal{X}_i$ with $y_i = x_i\rho$ an initial or terminal element of a semi-infinite Y-component of φ. We define ρ_0 to be the map $x_1 \mapsto y_1, \ldots, x_m \mapsto y_m$, where $y_i = x_i\rho$ for each $i = 1, \ldots, m$. Thus, ρ_0 is an element of the finite set $\mathcal{R}(\psi;\varphi)$. Now ρ_0 is the restriction of ρ to $\{x_1, \ldots, x_m\}$, so it certainly extends to ρ, as required. □

Example 5.26. Let $n = 2$, $r = 1$ and $V_{2,1}$ be free on $\mathbf{x} = \{x\}$. Let

$$Y = \{x\alpha_1, x\alpha_2\alpha_1^2, x\alpha_2\alpha_1\alpha_2, x\alpha_2^2\} \quad \text{and} \quad Z = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2, x\alpha_2\}$$

determine the automorphism ψ as illustrated below.

ψ :



Then Y is the minimal expansion of $\mathbf{x}$ associated to ψ and $Z = Y\psi$. The only element of $\mathbf{x}\langle A\rangle$ not in $Y\langle A\rangle \cup Z\langle A\rangle$ is x, so we take $X = \{x\alpha_1, x\alpha_2\}$ to be our candidate basis for a quasi-normal form. Then $X\langle A\rangle \backslash Y\langle A\rangle = \{x\alpha_2, x\alpha_2\alpha_1\}$ and $X\langle A\rangle \backslash Z\langle A\rangle = \{x\alpha_1, x\alpha_1^2\}$. The X-components of the first two elements are

$$x\alpha_2 \in \{x\alpha_2\alpha_1^{2k}\}_{k\geq 0} \quad \text{and} \quad x\alpha_2\alpha_1 \in \{x\alpha_2\alpha_1^{2k+1}\}_{k\geq 0},$$

both left semi-infinite with characteristic $(-1, \alpha_1^2)$. The latter two elements' X-components are

$$x\alpha_1 \in \{x\alpha_1^{2k+1}\}_{k\geq 0} \quad \text{and} \quad x\alpha_1^2 \in \{x\alpha_1^{2k+2}\}_{k\geq 0},$$

both right semi-infinite with characteristic $(1, \alpha_1^2)$. Hence ψ is in quasi-normal form with respect to X, both elements of X are of type (B) and $\mathcal{M}_\psi = \{(1, \alpha_1^2), (-1, \alpha_1^2)\}$. As $(x\alpha_2)\alpha_2\psi = (x\alpha_1)\alpha_2$ there is one equivalence class of $\equiv$, that is $\mathcal{X}_1 = X$.

Let φ be automorphism of Examples 5.15 and 5.18. Then φ is in quasi-normal form with respect to the A-basis $X_\varphi = \{x\alpha_1, x\alpha_2\alpha_1, x\alpha_2^2\}$ and $\mathcal{M}_\varphi = \mathcal{M}_\psi$. The initial elements of right semi-infinite X_φ-components are $x\alpha_1$ and $x\alpha_1^2$ and the terminal elements of left semi-infinite X_φ-components are $x\alpha_2^2$ and $x\alpha_2^2\alpha_1$.

The set $\mathcal{R}_1(\psi, \varphi)$ consists of the pairs $(x\alpha_1, x\alpha_1), (x\alpha_1, x\alpha_1^2), (x\alpha_2, x\alpha_2^2)$ and $(x\alpha_2, x\alpha_2^2\alpha_1)$. Let us choose $x\alpha_1$ as our type (B) representative in $\mathcal{X}_1$. We have two choices for the image of $x\alpha_1$ under ρ_0, corresponding to the two pairs $(x\alpha_1, x\alpha_1), (x\alpha_1, x\alpha_1^2) \in \mathcal{R}_1$. Denote these by ρ_1 and ρ_2, where

$$x\alpha_1\rho_1 = x\alpha_1 \quad \text{and} \quad x\alpha_1\rho_2 = x\alpha_1^2.$$

Next we determine the images of the other type (B) element $x\alpha_2$ of X under the action of ρ_1 and ρ_2, following the proof of Lemma 5.24.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

As noted above, $x\alpha_1 \equiv x\alpha_2$ because $(x\alpha_1)\alpha_2\psi^{-1} = (x\alpha_2)\alpha_2$, so in the notation of the proof of Lemma 5.24 we have $\Gamma = \alpha_2$, $\Delta = \alpha_2$ and $k = -1$. Substituting these values into Eq. (5.1), we wish to find l such that

$$w\alpha_2\varphi^{l+1} = (x\alpha_1)\rho_i\alpha_2,$$

where $i = 1$ or 2, and $w = x\alpha_2^2$ or $x\alpha_2^2\alpha_1$. Whenever we find such an l then we set $x\alpha_2\rho_i = w\varphi^l$ and check to see if ρ_i determines an automorphism. If so, we check if ρ_i is a conjugator i.e. if $\rho_i^{-1}\psi\rho = \varphi$.

Case $i = 1$: $x\alpha_1\rho_1 = x\alpha_1$.

(i) When $w = x\alpha_2^2$ we have

$$x\alpha_2^3\varphi^{l+1} = x\alpha_1\alpha_2 \quad \Longleftrightarrow \quad x\alpha_2\alpha_1\varphi^l = x\alpha_1\alpha_2,$$

which has no solutions, as may be verified using the process of Lemma 4.34.

(ii) When $w = x\alpha_2^2\alpha_1$ we have

$$x\alpha_2^2\alpha_1\alpha_2\varphi^{l+1} = x\alpha_1\alpha_2 \quad \Longleftrightarrow \quad x\alpha_1\alpha_2\varphi^l = x\alpha_1\alpha_2,$$

which has solution $l = 0$. Therefore we set $x\alpha_2\rho_1 = x\alpha_2^2\alpha_1$. Now ρ_1 maps X to $\{x\alpha_1, x\alpha_2^2\alpha_1\}$, which is not a basis of $V_{2,1}$ (see Lemma 3.16). So the set map ρ_1 extends to an endomorphism which is not an automorphism of $V_{2,1}$.

Neither value of w results in a potential conjugator ρ_1.

Case $i = 2$: $x\alpha_1\rho_2 = x\alpha_1^2$.

(i) When $w = x\alpha_2^2$ we have

$$x\alpha_2^3\varphi^{l+1} = x\alpha_1^2\alpha_2 \quad \Longleftrightarrow \quad x\alpha_2\alpha_1\varphi^l = x\alpha_1^2\alpha_2$$

which has solution $l = 1$. Therefore we set

$$\begin{aligned} x\alpha_2\rho_2 &= x\alpha_2^2\varphi \\ &= (x\alpha_2^2\alpha_1^2)(x\alpha_2^2\alpha_1\alpha_2)\lambda(x\alpha_2^3)\lambda\varphi \\ &= (x\alpha_2^2\alpha_1^2\varphi)(x\alpha_2^2\alpha_1\alpha_2\varphi)\lambda(x\alpha_2^3\varphi)\lambda \\ &= (x\alpha_2^2)(x\alpha_1\alpha_2)\lambda(x\alpha_2\alpha_1)\lambda. \end{aligned} \tag{5.2}$$

In this case $x\alpha_2^2$ is in $X_\varphi\langle A\rangle\backslash W\langle A\rangle$, where W is the minimal expansion associated to φ; this is why the standard form of $x\alpha_2\rho_2$ is written using contraction operations λ.

To define ρ_2 in terms of $X\langle A\rangle$, we must take an expansion of X at $x\alpha_2$. We take the minimal expansion which allows us to define the map into $\mathbf{x}\langle A\rangle$; namely $\{x\alpha_2\alpha_1^2, x\alpha_2\alpha_1\alpha_2, x\alpha_2^2\}$. From (5.2) we obtain

$$x\alpha_2\alpha_1^2\rho_2 = (x\alpha_2^2)\alpha_1^2\varphi = x\alpha_2^2,$$

$$x\alpha_2\alpha_1\alpha_2\rho_2 = (x\alpha_2^2)\alpha_1\alpha_2\varphi = x\alpha_1\alpha_2,$$

$$x\alpha_2^2\rho_2 = (x\alpha_2^2)a_2\varphi = x\alpha_2\alpha_1.$$

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

We see that ρ_2 maps the expansion $\{x\alpha_1, x\alpha_2\alpha_1^2, x\alpha_2\alpha_1\alpha_2, x\alpha_2^2\}$ of X to $\{x\alpha_1^2, x\alpha_2^2, x\alpha_1\alpha_2, x\alpha_2\alpha_1\}$ which is a basis for $V_{2,1}$; so ρ_2 determines an element of $G_{2,1}$. It can be verified $\rho_2^{-1}\psi\rho_2 = \varphi$, so ρ_2 is a conjugator. At this point we could stop but we give the final case for completeness.

(ii) When $w = x\alpha_2^2\alpha_1$ we have

$$x\alpha_2^2\alpha_1^3\alpha_2\psi^{l+1} = x\alpha_1^2\alpha_2 \quad \Longleftrightarrow \quad x\alpha_1\alpha_2 = x\alpha_1^2\alpha_2,$$

which has no solutions.

We find one conjugating element ρ_2 and we see that ψ and φ are conjugate via ρ_2.

The algorithm for the conjugacy of regular infinite elements of $G_{n,r}$ is as follows.

Algorithm 5.27. Let ψ and φ be regular infinite elements of $G_{n,r}$.

Step 1: Construct A-bases X_ψ and X_φ with respect to which ψ and φ are in quasi-normal form (Lemma 4.28).

Step 2: Construct the equivalence classes $\mathcal{X}_i$, $i = 1, \ldots, m$, of $\equiv$ on X_ψ (Lemma 5.20).

Step 3: Find the initial and terminal elements of semi-infinite X_φ-components of φ, by finding the minimal expansion of X_φ associated to φ (Lemma 4.9).

Step 4: Construct the sets $\mathcal{R}_i(\psi, \varphi)$.

Step 5: For each equivalence class $\mathcal{X}_i$ of $\equiv$ on X_ψ choose an element $x_i \in \mathcal{X}_i$, of type (B).

Step 6: For each i and each pair (x_i, y) of $\mathcal{R}_i(\psi, \varphi)$, construct a map $\rho_i : \mathcal{X}_i \mapsto X_\varphi$, using Eq. (5.1), as in the proof of Lemma 5.24, if possible. In each case check that ρ_i is an automorphism.

Step 7: For each m tuple $\rho_1, \ldots, \rho_m$ of automorphisms, from the previous step, check whether the map $\rho = \rho_1 * \cdots * \rho_m$ conjugates ψ to φ.

6. The Power Conjugacy Problem

For a group with presentation $\langle X \mid R\rangle$, the *power conjugacy problem* is to determine, given words $g, h \in \mathbb{F}(X)$ whether or not there exist nonzero integers a and b such that g^a is conjugate to h^b in G. We may in addition require that, if the answer to this question is "yes", then integers a and b, and an element $c \in \mathbb{F}(X)$, are found, such that $c^{-1}g^a c =_G h^b$. We say the power conjugacy problem is *decidable* if there is an algorithm which, given g and h outputs "yes" if they are conjugate and "no" otherwise. Again, the stronger form entails the obvious extra requirements. As before, in $G_{n,r}$ we work entirely with symbols for automorphisms, ignoring the presentation.

As in the case of the conjugacy problem, we break the power conjugacy problem down into two cases; one for periodic elements and one for regular infinite elements. Then, we construct an algorithm that combines the two parts.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

6.1. *The power conjugacy for periodic elements*

Let ψ and φ be periodic elements of $G_{n,r}$, of order k and m respectively, in quasi-normal form with respect to the A-bases X and Y. To test whether there exist a, $b \in \mathbb{Z}$ such that ψ^a is conjugate to φ^b, we apply Proposition 5.11 to the pair ψ^c, φ^d, for all $c \in \{1, \ldots, k\}$ and all $d \in \{1, \ldots, m\}$.

6.2. *Regular infinite elements*

The first step is to compare the sets $\mathcal{M}_\psi$ and $\mathcal{M}_{\psi^a}$, $a \in \mathbb{Z}$, $|a| > 1$, for a regular infinite automorphism ψ.

Lemma 6.1. *Let ψ be a regular infinite element of $G_{n,r}$ and let a be a non-negative integer. Then*

$$\mathcal{M}_{\psi^a} = \{(m/d, \Gamma^q) \mid (m, \Gamma) \in \mathcal{M}_\psi,\ \gcd(m, a) = d \text{ and } |a| = qd\}. \tag{6.1}$$

Proof. Let ψ be in semi-normal form with respect to X. The X-components of ψ^a are sub-sequences of the X-components of ψ, so ψ^a is also in semi-normal form with respect to X. Suppose to begin with that $a > 0$. First we show that the right-hand side of (6.1) is contained in the left-hand side. If $(m, \Gamma) \in \mathcal{M}_\psi$ then there exists an element u of $V_{n,r}$ in a semi-infinite X-component for ψ of characteristic (m, Γ); and we may assume $u \in X\langle A\rangle$. If $d = \gcd(m, a)$, $p = m/d$, $q = a/d$ and $k = ma/d$, then $u(\psi^a)^p = u\psi^{mq} = u\Gamma^q$, (as mq has the same sign as m). If $a < 0$ then, from the above, with $d = \gcd(m, -a)$, $p = m/d$, $q = -a/d$ and $k = -ma/d$, we have $u\psi^{-ap} = u\Gamma^q$. In all cases therefore u is a characteristic element of ψ^a. Furthermore, if $u(\psi^a)^r = u\Delta$, with $\Delta \neq 1$ then, from Lemma 4.25, $m|ar$, which we can rewrite as $pd|qdr$, so $p|qr$. As $\gcd(p, q) = 1$, this implies $p|r$, so that $|m/d| = |p| \leq |r|$. Hence u has characteristic $(m/d, \Gamma^q)$, with respect to ψ^a. As u belongs to a semi-infinite X-component for ψ^a, it follows that $(m/d, \Gamma^q)$ is in $\mathcal{M}_{\psi^a}$ and so we have

$$\mathcal{M}_{\psi^a} \supseteq \{(m, \Gamma^q) \mid (md, \Gamma) \in \mathcal{M}_\psi, d > 0, \gcd(m, q) = 1 \quad \text{and} \quad |a| = qd\}.$$

On the other hand, suppose that $(r, \Delta) \in \mathcal{M}_{\psi^a}$. Then again, there exists $u \in X\langle A\rangle$ such that u is a characteristic element of ψ^a, so $u\psi^{ar} = u\Delta$. Thus, from Lemma 4.25, u is a characteristic element for ψ, with characteristic $(m, \Gamma) \in \mathcal{M}_\psi$, such that $m|ar$ and $\Delta = \Gamma^t$, where $ar = mt$, $t > 0$. Let $d = \gcd(a, m)$, $m = pd$ and $a = qd$. Then $dqr = pdt$, so $qr = pt$ and $\gcd(p, q) = 1$, so $r = pr'$ and $t = qt'$, for some r', t'. However, we have $u(\psi^a)^p = u\psi^{dpq} = u\psi^{mq} = u\Gamma^q$, and so, by definition of $(r, \Delta) \in \mathcal{M}_{\psi^a}$, we see that $|p| \geq |r|$, so $r' = \pm 1$. Since $a > 0$, both m and r have the same sign, so $r' = 1$. It now follows that $r = p = m/d$ and $\Delta = \Gamma^q$, so (r, Δ) belongs to the set on the right-hand side of (6.1). That is

$$\mathcal{M}_{\psi^a} \subseteq \{(m, \Gamma^q) \mid (md, \Gamma) \in \mathcal{M}_\psi, d > 0, \gcd(m, q) = 1 \quad \text{and} \quad |a| = qd\}.$$

If $a < 0$ then the lemma follows by applying the result above to $\mathcal{M}_{\psi^{-1(-a)}}$, as for all $\theta \in G_{n,r}$ we have $(m, \Gamma) \in \mathcal{M}_\theta$ if and only if $(-m, \Gamma) \in \mathcal{M}_{\theta^{-1}}$. $\square$

Example 6.2. Let $n = 2$ and $r = 1$ and let $V_{2,1}$ be free on $\mathbf{x} = \{x\}$. Let φ be the regular infinite element of $G_{2,1}$ defined by the bijection from

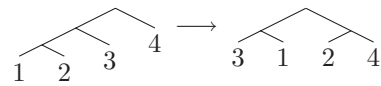
$$Y = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2, x\alpha_2\},$$

to

$$Z = \{x\alpha_1^2, x\alpha_1\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\},$$

given by the following tree pair diagram.

φ :



Then Y is the minimal expansion of $\{x\}$ associated to φ. The minimal expansion of $\{x\}$ contained in $Y\langle A\rangle \cup Z\langle A\rangle$ is $X = \{x\alpha_1^2, x\alpha_1\alpha_2, x\alpha_2\}$. $X\langle A\rangle \backslash Y\langle A\rangle = \{x\alpha_1^2\}$ and $X\langle A\rangle \backslash Z\langle A\rangle = \{x\alpha_2\}$. The X-components of these elements are

$$\cdots \mapsto x\alpha_1\alpha_2\alpha_1 \mapsto x\alpha_1^3 \mapsto x\alpha_1\alpha_2 \mapsto x\alpha_1^2$$

with characteristic $(-2, \alpha_1)$ and

$$x\alpha_2 \mapsto x\alpha_2^2 \mapsto x\alpha_2^3 \mapsto x\alpha_2^4 \mapsto \cdots$$

with characteristic $(1, \alpha_2)$. Hence φ is in quasi-normal form with respect to X and $\mathcal{M}_\varphi = \{(-2, \alpha_1), (1, \alpha_2)\}$.

The map φ^2 may be defined by the bijection from

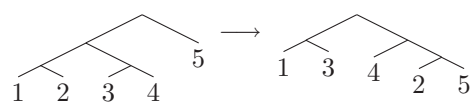
$$U = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2\alpha_1, x\alpha_1\alpha_2^2, x\alpha_2\}$$

to

$$V = \{x\alpha_1^2, x\alpha_1\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\alpha_1, x\alpha_2^3\}$$

given by a different tree pair diagram.

φ^2 :



Then U is the minimal expansion of $\{x\}$ associated to φ^2 and the minimal expansion of $\{x\}$ contained in $U\langle A\rangle \cup V\langle A\rangle$ is X again. $X\langle A\rangle \backslash U\langle A\rangle = \{x\alpha_1^2, x\alpha_1\alpha_2\}$ and $X\langle A\rangle \backslash V\langle A\rangle = \{x\alpha_2, x\alpha_2^2\}$; the corresponding X-components are

$$\cdots \mapsto x\alpha_1^3 \mapsto x\alpha_1^2, \qquad \cdots \mapsto x\alpha_1\alpha_2\alpha_1 \mapsto x\alpha_1\alpha_2$$

with characteristic $(-1, \alpha_1)$ and

$$x\alpha_2 \mapsto x\alpha_2^3 \mapsto \qquad \cdots, \; x\alpha_2^2 \mapsto x\alpha_2^4 \mapsto \cdots$$

with characteristic $(1, \alpha_2^2)$. Hence φ^2 is in quasi-normal form with respect to X and $\mathcal{M}_{\varphi^2} = \{(-1, \alpha_1), (1, \alpha_2^2)\}$, as asserted by Lemma 6.1.

Lemma 6.3 and Proposition 6.6 will allow us to find "minimal" pairs (a, b) such that ψ^a and φ^b are conjugate.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Lemma 6.3. *Let ψ and φ be regular infinite elements of $G_{n,r}$ and let c be an integer, such that c is coprime to m, for all $m \in \mathbb{Z}$ such that $(m, \Gamma) \in \mathcal{M}_\psi \cup \mathcal{M}_\varphi$. Then $\psi^c \sim \varphi^c$ if and only if $\psi \sim \varphi$.*

Proof. If $\psi \sim \varphi$ then it is immediate that $\psi^c \sim \varphi^c$. For the converse, let $\rho \in G_{n,r}$ be such that $\varphi^c = \rho^{-1}\psi^c\rho$ and observe that we may assume, without loss of generality, that $c > 0$. Suppose that ψ and φ are in quasi-normal form with respect to A-bases X and Y, respectively. From Lemma 6.1, $\mathcal{M}_{\psi^c} = \{(m, \Gamma^c) \mid (m, \Gamma) \in \mathcal{M}_\psi\}$ and $\mathcal{M}_{\varphi^c} = \{(m, \Delta^c) \mid (m, \Delta) \in \mathcal{M}_\varphi\}$.

Let u be an element of $V_{n,r}$ which is characteristic for ψ, with ψ-characteristic (m, Γ). Then, from Lemma 6.1 (and its proof), u has ψ^c-characteristic (m, Γ^c) and, as $\varphi^c = \rho^{-1}\psi^c\rho$, its image $u\rho$ has φ^c-characteristic (m, Γ^c). Hence, from Lemma 6.1 again, $u\rho$ has φ-characteristic (m, Γ). As $\gcd(c, m) = 1$, there exist integers s and t such that $ms + ct = 1$. Since $\psi^c\rho = \rho\varphi^c$ we have, in the case where $s > 0$,

$$\begin{aligned} u\psi\rho &= u\psi^{ms+ct}\rho = (u(\psi^m)^s)\psi^{ct}\rho = u\Gamma^s\psi^{ct}\rho = u\Gamma^s\rho\varphi^{ct} \\ &= (u\rho)\Gamma^s\varphi^{ct} = (u\rho)\varphi^{ms}\varphi^{ct} = (u\rho)\varphi^{ms+ct} \\ &= u\rho\varphi. \end{aligned}$$

If $s < 0$ then we have $m(-s) + c(-t) = -1$, with $-s > 0$ and the argument above implies instead that $u\psi^{-1}\rho = u\rho\varphi^{-1}$. In this case, let $v = u\psi$, so v also has ψ-characteristic (m, Γ) and, applying the argument above to v instead of u, consequently $v\psi^{-1}\rho = v\rho\varphi^{-1}$, from which it follows that $u\psi\rho = u\rho\varphi$. This applies in particular to all elements of X of type (B), with respect to ψ.

Let y' be an element of type (C), with respect to ψ; so there exists an integer k and an element $y \in X$ of type (B) such that $y'\psi^k = y\Omega$. Then $y' = y\Omega\psi^{-k}$, and $y\psi^j$ has the same ψ-characteristic as y, for all j: and so is a characteristic element for ψ. From the above then $y\psi^j\rho = (y\rho)\varphi^j$, for all j. Now

$$\begin{aligned} y'\psi\rho &= y\Omega\psi^{1-k}\rho = y\psi^{1-k}\rho\Omega = y\rho\varphi^{1-k}\Omega = y\rho\varphi^{-k}\varphi\Omega \\ &= y\psi^{-k}\rho\varphi\Omega = y\psi^{-k}\Omega\rho\varphi = y'\rho\varphi. \end{aligned}$$

Therefore, $y\psi\rho = y\rho\varphi$, for all $y \in X$, so $\psi \sim \varphi$. □

Definition 6.4. Let ψ be a regular infinite element of $G_{n,r}$ and let a be a positive integer. Define a map $\widehat{\psi}^a : \mathcal{M}_\psi \to \mathcal{M}_{\psi^a}$ by $\widehat{\psi}^a(m, \Gamma) = (p, \Gamma^\alpha)$, where $d = \gcd(m, a)$, $p = m/d$ and $\alpha = a/d$.

Example 6.5. For φ in Example 6.2, with $a = 2$, the map $\widehat{\varphi}^2 : \mathcal{M}_\varphi \to \mathcal{M}_{\varphi^2}$ is given by

$$\widehat{\varphi}^2(-2, \alpha_1) = (-1, \alpha_1) \quad \text{and} \quad \widehat{\varphi}^2(1, \alpha_2) = (1, \alpha_2^2).$$

From Lemma 6.1 this is a well defined map, and is surjective. In general it is not injective. For instance if p, s and t are pairwise coprime positive integers and we have

$m_1 = ps$, $m_2 = pt$ and $a = st$, then $d_1 = \gcd(m_1, a) = s$ and $d_2 = \gcd(m_2, a) = t$. If, for some nontrivial $\Lambda \in A^*$, we have (m_1, Λ^s) and (m_2, Λ^t) in $\mathcal{M}_\psi$ then both these elements are mapped by $\widehat{\psi}^a$ to (p, Λ^{st}).

Proposition 6.6. *Let ψ and φ be regular infinite elements of $G_{n,r}$, let a and b be positive integers and let the images of $\widehat{\psi}^a$ and $\widehat{\varphi}^b$ be*

$$\mathcal{M}_{\psi^a} = \{(p_i, \Gamma_i^{\alpha_i}) \,|\, i = 1, \ldots, M\} \quad \text{and} \quad \mathcal{M}_{\varphi^b} = \{(q_i, \Delta_i^{\beta_i}) \,|\, i = 1, \ldots, N\}.$$

For $i = 1, \ldots, M$, let

$$(\widehat{\psi}^a)^{-1}(p_i, \Gamma_i^{\alpha_i}) = \{(m_{i,j}, \Gamma_{i,j}) \,|\, 1 \le j \le M_i\}$$

and, for $i = 1, \ldots, N$, let

$$(\widehat{\varphi}^b)^{-1}(q_i, \Delta_i^{\beta_i}) = \{(n_{i,j}, \Delta_{i,j}) \,|\, 1 \le j \le N_i\}.$$

If $\psi^a \sim \varphi^b$ then $M = N$ and, after reordering if necessary, we have $p_i = q_i$ and $\Gamma_i^{\alpha_i} = \Delta_i^{\beta_i}$. Moreover, there exist positive integers $\alpha, \beta, g, d_{i,j}, e_{i,k}, s_{i,j,k}, t_{i,j,k}, f_{i,j,k}$, and $\Lambda_{i,j,k} \in A^*$, for $1 \le i \le M$, $1 \le j \le M_i$ and $1 \le k \le N_i$, such that

$$\alpha = \frac{a}{g} = d_{i,j} f_{i,j,k} t_{i,j,k} \quad \text{and} \quad \beta = \frac{b}{g} = e_{i,k} f_{i,j,k} s_{i,j,k}, \quad \text{for all } i, j, k,$$

and

$$\psi^\alpha \sim \varphi^\beta,$$

where $d_{i,j}$ is a positive divisor of $m_{i,j}$, $e_{i,k}$ is a positive divisor of $n_{i,k}$, $\Gamma_{i,j} = \Lambda_{i,j,k}^{s_{i,j,k}}$ and $\Delta_{i,j} = \Lambda_{i,j,k}^{t_{i,j,k}}$, and

$$f_{i',j',k'} \left| \left(\prod_{i,j,k} (t_{i,j,k} d_{i,j}) \right) / t_{i',j',k'} d_{i',j'}, \right.$$

for all i', j', k'.

Proof. Assume $\psi^a \sim \varphi^b$, with $a, b > 0$, and that $\rho^{-1}\psi^a\rho = \varphi^b$. From Lemma 5.16, $\mathcal{M}_{\psi^a}$ and $\mathcal{M}_{\varphi^b}$ are equal, so $M = N$, and we may order $\mathcal{M}_{\psi^a}$ so that $(p_i, \Gamma_i^{\alpha_i}) = (q_i, \Delta_i^{\beta_i})$, so $p_i = q_i$ and $\Gamma_i^{\alpha_i} = \Delta_i^{\beta_i}$. With the notation for $(\widehat{\psi}^a)^{-1}(p_i, \Gamma_i^{\alpha_i})$ and $(\widehat{\varphi}^b)^{-1}(q_i, \Delta_i^{\alpha_i})$ given in the statement of the proposition, let $d_{i,j} = \gcd(a, m_{i,j})$ and $e_{i,k} = \gcd(b, n_{i,k})$, so

$$m_{i,j}/d_{i,j} = p_i = q_i = n_{i,k}/e_{i,k}$$

and let

$$\alpha_{i,j} = a/d_{i,j}, \quad \beta_{i,k} = b/e_{i,k},$$

and

$$\Gamma_{i,j}^{\alpha_{i,j}} = \Gamma_i^{\alpha_i} = \Delta_i^{\beta_i} = \Delta_{i,k}^{\beta_{i,k}}, \tag{6.2}$$

by Definition 6.4, for $1 \le i \le M$, $1 \le j \le M_i$ and $1 \le k \le N_i$.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

As $\Gamma_{i,j}^{\alpha_{i,j}} = \Delta_{i,k}^{\beta_{i,k}}$, by Proposition 3.9, there exist $\Lambda_{i,j,k} \in A^*$ and positive integers $s_{i,j,k}, t_{i,j,k}$ such that $\Gamma_{i,j} = \Lambda_{i,j,k}^{s_{i,j,k}}$ and $\Delta_{i,j} = \Lambda_{i,j,k}^{t_{i,j,k}}$. Taking a power of $\Lambda_{i,j,k}$ if necessary, we may assume that $\gcd(s_{i,j,k}, t_{i,j,k}) = 1$. Then

$$\Lambda_{i,j,k}^{s_{i,j,k}\alpha_{i,j}} = \Gamma_{i,j}^{\alpha_{i,j}} = \Delta_{i,k}^{\beta_{i,k}} = \Lambda_{i,j,k}^{t_{i,j,k}\beta_{i,k}}, \tag{6.3}$$

so $s_{i,j,k}\alpha_{i,j} = t_{i,j,k}\beta_{i,k}$. As $s_{i,j,k}$ and $t_{i,j,k}$ are coprime this implies that $\alpha_{i,j}/t_{i,j,k} = \beta_{i,k}/s_{i,j,k} = c_{i,j,k} \in \mathbb{Z}$, and $\alpha_{i,j} = c_{i,j,k}t_{i,j,k}$ and $\beta_{i,k} = c_{i,j,k}s_{i,j,k}$.

Let

$$g = \gcd(\{c_{i,j,k} | 1 \le i \le M, 1 \le j \le M_i, 1 \le k \le N_i\}).$$

Then there exist integers $f_{i,j,k}$ such that $c_{i,j,k} = gf_{i,j,k}$, for all i, j, k. From Lemma 6.1, $\mathcal{M}_{\psi^{a/g}}$ consists of elements $(m/p, \Gamma^\alpha)$, where $(m, \Gamma) \in \mathcal{M}_\psi$, $p = \gcd(m, a/g)$ and $\alpha = a/gp$. Similarly, elements of $\mathcal{M}_{\varphi^{b/g}}$ are of the form $(n/q, \Delta^\beta)$, where $(n, \Delta) \in \mathcal{M}_\varphi$, $q = \gcd(n, b/g)$ and $\beta = b/gq$. Now $g | c_{i,j,k}$ and $c_{i,j,k} | \alpha_{i,j}$ and $c_{i,j,k} | \beta_{i,k}$. Therefore $\gcd(m_{i,j}, a/g) = \gcd(m_{i,j}, a) = d_{i,j}$ and similarly $\gcd(n_{i,k}, b/g) = e_{i,k}$. Thus g is coprime to

$$p_i = \frac{m_{i,j}}{\gcd(m_{i,j}, a/g)} = \frac{n_{i,k}}{\gcd(n_{i,k}, b/g)},$$

for all i, j, k. From Lemma 6.3, it follows that $\psi^{a/g} \sim \varphi^{b/g}$.

Now

$$a/g = \alpha_{i,j}d_{i,j}/g = c_{i,j,k}t_{i,j,k}d_{i,j}/g = f_{i,j,k}t_{i,j,k}d_{i,j}$$

and similarly

$$b/g = f_{i,j,k}s_{i,j,k}e_{i,k},$$

for all i, j, k. Also

$$\gcd(\{f_{i,j,k} \,|\, 1 \le i \le M, 1 \le j \le M_i, 1 \le k \le N_i\}) = 1$$

so, for fixed i', j', k',

$$f_{i',j',k'} \left| \left(\prod_{i,j,k} (t_{i,j,k}d_{i,j}) \right) / t_{i',j',k'}d_{i',j'}. \right.$$

□

Corollary 6.7. *The power conjugacy problem for regular infinite elements of $G_{n,r}$ is solvable.*

Proof. Let ψ and φ be regular infinite elements of $G_{n,r}$. Suppose that ψ^a is conjugate to φ^b, for some nonzero a, b. Replacing either ψ or φ or both by their inverse, we may assume that $a, b > 0$. Then, in the notation of the proposition above, we have $\psi^\alpha \sim \varphi^\beta$, where $\alpha = f_{i,j,k}t_{i,j,k}d_{i,j}$ and $\beta = f_{i,j,k}s_{i,j,k}e_{i,k}$. From the conclusion of the theorem it is clear that there are finitely many choices for $f_{i,j,k}$, $s_{i,j,k}$, $t_{i,j,k}$, $d_{i,j}$ and $e_{i,k}$. Hence there are finitely many possible α and β, and we may effectively construct a list of all possible pairs (α, β). Having constructed this list we

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

may check whether or not $\psi^\alpha \sim \varphi^\beta$, using Algorithm 5.27. Hence we may decide whether or not there exist a, b such that $\psi^a \sim \varphi^b$. □

The proof of Proposition 6.6 forms the basis for the algorithm for the power conjugacy problem. Given regular infinite elements $\psi, \varphi \in G_{n,r}$ we construct bounds $\hat{a}$ and $\hat{b}$ such that if some (positive) power of ψ is conjugate to a (positive) power of φ then $\psi^c \sim \varphi^d$, for $0 < c \leq \hat{a}$ and $0 < d \leq \hat{b}$. Following the proof of the proposition, if $\psi^a \sim \varphi^b$, for some $a, b > 0$, then the inverse images $\hat{\psi}_a$ and $\hat{\varphi}_b$ partition $\mathcal{M}_\psi$ and $\mathcal{M}_\varphi$, so we have integers L, M_i, N_i such that

$$\mathcal{M}_\psi = \bigcup_{i=1}^{L} \{(m_{i,j}, \Gamma_{i,j}) \mid 1 \leq j \leq M_i\}$$

and

$$\mathcal{M}_\varphi = \bigcup_{i=1}^{L} \{(n_{i,k}, \Delta_{i,k}) \mid 1 \leq k \leq N_i\}.$$

Given any $\Gamma \in A^*$ there exists unique $\Lambda \in A^*$ and $r \in \mathbb{N}$ such that $\Gamma = \Lambda^r$ and if $\Gamma = \Lambda'^s$ then $s \leq r$. We denote Λ by $\sqrt{\Gamma}$ and r by $m(\Gamma)$. From Eqs. (6.2) and (6.3), it follows that

$$\sqrt{\Lambda_{i,j,k}} = \sqrt{\Gamma_{i,j}} = \sqrt{\Gamma_i} = \sqrt{\Delta_i} = \sqrt{\Delta_{i,k}}$$

and

$$s_{i,j,k} \leq m(\Gamma_{i,j}) \quad \text{and} \quad t_{i,j,k} \leq m(\Delta_{i,k}),$$

for $1 \leq i \leq L$, $1 \leq j \leq M_i$ and $1 \leq k \leq N_i$.

From Proposition 6.6 we have $\alpha = d_{1,1} f_{1,1,1} t_{1,1,1}$ and $f_{1,1,1} \leq \prod_{(i,j,k) \neq (1,1,1)} d_{i,j} t_{i,j,k}$. As $d_{i,j} \leq |m_{i,j}|$ and $t_{i,j,k} \leq m(\Delta_{i,k})$, this means that

$$\begin{aligned}
\alpha &\leq \prod_{i=1}^{L} \prod_{j=1}^{M_i} \prod_{k=1}^{N_i} d_{i,j} t_{i,j,k} \\
&\leq \prod_{i=1}^{L} \prod_{j=1}^{M_i} \prod_{k=1}^{N_i} |m_{i,j}|\, m(\Delta_{i,k}) \\
&\leq \prod_{i=1}^{L} \prod_{j=1}^{M_i} \left(|m_{i,j}|^{N_i} \prod_{k=1}^{N_i} m(\Delta_{i,k}) \right) \\
&\leq \prod_{i=1}^{L} \left(\prod_{j=1}^{M_i} |m_{i,j}| \right)^{N_i} \left(\prod_{k=1}^{N_i} m(\Delta_{i,k}) \right)^{M_i}. \qquad (6.4)
\end{aligned}$$

Similarly

$$\beta \leq \prod_{i=1}^{L} \left[\left(\prod_{k=1}^{N_i} |n_{i,k}| \right)^{M_i} \left(\prod_{j=1}^{M_i} m(\Gamma_{i,j}) \right)^{N_i} \right]. \qquad (6.5)$$

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

Now suppose that a solution $\psi^{a'} \sim \varphi^{b'}$ gives rise to sub-partitions of the partitions of $\mathcal{M}_\psi$ and $\mathcal{M}_\varphi$ above. Straightforward calculation shows that in this case, the bounds on α and β obtained are again less than or equal to the right-hand sides of (6.4) and (6.5) (calculated using the original partitions). Thus, in computing (upper) bounds $\hat{a}$ and $\hat{b}$ we may take partitions of $\mathcal{M}_\psi = P_1 \cup \cdots \cup P_L$ and $\mathcal{M}_\varphi = Q_1 \cup \cdots \cup Q_L$ with L as small as possible, subject to the constraint that, for each i such that $1 \leq i \leq L$ we have $\sqrt{\Gamma} = \sqrt{\Delta}$, for all $(m, \Gamma) \in P_i$ and $(n, \Delta) \in Q_i$. If these partitions satisfy these properties, and this does not hold for any partition of fewer than L subsets, (in other words the partitions are formed by gathering together characteristics with the same root) then the bounds $\hat{a}$ and $\hat{b}$ are given by

$$\hat{a} = \prod_{i=1}^{L} \left[\left(\prod_{(m,\Gamma) \in P_i} |m| \right)^{|Q_i|} \left(\prod_{(n,\Delta) \in Q_i} m(\Delta) \right)^{|P_i|} \right] \tag{6.6}$$

and

$$\hat{b} = \prod_{i=1}^{L} \left[\left(\prod_{(n,\Delta) \in Q_i} |n| \right)^{|P_i|} \left(\prod_{(m,\Gamma) \in P_i} m(\Gamma) \right)^{|Q_i|} \right]. \tag{6.7}$$

Example 6.8. Let $n = 2$ and $r = 1$ and $V_{2,1}$ be free on $\{x\}$. Let ψ be the regular infinite element of $G_{2,1}$ of Examples 4.1 and 4.11. Then ψ is in quasi-normal form with respect to the A-basis $X = \{x\alpha_1, x\alpha_2\}$ and $\mathcal{M}_\psi = \{(1, \alpha_2), (\text{-}1, \alpha_1)\}$.

Let φ be the regular infinite element of $G_{2,1}$ defined by a bijective map from

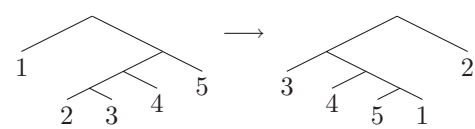
$$Y_\varphi = \{x\alpha_1, x\alpha_2\alpha_1^3, x\alpha_2\alpha_1^2\alpha_2, x\alpha_2\alpha_1\alpha_2, x\alpha_2^2\}$$

to

$$Z_\varphi = \{x\alpha_1^2, x\alpha_1\alpha_2\alpha_1, x\alpha_1\alpha_2^2\alpha_1, x\alpha_1\alpha_2^3, x\alpha_2\}$$

given as illustrated below.

φ :



Then Y_φ is the minimal expansion of $\{x\}$ associated to φ and the minimal expansion of $\{x\}$ contained in $Y_\varphi\langle A\rangle \cup Z_\varphi\langle A\rangle$ is X. We have $X\langle A\rangle \setminus Y_\varphi\langle A\rangle = \{x\alpha_2, x\alpha_2\alpha_1, x\alpha_2\alpha_1^2\}$ and $X\langle A\rangle \setminus Z_\varphi\langle A\rangle = \{x\alpha_1, x\alpha_1\alpha_2, x\alpha_1\alpha_2^2\}$. The X-components of these elements are:

$$x\alpha_1 \mapsto x\alpha_1\alpha_2^3 \mapsto x\alpha_1\alpha_2^6 \mapsto \cdots,$$

$$x\alpha_1\alpha_2 \mapsto x\alpha_1\alpha_2^4 \mapsto x\alpha_1\alpha_2^7 \mapsto \cdots,$$

$$x\alpha_1\alpha_2^2 \mapsto x\alpha_1\alpha_2^5 \mapsto x\alpha_1\alpha_2^8 \mapsto \cdots,$$

$$\cdots \mapsto x\alpha_2\alpha_1^6 \mapsto x\alpha_2\alpha_1^3 \mapsto x\alpha_2,$$

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

$$\cdots \mapsto x\alpha_2\alpha_1^7 \mapsto x\alpha_2\alpha_1^4 \mapsto x\alpha_2\alpha_1,$$
$$\cdots \mapsto x\alpha_2\alpha_1^8 \mapsto x\alpha_2\alpha_1^5 \mapsto x\alpha_2\alpha_1^2$$

so φ is in quasi-normal form with respect to X and $\mathcal{M}_\varphi = \{(1, \alpha_2^3), (-1, \alpha_1^3)\}$. In the notation above, we have partitions $\mathcal{M}_\psi = P_1 \cup P_2$ and $\mathcal{M}_\varphi = Q_1 \cup Q_2$ with $P_1 = \{(1, \alpha_2)\}$, $P_2 = \{, (-1, \alpha_1)\}$, $Q_1 = \{(1, \alpha_2^3)\}$ and $Q_2 = \{(-1, \alpha_1^3)\}$, so we obtain bounds $\hat{a} = 9$ and $\hat{b} = 1$.

Assume there exists positive integers a, b such that $\psi^a \sim \varphi^b$. We may now assume that $a \leq 9$ and $b = 1$. The map $\widehat{\psi}^a : \mathcal{M}_\psi \to \mathcal{M}_{\psi^a}$ is given by

$$\widehat{\psi}^a(1, \alpha_2) = (1/d_1, \alpha_2^{a/d_1}), \quad \widehat{\psi}^a(-1, \alpha_1) = (-1/d_2, \alpha_1^{a/d_2}),$$

where $d_1 = \gcd(1, a) = 1$ and $d_2 = \gcd(-1, a) = 1$. Thus

$$\mathcal{M}_{\psi^a} = \{(1, \alpha_2^a), (-1, \alpha_1^a)\}.$$

The only possible choice for a making $\mathcal{M}_{\psi^a} = \mathcal{M}_{\varphi^b} = \mathcal{M}_\varphi$ is $a = 3$. Applying Algorithm 5.27 to ψ^3 and φ we find a conjugating element ρ, given by $x\alpha_1\rho = x\alpha_2$ and $x\alpha_2\rho = x\alpha_1$.

Remark 6.9. In Corollary 6.7 the powers a and b were positive, giving us upper bounds $a \leq \hat{a}$ and $b \leq \hat{b}$ for the minimal powers which solve the power conjugacy problem. Now suppose that $a < 0$ and $b > 0$. We may write $\psi^a = (\psi^{-1})^{-a}$ and then $-a > 0$. If we apply Corollary 6.7 to (ψ^{-1}, φ), we obtain a second pair of bounds $-a \leq \bar{a}$ and $b \leq \bar{b}$. Observing that $(m, \Gamma) \in \mathcal{M}_\psi$ if and only if $(-m, \Gamma) \in \mathcal{M}_{\psi^{-1}}$, we note that this replacement $\psi \mapsto \psi^{-1}$ preserves the absolute value $|m|$ of all characteristic multipliers. Thus each of the terms $|m_{i,j}|$, $|n_{i,k}|$, $|m|$ and $|n|$ in Eq. (6.4)–(6.7) is unchanged. We conclude that $\bar{a} = \hat{a}$ and $\bar{b} = \hat{b}$.

The same argument applies equally well to the remaining two cases $a > 0$, $b < 0$ and $a < 0$, $b < 0$. Thus, once we have obtained $\hat{a}$ and $\hat{b}$, we need only to check the ranges $1 \leq |a| \leq \hat{a}$ and $1 \leq |b| \leq \hat{b}$ to find minimal conjugating powers.

Example 6.10. Let ψ be as in Example 6.8 and let φ be as in Example 6.2. Then $\mathcal{M}_\psi = \{(1, \alpha_2), (-1, \alpha_1)\}$ and $\mathcal{M}_\varphi = \{(-2, \alpha_1), (1, \alpha_2)\}$. In the notation above, we have partitions $\mathcal{M}_\psi = P_1 \cup P_2$ and $\mathcal{M}_\varphi = Q_1 \cup Q_2$ with $P_1 = \{(1, \alpha_2)\}$, $P_2 = \{(-1, \alpha_1)\}$, $Q_1 = \{(1, \alpha_2)\}$ and $Q_2 = \{(-2, \alpha_1)\}$, so we obtain bounds $\hat{a} = 1$ and $\hat{b} = 2$.

Assume there exist positive integers a, b such that $\psi^a \sim \varphi^b$; with $a = 1$ and $b \leq 2$. The map $\widehat{\varphi}^b : \mathcal{M}_\varphi \to \mathcal{M}_{\varphi^b}$ is given by

$$\widehat{\varphi}^b(1, \alpha_2) = (1/d_1, \alpha_2^{b/d_1}), \ \widehat{\varphi}^b(-2, \alpha_1) = (-2/d_2, \alpha_1^{b/d_2}),$$

where $d_1 = \gcd(1, b) = 1$ and $d_2 = \gcd(\text{-}2, b) = b$. Thus,

$$\mathcal{M}_{\varphi^b} = \{(1, \alpha_2), (-2, \alpha_1)\} \quad \text{or} \quad \{(1, \alpha_2^2), (-1, \alpha_1)\}.$$

As $\mathcal{M}_\psi \neq \mathcal{M}_{\varphi^b}$, for $b = 1$ and $b = 2$, there is no pair of positive integers a, b such that $\psi^a \sim \varphi^b$. The same argument applies on replacing φ or ψ by φ^{-1} or ψ^{-1}, respectively, so no nontrivial power of φ is conjugate to a power of ψ.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

In order to solve the power conjugacy problem for general regular infinite elements of $G_{n,r}$ we require an algorithm which finds all pairs (a, b), within the bounds calculated, rather than merely deciding whether or not such a pair exists. This is the algorithm we describe here. It constructs a set $\mathcal{PC}_{RI}$ consisting of triples (a, b, ρ), such that $\rho^{-1}\psi^a\rho = \varphi^b$.

Algorithm 6.11. Let ψ and φ be regular infinite elements of $G_{n,r}$.

Step 1: Construct A-bases X_ψ and X_φ with respect to which ψ and φ are in quasi-normal form (Lemma 4.28).
Step 2: Construct the sets $\mathcal{M}_\psi$ and $\mathcal{M}_\varphi$ (see Definition 5.14).
Step 3: Calculate the bounds on $\hat{a}$ and $\hat{b}$, using Eqs. (6.6) and (6.7).
Step 4: For all pairs a, b such that $1 \leq |a| \leq \hat{a}$ and $1 \leq |b| \leq \hat{b}$, input ψ^a and φ^b to Algorithm 5.27. If a conjugating automorphism ρ is returned, add (a, b, ρ) to the set $\mathcal{PC}_{RI}$.
Step 5: If $\mathcal{PC}_{RI} = \emptyset$, output "No" and halt. Otherwise output $\mathcal{PC}_{RI}$.

Corollary 6.7 may be strengthened.

Corollary 6.12. *Given regular infinite elements $\psi, \varphi \in G_{n,r}$ there is a finite subset $\mathcal{PC}_{RI}$ of $\mathbb{Z} \times \mathbb{Z} \times G_{n,r}$, which may be effectively constructed, such that $\psi^a \sim \varphi^b$ if and only if $a = cg$ and $b = dg$, for some $(c, d, \rho) \in \mathcal{PC}_{RI}$ and $g \in \mathbb{Z}$. Moreover, for all $(c, d, \rho) \in \mathcal{PC}_{RI}$ and $g \in \mathbb{Z}$, we have $\rho^{-1}\psi^{cg}\rho = \varphi^{dg}$.*

Proof. From Lemma 6.6 and the description of Algorithm 6.11, $\mathcal{PC}_{RI}$ is a finite set and it follows that if $\psi^a \sim \psi^b$, for some positive $a, b \in \mathbb{Z}$, then $(a/g, b/g, \rho) \in \mathcal{PC}_{RI}$ and in this case $\rho^{-1}\psi^a\rho = \varphi^b$. Replacing one or other, or both, of ψ and φ by their inverses the same holds, without the constraint that a, b be positive. On the other hand if (c, d, ρ) is in $\mathcal{PC}_{RI}$ then $\rho^{-1}\psi^c\rho = \varphi^d$, so $\rho^{-1}\psi^{cg}\rho = \varphi^{dg}$, for all $g \in \mathbb{Z}$. □

6.3. *The power conjugacy algorithm*

We combine the algorithms of Secs. 6.1 and 6.2 to give an algorithm for the power conjugacy problem in $G_{n,r}$. In fact in Secs. 6.1 and 6.2 we find a description of all solutions of the power conjugacy problem for periodic and regular infinite automorphisms, respectively and the algorithm in this section does the same for arbitrary elements of $G_{n,r}$.

If we are only interested in the existence of a solution to the power conjugacy problem then we may essentially ignore the periodic part of automorphisms, as long as the regular infinite part is nontrivial. To see this, suppose ψ and φ are elements of $G_{n,r}$ and we have decompositions $\psi = \psi_P * \psi_{RI}$, $\varphi = \varphi_P * \varphi_{RI}$. Assume that we have found that $V_{RI,\psi}$ is nontrivial and ψ^a_{RI} is conjugate to φ^b_{RI}, $a, b \neq 0$. In this case, ψ_P and φ_P have finite-orders, m and k say, and so we immediately have a solution $\psi^{amk} \sim \varphi^{bmk}$, $amk, bmk \neq 0$, of the power conjugacy problem. The algorithm described below allows this type of solution but also tries to find a

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

solution to the power conjugacy problem corresponding to each pair (c, d) such that $\psi_P^c \sim \varphi_P^d$. Thus, in Theorem 6.14, we obtain a description of all solutions to the power conjugacy problem, for ψ and φ. (That is, all pairs (a, b) such that $\psi^a \sim \varphi^b$. We do not find all possible conjugators ρ.)

Algorithm 6.13. Let ψ and φ be elements of $G_{n,r}$.

Step 1: Run Steps 1, 2, and 3 of Algorithm 5.6.

Step 2: Input ψ_{RI} and φ_{RI} to Algorithm 6.11.

Step 3: If $X_{RI,\psi}$ is non-empty (that is, $V_{RI,\psi}$ is non-empty) and $\mathcal{PC}_{RI}$ is empty, output "No" and stop.

Step 4: Compute the orders k and m of ψ_P and φ_P. Input ψ_P^a and φ_P^b to Algorithm 5.13, for all c, d such that $1 \leq c \leq k$ and $1 \leq d \leq m$. Construct the set $\mathcal{PC}_P$ of all triples (c, d, ρ) found such that $\rho^{-1}\psi^c\rho$ is conjugate to φ^d. If $X_{RI,\psi}$ is non-empty, adjoin the triple $(0, 0, \theta_0)$ to $\mathcal{PC}_P$, where θ_0 is the identity map of the algebra V_{n,s_P}, of Step 3 of Algorithm 5.6.

Step 5: If $\mathcal{PC}_P$ is empty, output "No" and stop. If $\mathcal{PC}_P$ is non-empty and $X_{RI,\psi}$ is empty output $\mathcal{PC}_P$ and stop.

Step 6: If this step is reached then both $\mathcal{PC}_P$ and $\mathcal{PC}_{RI}$ are non-empty. For all $(\alpha, \beta, \rho_{RI})$ in $\mathcal{PC}_{RI}$ and all pairs (c, d, ρ_P) in $\mathcal{PC}_P$ consider the simultaneous congruences

$$\alpha x \equiv c \bmod k \quad \text{and} \quad \beta x \equiv d \bmod m,$$

where k and m are the orders of ψ_P and φ_P found in Step 4. For each positive solution $x = g$ (less than $\operatorname{lcm}(k, m)$) add $(\alpha g, \beta g, g, \rho_P * \rho_{RI})$ to the set $\mathcal{PC}$ (which is empty at the start).

We verify that this algorithm solves the power conjugacy problem in the proof of the following theorem.

Theorem 6.14. *The power conjugacy problem for the Higman–Thompson group $G_{n,r}$ is solvable. Furthermore, given elements $\psi, \varphi \in G_{n,r}$, let ψ_P have order k, let φ_P have order m and let $l = \operatorname{lcm}(k, m)$. There is a finite subset $\mathcal{PC} \subseteq \mathbb{Z}^3 \times G_{n,r}$, which may be effectively constructed, such that $\psi^a \sim \varphi^b$ if and only if $(ag/h, bg/h, g, \rho) \in \mathcal{PC}$, where $\rho \in G_{n,r}$ and $g, h \in \mathbb{Z}$ such that $h \equiv g \bmod l$, $h|a$ and $h|b$. In this case $\rho^{-1}\psi^a\rho = \varphi^b$.*

Proof. Apply Algorithm 6.13 to ψ and φ. If there exist $a, b \in \mathbb{Z}$ such that $\psi^a \sim \varphi^b$ then $\psi_P^a \sim \varphi_P^b$ and $\psi_{RI}^a \sim \varphi_{RI}^b$. In this case let ψ_P and φ_P have orders k and m, respectively and let $a_1, b_1 \in \mathbb{Z}$ be such that $1 \leq a_1 < k$ and $1 \leq b_1 < m$ and $a_1 \equiv a \bmod k$, $b_1 \equiv b \bmod m$. Then there exists ρ_P such that $(a_1, b_1, \rho_P) \in \mathcal{PC}_I$. Furthermore, from Corollary 6.12, there exists $(a_2, b_2, \rho_{RI}) \in \mathcal{PC}_{RI}$ and $h \in \mathbb{Z}$ such that $a = a_2 h$ and $b = b_2 h$. Let g be such that $1 \leq g < \operatorname{lcm}(k, m)$, and $g \equiv h \bmod \operatorname{lcm}(k, m)$ so $g \equiv h \bmod k$ and $g \equiv h \bmod m$. As h is a solution to the congruences $a_2 x \equiv a_1 \bmod k$ and $b_2 x \equiv b_1 \bmod m$, it follows that g is also a

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

solution to these congruences. Therefore $(a_2g, b_2g, g, \rho_P * \rho_{RI}) \in \mathcal{PC}$. As $a_2 = a/h$ and $b_2 = b/h$, this is an element of $\mathbb{Z}^3 \times G_{n,r}$ of the required form.

Conversely, assume $(u, v, g, \rho_P * \rho_{RI}) \in \mathcal{PC}$, where $u = ag/h$ and $v = bg/h$, for some $a, h \in \mathbb{Z}$ satisfying the hypotheses of the theorem. Then there exist $(\alpha, \beta, \rho_{RI})$ in $\mathcal{PC}_{RI}$ and (c, d, ρ_P) in $\mathcal{PC}_P$ such that $u = \alpha g \equiv c \bmod k$ and $v = \beta g \equiv d \bmod m$. As $g \equiv h \bmod l$ this implies that $a = (u/g)h = \alpha h \equiv c \bmod k$ and $b = (v/g)h = \beta h \equiv d \bmod m$. Therefore $\psi_P^a = \psi_P^c \sim \varphi_P^d = \varphi_P^b$, by definition of $\mathcal{PC}_P$, and indeed $\rho_P^{-1}\psi_P^a\rho_P = \varphi_P^b$. Also, $a = \alpha h$ and $b = \beta h$ implies $\rho_{RI}^{-1}\psi_{RI}^a\rho_{RI} = \varphi_{RI}^b$, by Corollary 6.12, so

$$\psi^a = (\psi_P * \psi_{RI})^a = \psi_P^a * \psi_{RI}^a \sim \varphi_P^b * \varphi_{RI}^b = (\varphi_P * \varphi_{RI})^b = \varphi^b$$

and $\rho_P * \rho_{RI}$ is a conjugating element. □

Examples which illustrate how the algorithm works on automorphisms which are not necessarily periodic or regular infinite can be found in [26]: follow the link to "Examples" and refer to the examples named "`mixed_pconj_phi`" and "`mixed_pconj_psi`".

Acknowledgments

The authors thank Collin Bleak, for suggesting work on conjugacy problems in Thompson's group, and Claas Röver, who suggested the use of Higman's approach, and made many improvements to earlier versions of this work. We thank Sarah Rees for overall guidance and constructive suggestions. We thank Steve Pride for pointing us in the direction of the power conjugacy problem and Francesco Matucci, José Burillo and Matt Brin for helpful conversations.

This research was partially supported by the EPSRC Grant EP/K016687/1. The first author was supported by an EPSRC doctoral training grant. Parts of this paper appear in the first author's thesis.

References

[1] M. Anshel and P. Stebe, The solvability of the conjugacy problem for certain HNN groups, *Bull. Amer. Math. Soc.* **80**(2) (1974) 266–270.

[2] N. Barker, Topics in Algebra: The Higman–Thompson Group $G_{2,1}$ and Beauville p-groups, Thesis, Newcastle University (2014).

[3] J. M. Belk and F. Matucci, Conjugacy and dynamics in Thompson's groups, *Geom. Dedicata* **169**(1) (2014) 239–261.

[4] N. V. Bezverhnii, Ring diagrams with periodic labels and power conjugacy problem in groups with small cancellation conditions C (3) -T (6), *Sci. Edu. Bauman MSTU* **14**(11) (2014) 238–256.

[5] V. N. Bezverkhniĭ, A. N. Kuznetsova, Solvability of the power conjugacy problem for words in Artin groups of extra large type, *Chebyshevskii Sb.* **9**(1) (2008) 50–68.

[6] C. Bleak, H. Bowman, A. Gordon, G. Graham, J. Hughes, F. Matucci and J. Sapir, Centralizers in R.Thompson's group V_n, *Groups, Geom. Dyn.* **7**(4) (2013) 821–865.

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.

[7] O. Bogopolski, A. Martino, O. Maslakova and E. Ventura, The conjugacy problem is solvable in free-by-cyclic groups, *Bull. London Math. Soc.* **38**(10) (2006) 787–794.

[8] M. G. Brin, Higher dimensional Thompson groups, *Geom. Dedicata* **108** (2004) 163–192.

[9] K. S. Brown, Finiteness properties of groups, *J. Pure Appl. Algebra* **44** (1987) 45–75.

[10] J. Burillo, S. Cleary and C. E. Röver, Obstructions for subgroups of Thompson's group V, preprint (2014), `arXiv.org/abs/1402.3860`.

[11] J. W. Cannon, W. J. Floyd and W. R. Parry, Introductory notes on Richard Thompson's groups, *Enseign. Math.* (2) **42**(3–4) (1996) 215–256.

[12] P. M. Cohn, *Universal Algebra*, Mathematics and its Applications, Vol. 6 (D. Reidel Publisher, 1981).

[13] P. M. Cohn, *Algebra*, Vol. 3 (John Wiley, 1991).

[14] L. P. J. Comerford, A note on power-conjugacy, *Houston J. Math.* **3**(3) (1977) 337–341.

[15] W. Dicks, C. Martinez-Pérez, Isomorphisms of Brin–Higman–Thompson groups, *Israel J. Math.* **199** (2014) 189–218.

[16] A. V. Fesenko, Vulnerability of cryptographic primitives based on the power conjugacy search problem in quantum computing, *Cybern. Syst. Anal.* **50**(5) (2014) 815–816.

[17] G. Higman, *Finitely Presented Infinite Simple Groups*, Notes on Pure Math. Vol. 8 (1974). Dept. of Mathematics, I. A. S., Australian National University.

[18] B. Jónsson and A. Tarski, On two properties of free algebras, *Math. Scand.* **9** (1961) 95–101.

[19] D. Kahrobaei and M. Anshel, Decision and search in non-Abelian Cramer-Shoup public key cryptosystem, *Groups Complex. Cryptol.* **1**(2) (2009) 217–225.

[20] S. Lipschutz and C. F. Miller, Groups with certain solvable and unsolvable decision problems, *Comm. Pure Appl. Math.* **24** (1971) 7–15.

[21] M. Lothaire, *Combinatorics on Words*, Advanced Book Program, World Science Division (Addison-Wesley, 1983).

[22] C. Martinez-Perez and B. Nucinkis, Bredon cohomological finiteness conditions for generalisations of Thompson's groups, *Groups Geom. Dyn.* **7**(4) (2013) 931–959.

[23] R. McKenzie and R. J. Thompson, An elementary construction of unsolvable word problems in group theory, in *Word Problems*: *Decision Problems and the Burnside Problem in Group Theory*, Studies in Logic and the Foundations of Mathematics, Vol. 71 (North-Holland, Amsterdam, 1973), pp. 457–478.

[24] E. Pardo, The isomorphism problem for Higman–Thompson groups, *J. Algebra* **344** (2011) 172–183.

[25] S. J. Pride, On the residual finiteness and other properties of (relative) one-relator groups, *Proc. Amer. Math. Soc.* **136**(2) (2008) 377–386.

[26] D. M. Robertson, `thompson`: A package for Python 3.3+ to work with elements of the Higman–Thompson groups $G_{n,r}$, Source code available from https://github.com/DMRobertson/thompsons_v and documentation available from http://thompsons-v.readthedocs.org/.

[27] O. P. Salazar-Diaz, Thompson's group V from a dynamical viewpoint, *Internat. J. Algebra Comput.* **20** (2010) 39–70.

[28] R. J. Thompson, unpublished notes, http://www.math.binghamton.edu/matt/thompson/index.html

Int. J. Algebra Comput. 2016.26:309-374. Downloaded from www.worldscientific.com
by UNIVERSITY OF NEWCASTLE on 05/26/16. For personal use only.